p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE

Rully Mujiastuti[1], Ibnu Prasetyo[2]*
Teknik Informatika, Universitas Muhammadiyah Jakarta, Jalan Cempaka Putih Tengah 27 Jakarta Pusat, Kode Pos 10510
**Coresponding Author* : 2014470158@ftumj.ac.id

Abstrak

Setiap perangkat yang terhubung ke internet secara umum memiliki risiko pada keamanan jaringannya. Contoh risiko ini adalah serangan *Man In The Middle* (MITM), dan iklan online yang mengganggu. *Man In The Middle* (MITM) merupakan serangan *cyber* yang terjadi ketika ada pihak ketiga mencegat komunikasi dua orang secara diam-diam. Maka, *Virtual Private Network* (VPN) dan DNS *Filtering* dapat digunakan untuk mencegah serangan tersebut. VPN mengubah jalur koneksinya dan pertukaran data disembunyikan, sehingga akses ke website dapat dilakukan dengan aman. Sedangkan DNS *Filtering* digunakan untuk memblokir website dengan popup iklan online yang mengganggu di saat user sedang berselancar di internet. Dari pengujian melalui wireshark pada penggunaan VPN, diperoleh hasil koneksi yang aman dari serangan MITM. Agar isi data tidak terbaca oleh pihak yang tidak bertanggung jawab, maka paket data dikirim dengan enkripsi menggunakan Encryption cipher AES 256 bit dan hash algorithm SHA-512. Sementara, pada pengujian DNS *Filtering* dilakukan selancar pada website. Sudah tidak terlihat gambar, iklan online yang mengganggu pada halaman web. DNS *Filtering* melakukan *blocking* dengan memasukkan link iklan online ke dalam *blocklist* pada DNS *Filtering.*

Kata kunci: *Blocklist*, DNS *Filtering*, Iklan Online, MITM, VPN

Abstract

Every device connected to the internet, in general, poses a risk to the security of its network. Examples of this risk are the Man In The Middle (MITM) attack and intrusive online advertising. Man In The Middle (MITM) is a cyber-attack that occurs when a third party secretly intercepts two people's communications. So Virtual Private Network (VPN) and DNS Filtering can be used to prevent such attacks. VPN changes its connection path, and data exchange is hidden, so access to websites can be done safely. While DNS Filtering is used to block websites with annoying online ad popups when the user is surfing the internet. From testing through Wireshark on the use of VPN, the results obtained, are secure connections from MITM attacks. So that the contents of the data are not read by irresponsible parties, the data packets are sent with encryption using 256-bit AES encryption cipher and SHA-512 hash algorithm. Meanwhile, the DNS Filtering test was carried out surfing the website. No more visible images, annoying online advertisements on web pages. DNS Filtering performs blocking by including online advertising links into the blocklist in DNS Filtering.

Keywords: Blocklist, DNS Filtering, Online Advertising, MITM, VPN

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

PENDAHULUAN

Pesatnya perkembangan teknologi khususnya internet memudahkan pertukaran informasi dari dan ke berbagai tempat. Meskipun telah memiliki beragam jenis protokol keamanan, namun masih terdapat celah yang menembus keamanannya, yang berakibat pencurian data informasi penting. Salah satu contohnya adalah ketika seseorang sedang menggunakan sosial media di jaringan publik seperti wifi gratis yang ada di cafe. Di jaringan wifi gratis tersebut kemungkinan sudah ada pihak tidak bertanggung jawab yang dengan sengaja mengambil informasi privasi dan data penting dari orang tersebut. Tidak hanya sampai di situ, iklan online yang muncul di saat seseorang berselancar di internet tentu sangat mengganggu karena ada beberapa dari iklan online tersebut menghalangi isi dari website tersebut. Pada prosiding "Simulasi Keamanan Server Menggunakan OPENVPN" (Sandre Handoyo, 2015) menjelaskan bahwa pihak yang tidak bertanggung jawab dapat melakukan penyadapan data yang melewati jaringan publik. Kemudian pada jurnal "Analisis Celah Keamanan Jaringan Komputer dengan Menggunakan Raspberry PI 2" (Nur Ilham & Arif Candra, 2018) menjelaskan bahwa iklan yang muncul ketika sedang berselancar di internet dapat membuat waktu yang dibutuhkan untuk membuka website yang dituju menjadi lebih lama dan juga mengganggu. Dari penelitian sebelumnya tersebut dapat disimpulkan bahwa saat berselancar di internet ada risiko kerugian dengan adanya data dapat diambil orang yang tidak bertanggung jawab dan munculnya iklan online. Kebaharuan penelitian ini mencoba untuk mengangkat kedua masalah di atas dalam satu pembahasan. Setiap perangkat teknologi yang terhubung ke internet memiliki risiko pada keamanan jaringannya. Sebagai contoh seperti serangan *Man In The Middle (MITM)*, maupun iklan online yang mengganggu. *Man In The Middle* (MITM) merupakan serangan *cyber* yang terjadi ketika pihak ketiga secara diam-diam mencegat atau mengambil informasi penting saat ada dua pihak sedang berkomunikasi. Penggunaan Pritunl sebagai *Virtual Private Network* (VPN) server merupakan solusi tepat untuk permasalahan keamanan jaringan diatas. Akses ke website menjadi aman karena mengubah jalur koneksi melalui server dan menyembunyikan pertukaran data yang terjadi. Sedangkan integrasi Pihole yang menjadi DNS server dengan fitur DNS *Filtering* digunakan untuk memblokir website dengan popup iklan online yang mengganggu tersebut disaat user sedang berselancar di internet.

Virtual Private Network (VPN)

Para ahli mendefinisikan *Virtual Private Network* (VPN) sebagai berikut. Pertama; Menurut (Sofana, 2012), *Virtual Private Network* (VPN) merupakan teknologi jaringan komputer yang menghubungkan beberapa jaringan lokal dengan memanfaatkan media komunikasi publik seperti internet. Informasi yang mengalir melalui jaringan publik, berasal dari node-node *Virtual Private Network* (VPN) akan "dibungkus" (*tunneled*). Sehingga, informasi yang mengalir tadi menjadi aman dan tidak mudah dibaca oleh yang lain. Kedua; Menurut (Putra, Indriyani, & Angraini, 2018) *Virtual Private Network* (VPN) adalah sebuah teknologi komunikasi yang digunakan untuk dapat bergabung dengan jaringan lokal, setelah terkoneksi ke jaringan publik terlebih dahulu. Ketiga; Menurut Umam dan Roza (2016) dalam (Musril, 2019) bahwa Jaringan *Virtual Private Network* (VPN) merupakan pengguna teknologi GRE Tunnel, untuk menghubungkan lebih dari satu router lainnya. Dengan protokol GRE yang digunakan mampu menghantarkan paket.

Domain Name Services (DNS)

Menurut Athailah (2013) dalam (Putra, Indriyani, & Angraini, 2018) *Domain Name Services* (DNS) adalah alat penterjemah alamat website menjadi sebuah alamat IP. Hal ini perlu dilakukan karena komputer tidak dapat mengenali karakter-karakter yang terangkai membentuk sebuah alamat website selayaknya manusia, komputer hanya mengenal nomor. Maka dari itu, peranan DNS ini sangat penting pada sebuah jaringan komputer yang luas seperti internet, karena DNS inilah yang bekerja mencari nomor IP dari *website www.google.com* yang diketik pada browser, sehingga komputer menemukannya sebuah nomor 172.217.194.139 dan menampilkan halaman google di layar monitor.

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

DNS *Filtering*

DNS *Filtering* adalah praktik memblokir akses ke situs tertentu untuk tujuan tertentu. Jika sebuah situs, atau kategori situs, telah dianggap sebagai ancaman, maka alamat akan diblokir. Contoh situs yang mungkin diblokir termasuk iklan online, situs dewasa, perjudian, penurunan produktivitas, atau yang diketahui menimbulkan risiko malware yang signifikan. Cara agar DNS *Filtering* dapat melakukan *blocking* adalah dengan memasukkan link tersebut ke dalam *blocklist* di DNS *Filtering* tersebut.

Iklan Online

Iklan online merupakan iklan yang ditampilkan melalui komputer desktop maupun mobile yang menggunakan internet sebagai media penyampaian pesan promosinya. Iklan online berisi informasi atau pesan yang akan disampaikan kepada masyarakat umum dengan tujuan untuk mengajak, memperkenalkan atau membujuk agar masyarakat umum ikut pada suatu ajakan tertentu yang terpasang. Iklan online pun memiliki berbagai macam jenisnya. Iklan muncul berupa video dengan promosi produk yang diberi nama video pemasaran online atau *video online advertising* (Utami, 2021).

Topologi Jaringan Star

Menurut (Sofana, 2012), Topologi menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan didesain. Dalam definisi topologi terbagi menjadi dua, yaitu topologi fisik (*physical topology*) yang menunjukan posisi pemasangan kabel secara fisik dan topologi logika (*logical topology*) yang menunjukan bagaimana suatu media diakses oleh host. Dalam topologi jaringan star, komputer dihubungkan oleh kabel-kabel menuju komponen sentral, yang biasa disebut switch. Sinyal-sinyal ditransmisikan dari komputer pengirim menuju semua komputer dalam jaringan. Topologi ini berasal dari masa awal pengembangan jaringan ketika semua komputer dihubungkan ke *mainframe* komputer sentral.

(*Open Systems* Interconnection) OSI Layer

Menurut (Sofana, 2012), Model *Open Systems Interconnection* (OSI) adalah model kerangka logika terstruktur yang disediakan oleh *International Organization for Standardization* (ISO) untuk mengetahui bagaimana proses komunikasi data berinteraksi melalui jaringan. Standard ini dikembangkan untuk industri komputer agar komunikasi dapat dilakukan oleh komputer pada jaringan yang berbeda. OSI sebagai model referensi dan membagi tugas-tugas jaringan ke dalam 7 layer. Ketujuh *layer* tersebut, sesuai urutan paling bawah adalah layer: *Physical, Data Link, Network, Transport, Session, Presentation,* dan *Application.*

Dari dua permasalahan yang ada, yaitu serangan MITM dan iklan online yang mengganggu, maka dibangunlah sistem keamanan jaringan berbasis *Virtual Private Network* (VPN) yang terintegrasi dengan *Domain Name Services* (DNS). Server VPN menggunakan pritunl dengan openvpn client sebagai aplikasi clientnya. Sedangkan server DNS adalah pihole. Dengan adanya sistem keamanan jaringan ini, maka diharapkan Informasi privasi dan data penting seseorang yang menggunakan jaringan publik dapat diamankan dan Iklan online yang mengganggu dapat diblokir ketika seseorang berselancar di internet.

METODE PENELITIAN

Pada penelitian ini peneliti melakukan beberapa langkah dalam metodenya, yaitu :

a. Identifikasi masalah
   Tahap pertama dilakukan dengan mengidentifikasi permasalahan yang muncul. Sehingga, dapat disusun rencana awal, perumusan masalah, metode dan solusi akhirnya.
b. Pengumpulan data
   Tahap kedua dilakukan pengumpulan data dataset domain iklan yang akan di blokir dan data atribut user.
   Dataset domain iklan didapatkan dengan 2 cara; pertama, data internet tentang dataset domain iklan yang akan di blokir, kedua dengan melakukan observasi pengamatan langsung terhadap website yang memiliki iklan mengganggu melalui domain popup

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

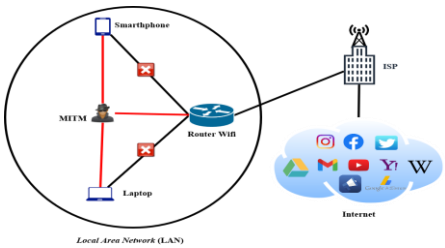
iklan yang muncul di website tersebut ke daftar yang dibuat peneliti.Data atribut user berupa sistem operasi, IP *private* dan IP publik yang digunakan user. Data atribut user ini didapat dari database server VPN dan server DNS.

c. Analisis penyelesaian
Analisis penyelesaian terhadap serangan *Man In The Middle* (MITM) yang dilakukan menggunakan VPN server yaitu dengan cara menyembunyikan pertukaran data dengan mengubah jalur koneksi melalui server. Seluruh paket data yang terkirim akan dienkripsi sebelum dikirim agar isi data tersebut tidak dapat dibaca oleh pihak yang tidak bertanggung jawab. Adapun analisis serangan permasalahan iklan online yang mengganggu, dilakukan dengan menggunakan *DNS Filtering* untuk memblokir website dengan popup iklan online yang mengganggu tersebut disaat user sedang browsing di internet.

HASIL DAN PEMBAHASAN

Perancangan Infrastruktur keamanan jaringan *Virtual Private Network* (VPN) dan *Domain Name Services* (DNS)

Perancangan infrastruktur yang dilakukan adalah perancangan topologi, perangkat keras, dan perangkat lunak yang akan digunakan pada sistem keamanan jaringan VPN dan DNS. Perancangan dilakukan untuk memudahkan saat mengkonfigurasi sistem yang akan dibuat. Kondisi jaringan yang sedang berjalan dapat dilihat pada Gambar 1. Dimana semua perangkat *smartphone* dan laptop terhubung ke modem wifi di sisi LAN. Setelah itu data diteruskan ke ISP dan kemudian ISP meneruskan ke internet.



Gambar 1. Simulasi Jaringan berjalan

Adapun tabel 1. OSI layer pada jaringan berjalan adalah sebagai berikut :

Tabel 1. OSI Layer Sistem Berjalan

NO	OSI *LAYER*	PERANGKAT	KETERANGAN
1	*Layer* 1 (*Physical Layer*)	NIC WIFI	NIC WIFI Pada Perangkat *Client*
2	*Layer* 2 (*Data-Link Layer*)	MAC *Address* Pada Perangkat *Client*	10:5B:AD:C7:F8:21 33:7C:B2:55:A1:32
3	*Layer* 3 (*Network Layer*)	IP *Address* Pada Perangkat *Client*	192.168.1.1, 192.168.1.2, 192.168.1.3
4	*Layer* 4 (*Transport Layer*)	*Protocol* TCP Dan UDP	Port TCP 80 dan 443 untuk membuka website Port TCP dan UDP 53 untuk DNS

Sementara untuk secara fisik perangkat keras (*hardware*) dan perangkat lunak (*software*) jaringan berjalan adalah seperti pada tabel 2 dan 3 sbb :

Tabel 2. Perangkat keras (*hardware*)

NO	PERANGKAT	JUMLAH	SPESIFIKASI	KETERANGAN
1	Laptop	1	Lenovo 320-14IKB Intel(R) Core(TM) i5-7200U RAM DDR4 12GB SSD 256GB	Sebagai *Client* Laptop
2	Smartphone	1	Redmi 10 Snapdragon 678 RAM 4GB Internal 64GB	Sebagai *Client* Smartphone
3	Router WIFI	1	Modem Huawei E5577	Sebagai *Gateway* Internet

Perangkat laptop dan smartphone digunakan sebagai host *client*. Sedangkan perangkat router wifi digunakan sebagai *gateway* ke internet. Adapun untuk perangkat

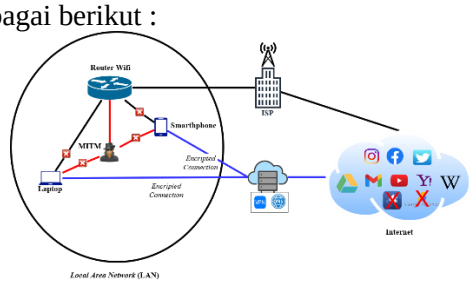
p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

lunak yang digunakan adalah seperti tabel 3 berikut :

Tabel 3. Perangkat Lunak (*software*)

NO	SOFTWARE	VERSION	KETERANGAN
1	Windows	Windows 10	Digunakan sebagai sistem operasi *Client* Laptop
2	Android	Android 7	Digunakan sebagai sistem operasi *Client* Smartphone
3	Wireshark	Wireshark 3.4.5	Digunakan untuk *monitoring* port dan *protocol* jaringan di server dan *Client*
4	Browser	Firefox 88.0	Digunakan untuk membuka halaman website

Windows dan smartphone digunakan sebagai sistem operasi *client*. Digunakan untuk *monitoring* port dan *protocol* jaringan di server dan *Client*. Kemudian browser digunakan untuk melihat *content* pada halaman website. Jika dilihat pada jaringan berjalan diatas, *client* langsung terhubung ke jaringan publik. *Client* menjadi sangat rentan terhadap serangan keamanan jaringan. Sehingga adalah beberapa serangan yang mungkin dapat terjadi pada jaringan tersebut adalah serangan *Man In The Middle* (MITM) dan iklan online yang mengganggu. Untuk menyelesaikan masalah di atas maka dibuatlah perancangan infrastruktur keamanan jaringan seperti pada gambar 2. sebagai berikut :



Gambar 2. Topologi Keamanan Jaringan VPN dan DNS

Untuk penyelesaian masalahnya yaitu merancang topologi dengan menambah 1 server untuk nantinya dipasangkan sebagai VPN server dan DNS server. Berikut adalah metode yang digunakan untuk menyelesaikan 2 permasalahan jaringan diatas:

1. Metode menyelesaikan permasalahan serangan *Man In The Middle* (MITM). Dengan menggunakan VPN server akses ke website menjadi aman dengan cara menyembunyikan pertukaran data dengan mengubah jalur koneksi melalui server. Seluruh paket data yang terkirim akan dienkripsi sebelum dikirim agar isi data tersebut tidak dapat dibaca oleh pihak yang tidak bertanggung jawab.
2. Metode menyelesaikan permasalahan iklan online yang mengganggu. *DNS Filtering* digunakan untuk memblokir website dengan popup iklan online yang mengganggu tersebut disaat user sedang berselancar di internet. Cara agar *DNS Filtering* dapat melakukan *blocking* adalah dengan memasukan link iklan online tersebut ke dalam *blocklist* di *DNS Filtering* tersebut.

Tabel 4 adalah OSI layer yang dirancang sebagai usulan.

Tabel 4. OSI Layer Usulan

NO	OSI *LAYER*	PERANGKAT	KETERANGAN
1	*Layer* 1 (*Physical Layer*)	NIC WIFI	NIC WIFI Pada Perangkat *Client*
2	*Layer* 2 (*Data-Link Layer*)	MAC *Address* Pada Perangkat *Client*	10:5B:AD:C7:F8:21 33:7C:B2:55:A1:32
3	*Layer* 3 (*Network Layer*)	IP *Address* Pada Perangkat *Client*	172.20.0.1 36.90.152.75
4	*Layer* 4 (*Transport Layer*)	*Protocol* TCP Dan UDP	Port TCP 80 dan 443 untuk membuka website Port TCP 1194 untuk VPN Port TCP dan UDP 53 untuk DNS
5	*Layer* 5 (*Session Layer*)	SQL pada server *monitoring*	Database yang digunakan server VPN
6	*Layer* 6	SSL pada	*Encryption*

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

	(*Presentation Layer*)	VPN	*cipher* AES 256 bit dan hash algorithm SHA-512 Pada VPN
7	*Layer* 7 (*Application Layer*)	HTTP, HTTPS, DNS	Management server VPN dan server DNS Website yang dibuka oleh *user*

Adapun spesifikasi perangkat keras usulan yang digunakan untuk infrastruktur jaringan adalah seperti pada tabel 5. berikut:

Tabel 5. Spesifikasi Perangkat Keras Usulan

PERANGKAT	SPESIFIKASI
Laptop	Lenovo 320-14IKB Intel(R) Core(TM) i5-7200U RAM DDR4 12GB SSD 256GB
Smartphone	Redmi 10 Snapdragon 678 RAM 4GB Internal 64GB
Router WIFI	Modem Huawei E5577
Cloud Server	vCPU 1 Core RAM 1GB SSD 8GB

Sedangkan tabel 6 berikut adalah spesifikasi perangkat lunak usulan yang digunakan untuk infrastruktur.

Tabel 6. Spesifikasi Perangkat Lunak Usulan

SOFTWARE	KETERANGAN
Windows	Digunakan sebagai sistem operasi *Client* Laptop
Android	Digunakan sebagai sistem operasi *Client* Smartphone
Wireshark	Digunakan untuk *monitoring* port dan *protocol* jaringan di server dan *Client*
WebBrowser	Digunakan untuk membuka halaman website
Inspect Element pada Browser	Digunakan untuk mengecek content pada halaman website
OpenVPN*Client*	Digunakan untuk koneksi VPN di sisi *client*
Linux	Digunakan sebagai sistem operasi Server
Pritunl	Digunakan sebagai sistem VPN server
Mongodb	Digunakan sebagai database *user* VPN
Pihole	Digunakan sebagai DNS Server

Adapun pengalamatan ip *address* baik IP Private maupun IP Publik pada jaringan yang diusulkan untuk VPN dan DNS ada pada tabel 7 berikut ini :

Tabel 7. Pengalamatan IP *Address* Pada Jaringan Usulan VPN Dan DNS

NO	PERANGKAT	JENIS IP *ADDRESS*	IP *ADDRESS*	SUBNET MASK	*GATEWAY*
1	Router WIFI	IP Private	192.168.1.1	255.255.255.0	-
2	Laptop	IP Private	192.168.1.2	255.255.255.0	192.168.1.1
3	Smartphone	IP Private	192.168.1.3	255.255.255.0	192.168.1.1
4	IP External *Cloud* Server	IP Public	122.248.231.68	-	-
5	IP Internal *Cloud* Server	IP Private	172.31.28.92	255.255.240.0	172.31.16.1
6	IP *User* VPN	IP Private	172.20.1.0/24	255.255.255.0	-

IP private digunakan pada jaringan bersifat lokal dan IP publik digunakan pada jaringan internet. Router WIFI sebagai *gateway client* ke internet memiliki ip *private* 192.168.1.1. Laptop sebagai *client* memiliki ip *private* 192.168.1.2 dengan *gateway* internet ke router WIFI. Smartphone sebagai *client* memiliki ip *private* 192.168.1.3 dengan *gateway* internet ke router WIFI. *Cloud* server memiliki 2 ip, yaitu ip *external* dan ip *internal*. IP *external cloud* server digunakan untuk tujuan *client* mengkoneksikan dirinya ke VPN dengan ip publik 122.248.231.68. IP *internal cloud* server memiliki ip *private* 172.31.28.92. IP *user* VPN digunakan ketika *client* terkoneksi dengan server VPN dengan range ip 172.10.1.0/24. Sementara List domain blokir diperlukan untuk memblokir domain iklan online yang mengganggu. List domain ini akan

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

digunakan pada DNS *filtering*. Tabel 8 berikut adalah beberapa contoh domain pada list domain blokir.

Tabel 8. Contoh Domain yang Diblok

NO	DOMAIN	STATUS AKSES	KETERANGAN
1	adservice.google.com	BLOK	Iklan Popup Google
2	servicegoogle.com	BLOK	Iklan Popup Google
3	googleadapis.l.google.com	BLOK	Iklan Google Pada Game
4	gstaticadssl.l.google.com	BLOK	Iklan Google Pada Game
5	ads.facebook.com	BLOK	Iklan Facebook
6	creative.ak.facebook.com	BLOK	Iklan Facebook
7	itgiblean.com	BLOK	Iklan Pada Website Forum
8	onmarshtompor.com	BLOK	Iklan Pada Website Forum
9	jsc.adskeeper.co.uk	BLOK	Iklan Pada Website Steaming
10	whugesto.net	BLOK	Iklan Pada Website Streaming

Jumlah total list domain blokir ini adalah 511.676 domain. List domain blokir yang sudah dikumpulkan oleh penulis dapat dilihat pada link https://raw.githubusercontent.com/elvirzash/list/main/block. Untuk domain yang diizinkan adalah domain yang tidak terdaftar di list tersebut.

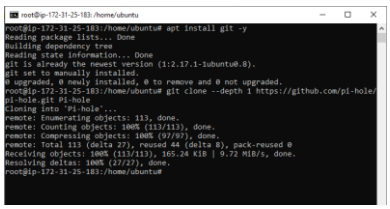
Membangun sistem keamanan jaringan *Virtual Private Network* (VPN) dan *Domain Name Services* (DNS)

Pada bagian ini akan dijelaskan tentang pembangunan *Virtual Private Network* (VPN) dan *Domain Name Services* (DNS). Pembangunan meliputi infrastruktur, tahap konfigurasi dan tahap pengujian. Infrastruktur dibangun dengan membuat topologi dan pengalamatan IP Addressnya seperti pada tahap perancangan di atas. Kemudian dilanjutkan ke tahap konfigurasi dan tahap pengujian.

Konfigurasi Server DNS

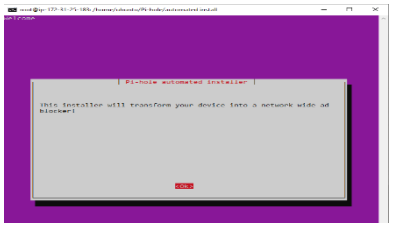
Konfigurasi server DNS dilakukan dengan beberapa langkah berikut ini :

a. Mengistall git dan melakukan clone aplikasi pihole di github dengan sintak " apt install git -y " dan " git clone --depth 1 https://github.com/pi-hole/pi-hole.git Pi-hole ".



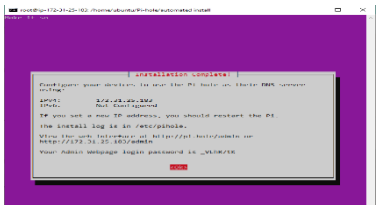
Gambar 3. Menginstall Git

b. Menginstall pihole dengan sintak " sudo bash basic-install.sh ".



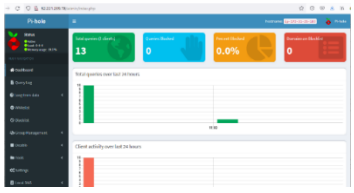
Gambar 4 Mengistall Pihole

c. Setelah selesai menginstall pihole. Selanjutnya diminta untuk mengkonfigurasi pihole dari web management. http://52.221.239.78/admin



Gambar 5. Selesai Mengistall Pihole

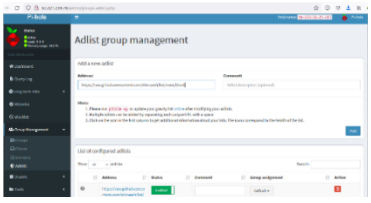
d. Tampilan Dashboard Pihole



Gambar 6. Dashboard Pihole

e. Memasukan list domain yang akan diblokir. Memasukan list domain tersebut pada menu Group Management > Adlist > Add.

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

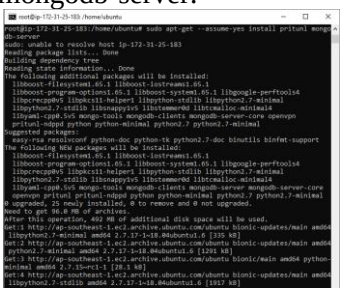


Gambar 7. Memasukan Blocklist Di Pihole

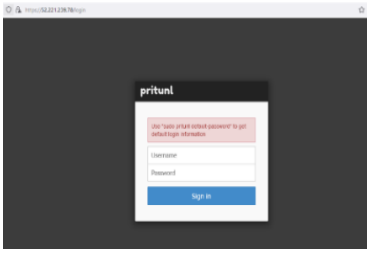
Konfigurasi Server VPN

Konfigurasi server VPN dilakukan dengan beberapa langkah berikut ini :

a. Menginstall pritunl dan mongoDB dengan sintax. sudo apt-get --assume-yes install pritunl mongodb-server.

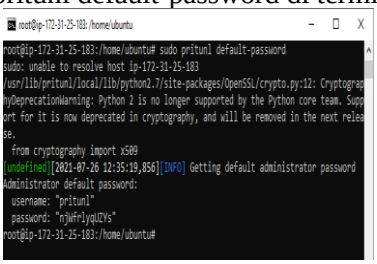

Gambar 8. Mengistall Pritunl Dan MongoDB

b. Jika Install telah berhasil maka web management dapat diakses pada https://ip-public-server/. Saat pertama membuka web management VPN akan meminta default login



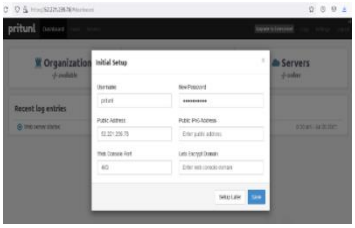
Gambar 9. Login Pritunl

c. Default login diperoleh dengan mengetikan sudo pritunl default-password di terminal



Gambar 10. Default Password Login Pritunl

d. Jika sudah berhasil login, pertama kali admin harus melakukan ganti password.

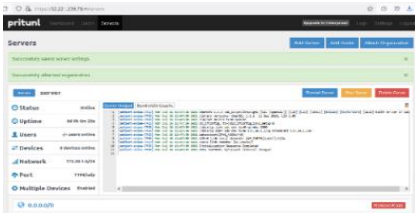


Gambar 11. Ganti Password Pritunl

e. Langkah selanjutnya adalah mengkonfigurasi server VPN.
DNS Server : 172.31.25.183
Port : 1194 UDP
Virtual network : 172.20.1.0/24
Encryption Cipher : AES 256bit
Hash Algorithm : SHA-512

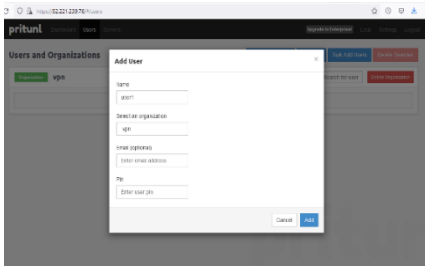
Gambar 12. Setup Server VPN

f. Klik start server, ini akan menjalankan server VPN.



Gambar 13. Start Server VPN

g. Tambah user VPN



Gambar 14 Membuat User VPN

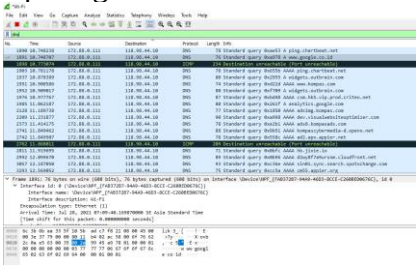
Pengujian Pada *Virtual Private Network* (VPN) dan *Domain Name Services* (DNS)

Pengujian Pada VPN

Pengujian pada VPN perlu dilakukan untuk memastikan apakah koneksi user sudah menggunakan koneksi VPN. Pengujian VPN dapat dilakukan dengan cara membandingkan hasil wireshark

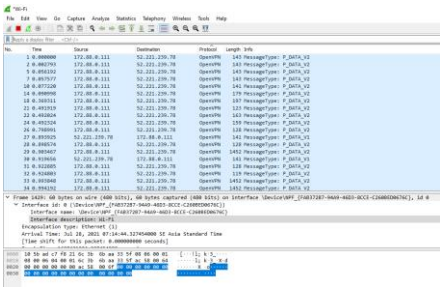
p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

sebelum dan sesudah menggunakan VPN, seperti pada gambar 15 dan 16 berikut ini.



Gambar 15. Koneksi Sebelum Terkoneksi VPN

Dari gambar 15 di atas dapat disimpulkan bahwa koneksi yang digunakan user tidak aman. Sebagai contohnya dari gambar tersebut website yang dituju oleh user dapat terlihat oleh pihak ketiga atau orang yang tidak berkepentingan. Tidak hanya website tujuan yang terlihat, tetapi juga memungkinkan data data penting lainnya seperti password dapat terlihat oleh orang yang tidak bertanggung jawab.



Gambar 16. Koneksi Sesudah Terkoneksi VPN

Dari gambar 16. dapat disimpulkan bahwa koneksi yang digunakan user sudah aman.

Pengujian Pada Domain Name Services (DNS)

Pengujian pada DNS perlu dilakukan untuk memastikan apakah iklan online yang mengganggu sudah benar benar terblokir. Pengujian DNS dapat dilakukan dengan cara membandingkan hasil *browsing* sebelum dan sesudah menggunakan DNS di website yang memiliki banyak iklan online seperti contohnya kompas.com. Gambar 17 dan gambar 18 berikut adalah perbandingan hasil wireshark sebelum dan sesudah menggunakan DNS.

Gambar 17. Sebelum Menggunakan DNS Filtering

Penulis menggunakan website kompas.com sebagai pengujian DNS. Dari gambar 18 di atas dapat disimpulkan bahwa iklan online sangat mengganggu disaat user sedang *browsing.* Terlihat seperti di gambar, iklan online menutupi sebagian halaman website.

Gambar 18. Sesudah Menggunakan DNS Filtering

Gambar 18 menunjukkan pengujian *browsing* website sesudah menggunakan DNS. Disini penulis menggunakan website kompas.com sebagai pengujiannya. Dapat disimpulkan bahwa iklan online sangat mengganggu sudah tidak ada disaat user sedang *browsing.* Terlihat seperti di gambar, iklan online sudah tidak ada pada halaman website. Akan tetapi *frame* dari iklan online tersebut masih tertinggal di halaman website.

SIMPULAN DAN SARAN

Dari hasil sistem keamanan jaringan *Virtual Private Network* (VPN) dan *Domain Name Services* (DNS) yang dibangun, dapat diambil beberapa simpulan, yaitu dengan menggunakan VPN server akses ke website menjadi aman dari serangan serangan *Man In The Middle* (MITM). Seluruh paket data yang terkirim akan dienkripsi sebelum dikirim agar isi data tersebut tidak dapat dibaca oleh pihak yang tidak bertanggung jawab. Kemudian, iklan online yang mengganggu dapat diblokir ketika seseorang berselancar di internet dengan menggunakan DNS *filtering.* Untuk server *Virtual Private Network* (VPN) sebaiknya

p - ISSN : 2407 – 1846
e - ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

menggunakan provider yang memiliki koneksi stabil agar koneksi dari *client* ke website tujuan menjadi stabil. Diperlukan *update* pada list domain yang akan diblokir agar iklan dengan domain baru juga terblokir dan diperlukan pemeliharan untuk mengurangi *false positif* ketika memblokir domain.

DAFTAR PUSTAKA

Musril, H. A. (2019). Desain Virtual Private Network (VPN) Berbasis Open Shortest Path First (OSPF). *Info Tekjar Jurnal Nasional Informatika dan Teknologi Jaringan* .

Nur Ilham, D., & Arif Candra, R. (2018). ANALISIS CELAH KEAMANAN JARINGAN KOMPUTER DENGAN MENGGUNAKAN RASPBERRY PI 2. *METHOMIKA : Jurnal Manajemen Informatika dan Komputerisasi Akuntansi*.

Putra, J. L., Indriyani, L., & Angraini, Y. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna. *IJCIT : Indonesian Jurnal On Computer and Information Technoogy*.

Sandre Handoyo, M. F. (2015). Simulasi Keamanan Server Menggunakan Openvpn. *eProceedings of Applied Science.* telkomuniversity.ac.id.

Sofana, I. (2012). *CISCO CCNP DAN JARINGAN KOMPUTER (MATERI ROUTE, SWITCH, & TROUBLESHOOTING).* Bandung: Informatika Bandung.

Utami, S. N. (2021, Juni 17). *www.kompas.com*. Dipetik November 5, 2021, dari https://www.kompas.com/skola/read/2021/06/17/100000469/video-online-advertising--definisi-jenis-dan-cara-membuatnya