

Penerapan Sistem Keamanan (Firewall) pada Jaringan Smart Home

Algazali Raihan Batubara^{1*}, Ilham Faisal², Imran Lubis³

^{1*,2,3}Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan, Indonesia

^{1*}algazaliraihan28@gmail.com, ²ilhamoppa11@gmail.com, ³imran.loebis.medan@gmail.com

Abstrak– Saat ini perkembangan teknologi semakin maju dan berkembang, perkembangan teknologi yang sangat pesat seiring perkembangan zaman untuk memenuhi kebutuhan manusia. Salah satunya yaitu kebutuhan teknologi rumah yang aman dan nyaman. Penerapan teknologi pada rumah tersebut yaitu menggunakan konsep smart home dengan menggunakan keamanan jaringan firewall. Firewall pada jaringan smart home merupakan sebuah konsep dimana perangkat Internet of Things (IoT) aman dari peretasan orang yang tidak dikenal dan tidak dapat dikendalikan oleh perangkat smartphone lain. Simulasi menjadi bagian yang penting dalam penerapan konsep yang akan dilakukan, terutama untuk mengetahui penelitian dan kajian dilaksanakan menggunakan metode simulasi sebagai salah satu cara untuk memecahkan permasalahan. Cisco Packet Tracer 7.3 merupakan aplikasi yang dapat membantu dalam hal melakukan simulasi pada perangkat Internet of Things. Hasil yang diperoleh dari simulasi konsep keamanan firewall adalah dalam penggunaan perangkat IoT seperti pintu rumah, jendela, garasi, lampu, webcam dan pendingin ruangan terjamin keamanannya karena perangkat yang memiliki izin yang dapat terkoneksi.

Kata Kunci: Smart Home, Firewall, Internet of Things, Simulasi, Cisco Packet Tracer

Abstract– Currently, technological developments are increasingly advanced and developing, technological developments that are very rapid with the development of the times to meet human needs. One of them is the need for safe and comfortable home technology. The application of technology in the house is to use the concept of smart home by using firewall network security. Firewall on a smart home network is a concept where Internet of Things (IoT) devices are safe from hacking by unknown people and cannot be controlled by other smartphone devices. Simulation is an important part of the application of the concept that will be carried out, especially to find out that research and studies are carried out using the simulation method as a way to solve problems. Cisco Packet Tracer 7.3 is an application that can help in terms of simulating Internet of Things devices. The results obtained from the firewall security concept simulation are that in the use of IoT devices such as house doors, windows, garages, lights, webcams and air conditioners are guaranteed to be secure because the devices that have permissions that can be connected.

Keywords: Smart Home, Firewall, Internet of Things, Simulation, Cisco Packet Tracer

1. PENDAHULUAN

Saat ini perkembangan teknologi semakin maju dan berkembang, perkembangan teknologi yang sangat pesat seiring perkembangan zaman untuk memenuhi kebutuhan manusia. Salah satunya yaitu kebutuhan teknologi rumah yang aman dan nyaman. Penerapan teknologi pada rumah tersebut dapat ditemui pada konsep smart home. Smart Home merupakan sebuah konsep rumah yang menggunakan berbagai macam perangkat Internet of Things (IoT) yang terhubung dalam jaringan untuk digunakan di rumah. Perangkat smart home biasanya seperti pintu, kipas angin, garasi, jendela dan perangkat Internet of Things (IoT) lainnya, perangkat tersebut dikoneksikan memanfaatkan gateway rumah ke sebuah internet agar perangkat-perangkat tersebut bisa dikendalikan secara remote melalui smartphone [1]. Smart Home adalah konsep konsep smart living yang berkembang berdasarkan pemanfaatan peralatan digital dan interkoneksi dari berbagai perangkat pintar, yang dapat memberikan banyak keuntungan seperti kenyamanan, keamanan serta efisiensi penggunaan energi dalam kehidupan sehari-hari. Manfaat inilah yang memicu semakin berkembangnya penerapan konsep smart living dalam kehidupan modern sehari-hari [2]. Keamanan infrastruktur jaringan telah menjadi prioritas utama bagi organisasi mana pun. Di antara solusi keamanan multilayer yang tersedia untuk infrastruktur jaringan, lapisan firewall adalah salah satu pertahanan tertua dan utama untuk jaringan apa pun. Firewall adalah perangkat keras atau perangkat lunak yang melindungi komputer dan jaringan dari lalu lintas jaringan yang tidak diinginkan dan mencegah pengguna internet yang tidak berwenang mengakses jaringan pribadi [3]. Firewall memiliki kelebihan dapat mendeteksi adanya malware atau ancaman berbahaya dari sebuah situs yang dikunjungi dan firewall juga memiliki kelebihan berupa pemblokiran terhadap beberapa situs tertentu, dan alamat ip dari sebuah situs [4]. Namun masalah juga terdapat pada jaringan smart home dimana keamanan jaringan dapat diretas oleh seseorang yang tidak dikenal, maka keamanan jaringan harus dilakukan pada setiap jaringan yang terhubung dan akan diawasi oleh firewall, masalah tersebut merupakan masalah yang cukup besar apabila terjadinya peretasan.



Peretasan Smart Home juga merupakan suatu masalah yang dapat membuat perangkat jaringan Smart Home dapat dikendalikan oleh orang tidak dikenal. Untuk mengatasi permasalahan ini peneliti mengusulkan penggunaan firewall sebagai keamanan pada jaringan smart home. Diharapkan bahwa dengan mengimplementasikan firewall, keamanan pada jaringan smart home dapat aman dari peretasan. Pada penelitian terdahulu artikel ini melakukan perancangan smart home dengan konsep Internet of Things berbasis microcontroller yang bertujuan untuk mengembangkan sistem smart home yang dapat mengontrol perangkat elektronik dan benda-benda di dalam rumah yang di implementasikan dalam sebuah miniatur rumah [5]. Penelitian lainnya artikel ini merancang dan merealisasikan smart home system berbasis IoT dan layanan pemberitahuan kejadian penting melalui SMS [6]. Penelitian berikutnya artikel ini membuat rancangan smarhome menggunakan mikrokontroler sebagai pengendali rumah seperti pintu rumah, garasi serta lampu untuk membantu permasalahan keamanan rumah dengan menjadikan rumah lebih aman dan praktis dalam mengontrol dan terhindar dari kejahatan yang tidak diinginkan [7].

Tujuan dari penelitian ini adalah untuk membuat simulasi sistem jaringan smart home dengan keamanan firewall yang dapat memberikan keamanan pada jaringan smart home dan memperkenalkan teknologi smart home dengan keamanan firewall agar dapat dikembangkan dan dimaksimalkan lebih efektif dan efisien secara nyata.

2. METODOLOGI PENELITIAN

2.1 Internet of Things (IoT)

Internet of Things atau dikenal juga dengan singkatan IoT, merupakan sebuah konsep yang bertujuan untuk memperluas manfaat dari konektivitas internet yang tersambung secara terus-menerus yang memungkinkan kita untuk menghubungkan mesin, peralatan, dan benda fisik lainnya dengan sensor jaringan dan aktuator untuk memperoleh data dan mengelola kinerjanya sendiri, sehingga memungkinkan mesin untuk berkolaborasi dan bahkan bertindak berdasarkan informasi baru yang diperoleh secara independen [8]. Internet of things adalah konsep dimana suatu device dapat memiliki kemampuan untuk mengirim data melalui jaringan internet tanpa adanya interaksi manusia ke manusia atau antara manusia ke komputer [9]. Internet of Things lebih sering disebut dengan singkatannya yaitu IoT. IoT ini sudah berkembang pesat mulai dari konvergensi teknologi nirkabel, micro-electromechanical systems (MEMS) dan juga Internet. IoT ini juga kerap diidentifikasi dengan RFID sebagai metode komunikasi. Walaupun begitu, IoT juga bisa mencakup teknologi-teknologi sensor lainnya, semacam teknologi nirkabel maupun kode QR yang sering kita temukan di sekitar kita [10]. Penerapan Internet of Things (IoT) mencakup fitur-fitur seperti berbagi informasi, pengendalian jarak jauh, serta pemrosesan data dari sensor yang terpasang pada berbagai objek. Objek-objek tersebut mencakup bahan makanan, perangkat elektronik, koleksi, peralatan, hingga makhluk hidup. Semua ini terhubung ke jaringan lokal atau global melalui sensor yang aktif secara terus-menerus [11].

2.2 Smart Home

Smart Home atau Rumah Pintar merupakan sebuah konsep desain teknis yang diterapkan untuk membangun sebuah rumah pintar. Konsep ini berkaitan dengan pemanfaatan teknologi yang diterapkan pada lingkungan rumah dengan fungsi tertentu yang bertujuan meningkatkan efisiensi serta kenyamanan penghuninya. Smart Home biasanya terdiri dari beberapa perangkat yang dikendalikan melalui smartphone [5]. Hal ini dapat dilakukan dengan mudah melalui perangkat pintar seperti smartphone atau laptop. Dengan menggunakan aplikasi atau perangkat lunak khusus, penghuni dapat mengelola pencahayaan di rumah, mengatur suhu ruangan, mengontrol sistem keamanan, dan bahkan memantau konsumsi energi [12]. Smart Home merupakan sebuah konsep di mana dari berbagai macam perangkat IoT yang tersedia untuk digunakan di rumah membuatnya menjadi pintar. Perangkat tersebut meliputi detektor gerakan, penyiram rumput, pintu pintar, panel surya, dan banyak perangkat IoT lainnya. Perangkat ini dapat dihubungkan menggunakan gateway rumah ke sebuah internet untuk dikendalikan dari jarak jauh dengan smartphone kita [13].

2.3 Firewall

Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya (jaringan eksternal) [14]. Firewall merupakan suatu jenis teknologi keamanan jaringan yang berguna untuk mengatur paket data yang masuk ke dalam jaringan dan paket data yang di blokir, firewall juga digunakan untuk melindungi, membatasi maupun menolak jaringan pribadi dengan jaringan luar yang berbahaya [15]. Sistem keamanan jaringan yang dikenal sebagai firewall berfungsi untuk mengawasi dan mengontrol lalu lintas data yang masuk dan keluar dari suatu jaringan komputer. Firewall berfungsi sebagai "pagar" antara jaringan

internal (seperti jaringan pribadi atau perusahaan) dan jaringan eksternal (seperti internet) untuk melindungi jaringan dari ancaman luar (seperti peretas, virus, dan malware) serta memastikan bahwa komunikasi yang terjadi hanya berasal dari sumber yang sah dan dapat dipercaya [16].

2.4 Access Control List (ACL)

Access Control List (ACL) merupakan salah satu metode yang digunakan untuk mengamankan jaringan komputer. Pengemasan paket berdasarkan kategori adalah konsep dasar dari penerapan ACL. Pengamanan menggunakan ACL ini akan sangat tepat jika kita ingin mengkonfigurasi lalu lintas pada jaringan yang kita bangun. Access Control list (ACL) sangat mudah dimanfaatkan atau digunakan jika kita ingin mengalihkan paket transmisi ataupun mengatur ulang dari host ke tujuan yang diinginkan. Teknik ACL digunakan untuk mentransfer sumber menuju alamat tujuan. ACL yang digunakan akan menerima paket yang berisikan data permission dan selanjutnya akan melarang paket data deny yang akan disampaikan ke alamat tujuan [17]. ACL yang berisi string numerik alfa (nama) dapat digunakan untuk mengidentifikasi IP Standar dan ACL yang Diperluas. ACL (Daftar Kontrol Akses), Alamat IP sumber dalam paket IP adalah satu satunya kriteria yang diverifikasi oleh standar ACL. Alamat IP sumber digunakan untuk menetapkan semua kebijakan kontrol. ACL standar, dengan kata lain, melewati atau menolak semua paket protokol. ACL ini tidak membedakan jenis trafik IP seperti WWW, telnet, UDP, dan DSP [18]. Untuk memenuhi aturan-aturan penentuan keamanan pada aplikasi web, maka dibutuhkan daftar akses kontrol (access control list, ACL) kepada tiap-tiap pengguna berdasarkan wewenang akses masing-masing dengan tipe pengguna yang berbeda. Dibutuhkannya ACL karena memiliki implementasi umum di semua platform [19].

2.5 Cisco Packet Tracer

Packet Tracer adalah sebuah platform simulasi visual alat yang dirancang oleh Cisco sehingga memungkinkan user untuk membuat topologi jaringan dan meniru jaringan computer yang lebih modern. Aplikasi ini dikembangkan oleh Cisco, aplikasi ini mempermudah dalam pengembangan jaringan dan melakukan simulator jaringan [20]. Cisco Packet Tracer merupakan alat simulasi yang digunakan dalam pembelajaran jaringan komputer dan IoT. Packet Tracer menggunakan antarmuka drag and drop user interface untuk memungkinkan pengguna dapat menambah dan menghapus perangkat jaringan yang disimulasikan sesuai dengan keinginan dan kebutuhan. Selain itu, dimungkinkan untuk membuat simulasi aspek tertentu dari jaringan komputer, dan Packet Tracer bisa menggabungkannya [21].

2.6 Internet Protocol version4 (IPv4)

IPv4 (Internet Protocol version 4) adalah versi keempat dari protokol Internet (IP) yang digunakan untuk mengidentifikasi dan mengirimkan paket data melalui jaringan komputer. Alamat IP versi 4 atau IPv4 sebuah jenis pengalamatan jaringan komputer yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol TCP/IP versi 4. Panjang totalnya adalah 32- bit nomor, dan secara teoritis dapat mengalami hingga 4 miliar host komputer atau lebih tepatnya 4.294.967.296 alamat host di seluruh dunia, jumlah host tersebut didapatkan dari $256 \times 4 =$ (didapatkan dari 8 bit) dipangkat 4 (karena terdapat 4 oktet) sehingga nilai maksimal dari alamat IP versi 4 tersebut adalah 255.255.255.255 dimana nilai dihitung dari nol sehingga nilai host yang dapat ditampung adalah $256 \times 256 \times 256 \times 256 = 4.294.967.296$ alamat host. Sehingga jika host yang ada diseluruh dunia melebihi kuota tersebut maka diperlukan pengalamatan IP versi 6 atau IPv6. Contoh alamat IPv4: 192.168.0.10 [22].

Tabel 1. Kelas IPV4

Kelas	Range IP Address	Jumlah Host	Jumlah Network
A	0.0.0.0 – 127.255.255.255	16,777,216	128
B	128.0.0.0 – 191.255.255.255	1,048,576	16.384
C	192.0.0.0 – 223.255.255.255	65,536	2.097.152
D	224.0.0.0 – 239.255.255.255	Tidak Didefinisikan	Tidak Didefinisikan
E	240.0.0.0 – 255.255.255.255	Tidak Didefinisikan	Tidak Didefinisikan

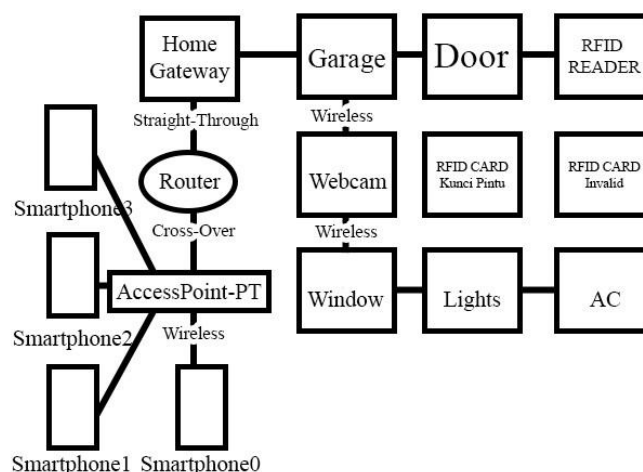
Pada Tabel 1, Pembagian kelas IP Address untuk alokasi alamat IP di jaringan memudahkan identifikasi dan pemisahan host.

2.7 Perancangan Sistem

Perancangan sistem dilakukan sebagai perencanaan terhadap sistem yang akan dibangun pada konsep simulasi penerapan firewall pada jaringan smart home yang berbasis Internet of Things meliputi pengkabelan dan



konfigurasi perangkat-perangkat yang digunakan pada penelitian. Beberapa rancangan sistem yang akan dibangun yaitu : topologi jaringan, firewall access control list, keamanan pintu rumah, jendela, garasi, lampu, webcam dan pendingin ruangan.



Gambar 1. Topologi Jaringan Smart Home

Gambar 1 merupakan proses pengkabelan yang digunakan pada simulasi yaitu pada Smartphone0, 1, 2, dan 3 terhubung dengan perangkat AccessPoint-PT secara wireless. AccessPoint-PT terhubung dengan router menggunakan kabel Cross-Over dengan Port0 dan pada router FastEthernet0/0. Perangkat Home Gateway terhubung dengan router menggunakan kabel Straight-Through dengan Ethernet 1 dan FastEthernet0/1 pada router, perangkat Smart Home terhubung dengan Home Gateway. Adapun beberapa konfigurasi yang dilakukan pada perangkat-perangkat yang digunakan tampak pada tabel 2.

Tabel 2. Konfigurasi IP Address Router

Port Interface	Konfigurasi	Detail
FastEthernet0/0	CIDR	/24
	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Port Status	No Shutdown (ON)
FastEthernet0/1	CIDR	/24
	IP Address	192.168.2.1
	Subnet Mask	255.255.255.0
	Port Status	No Shutdown (ON)

Pada tabel 2, Mengkonfigurasi IP pada perangkat router untuk FastEthernet0/0 yang terhubung dengan AccessPoint-PT yang akan diberikan IP address dengan IP 192.168.1.1/24 dan pada perangkat router untuk FastEthernet0/1 yang terhubung dengan Home Gateway akan diberikan IP address dengan IP 192.168.2.1/24

Tabel 3. Konfigurasi Firewall Access Control List

Port Interface	Konfigurasi	Detail
FastEthernet0/0	CIDR	/24
	IP Address	192.168.1.2

Pada tabel 3, Mengkonfigurasi Firewall Access Control List agar perangkat smartphone yang tersambung dalam jaringan tidak semua dapat mengakses perangkat Smart Home hanya perangkat smartphone yang terdaftar dapat mengontrol perangkat Smart Home. Perangkat smartphone yang terdaftar akan diberikan IP address dengan IP 192.168.1.2

Tabel 4. Konfigurasi AccessPoint-PT

Perangkat	Interface	Wireless Setting	
		SSID	Authentication : WPA2-PSK
AccessPoint-PT	Port1	Home	12345678

Pada tabel 4, Mengkonfigurasi perangkat AccessPoint-PT yaitu membuat jaringan wireless untuk perangkat smartphone. Dengan melakukan konfigurasi interface pada AccessPoint-PT dan memberi SSID dan Authentication

Tabel 5. Konfigurasi SMARTPHONE-PT

Perangkat	Interface	Wireless Setting	
		Konfigurasi	Detail
Smartphone0	Wireless0	SSID	Home
		Authentication : WPA2-PSK	12345678
		IP Address	192.168.1.2
		Subnet Mask	255.255.255.0
		Gateway	192.168.1.1
Smartphone1	Wireless0	SSID	Home
		Authentication : WPA2-PSK	12345678
		IP Address	192.168.1.3
		Subnet Mask	255.255.255.0
		Gateway	192.168.1.1
Smartphone2	Wireless0	SSID	Home
		Authentication : WPA2-PSK	12345678
		IP Address	192.168.1.4
		Subnet Mask	255.255.255.0
		Gateway	192.168.1.1
Smartphone3	Wireless0	SSID	Home
		Authentication : WPA2-PSK	12345678
		IP Address	192.168.1.5
		Subnet Mask	255.255.255.0
		Gateway	192.168.1.1

Tabel 5 merupakan mengkonfigurasi perangkat SMARTPHONE-PT yaitu menghubungkan jaringan wireless ke perangkat AccessPoint-PT dengan melakukan konfigurasi interface SSID dan Authentication serta IP Configuration pada SMARTPHONE-PT

Tabel 6. Konfigurasi Home Gateway

Perangkat	Interface	Wireless Setting	
		Konfigurasi	Detail
Home Gateway0	Wireless	SSID	Home
		Authentication : WPA2-PSK	12345678
		IP Address	192.168.1.2
	LAN	Subnet Mask	255.255.255.0
		Gateway	192.168.1.1

Pada tabel 6, mengkonfigurasi perangkat Home Gateway yaitu membuat jaringan wireless untuk perangkat Smart Home yang akan terhubung dengan Home Gateway dengan memberi SSID, Authentication WPA2-PSK, IP Address dan Gateway

Tabel 7. Konfigurasi Interface Wireless Perangkat Smart Home Internet of Things

Perangkat	Interface	Wireless Setting	
		SSID	Authentication : WPA2-PSK
Pintu	Wireless	Smart Home	12345678
RFID Reader	Wireless	Smart Home	12345678
Garasi	Wireless	Smart Home	12345678
Webcam	Wireless	Smart Home	12345678
Jendela	Wireless	Smart Home	12345678
Lampu	Wireless	Smart Home	12345678
Air Conditioner	Wireless	Smart Home	12345678

Tabel 7 adalah mengkonfigurasi interface wireless masing-masing perangkat Smart Home dengan memberi SSID dan Authentication sesuai dengan yang ada pada Home Gateway

Tabel 8. Konfigurasi RFID Card Kunci Pintu

Attributes		
Properties	Property	Card ID
	Value	10

Tabel 8 adalah mengkonfigurasi RFID Card Kunci Pintu agar perangkat pintu dapat membuka card yang terdaftar dalam jaringan Smart Home

Tabel 9. Konfigurasi RFID Card Invalid

Attributes		
Properties	Property	Card ID
	Value	11

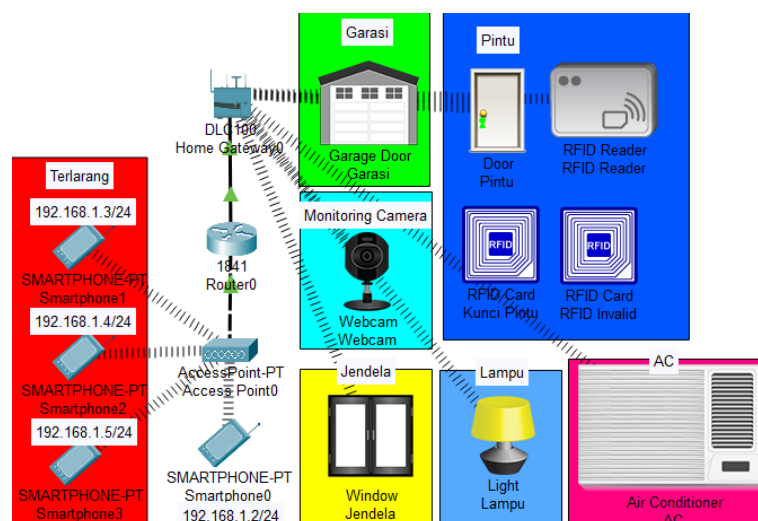
Tabel 9 adalah mengkonfigurasi RFID Card Invalid agar perangkat pintu tidak dapat membuka card yang tidak terdaftar dalam jaringan Smart Home

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Perancangan Sistem

Implementasi perancangan sistem yang diterapkan ke dalam bentuk simulasi menggunakan bantuan software Cisco Packet Tracer 7.3. Perangkat lunak ini digunakan dalam melakukan pengujian dan simulasi jaringan smarthome pada penelitian yang dilakukan.

Pada Gambar 2, Tampilan simulasi jaringan smart home pada cisco packet tracer 7.3 menampilkan perangkat yang nanti akan dilakukan pengujian dalam penerapan firewall.



Gambar 2. Tampilan Simulasi Jaringan Smart Home Pada Cisco Packet Tracer 7.3

3.2 Pengujian Koneksi

1. Uji Coba Ping Perangkat SMARTPHONE-PT

Uji coba yang dilakukan yaitu ping dari perangkat smartphone 0 dan 1 ke perangkat router

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=34ms TTL=255
Reply from 192.168.1.1: bytes=32 time=10ms TTL=255
Reply from 192.168.1.1: bytes=32 time=11ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 34ms, Average = 18ms

Control-C
^C
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=14ms TTL=255
Reply from 192.168.2.1: bytes=32 time=14ms TTL=255
Reply from 192.168.2.1: bytes=32 time=19ms TTL=255
Reply from 192.168.2.1: bytes=32 time=14ms TTL=255
```

Gambar 3. Ping Smartphone0 ke Perangkat Router

Berdasarkan pada gambar 3, pengujian yang dilakukan pada Smartphone0 dengan melakukan ping ke perangkat router dengan Interface Fa0/0 IP Address 192.168.1.1 dan Interface Fa0/1 IP Address 192.168.2.1. Hasil yang didapat yaitu kedua perangkat yakni Smartphone0 dan Router saling terkoneksi dan dapat bertukar pesan. Hasil dari uji coba konektivitas perangkat berhasil.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

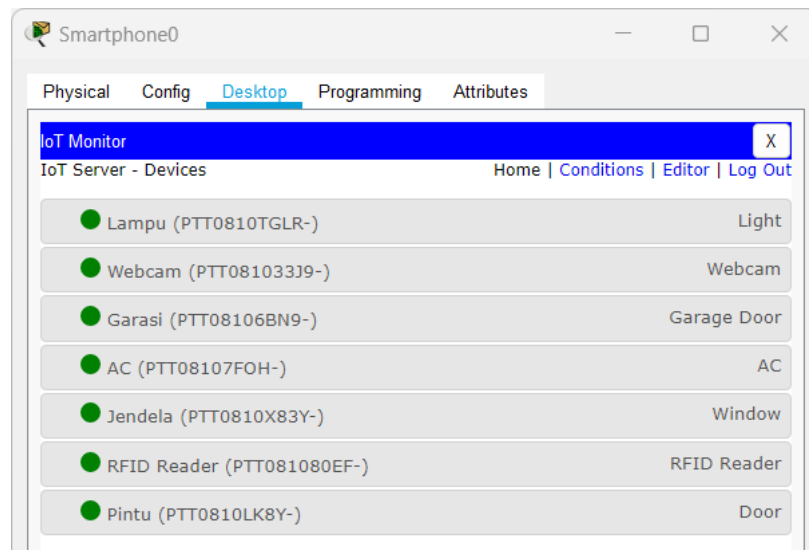
Gambar 4. Ping Smartphone1 ke Perangkat Router



Berdasarkan gambar 4, pengujian yang dilakukan pada Smartphone1 dengan melakukan ping ke perangkat Home Gateway dan salah satu perangkat Smart Home Internet of Things dengan IP Address 192.168.2.2 dan IP Address 192.168.2.108. Hasil yang didapat yaitu perangkat Smartphone1 ke perangkat Home Gateway dan salah satu perangkat Smart Home Internet of Things tidak mendapat izin terhubung karena Firewall Access Control List yang dikonfigurasi pada router. Hasil dari uji coba firewall perangkat berhasil.

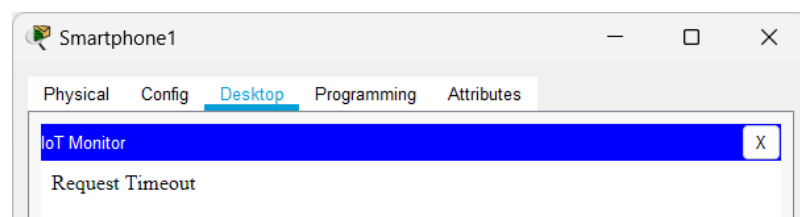
2. Uji Perangkat Smarthome Internet of Things pada IoT Monitor

Untuk memastikan apakah perangkat-perangkat Smart Home Internet of Things yang sudah dirancang dan dikonfigurasi sudah terhubung ke IoT Monitor yaitu dengan masuk ke IoT Monitor pada perangkat smartphone. Apabila sudah terhubung maka pada tampilan Home pada IoT Server akan muncul perangkat-perangkat Smart Home Internet of Things yang sudah terhubung.



Gambar 5. Tampilan Perangkat Internet of Things pada IoT Monitor Pada Perangkat Smartphone0

Gambar 5 merupakan hasil yang diperoleh pada tampilan monitoring IoT Monitor pada Smartphone0 muncul perangkat-perangkat Smart Home Internet of Things yang sudah dirancang dan dikonfigurasi sebelumnya dengan status berwarna hijau yang memiliki arti, bahwa perangkat-perangkat tersebut telah terhubung dengan perangkat Home Gateway dan dapat dikendalikan oleh perangkat smartphone. Hasil dari uji coba konektivitas perangkat berhasil.



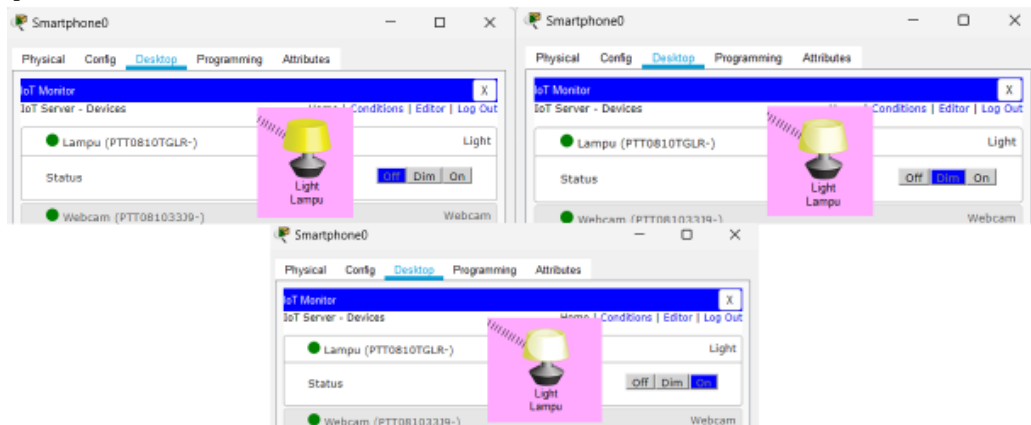
Gambar 6. Tampilan Perangkat Internet of Things pada IoT Monitor Pada Perangkat Smartphone1

Pada Gambar 6, hasil yang diperoleh adalah pada tampilan monitoring Internet of Things Monitor pada Smartphone1 muncul pemberitahuan dengan pesan Request Time out yang di mana perangkat-perangkat Smart Home Internet of Things tidak dapat dikendalikan. Hasil dari uji coba firewall perangkat berhasil.

3.3 Pengujian Perangkat Smartphone

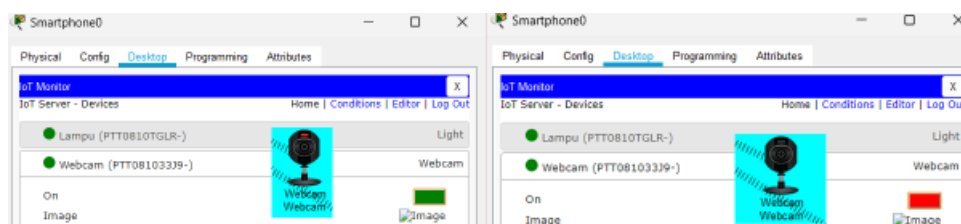
1. Smartphone0

Perangkat Smartphone0 dapat mengontrol perangkat Smart Home Internet of Things pada Iot Monitor meliputi :



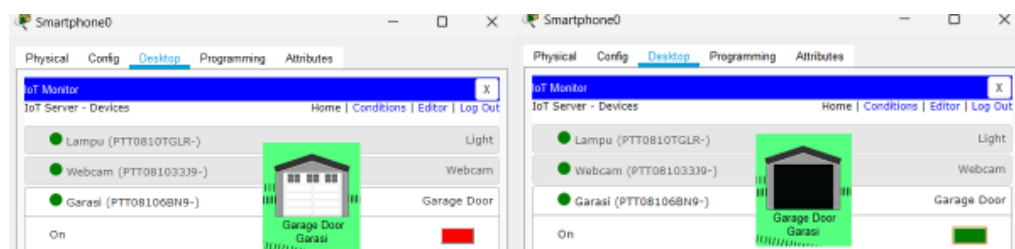
Gambar 7. Kontrol Lampu

Pada gambar 7, kontrol yang dilakukan kepada lampu di mana status Off atau tidak aktif maka lampu tidak memiliki cahaya. Dan jika kontrol yang dilakukan kepada lampu di mana status Dim maka tampilan pada lampu adalah cahaya jauh. Dan kontrol yang dilakukan kepada lampu di mana status On atau aktif maka tampilan pada lampu adalah cahaya normal.



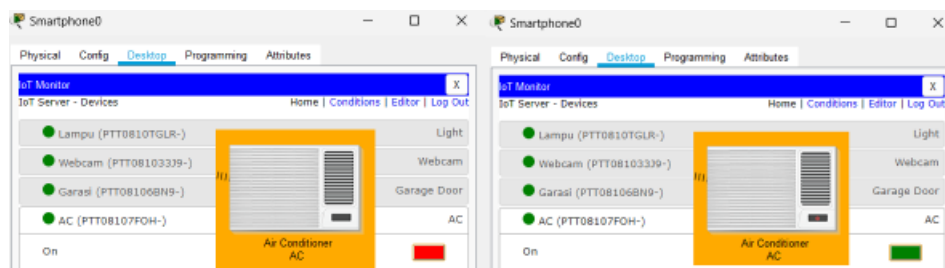
Gambar 8. Kontrol Webcam

Pada gambar 8, kontrol yang dilakukan kepada webcam dimana status Off atau tidak aktif maka pada tampilan IoT Monitor akan memberikan sinyal merah dan perangkat tidak menyala. Lalu, jika kontrol yang dilakukan kepada webcam dimana status On atau aktif maka pada tampilan IoT Monitor akan memberikan sinyal hijau dan perangkat menyala.



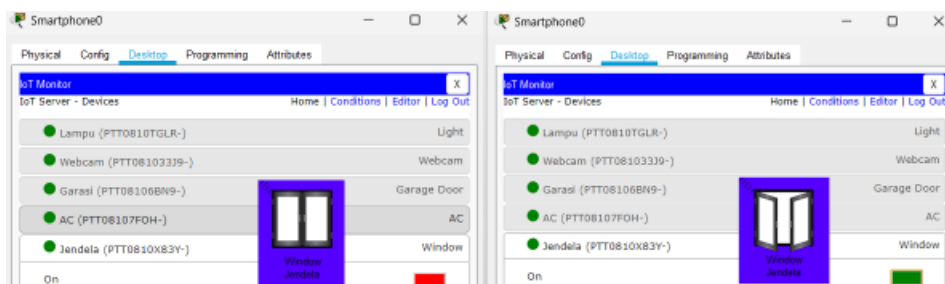
Gambar 9. Kontrol Garasi

Pada gambar 8, kontrol yang dilakukan kepada garasi dimana status Off atau tidak aktif maka pada tampilan IoT Monitor akan memberikan sinyal merah dan perangkat tidak menyala. Lalu, jika kontrol yang dilakukan kepada Garasi dimana status On atau aktif maka pada tampilan IoT Monitor akan memberikan sinyal hijau dan perangkat menyala.



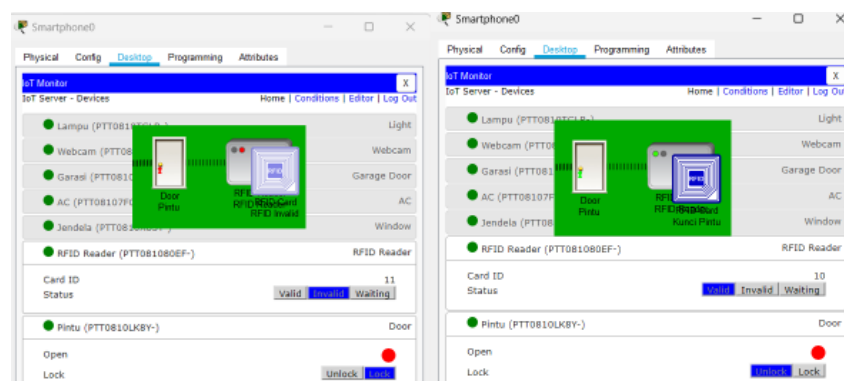
Gambar 10. Kontrol AC

Pada gambar 10, kontrol yang dilakukan kepada AC dimana status Off atau tidak aktif maka pada tampilan IoT Monitor akan memberikan sinyal merah dan perangkat tidak menyala. Lalu, jika kontrol yang dilakukan kepada AC dimana status On atau aktif maka pada tampilan IoT Monitor akan memberikan sinyal hijau dan perangkat menyala.



Gambar 11. Kontrol Jendela

Pada gambar 11, kontrol yang dilakukan kepada Jendela dimana status Off atau tidak aktif maka pada tampilan IoT Monitor akan memberikan sinyal merah dan perangkat tidak menyala. Lalu, jika kontrol yang dilakukan kepada Jendela dimana status On atau aktif maka pada tampilan IoT Monitor akan memberikan sinyal hijau dan perangkat menyala.



Gambar 12. Kontrol Pintu dan ID Card

Pada gambar 12, kontrol yang dilakukan kepada pintu dan RFID reader dimana status invalid atau tidak terhubung maka pada tampilan pintu dan RFID reader akan memberikan indikator merah pada perangkat dan pintu terkunci. Lalu, jika kontrol yang dilakukan kepada pintu dan RFID reader dimana status valid atau terhubung maka pada tampilan pintu dan RFID reader akan memberikan indikator hijau pada perangkat dan pintu terbuka.

2. Smartphone1

Perangkat Smartphone1 tidak dapat mengontrol perangkat Smart Home Internet of Things pada IoT Monitor.

Pada gambar 12, riwayat pengiriman data yang dilakukan perangkat Smartphone1 kepada perangkat Smart Home Internet of Things dengan hasil Failed atau tidak berhasil dikarenakan konfigurasi firewall access control list yang dilakukan pada router.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Failed	Smartphone1	Garasi	ICMP		0.000	N	0
	Failed	Smartphone1	Webcam	ICMP		0.000	N	1
	Failed	Smartphone1	Jendela	ICMP		0.000	N	2
	Failed	Smartphone1	Pintu	ICMP		0.000	N	3
	Failed	Smartphone1	RFID Reader	ICMP		0.000	N	4
	Failed	Smartphone1	Lampu	ICMP		0.000	N	5
	Failed	Smartphone1	AC	ICMP		0.000	N	6

Gambar 12. Riwayat Perangkat Smartphone1 Pada Perangkat Smart Home

4. KESIMPULAN

Berdasarkan pengujian PING pada gambar 4, smartphone1 tidak memiliki akses untuk terhubung dengan router dan pengujian pada IoT Monitor pada gambar 6 Smartphone1 tidak dapat memasuki server IoT Monitor karena router tidak mengizinkan dan pengujian pada perangkat Smartphone0 dapat mengendalikan perangkat Smart Home Internet of Things dan ketika melakukan pengujian PING pada gambar 3. Smartphone0 dapat terkoneksi dengan perangkat router. Konsep sistem keamanan firewall pada jaringan smart home adalah melarang atau tidak memberikan izin terhadap perangkat yang tidak terdaftar pada konfigurasi yang telah dibuat sehingga perangkat yang tidak terdaftar tidak dapat masuk ke dalam jaringan smart home dan dapat memberikan keamanan dalam hal peretasan perangkat smart home yang dilakukan oleh orang tidak dikenal. Konsep perangkat smart home dapat memberikan kemudahan aktivitas dan melindungi keamanan rumah melalui kontrol smartphone0 yaitu kontrol lampu, webcam, garasi, AC, jendela dan pintu rumah smarhome menggunakan perangkat RFID Reader yang berfungsi untuk sebagai pengamanan pintu rumah yang dapat membuka pintu secara otomatis apabila ID Card pada RFID Card valid dan jika RFID Card invalid pintu tidak akan terbuka secara otomatis.

REFERENSI

- [1] T. Aziz and R. Liza, "Model Simulasi Smarthome Berbasis Internet of Things dan Cloud Computing Menggunakan Cisco Packet Tracer," *Snastikom*, 2022, [Online]. Available: <https://prosiding.snastikom.com/index.php/SNASTIKOM2020/article/download/41/37>
- [2] R. I. Akbar, D. G. Purnama, and A. Salsabila, "Pengembangan Model SmartHome berbasis IoT," *Pros. Semin. Nas. Penelit. LPPM UMJ*, pp. 1–8, 2023.
- [3] D. Durianto, Ananta, "Konfigurasi Cicso ASA Firewall Menggunakan ASDM," vol. 5, no. Volume 5 No. 2, p. 305, 2021.
- [4] M. U. Dewi, "Kelebihan Firewall Kekurangan Firewall," 2021.
- [5] A. Restu Mukti, C. Mukmin, E. Randa Kasih, D. Palembang Jalan Jenderal Ahmad Yani No, S. I. Ulu, and S. Selatan, "Perancangan Smart Home Menggunakan Konsep Internet of Things (IoT) Berbasis Microcontroller," *J. JUPITER*, vol. 14, no. 2, pp. 516–522, 2022.
- [6] H. Andrianto and G. Intan Saputra, "Smart Home System Berbasis IoT dan SMS Smart Home System Based on IoT and SMS," *Telka*, vol. 6, no. 1, pp. 40–48, 2020.
- [7] A. Gallileo *et al.*, "Rancangan smarhome berbasis mikrokontroler sebagai pengendali pintu rumah dan garasi serta lampu," vol. 12, no. 1, 2025.
- [8] Y. Efendi, "Internet Of Things (Iot) Sistem Pengendalian Lampu Menggunakan Raspberry Pi Berbasis Mobile," *J. Ilm. Ilmu Komput.*, vol. 4, no. 2, pp. 21–27, 2018, doi: 10.35329/jiik.v4i2.41.
- [9] D. Suarna and E. S. Edy, "Implementasi Internet of Things (IoT) dalam Memonitoring Komsumsi Listrik," *Bull. Inf. Technol.*, vol. 4, no. 2, pp. 163–170, 2023, doi: 10.47065/bit.v4i2.631.
- [10] A. N. Ismail and F. Nuryana, "Angan Jaringan Smart Home," 2024.
- [11] F. Adani and S. Salsabil, "Internet of Things: Sejarah Teknologi Dan Penerapannya," *Isu Teknol. Stt Mandala*, vol. 14, no. 2, pp. 92–99, 2019.
- [12] M. Faqih Febriansyah, R. Setiawan, and T. Sutabri, "IJM: Indonesian Journal of Multidisciplinary Kemudahan dan Keamanan Dalam Rumah Pintar: Tinjauan Terhadap Teknologi Smart Home," *IJM Indones. J. Multidiscip.*, vol. 2, pp. 24–31, 2024, [Online]. Available: <https://journal.csspublishing/index.php/ijm>
- [13] A. Dogman and M. Jewiley, "Design and Implement IoT Smart Home via Cisco Packet Tracer : Applications & Simulations," *Sixth Int. Conf. - Smart Cities State Map -Libya*, no. December, p. 2,

- 2020.
- [14] S. T. Kurniawan, "Perancangan Dan Penerapan Stateful Firewall Pada Arsitektur Dual-Homed Host," *J. Teknol. Pint.*, vol. 3, no. 2, pp. 1–17, 2023, [Online]. Available: <http://teknologipintar.org/index.php/teknologipintar/article/view/356%0Ahttp://teknologipintar.org/index.php/teknologipintar/article/download/356/340>
 - [15] D. Wicaksono, "Firewall Sistem Keamanan Jaringan Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1380–1392, 2022, doi: 10.35957/jatisi.v9i2.2103.
 - [16] F. A. Syaifuddin, D. A. Maulana, and M. F. Amrulloh, "Analisis Keamanan Jaringan Menggunakan Firewall untuk Mencegah Serangan Brute Force dan Fraud," vol. 4, no. 2, pp. 895–902, 2024.
 - [17] R. Sulaiman, R. S. Al Fathul, and A. M. Raya, "Implementasi Metode Access Control List Pada Mikrotik Dalam Mengamankan Jaringan Internet Di Kantor Lurah Air Selemba," *J. Tek. Inform. dan Teknol. Inf.*, vol. 4, no. 1, pp. 75–85, 2024, doi: 10.55606/jutiti.v4i1.2880.
 - [18] S. Dewi, F. Firmansyah, and U. Hasan, "Penerapan Metode Access Control List Pada Jaringan VLAN Menggunakan Router Cisco," *IMTechno J. Ind. Manag. Technol.*, vol. 3, no. 1, pp. 37–41, 2022, doi: 10.31294/imtechno.v3i1.927.
 - [19] K. Kamarudin and M. Gazali, "Sistem Keamanan Berlapis Menggunakan Metode Access Control List Dan Enkripsi Source Code Pada Web Login," *J. Teknol. Inf.*, vol. 2, no. 2, pp. 48–60, 2021, doi: 10.32546/jutech.v2i2.1657.
 - [20] S. Jayanto, A. Tanton, and H. Asyari, "Implementasi Keamanan Jaringan dengan Packet Filtering Berbasis Mikrotik Untuk Internet Positif Di SMKN 1 Praya," *J. Ranah Publik Indones. Kontemporer*, vol. 1, no. 2, pp. 65–77, 2021, doi: 10.47134/rapik.v1i2.10.
 - [21] R. Prahastian, "Penggunaan Simulator Cisco Packet Tracer 7.2 Pada Rumah Kaca Pintar Untuk Tanaman Kopi Berbasis IoT," Universitas Islam Negeri Sayarif Hidayatullah Jakarta, 2019.
 - [22] A. Afrizal and F. Fitriani, "Penerapan IPV4 dan IPV6 pada Jaringan yang Terhubung," *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 3, no. 1, p. 13, 2019, doi: 10.35870/jtik.v3i1.78.