Cyberspace: Jurnal Pendidikan Teknologi informasi
Volume 9, Nomor 1, Maret 2025, hal. 63 – 74
ISSN 2598-2079 (print) | ISSN 2597-9671 (online)

PENERAPAN HIERARKI *CERTIFICATE AUTHORITY* DAN *PUBLIC KEY INFRASTRUCTURE* UNTUK MEMPERKUAT KEAMANAN JARINGAN

[1]Husaini, [2]Teuku Hafiez Ramadhan, [3]Mahyus Ihsan

[1,3]Departemen Informatika, FMIPA Universitas Syiah Kuala, Banda Aceh
[2]Program Studi Sistem Informasi Universitas Bina Nusantara

E-mail: husaini.muhammad@usk.ac.id

Abstract

Nowadays, network security has become increasingly crucial, especially in a globally interconnected business environment. Communication between branch offices and headquarters through global networks poses risks such as data theft, surveillance, and cyberattacks. These risks undoubtedly present a serious threat to the confidentiality and integrity of a company's sensitive information. To mitigate these risks, this research proposes the implementation of a hierarchical Certificate Authority (CA) and Public Key Infrastructure (PKI) system, leveraging asymmetric keys for enhanced security. The hierarchical CA system ensures robust security measures through effective key management practices. The primary aim of this study is to enhance network security by safeguarding communications between branch and headquarters offices using a *Site-to-Site* Virtual Private Network (VPN) implemented with OpenVPN technology. This comprehensive approach involves various methodologies including Graphical Network Simulator-3 (GNS3) simulation for network architecture testing, rigorous evaluation of digital certificate security, continuous traffic monitoring, comprehensive network performance testing, and meticulous server security protocols. The anticipated outcomes of this research are expected to provide valuable insights for organizations aiming to mitigate network security risks effectively. Moreover, the findings are poised to contribute significantly to the advancement of network security frameworks tailored for the demands of a globally connected business environment.

Keywords: *Certificate Authority, network security, OpenVPN Site-to-Site, Public Key Infrastructure*

Abstrak

Dewasa ini, keamanan jaringan telah menjadi semakin krusial terutama dalam lingkungan bisnis yang saling terhubung secara global. Komunikasi antara kantor cabang dan kantor pusat melalui jaringan global memunculkan risiko seperti pencurian data, pengawasan, dan serangan siber. Hal ini tentu akan menjadi ancaman yang nyata terhadap kerahasiaan dan integritas informasi sensitif perusahaan. Untuk mengurangi risiko ini, penelitian ini mengusulkan implementasi sistem hierarki *Certificate Authority* (CA) dan *Public Key Infrastructure* (PKI) dengan memanfaatkan kunci asimetris untuk meningkatkan keamanan. Sistem hierarki CA memastikan langkah-langkah keamanan yang kuat melalui praktik manajemen kunci yang efektif. Tujuan utama dari penelitian ini adalah untuk meningkatkan keamanan

jaringan dengan melindungi komunikasi antara kantor cabang dan kantor pusat menggunakan *Site-to-Site Virtual Private Network* (VPN) yang diimplementasikan dengan teknologi OpenVPN. Pendekatan komprehensif ini melibatkan berbagai metodologi, termasuk simulasi *Graphical Network Simulator*-3 (GNS3) untuk pengujian arsitektur jaringan, evaluasi ketat terhadap keamanan sertifikat digital, pemantauan lalu lintas yang berkelanjutan, pengujian kinerja jaringan secara menyeluruh, dan protokol keamanan *server* yang teliti. Hasil yang diharapkan dari penelitian ini diharapkan dapat memberikan wawasan berharga bagi organisasi yang bertujuan untuk mengurangi risiko keamanan jaringan secara efektif. Selain itu, temuan penelitian ini diharapkan dapat memberikan kontribusi signifikan terhadap pengembangan kerangka kerja keamanan jaringan yang disesuaikan dengan kebutuhan lingkungan bisnis yang terhubung secara global.

Kata Kunci: *Certificate Authority, keamanan jaringan, OpenVPN Site-to-Site*, *Public Key Infrastructure*

1. Pendahuluan

Dalam era globalisasi dan kemajuan teknologi informasi, menjaga keamanan data dan privasi merupakan prioritas utama bagi perusahaan. Saat ini, perusahaan semakin terhubung satu sama lain melalui jaringan global, sehingga menyebabkan peningkatan risiko serangan siber, pencurian data, dan spionase yang mengancam integritas serta kerahasiaan informasi. Salah satu metode untuk melindungi keamanan jaringan adalah dengan menggunakan *Virtual Private Network* (VPN). VPN mengamankan komunikasi antara dua titik dalam jaringan dengan mengenkripsi data yang dikirimkan, sehingga menyulitkan pihak ketiga untuk mengaksesnya. Namun, VPN yang menggunakan kunci simetris memiliki kelemahan signifikan. Kunci simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi, sehingga jika kunci tersebut jatuh ke tangan pihak yang tidak berwenang, mereka dapat mengakses komunikasi yang seharusnya aman.

Penerapan sistem *Certificate Authority* (CA) dan *Public Key Infrastructure* (PKI) merupakan salah satu solusi untuk menjaga keamanan data dan privasi. Dalam skema ini, pihak ketiga yang terpercaya (CA) memverifikasi identitas entitas yang berkomunikasi, seperti *server* dan klien, serta menerbitkan sertifikat digital yang mengkonfirmasi keaslian dan kepercayaan terhadap kunci publik entitas tersebut. Kunci asimetris akan menggantikan kunci simetris dalam skema ini. Dengan kunci asimetris, setiap entitas memiliki sepasang kunci-kunci privat yang disimpan dengan aman oleh pemiliknya dan kunci publik yang dibagikan kepada pihak lain untuk mengenkripsi data yang akan dikirim. Kunci privat kemudian digunakan untuk mendekripsi data yang diterima.

Penggunaan hierarki CA bertujuan untuk menerapkan manajemen kunci yang efektif, sehingga memperkuat keamanan jaringan dengan menyediakan kunci yang unik dan aman untuk setiap entitas. Dalam sistem hierarki CA, terdapat hierarki khusus yang menangani kunci untuk entitas pengguna akhir (Sub-CA) dan hierarki yang mengelola tingkatan di bawahnya (Root CA).

Ada beberapa penelitian terkait yang membahas keamanan jaringan dan infrastruktur komunikasi. Danquah dan Kwabena-Adade [1] telah melakukan analisis terhadap mekanisme validasi *Public Key Infrastructure* (PKI) saat ini, mengidentifikasi kelemahan seperti integritas yang tidak pasti, kepercayaan terhadap otoritas sertifikat, dan risiko titik kegagalan tunggal, serta mengusulkan solusi berupa otoritas sertifikat ganda dan repositori publik. Ishag dan Hamid [4] telah mengkaji koneksi VPN Site-to-Site, yang memungkinkan jaringan berbeda terhubung secara aman tanpa memerlukan klien VPN

di perangkat pengguna. Penelitian Sherwood [5] fokus pada tantangan dalam implementasi PKI secara luas, terutama untuk organisasi kecil, dan menyoroti pentingnya pengelolaan siklus hidup sertifikat. Usanto [7] serta Varianto dan Badrul [8] meninjau penerapan VPN di perusahaan yang menggunakan VPN *Site-to-Site* untuk menghubungkan kantor pusat dengan cabang secara *real-time*. Namun, penelitian ini dengan menggunakan ClearOS ini masih terbatas pada aspek teknis. Penelitian yang dilakukan oleh Wulandari dkk. [9] menyoroti pengaturan keamanan jaringan di institusi pendidikan yang lebih berfokus pada topologi dan perangkat keras tanpa menyoroti hubungan antara kantor cabang dan pusat.

Meskipun berbagai penelitian telah dilakukan, masih terdapat kekurangan dalam implementasi teknologi keamanan jaringan untuk mendukung hubungan yang efisien dan aman antara kantor pusat dan cabang di dunia industri. Untuk itu, tujuan dari penelitian ini adalah untuk meningkatkan keamanan jaringan antara kantor cabang dan kantor pusat dengan mengimplementasikan sistem CA dan PKI menggunakan *Site-to-Site* VPN dengan OpenVPN. Hal ini akan menyediakan koneksi yang aman dan terenkripsi antara kantor cabang dan kantor pusat, sehingga mengurangi risiko gangguan dan pelanggaran data.

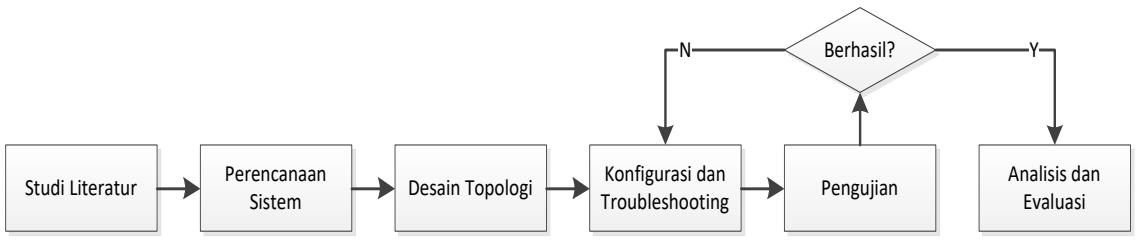
Penelitian ini menggunakan simulasi berbasis skenario menggunakan GNS3 untuk menguji keamanan jaringan di kantor cabang dan kantor pusat. Dalam simulasi ini, CA dan PKI digunakan untuk menerbitkan sertifikat digital yang diperlukan guna mengamankan koneksi jaringan antara kantor-kantor tersebut. Skenario juga mencakup pengujian keamanan untuk mengevaluasi keandalan sistem yang diimplementasikan serta pengujian kinerja jaringan antara kantor cabang dan pusat.

Hasil penelitian ini diharapkan dapat memberikan manfaat bagi perusahaan dengan meningkatkan keamanan jaringan mereka dan mengurangi risiko keamanan yang tidak diinginkan. Dengan mengimplementasikan sistem CA dan PKI bersama dengan OpenVPN *Site-to-Site*, koneksi jaringan antara kantor cabang dan pusat dapat dilindungi secara efektif. Selain itu, temuan dari penelitian ini dapat memberikan panduan praktis bagi perusahaan yang ingin meningkatkan keamanan jaringan mereka menggunakan sertifikat digital dan teknologi VPN.

Sebagai kesimpulan, penelitian ini dapat memberikan manfaat signifikan bagi perusahaan dengan mengurangi risiko keamanan jaringan yang tidak diinginkan dan meningkatkan keamanan jaringan secara keseluruhan. Selain itu, penelitian ini juga dapat memberikan kontribusi penting bagi pengembangan sistem keamanan jaringan dalam lingkungan bisnis global yang semakin terhubung.

2. Metodologi Penelitian

Langkah-langkah yang dilakukan di dalam penelitian ini meliputi studi literatur, perencanaan sistem, desain topologi, konfigurasi dan *troubleshooting*, pengujian, serta analisis dan evaluasi seperti tampak pada Gambar 1.



Gambar 1. Diagram Alir Penelitian

A. Studi Literarur

Pada tahap ini, peneliti melakukan studi literatur tentang konsep PKI dengan CA dan teknologi jaringan *Site-to-Site* VPN antara perusahaan cabang dan pusat, serta landasan teori terkait dengan topik yang dapat menunjang literatur dalam penelitian. Penelitian literatur dilakukan dengan mencari sumber-sumber yang terpercaya seperti jurnal akademis, buku, situs web, dan publikasi teknis untuk memperoleh pemahaman yang mendalam tentang topik ini.

B. Perencanaan Sistem

Pada tahap ini, peneliti merencanakan sistem yang akan diimplementasikan. Beberapa faktor yang dipertimbangkan seperti desain topologi jaringan yang optimal, pemilihan perangkat lunak dan perangkat keras yang tepat, serta identifikasi kebutuhan bisnis perusahaan. Perencanaan ini bertujuan untuk memastikan bahwa jaringan *Site-to-Site* VPN yang diimplementasikan dapat memenuhi kebutuhan dan tujuan bisnis perusahaan.

C. Desain Topologi

Pada tahap ini, peneliti mendesain topologi jaringan *Site-to-Site* VPN yang optimal. Peneliti membuat desain hierarki CA yang sesuai dengan kebutuhan perusahaan, dan mempertimbangkan faktor-faktor seperti skalabilitas, keamanan, dan kinerja jaringan. Selain itu, peneliti menentukan bagaimana sertifikat digital akan dikonfigurasi untuk setiap perangkat yang terhubung ke jaringan VPN.

D. Konfigurasi dan *Troubleshooting*

Pada tahap ini, peneliti mengimplementasikan konfigurasi jaringan *Site-to-Site* VPN yang diusulkan dan menangani masalah yang mungkin terjadi selama implementasi. Peneliti mengonfigurasi perangkat keras dan perangkat lunak yang dibutuhkan untuk jaringan *Site-to-Site* VPN dan dilanjutkan dengan melakukan tes pada konfigurasi yang telah diimplementasikan.

E. Pengujian

Pada tahap ini, peneliti melakukan pengujian untuk memastikan bahwa jaringan *Site-to-Site* VPN yang diimplementasikan berfungsi dengan benar dan dapat menjamin keamanan dan integritas data yang ditransmisikan melalui jaringan. Peneliti menggunakan perangkat lunak Wireshark dan perangkat lunak lainnya untuk memverifikasi keabsahan pesan dan mengukur kinerja jaringan, termasuk kecepatan, latensi, dan *throughput*, serta melakukan *penetration testing*.

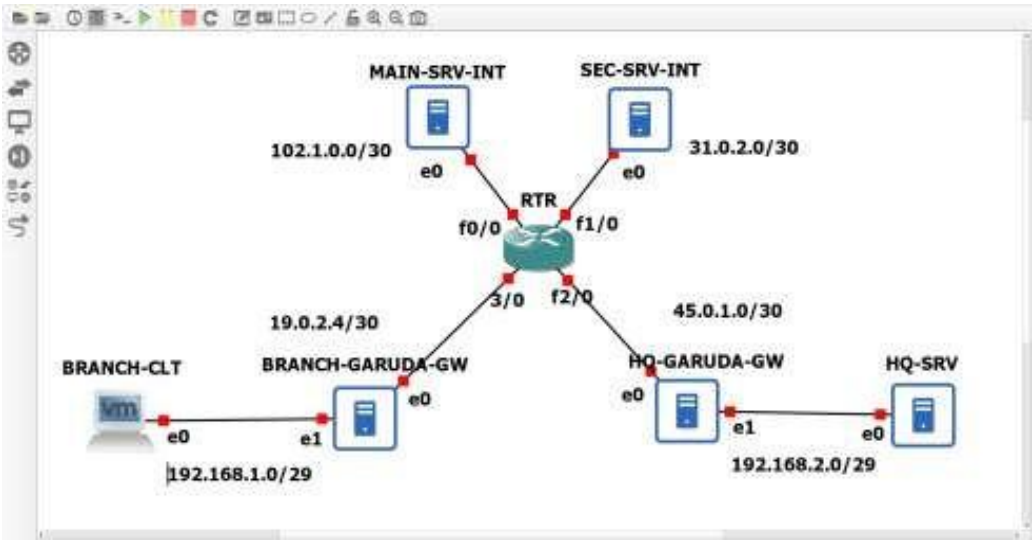
F. Analisis dan Evaluasi

Pada tahap ini, peneliti menganalisis dan mengevaluasi hasil pengujian untuk memastikan bahwa jaringan *Site-to-Site* VPN yang diimplementasikan telah mencapai tujuan keamanan dan kinerja jaringan yang diinginkan. Peneliti menganalisis hasil pengujian dan melakukan evaluasi terhadap keandalan jaringan dan kesesuaian sertifikat digital yang dikeluarkan oleh CA.

3. Hasil dan Pembahasan

A. Topologi dan Konfigurasi Jaringan

Topologi jaringan yang digunakan pada penelitian ini diimplementasikan dengan menggunakan software GNS3. Visualisasi topologi dapat dilihat pada Gambar 2 yang terdiri dari satu *router* yang berlabel "RTR" untuk mensimulasikan segmen jaringan yang berbeda antara satu dengan yang lainnya, lalu PKI diimplementasikan dengan dua *server* CA dengan hierarki, lalu pada BRANCH-GARUDA-GW ada sebuah *client* yang menjadi menjalankan pengujian, dan pada HQ-GARUDA-GW ada sebuah *server* yang berfungsi menyimpan data perusahaan.



Gambar 2. Topologi jaringan menggunakan GNS3.

Tabel 1 menunjukkan semua pengalamatan IP versi 4 dan *interface* jaringan dari seluruh perangkat yang terhubung. Disini, setiap *gateway* dan *server* CA menggunakan IP Publik, hal ini dilakukan untuk mensimulasikan jaringan yang terhubung secara global, dengan *netmask* yang diekspresikan dengan CIDR, dan disesuaikan dengan kebutuhan topologi. Sedangkan untuk konfigurasi IPv4 dan *interface* VPN pada kedua *server* HQ-GARUDA-GW dan BRANCH-GARUDA-GW dapat dilihat pada Tabel 2. Selanjutnya konfigurasi *routing* dinamis menggunakan OSPF dari *router* dengan label RTR ditampilkan pada Tabel 3 berikut.

TABEL 1 PENGALAMATAN IPV4 DAN *INTERFACE* JARINGAN

No	Nama	*Interface*	*IP Address*	CIDR
1	MAIN-SRV-INT	fa0	102.1.0.2	/30
2	SEC-SRV-INT	fa0	31.0.2.2	/30
3	RTR	fa0/0	102.1.0.1	/30
		fa1/0	31.0.2.1	/30
		fa2/0	45.0.1.1	/30
		fa3/0	19.0.2.5	/30
4	BRANCH-GARUDA-GW	fa0	19.0.2.6	/30
		fa1	192.168.1.1	/29

		tun0	10.0.0.1	/30
5	HQ-GARUDA-GW	fa0	45.0.1.2	/30
		fa1	192.168.2.1	/29
		tun0	10.0.0.2	/30
6	HQ-SRV	fa0	192.168.2.2	/29
7	BRANCH-CLT	fa0	192.168.1.2	/29

TABEL 2 KONFIGURASI *INTERFACE* VPN SITE-TO-SITE

No	Nama	*Interface*	*IP Address*	CIDR
1	HQ-GARUDA-GW	tun0	10.0.0.2	/30
2	BRANCH-GARUDA-GW	tun0	10.0.0.1	/30

TABEL 3 KONFIGURASU *ROUTING* OSPF PADA NODE RTR

No	*Node*	*Network*	*Wildcard*	*Area*
1	MAIN-SRV-INT	102.1.0.0	0.0.0.3	0
2	SEC-SRV-INT	31.0.2.0	0.0.0.3	
3	HQ-GARUDA-GW	45.0.1.0	0.0.0.3	
4	BRANCH-GARUDA-GW	19.0.2.4	0.0.0.3	

B. Implementasi *Firewall* dan IP *Forwarding*

Firewall dan IP Forwarding sangat penting dalam menjamin keamanan dari jaringan komputer. Seperti yang ditampilkan pada Tabel 4, koneksi untuk node MAIN-SRV-INT dan SEC-SRV-INT hanya diizinkan melalui protokol SSH saja. Hal ini dikarenakan kedua *server* ini adalah bagian dari hierarki CA, yang menangani permintaan sertifikat digital melalui protokol SCP untuk mengirim file secara aman. Sedangkan untuk node HQ-GARUDA-GW dan BRANCH-GARUDA-GW hanya koneksi untuk protokol SSH dan OpenVPN yang diizinkan. Ini bertujuan agar node dapat menjalin koneksi terenkripsi melalui OpenVPN dan SSH sebagai protokol untuk melakukan proses penyalinan data secara aman.

TABEL 4 INFORMASI ATURAN *FIREWALL* DAN IP *FORWARDING*

Node	*Allowed Protocol*	*All*	*IP Forwarding*
MAIN-SRV-INT	SSH	*Deny*	*FALSE*
SEC-SRV-INT	SSH	*Deny*	*FALSE*
HQ-GARUDA-GW	SSH, OPENVPN, ICMP	*Deny*	*TRUE*
BRANCH-GARUDA-GW	SSH, OPENVPN, ICMP	*Deny*	*TRUE*

C. Implementasi Hierarki *Certificate Authority*

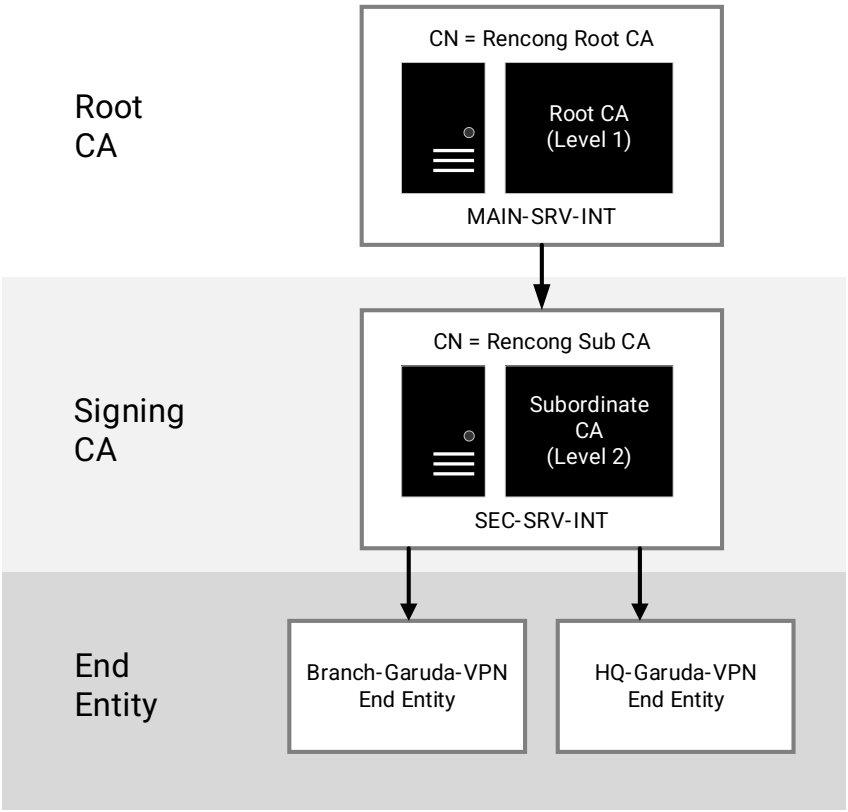
Gambar 3 berikut menunjukkan hierarki dari *Root* CA, *Subordinate* CA hingga ke *End-Entity Certificate* masing-masing untuk HQ-Garuda-VPN dan Branch-Garuda-VPN yang ditandatangani oleh SEC-SRV-INT sebagai Subordinate CA dengan menggunakan *public key* Root CA. Selanjutnya untuk *Common Name* (CN), informasi jenis dan *issuer* dari sertifikat dapat mengacu pada Tabel 5 yang merupakan gambaran *Chain of Trust* dari *Root* CA, *Subordinate* CA dan *End Entity Certificate*.

TABEL 5 SKEMA CHAIN OF TRUST SERTIFIKAT

No	Common Name (CN)	Type	Issued By	Issued to

1	RENCONG-ROOT-CA	Root CA	RENCONG-ROOT-CA	RENCONG-ROOT-CA
2	RENCONG-SUB-CA	Sub CA	RENCONG-ROOT-CA	RENCONG-SUB-CA
3	GARUDA-HQ-VPN	End Entity	RENCONG-SUB-CA	GARUDA-HQ-VPN
4	GARUDA-BRANCH-VPN	End Entity	RENCONG-SUB-CA	GARUDA-BRANCH-VPN

Pembatasan hak akses yang ketat untuk pengguna diperlukan agar tidak ada pengguna lain yang bisa mengakses *private key* pada setiap *server*. Informasi mengenai direktori beserta hak aksesnya dapat dilihat pada Tabel 6.



Gambar 3. Hierarki *Certificate Authority.*

TABEL 6 PENYIMPANAN DAN HAK AKSES DIREKTORI PKI DAN END-ENTITY

No	Server	Type	Direktori	Hak Akses
1	MAIN-SRV-INT	Root CA	/CA-ROOT/PKI/	User(full), Group(no_access), Other(no_access).
2	SEC-SRV-INT	Sub CA	/CA-SUB/PKI/	User(full), Group(no_access), Other(no_access).
3	HQ-GARUDA-GW	End Entity	/etc/openvpn/	User(full), Group(no_access), Other(no_access).

4	BRANCH-GARUDA-GW	End Entity	/etc/openvpn/	User(full), Group(no_access), Other(no_access).

D. Pengujian Keamanan Jaringan VPN Site-to-Site

Pengujian keamanan jaringan VPN *Site-to-Site* ini dilakukan dengan menggunakan iPerf. Pengujian ini bertujuan untuk memastikan bahwa jaringan VPN *Site-to-Site* yang diimplementasikan dapat beroperasi dengan baik dan sesuai dengan yang diharapkan.

Dari hasil pengujian pada Tabel 7, terlihat bahwa rata-rata transfer data selama 10 interval pengujian adalah 646,7 KByte dengan kecepatan rata-rata 473 Kbits/detik. Selama pengujian, rata-rata retransmisi (retry) adalah 10,7 kali. Pada interval kedua, terjadi 22 kali *retry*, sedangkan pada interval kelima dan keenam, terdapat nilai *retry* yang signifikan masing-masing sebanyak 20 dan 19 kali. Interval kedelapan mencatat retransmisi sebanyak 46 kali. Hasil pengujian menunjukkan bahwa interval kedua, kelima, dan keenam mengalami masalah atau gangguan pada jaringan yang menyebabkan retransmisi tinggi. Interval kedelapan mencatat nilai *retry* tertinggi, sehingga menjadi fokus utama perbaikan dalam pengujian selanjutnya.

TABEL 7 HASIL PENGUJIAN IPERF MENGGUNAKAN PROTOKOL UDP

No.	Interval	*Transfer*	*Bandwidth*	*Retry*
1	ke-1	662 KByte	527 Kbits/sec	0
2	ke-2	629 KByte	481 Kbits/sec	22
3	ke-3	633 KByte	461 Kbits/sec	0
4	ke-4	711 KByte	491 Kbits/sec	0
5	ke-5	511 KByte	363 Kbits/sec	20
6	ke-6	617 KByte	440 Kbits/sec	19
7	ke-7	569 KByte	456 Kbits/sec	0
8	ke-8	728 KByte	560 Kbits/sec	46
9	ke-9	475 KByte	370 Kbits/sec	0
10	ke-10	802 KByte	577 Kbits/sec	0
Rata-rata		646,7 KByte	473 Kbits/sec	10,7

Tabel 8 menampilkan hasil pengujian transfer data menggunakan aplikasi iPerf dengan protokol TCP. Setiap baris dalam tabel merepresentasikan interval pengujian yang dilakukan, sedangkan kolom-kolom di sebelah kanan menyajikan nilai transfer data dalam satuan byte dan kecepatan transfer data dalam satuan bit per detik (bps). Kolom terakhir menunjukkan jumlah percobaan ulang (*retry*) yang terjadi selama interval pengujian.

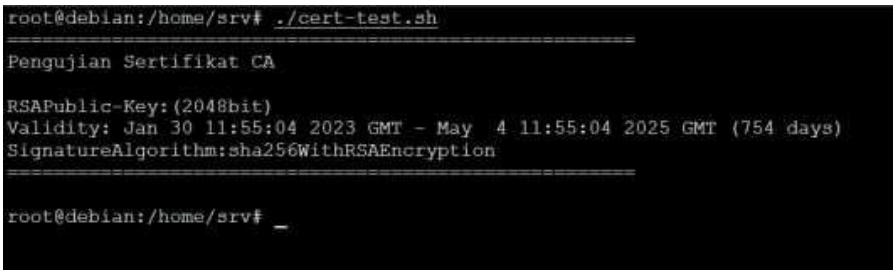
Dari hasil pengujian terlihat bahwa kecepatan transfer data (*bandwidth*) bervariasi antara interval, dengan kecepatan terendah sekitar 470 Kbit/detik dan kecepatan tertinggi mencapai sekitar 1,53 Mbit/detik. Rata-rata kecepatan transfer data selama seluruh pengujian adalah sekitar 772,4 Kbit/detik. Selain itu, jumlah percobaan ulang (*retry*) selalu kurang dari 3, yang mengindikasikan koneksi yang stabil dan minim gangguan.

TABEL 8 HASIL PENGUJIAN IPERF MENGGUNAKAN PROTOKOL TCP

No.	Interval	*Transfer*	*Bandwidth*	*Retry*
1	ke-1	1,30 MBytes	884 Kbits/sec	0

2	ke-2	1,26 MBytes	1,04 Mbits/sec	0
3	ke-3	1,12 MBytes	749 Kbits/sec	0
4	ke-4	629 KBytes	470 Kbits/sec	2
5	ke-5	794 KBytes	531 Kbits/sec	0
6	ke-6	871 KBytes	664 Kbits/sec	0
7	ke-7	820 KBytes	566 Kbits/sec	0
8	ke-8	748 KBytes	555 Kbits/sec	0
9	ke-9	938 KBytes	735 Kbits/sec	0
10	ke-10	1005 KBytes	1,53 Mbits/sec	0
Rata-Rata		1006,35 KBytes	772,4 Kbits/sec	0,2

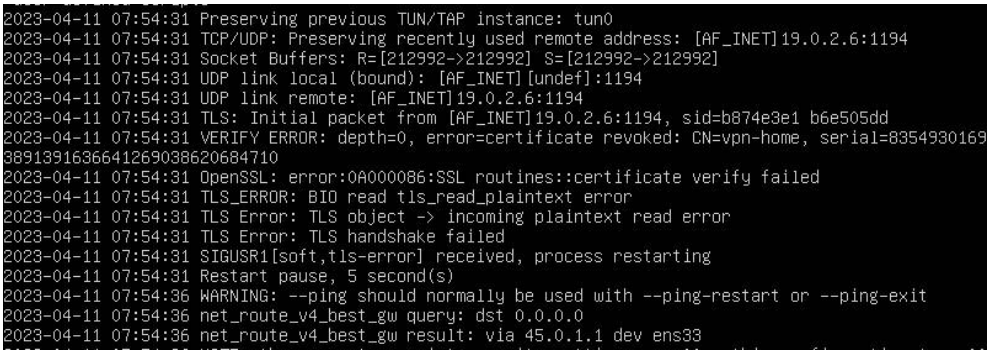
Hasil pengujian pada sertifikat publik Sub-CA menunjukkan bahwa sertifikat tersebut dibuat dengan parameter keamanan yang kuat. Sertifikat memiliki panjang kunci RSA sebesar 2048 bit, yang dianggap aman dan tahan terhadap serangan pemecahan kunci pada saat ini. Selain itu, algoritma hashing SHA-256 digunakan, yang merupakan algoritma *hashing* yang kuat dan umum direkomendasikan untuk digunakan dalam penerapan keamanan saat ini.



Gambar 4. Pengujian Sertifikat Publik Sub-CA.

Gambar 5 menunjukkan pengujian terhadap pencabutan sertifikat *server* VPN perusahaan. Pengujian pencabutan sertifikat salah satu *server* VPN perusahaan menggunakan *Certificate Revocation List* (CRL) menunjukkan bahwa infrastruktur ini mampu menangani situasi di mana sertifikat harus dicabut karena alasan keamanan. Hasil pengujian ini menunjukkan bahwa ketika sertifikat menjadi tidak valid, koneksi VPN antara kantor pusat dan cabang tidak dapat terjalin.

Setelah sertifikat VPN Branch dicabut, muncul pesan VERIFY ERROR dan Transport Layer Security (TLS) ERROR seperti yang terlihat pada Gambar 5. Ini menunjukkan bahwa mekanisme pencabutan sertifikat dan penggunaan CRL berfungsi dengan baik untuk menjaga integritas dan keamanan koneksi VPN. Dengan sistem pencabutan sertifikat yang efektif, perusahaan dapat memastikan bahwa sertifikat yang dicabut tidak lagi dapat digunakan untuk mengakses sumber daya dalam jaringan, sehingga dapat mengurangi risiko kebocoran data dan akses yang tidak sah.



Gambar 5. Pengujian *Revoke Branch Certificate.*

E. Pengujian Performa OpenVPN *Site-to-Site* Berdasarkan Jenis Kriptografi

Pengujian performa OpenVPN *Site-to-Site* ini bertujuan untuk membandingkan 2 jenis kriptografi yang digunakan yaitu: menggunakan kunci simetris yang merupakan konfigurasi *default* dan menggunakan kunci asimetris. Pengujian dilakukan dengan mengukur nilai *bandwidth* dan *jitter* menggunakan iPerf untuk kedua konfigurasi VPN tersebut.

TABEL 9 PENGUJIAN PERFORMA PADA VPN DENGAN KRIPTOGRAFI SIMETRIS

No	*Bandwidth*	*Jitter*
1	920 Kbits/sec	10.003 ms
2	904 Kbits/sec	15.787 ms
3	918 Kbits/sec	10.006 ms
4	919 Kbits/sec	10.687 ms
5	918 Kbits/sec	11.895 ms
6	920 Kbits/sec	11.303 ms
Total	**918.1 Kbits/sec**	**11.1143 ms**

TABEL 10 PENGUJIAN PERFORMA PADA VPN DENGAN KRIPTOGRAFI ASIMETRIS

No	*Bandwidth*	*Jitter*
1	944 Kbits/sec	16.123 ms
2	937 Kbits/sec	12.915 ms
3	941 Kbits/sec	13.838 ms
4	933 Kbits/sec	16.696 ms
5	936 Kbits/sec	14.838 ms
6	934 Kbits/sec	13.915 ms
Total	**937.5 Kbits/sec**	**14.721 ms**

Berdasarkan hasil pengujian pada Tabel 9 dan Tabel 10, penggunaan kunci asimetris pada konfigurasi OpenVPN *Site-to-Site* menunjukkan peningkatan rata-rata *bandwidth* menjadi 937.5 Kbits/sec, dibandingkan dengan 918.16 Kbits/sec pada kunci simetris (Tabel 10). Namun, terjadi peningkatan nilai *jitter* dari 11.114 ms menjadi 14.721 ms, yang menunjukkan adanya penurunan stabilitas dalam pengiriman data. Peningkatan *throughput* sebesar 19.34 Kbits/sec mencerminkan efisiensi transfer data yang lebih baik, meskipun penurunan *jitter* sebesar 3.607 ms menandakan adanya tambahan *delay* yang bisa mempengaruhi kualitas pengalaman pengguna.

Meskipun demikian, penggunaan kunci asimetris memiliki keunggulan signifikan dari sisi keamanan karena algoritma *public key* yang lebih kompleks dan tahan terhadap

serangan. Oleh karena itu, pemilihan konfigurasi OpenVPN *Site-to-Site* harus memperhatikan kebutuhan keseimbangan antara performa jaringan dan tingkat keamanan data yang diinginkan, sesuai dengan prioritas dan kondisi operasional yang ada.

F. Hasil Evaluasi Keamanan Jaringan VPN Site-to-Site

Hasil evaluasi keamanan jaringan OpenVPN menunjukkan bahwa infrastruktur telah menerapkan prinsip-prinsip keamanan yang kuat. Penggunaan versi terbaru OpenSSL (3.1) memberikan perlindungan optimal dengan fitur keamanan terbaru. Selain itu, implementasi protokol TLS minimal versi 1.2 atau lebih tinggi mengurangi potensi serangan yang dapat terjadi pada versi TLS yang lebih lama. Penggunaan *cipher suites* yang aman seperti TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384 dan TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256 memperkuat enkripsi, memberikan keamanan yang lebih baik dalam koneksi VPN.

Autentikasi dan pengelolaan sertifikat digital dilakukan dengan baik melalui penggunaan Sub-CA dan sinkronisasi CRL, memastikan sertifikat yang digunakan valid dan terverifikasi. Sertifikat digital sangat penting untuk menjaga keamanan komunikasi antara *server* dan *client* pada jaringan VPN. Penggunaan hierarki CA dalam sistem ini memberikan fleksibilitas dalam pengelolaan sertifikat, terutama pada perusahaan dengan banyak cabang, sambil tetap menjaga integritas jaringan.

Namun, kerentanan pada hierarki CA perlu diwaspadai, termasuk risiko pada *Root* CA, serangan *man-in-the-middle*, serta potensi penyalahgunaan hak akses. Untuk itu, pengamanan *Root* CA dan penerapan protokol keamanan yang kuat sangat penting untuk mengurangi risiko ini. Model kepercayaan yang digunakan dalam hierarki CA juga bergantung pada perlindungan akses dan edukasi pengguna untuk menjaga keamanan secara menyeluruh.

4. Kesimpulan

Berdasarkan hasil penelitian, penerapan sistem *Certificate Authority* (CA) dan *Public Key Infrastructure* (PKI) berhasil meningkatkan keamanan, privasi data, serta autentikasi pengguna pada jaringan antara kantor cabang dan pusat. Dengan implementasi hierarki CA, keamanan jaringan diperkuat melalui autentikasi yang lebih kuat dan enkripsi data yang lebih baik.

Teknologi OpenVPN *Site-to-Site* yang terintegrasi dengan sertifikat digital dari sistem CA dan PKI juga berhasil meningkatkan keamanan jaringan antara kantor cabang dan pusat. Koneksi yang aman dan terenkripsi dapat terwujud berkat penggunaan sertifikat digital yang dikeluarkan oleh sistem CA, memastikan perlindungan data dalam komunikasi antar entitas.

Selain itu, penelitian ini juga menunjukkan bahwa penerapan sistem CA dan PKI efektif dalam mengurangi risiko keamanan dan meningkatkan kepercayaan antar entitas yang berkomunikasi dalam jaringan. Manfaat ini memperkuat keandalan jaringan dan mencegah potensi serangan keamanan yang bisa terjadi.

Pengujian performa dan kehandalan jaringan setelah penerapan sistem CA, PKI, dan OpenVPN *Site-to-Site* menunjukkan hasil yang memadai, dengan peningkatan keamanan yang signifikan tanpa mengorbankan performa. Lebih lanjut, penggunaan kunci asimetris pada konfigurasi OpenVPN *Site-to-Site* menunjukkan peningkatan rata-rata *bandwidth* jaringan dan adanya sedikit penurunan stabilitas dalam pengiriman data. Penelitian ini berhasil mencapai tujuannya, memberikan kontribusi nyata dalam meningkatkan keamanan dan kepercayaan dalam komunikasi jaringan perusahaan cabang dan pusat.

References

[1] P. Danquah, & H, Kwabena-Adade, "Public Key Infrastructure: An Enhanced Validation Framework", *Journal of Information Security*, Vol. 11, No. 4, pp. 241-260, Oct. 2020.

[2] M. Feilner, "OpenVPN: Building and Integrating Virtual Private Networks: Learn how to build secure VPNs using this powerful OpenVPN tool", Packt Publishing Ltd, 2017.

[3] Fyodor, "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning", Nmap Project, 2020.

[4] M. N. Ishag, & N. E. Hamid, "Site to Site Open VPN", *International Research Journal of Engineering and Technology*, Vol. 07, No. 03, pp. 4291-4298, March 2020.

[5] R. Sherwood, "Practical Implications of Public Key Infrastructure for Identity Professionals", *IDPro Body of Knowledge*, Vol. 1, No. 6, Sept. 2021.

[6] M. Syafrizal, "Pengantar Jaringan Komputer", Andi, Yogyakarta, 2020.

[7] S. Usanto, "Rancang Bangun Jaringan Site To Site VPN (Virtual Private Network) Dengan Protokol OpenVPN", *Jurnal Elektro dan Informatika Swadharma*, Vol. 01, No. 02, pp. 55-65, July 2021.

[8] E. Varianto, & M. Badrul, "Implementasi Virtual Private Network Dan Proxy Server Menggunakan Clear Os Pada PT. Valdo International", *Jurnal Teknik Komputer AMIK BSI*, Vol. 1, No. 1, pp. 54-65, Feb. 2015.

[9] T. P. Wulandari, N. R. Reza, E. Z. Deswana, M. R. Adillah, & D. Aribowo, "Penerapan VPN Dalam Topologi Star Untuk Keamanan Pengiriman Data", *Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi*, Vol. 2, No. 2, pp. 63-70, May 2024.

[10] S. M. Yacub, R. Ramadi, & D. Ernawati, "Public Key Infrastructure : Kerangka Validasi yang Disempurnakan", *TRIPLE A : Jurnal Pendidikan Teknologi Informasi*, Vol. 1, No. 2, pp. 77-80, Dec. 2022.

[11] G. Yugianto, & O. Rachman, "Router: Teknologi, Konsep, Konfigurasi, dan Troubleshooting Berbasis Windows, Cisco, MacOS, Linux & Mikrotik Router", Informatika, Bandung, 2012.