JIMU: Jurnal Ilmiah Multi Disiplin
Vol. 02, N0. 04, Tahun 2024, Hal. 1095 - 1105, ISSN: 3031-9498 (Online)

Implementasi *Firewall* untuk Mencegah Ancaman Keamanan pada Akses *Remote Dekstop Protocol* di Sistem Operasi *Windows*

Nur Syafitri[1], Mustari S. Lamada[2], Iwan Suhardi[3]
[1,2,3] Universitas Negeri Makassar
Email: *nursyafitri998@gmail.com*

Article Info

Article history:

Received August 5, 2024
Revised August 9, 2024
Accepted August 14, 2024

Keywords:

LAN, Mesh, MPLS,

ABSTRACT

Chrome Remote Desktop (CRD) is a protocol used to access computers remotely via the Google Chrome web browser. Despite its high flexibility, CRD also poses significant security risks. This research was conducted by implementing a Firewall on Windows to monitor the network and identify data security threats. Testing was carried out using the Windows Defender Firewall method and without using this method on the Windows operating system. The main focus of the testing was network security and blocking unauthorized connections on CRD. The test results showed that using the Windows Defender Firewall method on CRD can enhance system security and monitor incoming and outgoing data traffic from the device. In contrast, testing without the Windows Defender Firewall method can lead to security threats such as unauthorized access. Implementing a Firewall can help reduce attacks and restrict access only to trusted IP addresses and limit open ports to those used by CRD.

Article Info

Article history:

Received August 5, 2024
Revised August 9, 2024
Accepted August 14, 2024

Keywords:

Firewall ,CRD, Windows

ABSTRACT

Chrome Remote Desktop (CRD) adalah protocol yang digunakan untuk mengakses komputer dari jarak jauh melalui peramban web Google Chrome. Meskipun memiliki fleksibilitas yang tinggi, CRD juga membawa resiko keamanan yang signifikan. Penelitian ini dilakukan dengan mengimplementasikan Firewall pada Windows untuk memonitor jaringan dan mengetahui ancaman keamanan data. Pengujian dilakukan dengan menggunakan metode Windows Defender Firewall dan tanpa menggunakan metode tersebut di sistem operasi windows. Fokus utama pengujian adalah sistem keamanan jaringan dan pemblokiran koneksi tidak sah pada CRD. Hasil pengujian menunjukkan bahwa penggunaan metode Windows Defender Firewall pada CRD dapat meningkatkan keamanan sistem dan memonitor lalu lintas data yang masuk dan keluar dari perangkat. Sedangkan pengujian tanpa metode Windows Defender Firewall dapat menimbulkan ancaman keamanan seperti akses yang tidak sah.

Pengimplementasian Firewall dapat membantu mengurangi serangan dan membatasi akses hanya dari Alamat IP yang terpercaya serta membatasi port yang terbuka ke port yang digunakan CRD.

Corresponding Author:

Nama penulis: Yulfiana
Universitas Negeri Makassar
Email: yulfianafiana5@gmail.com

Pendahuluan

Dalam perkembangan teknologi informasi yang pesat, kebutuhan akan akses jarak jauh atau remote access menjadi semakin penting. Akses Remote Desktop Protocol (RDP) pada sistem operasi Windows merupakan salah satu solusi yang umum digunakan pengguna untuk terhubung dan mengelola sistem dari lokasi yang jauh. Meskipun memberikan fleksibilitas yang tinggi, penggunaan RDP juga membawa risiko keamanan yang signifikan.[1] [2]

Ancaman keamanan terhadap akses RDP telah meningkat secara signifikan dalam beberapa tahun terakhir. Penjahat dunia maya seringkali mencoba memanfaatkan kelemahan keamanan dalam implementasi RDP untuk mendapatkan akses tidak sah ke sistem, yang dapat mengakibatkan kerugian data, pencurian informasi sensitif, atau bahkan merusak integritas sistem secara keseluruhan. Ancaman Remote Desktop Protocol adalah upaya untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Oleh karena itu, adanya implementasi firewall untuk mencegah ancaman keamanan pada akses Remote Desktop Protocol di sistem operasi windows menjadi sangat penting.[2][4]

Serangan Remote Desktop Protocol adalah salah satu teknik serangan yang paling sederhana dan paling umum dalam dunia keamanan. Hal ini memerlukan waktu dan sumber daya yang cukup besar, terutama jika data akses yang benar memiliki kompleksitas yang tinggi. Namun, dengan perkembangan teknologi, serangan ini menjadi semakin efektif, terutama jika data pengguna terlalu lemah atau mudah ditebak.[5]

Salah satu langkah paling efektif dalam melindungi Windows dari serangan Remote Desktop Protocol adalah adanya implementasi firewall. Ini adalah Teknik untuk memonitor jaringan internet dan mengetahui apabila akses yang mengancam keamanan data serta privasi muncul seketika. Adanya implementasi firewall yang berfungsi mencegah ancaman Remote Desktop Protocol sehingga dapat memainkan peran penting dalam keamanan informasi modern. Ini membantu melindungi sistem dari serangan Remote Desktop Protocol dengan membatasi perlindungan sumber daya yang datang. Namun, adanya kustomisasi firewall ini harus dilakukan dengan hati-hati untuk memperkirakan kemungkinan penjebolan keamanan atau memberikan umpan balik. [3]

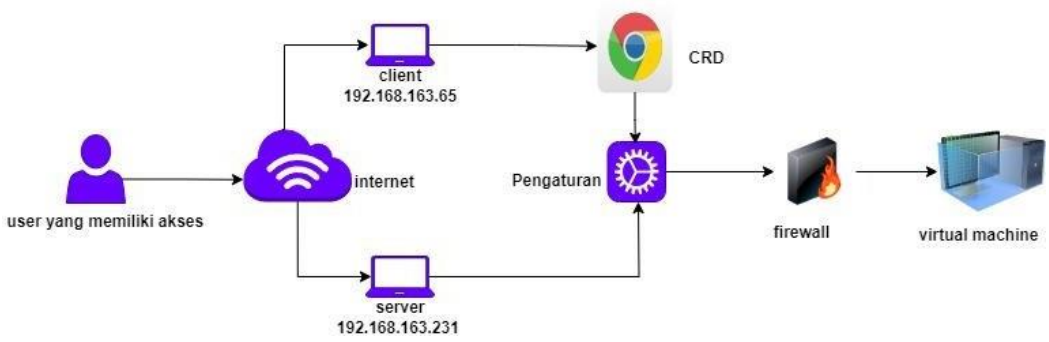
Untuk mengimplementasikan firewall deteksi serangan remote desktop protocol, ada beberapa teknologi dan metode yang dapat digunakan. Berikut adalah beberapa di antaranya: adalah Penggunaan firewall yang dapat membantu dalam mendeteksi dan memblokir serangan Remote Desktop Protocol dengan mengawasi lalu lintas masuk. Serta membatasi akses kejaringan dan sistem berdasarkan kriteria tertentu. Ini dapat digunakan untuk mendeteksi serangan Remote Desktop Protocol termasuk pada metode chrome remot dekstop. Selain itu membatasi jenis data yang diperbolehkan masuk dan keluar dari jaringan, seperti email atau file yang terkait dengan bisnis organisasi serangan remote desktop protocol. Oleh karena itu dapat digunakan untuk melindungi data akses yang disimpan dan dipertukarkan dalam sistem. Ini membuat lebih sulit bagi penyerang untuk mendapatkan data akses.[1] [4]

Berdasarkan paparan di atas, maka peneliti tertarik untuk melakukan penelitian dengan topik “Implementasi Firewall untuk Mencegah Ancaman Keamanan pada Akses Remote Desktop Protocol di Sistem Operasi Windows".

Metode

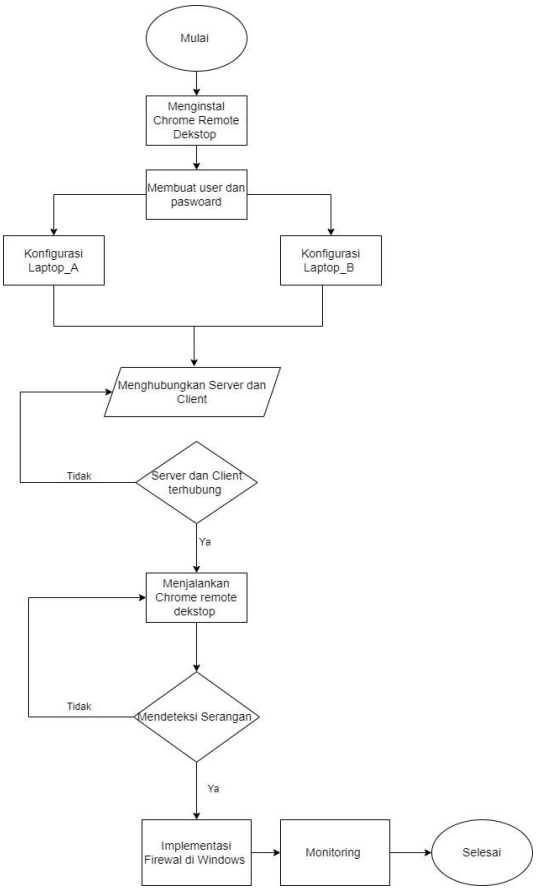
Jenis penelitian yang digunakan adalah eksperimen dengan memanfaatkan Firewall dalam mengamankan Remote Desktop Protocol yaitu extensions chrome sebagai keamanan tambahan bagi pengguna Windows.

Penelitian ini dilakukan di Universitas Negeri Makassar Parang Tambung, yang beralamat di Jalan Malengkeri Raya, Parang Tambung, Kec. Tamalate, Kota Makassar, Sulawesi Selatan. Penelitian ini direncanakan selama 2 bulan yaitu bulan Januari-Maret tahun 2024.



Gambar 1. Desain Sistem

Gambar diatas menunjukkan desain dan perancangan sistem yang terdiri dari beberapa komponen utama yaitu Client/User merupakan perangkat yang digunakan untuk menggunakan CRD untuk mengakses Server. Client akan menggunakan IP address 192.168.163.65. Kemudian Firewall yang berfungsi sebagai pelindung sistem dengan memblokir akses yang tidak sah dan melindungi Server. CRD digunakan untuk mengakses Server dari jarak jauh. Server merupakan pusat dari sistem yang akan di uji coba untuk melakukan monitoring dari Client dengan menggunakan IP Address Server yaitu 192.168.163.231. Pengguna yang memiliki akses internet dapat membuka apapun terkhusus browser google chrome untuk melakukan monitoring sistem. Melalui antarmuka browser ini, clinet dapat mengakses layanan yang telah di implementasikan pada server. Proses ini dilakukan dengan menggunakan firewall sebagai keamanan tambahan Ketika menggunakan CRD.



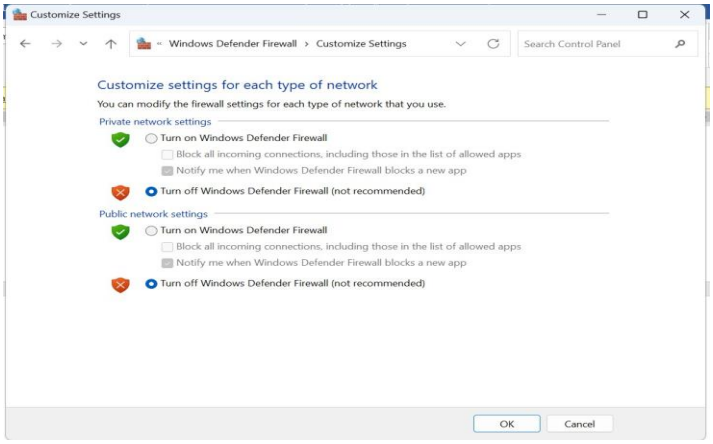
Gambar 2. *Flowchart* Perancangan Sistem

Pada Gambar 3.2 merupakan flowchart pada penelitian ini yaitu untuk menggunakan Chrome Remote Desktop, perlu mengatur akses di kedua komputer yang akan terhubung. Laptop A sebagai host dan Laptop B sebagai Client. Di Laptop A, buka browser Chrome dan pasang ekstensi Chrome Remote Desktop. Laptop A digunakan untuk mengunduh dan menginstal Chrome Remote Desktop. Untuk Laptop B dilakukan juga pengunduhan dan penginstalan Chrome Remote Desktop seperti settingan pada Laptop A. Selanjutnya menetapkan PIN keamanan pada kedua Laptop untuk memberikan akses secara remote atau jarak jauh. Menjalankan Chrome Remote Desktop di Laptop B (Client) dengan melakukan praktikum Debian di virtualbox. Dimana, praktikum yang dilakukan akan muncul di Laptop A. Kemudian mendeteksi serangan di Laptop A (Server) menggunakan zanmap dan winbox. Jika terdapat serangan, maka dilakukan implementasi firewall yang ada pada windows untuk mengatasi serangan yang mencoba masuk pada Laptop A (Server).

Hasil

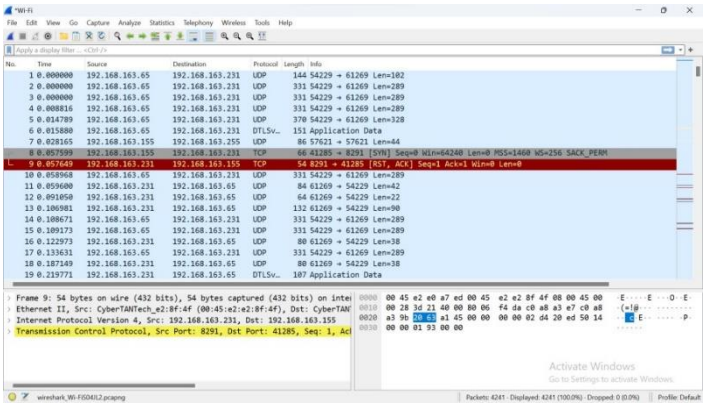
1. Pengujian Non Windows Defender Firewall

a. Pengujian tanpa menggunakan layanan keamanan windows defender firewall yang di non aktifkan



Gambar 1. Windows Defender Firewall

b. Mendeteksi serangan menggunakan alat penganalisis paket jaringan yang digunakan secara khusus dengan mencatat beberapa serangan yang mencurigakan.



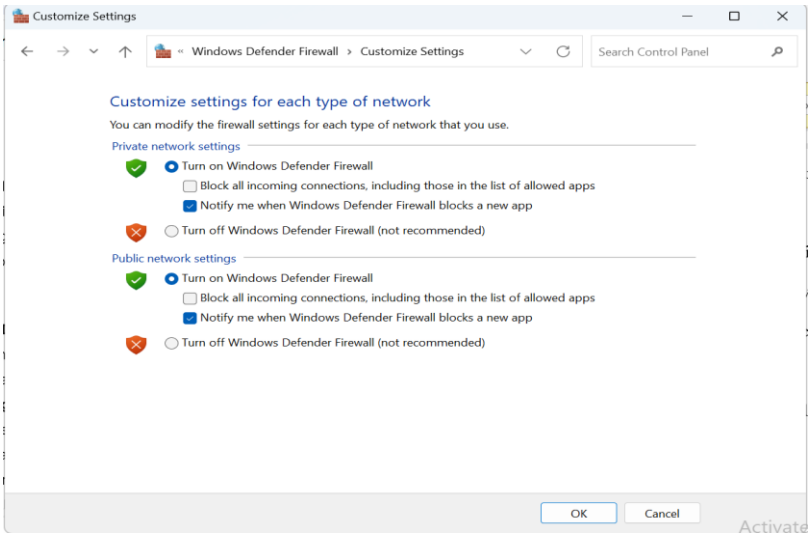
Gambar 2. Hasil Ujian Coba Wireshark Non Firewall

c. Melakukan praktikum secara jarak jauh pada virtual mesin debian di kedua laptop. Dimana latpto_a bisa di kendalikan di laptop_b begitupun sebaliknya.

Gambar 3. Praktikum Debian 1

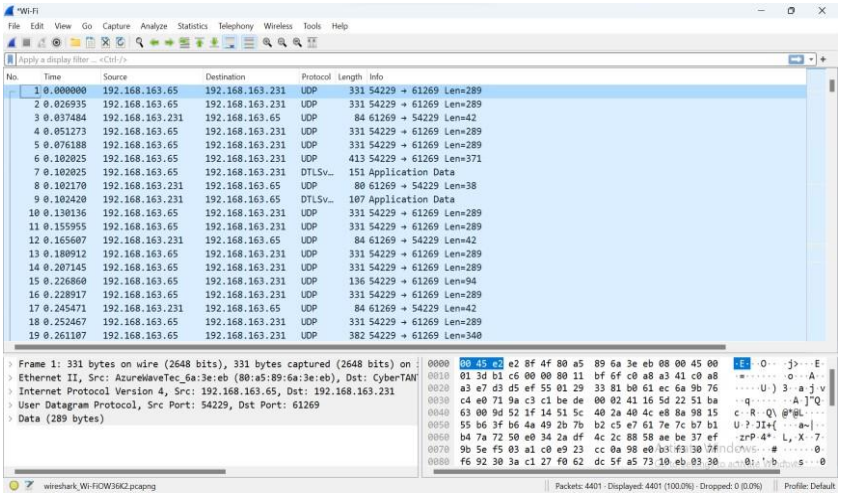
2. *Pengujian Menggunakan Windows Defender Firewall*

a. Pengujian menggunakan windows defender firewall yang diaktifkan untuk mengamankan sistem operasi windows pada sistem remote desktop serta melindungi computer dari ancaman jaringan dengan mengontrol lalu lintas data yang masuk dan keluar dari perangkat. Selain itu firewall dapat menjadi penghalang lalu lintas yang tidak di izinkan.



Gambar Windows Defender Firewall

b. Mendeteksi serangan menggunakan alat penganalisis paket jaringan yang digunakan secara khusus dengan mencatat beberapa serangan yang mencurigakan. ketika menggunakan windows firewall defender yang di aktifkan.



Gambar Hasil Uji Coba Wireshark Firewall

Tabel Hasil Pengujian Koneksi Firewall Aktif dan Tidak Aktif

No.	Skenario Pengujian	Konfigurasi Firewall	Hasil Pengujian	Ket.
1.	Koneksi dengan firewall dinonaktifkan	Windows Defender Firewall dimatiakan	Berhasil	Stabil
2.	Koneksi dengan firewall aktif	Pengaturan default firewall	Berhasil	Stabil
3.	Koneksi dengan Praktikum di Virtual Machine	Chrome Remote Desktop diizinkan dalam firewall	Berhasil	Stabil

Pada pengimplementasian Firewall dengan menggunakan Chrome Remote Desktop yang telah diuji adalah dengan berfokus pada performa yang didapatkan serta keamanan yang sistem. Windows Defender Firewall dapat dikonfigurasi untuk mengizinkan atau memblokir akses yang tidak sah ketika menggunakan Chrome Remote Desktop dengan beberapa pengujian yang dilakukan di virtual machine. Dalam pengujian ini, berbagai skenario diuji untuk mengevaluasi waktu respons koneksi, penggunaan sumber daya sistem, serta kemampuan firewall dalam mendeteksi dan menghentikan ancaman. Hasil pengujian menunjukkan bahwa dengan konfigurasi yang tepat, Windows Defender Firewall dapat menjaga keseimbangan antara performa yang optimal dan keamanan yang kuat, memastikan bahwa hanya lalu lintas yang sah yang diizinkan dan data tetap terlindungi dari potensi ancaman

3. Pengujian Performa

Pengujian performa berfokus pada kinerja sistem menggunakan metode windows defender firewall dan tanpa menggunakan metode windows defender firewall.

No	Tanpa Windows Defender *Firewall*	CPU	Memori footprint	ID
1.	Chrome *Remote* Dekstop	12,5%	73%	8508
2.	Tanpa Chrome *Remote* Dekstop	72%%	80%%	142
3.	Chrome *Remote* Dekstop	41%	55%	2428
4.	Tanpa Chrome *Remote* Dekstop	31%	13%	139

Pada pengujian tanpa Windows Defender Firewall dengan menggunakan Chrome Remote Desktop:

a. Penggunaan CPU mencapai 12,5% saat Chrome Remote Desktop aktif tanpa penggunaan windows defender firewall. Beban CPU yang diperlukan cukup rendah ketika melakukan praktikum di sistem ini. Persentase CPU dalam pengujian ini tidak terlalu membutuhkan ruang yang banyak sehingga masih dapat digunakan oleh aplikasi lain.
b. Penggunaan memori footprint mencapai 73% saat Chrome Remote Desktop aktif. Ini menunjukkan bahwa Chrome Remote Desktop pada pengujian ini membutuhkan memori yang tinggi. Pengujian ini melibatkan praktikum di virtual machine dengan koneksi remote yang tidak stabil termasuk proses untuk pengelolaan konkesi, enkripsi dan autentikasi.
c. Penggunaan CPU mencapai 41% saat Chrome Remote Desktop aktif. Saat menggunakan Windows Defender Firewall yang aktif, beban CPU yang diperlukan cukup tinggi Ketika melakukan praktikum di sistem ini karena Firewall berfungsi untuk memantau dan mengelola lalu lintas jaringan. Ini dapat disebabkan oleh beberapa faktor, antara lain:
    1) Proses Enkripsi dan Dekripsi: Chrome Remote Desktop menggunakan enkripsi untuk mengamankan koneksi jarak jauh, yang memerlukan pemrosesan tambahan.
    2) Komunikasi Jaringan: Aktivitas komunikasi data antara komputer lokal dan remote melalui jaringan juga dapat membebani CPU.
    3) Rendering dan Streaming: Proses rendering dan streaming layar dari komputer remote ke komputer lokal memerlukan sumber daya CPU yang signifikan untuk memastikan performa yang halus dan responsif.

Pada pengujian tanpa Windows Defender Firewall tanpa menggunakan Chrome Remote Desktop:

- Penggunaan CPU mencapai 72% tanpa menggunakan Chrome Remote Desktop. Persentase dari CPU yang digunakan tinggi ketika melakukan praktikum di sistem ini yang menunjukan bahwa beban kerja lebih tinggi menandakan bahwa sistem ini membebani CPU. Ini menyebabkan sistem menjadi lambat dan tidak responsive.
- Penggunaan memori footprint mencapai 80% saat Chrome Remote Desktop aktif. Ini menunjukkan bahwa memori footprint yang digunakan tinggi ketika melakukan praktikum yang menandakan bahwa memori hamper penuh dengan aplikasi lain. Performa dari penggunaan memori menjadi buruk dan tidak stabil.
- penggunaan CPU mencapai 31% tanpa menggunakan Chrome Remote Desktop dengen windows defender firewall. Ini termasuk proses sistem, aplikasi keamanan dan layanan latar belakang. Persentase dari CPU yang digunakan cukup rendah Ketika melakukan praktikum di sistem ini yang menunjukan bahwa beban kerja lebih ringan menandakan bahwa sistem ini lebih responsive dan stabil. Beberpa pengaruh penggunaan CPU pada sistem ini:
    1. Firewall dapat memeriksa paket data yang masuk dan keluar termasuk menerapkan aturan firewall dan melakukan inspeksi paket.
    2. Evisiensi yang lebih rendah menunjukan bahwa konsumsi daya yang digunakan lebih rendah sehingga dapat memperpanjang masa pakai baterai.

4. Pengujian Keamanan

Pengujian keamanan Chrome Remote Desktop dengan metode Windows Defender Firewall melibatkan beberapa skenario dan parameter yang bertujuan untuk memastikan keamanan dan kinerja optimal dari aplikasi remote desktop ini. Pengujian ini dilakukan dengan menggunakan firewall bawaan dari windows.

No.	Skenario Pengujian	Deskripsi Pengujian	Hasil pengujian menggunakan firewall	Hasil pengujian (Tanpa firewall)
1.	Deteksi serangan	Melakukan serangkaian serangan yang bertujuan untuk enguji kemampuan windows defender firewall dalam mendeteksi anacaman.	Hasil pengujian menunjukkan bahwa firewall berhasil mendeteksi dan menecegah anacaman yang mencoba menembus sistem	Sistem tidak memiliki mekanisme tambahan untuk mendeteksi serangan. Serangan seperti scanning mungkin tidak terdeteksi, meningkatkan risiko.
2.	Respon terhadap serangan	Melakukan serangan spesifik dan memeriksa respons sistem terharap serangan saat windows defender aktif dan non aktif	Memberikan respon yang tepat terhadap serngan dan melindungi sistem dari eksplotasi	Sistem lebih rentan terhadap eksploitasi karena tidak ada perlindungan tambahan dari firewall. Serangan dapat menyebabkan kerusakan serius.
3.	Penggunaan Email	Menggunakan email yang sama pada *server* dan *clinet* untuk memastikan hanya pengguna yang sah dan terdaftar yang dapat mengakses remote dekstop untuk mengurangi resiko yang tidak sah .	Pengujian memastikan bahwa otentikasi berbasis email pada server dan client Chrome Remote Desktop berfungsi tanpa kendala, efektif mengontrol akses sistem.	Sistem tetap mengontrol akses melalui email, tetapi lebih rentan terhadap serangan jaringan yang bisa mengkompromikan keamanan.
4.	Penggunaan PIN	sebagai lapisan tambahan dalam otentikasi untuk Chrome Remote Desktop pada server dan client. PIN adalah kode rahasia yang digunakan untuk mengamankan akses	Ini memberikan tingkat keamanan tambahan dan mencegah akses tidak sah jika seseorang mengetahui email tetapi tidak PIN.	Sistem masih memerlukan PIN untuk akses, tetapi lebih rentan terhadap upaya brute force tanpa perlindungan firewall.

5.	Enkripsi koneksi	Memastikan koneksi Terenkripsi dan melindungi data sensitif yang di transfer antara server dan clinet sehingga menjamin kerahasiaan data selama proses remote dekstop	memastikan bahwa data tetap aman dan terlindungi dari serangan selama transmisi	Koneksi tetap terenkripsi, tetapi sistem lebih rentan terhadap serangan man-in-the-middle atau sniffing tanpa firewall yang memantau lalu lintas.
6.	Audit Log	Mencatat semua aktivitas IP yang tidak sah untuk pemantauan dan analisis lebih lanjut.	Firewall mendukung pencatatan aktivitas jaringan, membantu dalam pemantauan yang lebih rinci dan deteksi dini aktivitas mencurigakan.	Sistem mungkin tidak memiliki pencatatan aktivitas jaringan yang komprehensif, menyulitkan deteksi dan analisis aktivitas tidak sah.

Pembahasan

Berdasarkan pengujian keamanan Chrome Remote Desktop (CRD) dengan dan tanpa Windows Defender Firewall, menggunakan firewall terbukti lebih menguntungkan dari segi keamanan dan stabilitas sistem. Dengan Windows Defender Firewall aktif, sistem dapat mendeteksi dan mencegah berbagai serangan seperti pemindaian port dan serangan brute force dengan efektif. Firewall tidak hanya memblokir akses yang tidak sah tetapi juga mencatat aktivitas mencurigakan, memberikan perlindungan yang lebih kuat terhadap potensi ancaman jaringan. Selain itu, firewall membantu menjaga integritas data dengan memastikan bahwa hanya lalu lintas terenkripsi yang diizinkan, melindungi informasi sensitif selama transmisi. Di sisi lain, tanpa firewall, sistem lebih rentan terhadap serangan karena tidak ada lapisan perlindungan tambahan yang secara aktif memonitor dan memblokir aktivitas jaringan berbahaya. Ancaman seperti serangan brute force atau pencurian data dapat lebih mudah dieksploitasi, mengancam keamanan dan stabilitas operasi remote desktop secara keseluruhan. Dengan demikian, penggunaan Windows Defender Firewall bersama Chrome Remote Desktop direkomendasikan untuk memastikan tingkat keamanan yang optimal dan perlindungan yang efektif terhadap berbagai ancaman.

Kesimpulan

Berdasarkan hasil pengujian, implementasi firewall pada Remote Desktop Protocol (RDP) terbukti dapat meningkatkan keamanan sistem secara signifikan tanpa memberikan dampak yang berarti pada performa sistem. Firewall berfungsi bagi pengguna untuk menetapkan aturan keamanan spesifik, termasuk membatasi akses hanya dari alamat IP yang tepercaya dan membatasi port yang terbuka ke port yang digunakan oleh RDP. Dengan cara ini, firewall

membantu mengurangi permukaan serangan potensial dan mencegah serangan yang berfokus pada kelemahan protocol RDP.

1. Firewall dapat diimplementasikan untuk membatasi akses yang tidak sah pada Remote Desktop Protocol (RDP) termasuk mengizinkan hanya alamat IP tepercaya dan mengatur port yang digunakan untuk koneksi RDP.
2. Pengoptimalan keamanan pada akses Remote Desktop Protocol mengontrol lalu lintas dan melindungi dari potensi serangan, firewall membantu meningkatkan keamanan sistem Windows saat menggunakan RDP.
3. Melalui pengujian keamanan Chrome Remote Desktop (CRD) dengan dan tanpa Windows Defender Firewall, menggunakan firewall terbukti lebih menguntungkan dari segi keamanan dan stabilitas sistem.

Daftar Pustaka

[1] Putra, I. M. D. (2022). Analisis Ancaman Keamanan pada Akses *Remote Desktop Protocol* di Sistem Operasi Windows. Jurnal Teknik Informatika, 15(2), 101-111.

[2] Ashfaq, T. &. (2022). The Forensics Artifacts on *Remote Desktop Protocol* and Service. International Journal for Electronic Crime Investigation, 6(3), 15- 21.

[3] Aditya, R., & Ilahi, M. R. I. (2022). Kustomisasi Firewall untuk Mencegah Ancaman Keamanan pada Akses Remote Desktop Protocol di Sistem Operasi Virtual Private Server. Jurnal Teknik Elektro, 12(2), 101-111

[4] Tudosi, A. D. (2023). Design and Implementation of an Automated Dynamic Rule System for Distributed Firewalls. Advances in Electrical & Computer Engineering, 23(3)

[5] Ridatu Ocanitra, Muhamad Ryansyah (2019). Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen..

[6] Tudosi, A. D. (2022). Secure network architecture based on distributed firewalls. In 2022 International Conference on Development and Application Systems (DAS) (pp. 85-90). IEEE.