Contents lists available at MID Publisher International

Technology Sciences Insights Journal

Journal homepage: https://journal.midpublisher.com/index.php/tsij

Keamanan Jaringan *Cloud-Native* dan Implementasi Solusi Keamanan Menggunakan *Cloud Computing*

Rakhmadi Rahman, Umi Kalsum

Prodi Sistem Informasi, Fakultas Sains, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Juni 2024
Revisi Juni 2024
Diterima Juli 2024

Kata Kunci:
Keamanan Jaringan, Cloud-Native, Solusi Keamanan, Otomatisasi, Microservices, Kontainerisasi.

*Penulis Korespondensi:
ummikalsum2909@gmail.com

ABSTRAK

Studi ini menginvestigasi penerapan tentang keamanan jaringan cloud-native dan implementasi solusi keamanan yang efektif untuk melindungi aplikasi dan data dari ancaman-ancaman. Cloud-native telah menjadi suatu kebutuhan yang sangat penting dalam era digital saat ini, memungkinkan pengembangan aplikasi yang lebih cepat dan efisien. Namun, hal ini juga memerlukan strategi keamanan yang lebih efektif. Solusi keamanan cloud-native harus dapat menghadapi tantangan-tantangan keamanan yang terkait dengan penggunaan cloud computing, seperti manajemen identitas dan akses, keamanan jaringan, dan investigasi serta respons otomatis. Penelitian ini bertujuan untuk menganalisis dan mengembangkan cloud-native yang lebih aman untuk meningkatkan keamanan aplikasi. Implementasinya meliputi integrasi teknologi cloudnative dengan keamanan terbaik, seperti otomatisasi, microservices, dan kontainerisasi, untuk meningkatkan visibilitas, otomatisasi keamanan, skalabilitas, dan keandalan aplikasi. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan jaringan cloud-native dan implementasi solusi keamanan yang efektif.

ABSTRACT

This study investigates the implementation of cloud-native network security and the deployment of effective security solutions to protect applications and data from threats. Cloud-native has become a crucial need in the current digital era, enabling faster and more efficient application development. However, it also requires a more effective security strategy. Cloud-native security solutions must be able to address the security challenges associated with the use of cloud computing, such as identity and access management, network security, and automated investigation and response. This research aims to analyze and develop more secure cloud-native environments to enhance application security. The implementation includes integrating cloudnative technologies with best-in-class security, such as automation, microservices, and containerization, to improve visibility, security automation, scalability, and application reliability. The results of this research are expected to contribute to enhancing cloud-native network security and the implementation of effective security solutions.

PENDAHULUAN

Keamanan jaringan cloud-native telah menjadi kebutuhan penting di era digital saat ini. Perkembangan teknologi cloud computing memungkinkan akses aplikasi dan data dari mana saja dan kapan saja. Cloudnative memfasilitasi pengembangan aplikasi yang lebih cepat dan efisien melalui kontainer dan layanan mikro. Namun, hal ini juga memerlukan strategi keamanan yang lebih efektif untuk melindungi aplikasi dan data dari ancaman.

Solusi keamanan cloud-native harus mampu menghadapi tantangan-tantangan terkait

Copyright © 2024 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (http://creativecommons.org/licences/by-sa/4.0/)

penggunaan cloud computing, seperti manajemen identitas dan akses, keamanan jaringan, serta investigasi dan respons otomatis. Oleh karena itu, keamanan jaringan cloud-native harus dapat memberikan perlindungan yang lebih baik dan fleksibel bagi aplikasi dan data di lingkungan cloud.

Penelitian ini bertujuan untuk menganalisis dan mengembangkan cloud-native yang lebih aman guna meningkatkan keamanan aplikasi. Implementasinya meliputi integrasi teknologi cloud-native terbaik, seperti otomatisasi, microservices, dan kontainerisasi, untuk meningkatkan visibilitas, otomatisasi keamanan, skalabilitas, dan keandalan aplikasi.

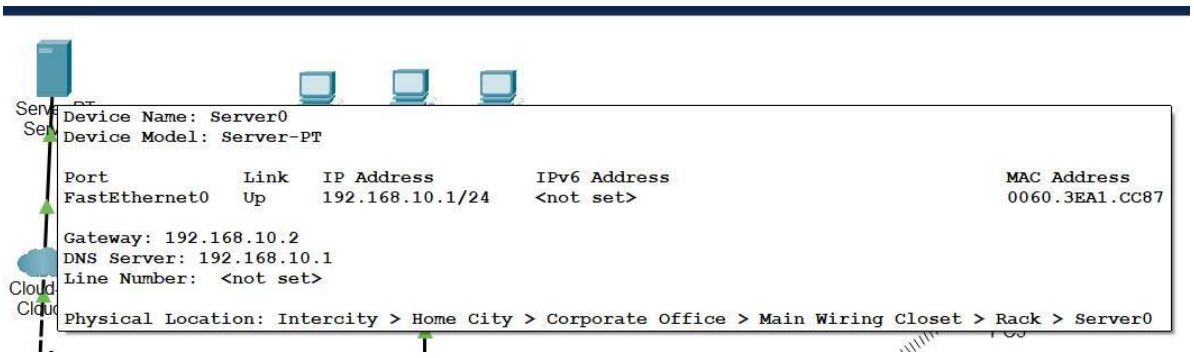
METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan studi literatur sebagai metode utama Solusi keamanan cloud-native harus mampu menghadapi tantangan-tantangan terkait penggunaan cloud computing, seperti manajemen identitas dan akses, keamanan jaringan, serta investigasi dan respons otomatis. Berikut ini adalah tahapan-tahapan dalam metode penelitian yang dilakukan:

1. Konfigurasi Lingkungan Uji Coba.

   Berikut Langkah awal dalam penelitian ini adalah mempersiapkan Konfigurasi Pada Uji Coba Cisco yang mencakup

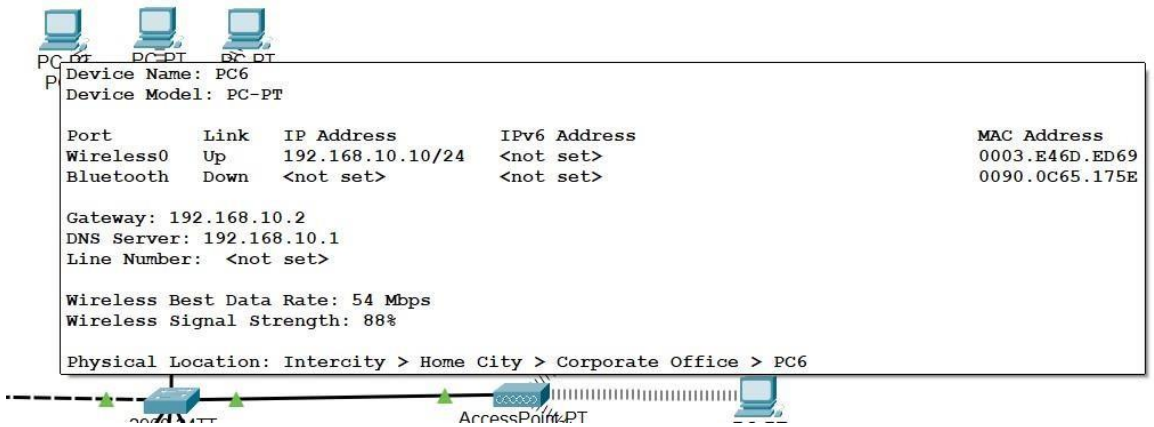
   a. Perangkat Lunak: Menginstal Aplikasi Cisco Packet Traker menyediakan lingkungan virtual untuk merancang, mengkonfigurasi, dan mensimulasikan topologi jaringan komputer.
   b. Konfigurasi Jaringan: mengkonfigurasi setiap perangkat jaringan secara individual. Konfigurasi dapat mencakup pengaturan interface, protokol routing, access control list (ACL), VLAN, WIRELES

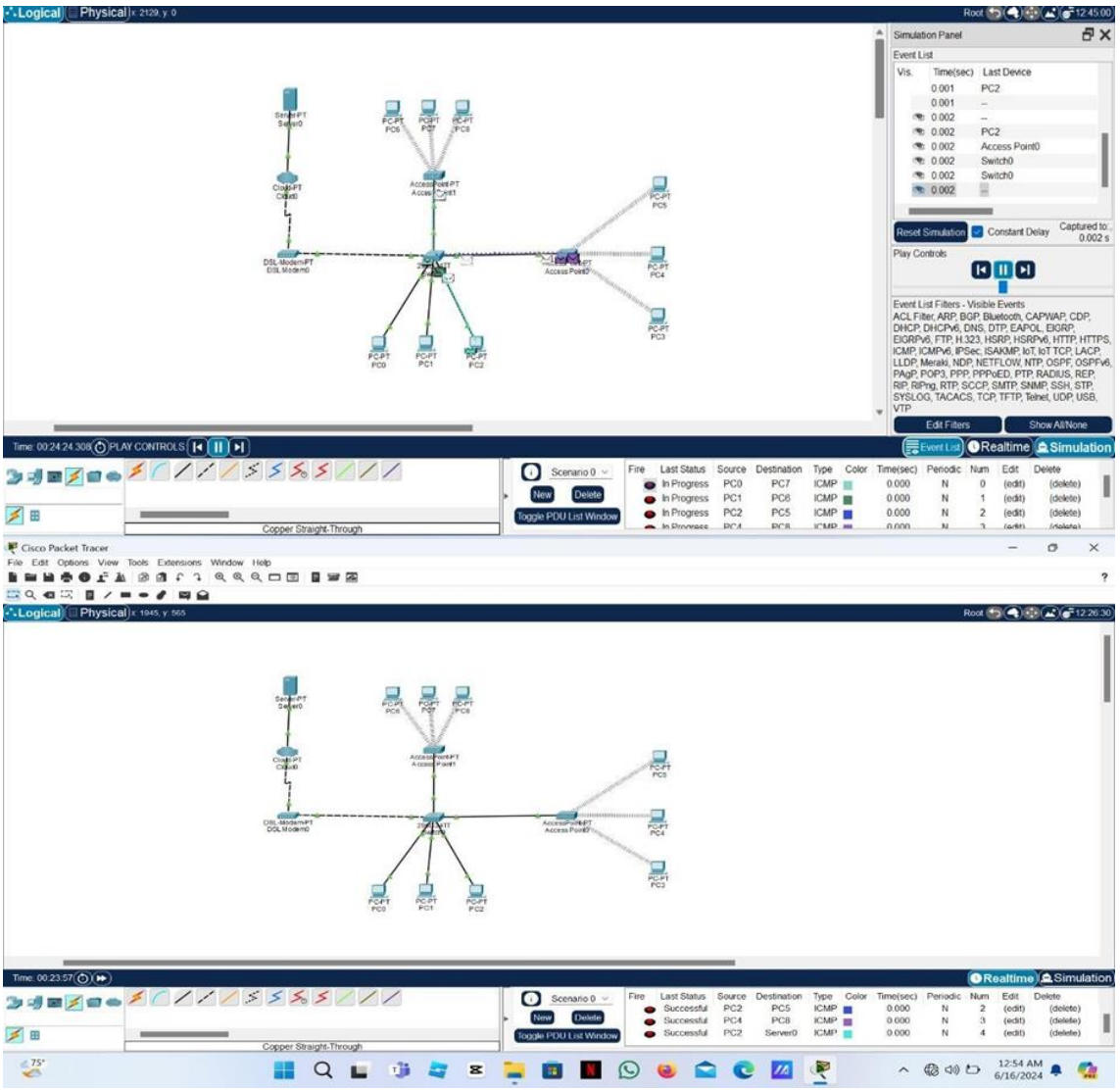


Berikut adalah gambaran konfigurasi pada server

Gateaway: 192.168.10.2

DNS Server: 192.168.10.1





2. Pengujian Konfigurasi

Setelah konfigurasi pada Aplikasi Cisco selesai, dilakukan pengujian untuk memastikan semuanya berjalan dengan baik:

a. Perintah Pengujian: Menjalankan perintah mengirimkannya data, untuk mengirimkan data dari misi ke depan ke server.
b. Pemantauan Aktif: Setelah pengujian berhasil, Simulasi pada PC Sukses untuk mengirim data.

3. Analisis Hasil

Setelah dilakukan analisis terhadap data yang dikumpulkan, dengan menggunakan simulasi, pengguna dapat menguji dan memvalidasi konfigurasi jaringan yang telah dibuat. Hal ini memungkinkan pengguna untuk mengidentifikasi dan memperbaiki masalah sebelum menerapkan konfigurasi di lingkungan nyata.

4. Penyusunan Laporan

Tahap akhir adalah penyusunan laporan penelitian yang mencakup:

a. Metode Penelitian: Menjelaskan secara rinci prosedur dan teknik yang digunakan dalam penelitian. Pendekatan Metodologis: Memaparkan dengan detail metode yang diterapkan dalam pelaksanaan penelitian. Menjelaskan secara rinci metode penelitian yang digunakan.
b. Temuan dan Analisis: Menyajikan hasil pengujian serta menganalisis dan membahas temuan utama. Hasil Penelitian dan Pembahasan: Menyampaikan temuan penelitian dan mendiskusikan implikasinya.
c. Kesimpulan: Menyimpulkan penelitian dan memberikan saran untuk pengembangan

selanjutnya.

Metode Penelitian ini bertujuan untuk menganalisis dan mengembangkan pendekatan cloud-native yang lebih aman untuk meningkatkan keamanan aplikasi. Implementasinya akan mencakup integrasi teknologi cloudnative terkini, seperti otomatisasi, microservices, dan kontainerisasi, dengan praktik-praktik keamanan terbaik. Hal ini diharapkan dapat meningkatkan visibilitas, otomatisasi keamanan, skalabilitas, dan keandalan aplikasi cloud-native.

HASIL DAN PEMBAHASAN

Hasil

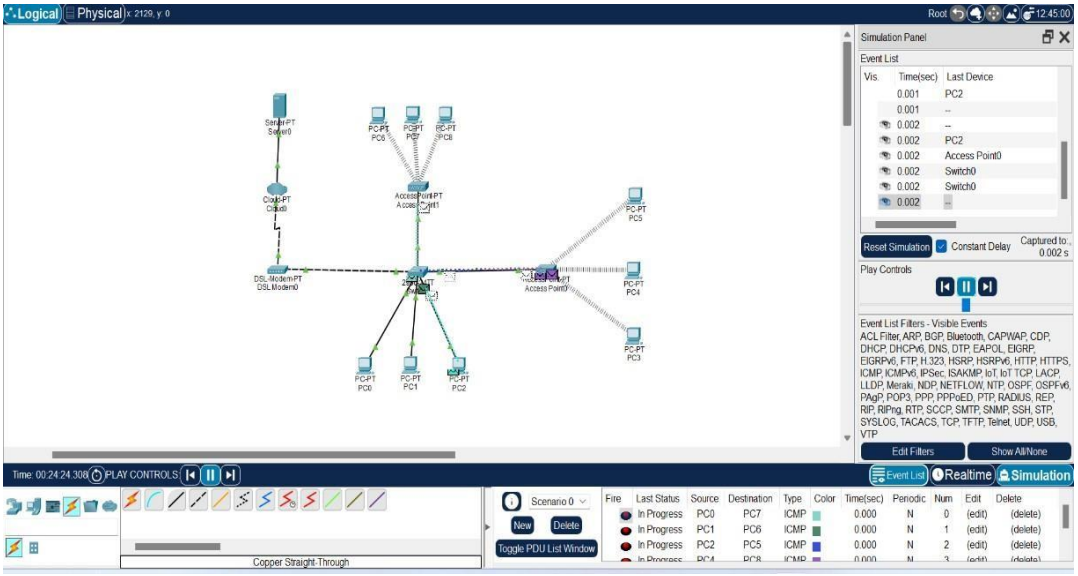
Penelitian ini menghasilkan beberapa temuan penting terkait dengan efektivitas Snort dalam mendeteksi dan menganalisis ancaman dari dalam di lingkungan jaringan Linux. Berikut adalah hasil dari setiap tahap yang telah dilakukan:

1. Pengujian Cloud-native adalah pendekatan pengembangan aplikasi di mana aplikasi dibangun dengan memanfaatkan layanan cloud, seperti komputasi awan, penyimpanan awan, dan jaringan awan. Aplikasi cloud-native dirancang untuk dapat beradaptasi dengan cepat, skalabel, dan tahan terhadap kegagalan. Karakteristik utama cloud-native adalah:
   - Berbasis kontainer
   - Menggunakan layanan mikro
   - Adanya otomasi untuk deployment dan scaling
   - Desain yang berorientasi pada API
   - Mengutamakan pengalaman pengguna
2. Solusi Jaringan Cloud Computing

   Beberapa solusi jaringan yang umum digunakan dalam lingkungan cloud computing adalah:
   a. Virtual Private Cloud (VPC)
      - Menyediakan jaringan virtual terisolasi di dalam cloud provider
      - Memungkinkan kontrol penuh terhadap blok IP, tabel routing, dan firewall
   b. Software-Defined Networking (SDN)
      - Memisahkan kontrol dan forwarding plane pada jaringan
      - Memungkinkan otomasi dan pemrograman jaringan secara dinamis
   c. Jaringan Overlay
      - Membangun jaringan virtual di atas infrastruktur jaringan fisik
      - Menyediakan konektivitas yang fleksibel dan abstraksi dari jaringan fisik
   d. Content Delivery Network (CDN)
      - Mendistribusikan konten secara global melalui jaringan server yang tersebar
      - Meningkatkan kecepatan akses dan mengurangi beban pada sumber asal
3. Melakukan Setting IP

   Berikut adalah langkah-langkah untuk melakukan setting IP pada perangkat jaringan:
   a. Agar semua perangkat jaringan terhubung harus menghubungkan perangkat dengan menggunakan kabel dengan ketentuan sebagai berikut:
      - Hubungkan Server dengan Cloud menggunakan kabel Straight
      - Hubungkan Cloud dengan DSL-Modem menggunakan kabel Phone
      - Hubungkan DSL-Modem dengan Switch menggunakan kabel Cross
      - Hubungkan Switch dengan PC 1-3 menggunakan kabel Straight
      - Hubungkan AccesesPoinPT dengan Switch menggunakan kabel Straight
      - Hubungkan AccessesPoinPT dengan 1-3 PC menggunakan Jaringan Wireles yang sudah di Setting
      - Hubungkan lagi AccessesPoinPT dengan 1-3 PC menggunakan Wireles yang sudah di

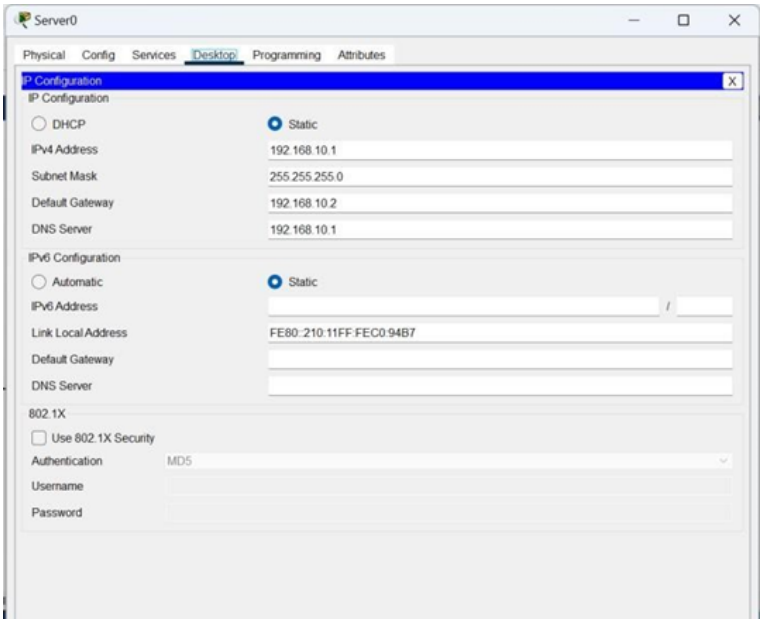
Setting



Perangkat yang digunakan:

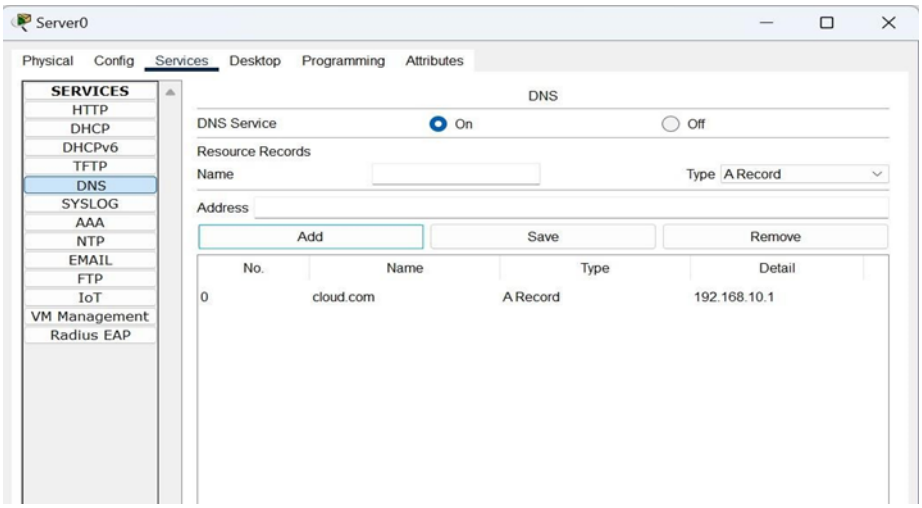
- 9 Pc
- 1 server
- 1 Cloud
- 1 DSL Modem
- 1 Switch
- 2 AccessesPointPT

4. Melakukan Setting IP
   Server
   IP Configurasi Server
   IP address: 192.168.10.1
   IP Default: 192.168.10.2
   DNS Server: 192.168.10.1

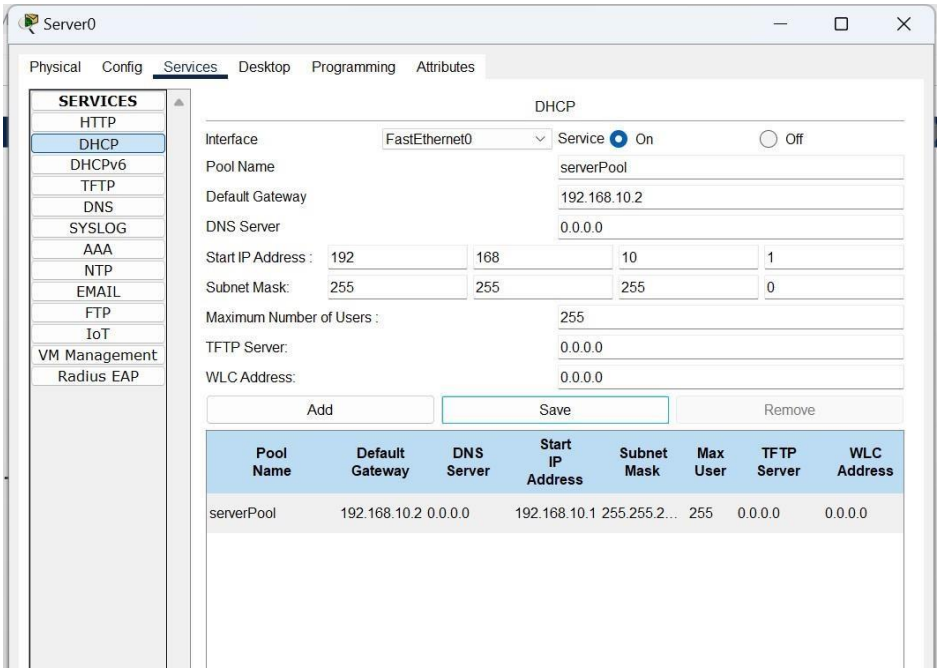


Services
DNS: masukkan pada Name cloud.com

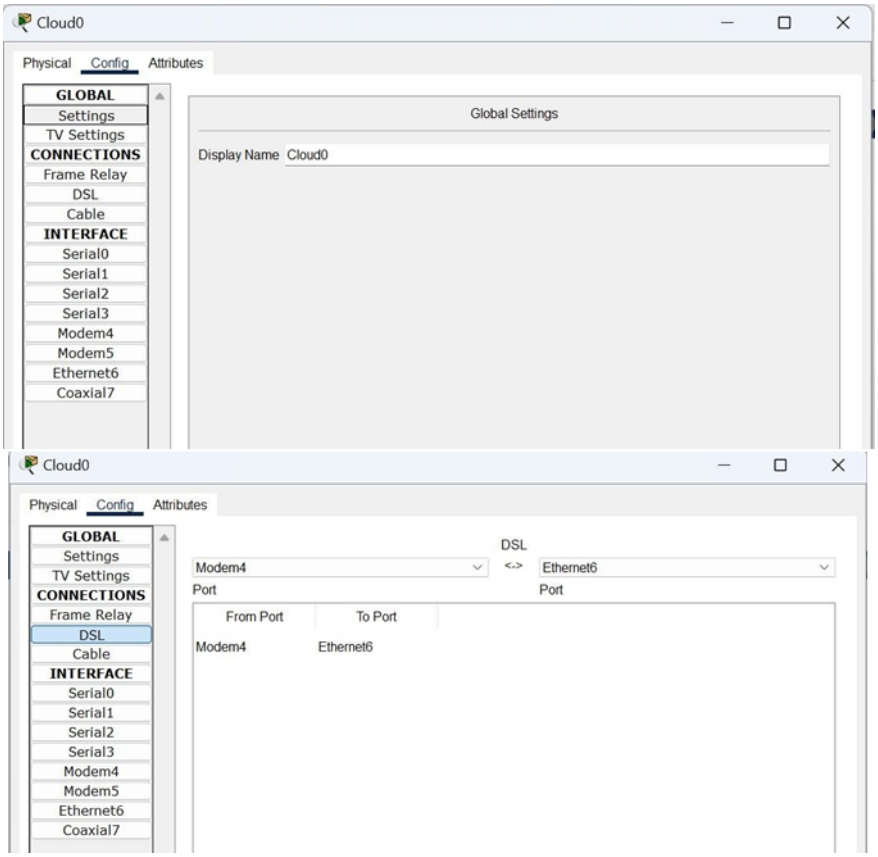
Addres: 192.168.10.1 lalu ADD



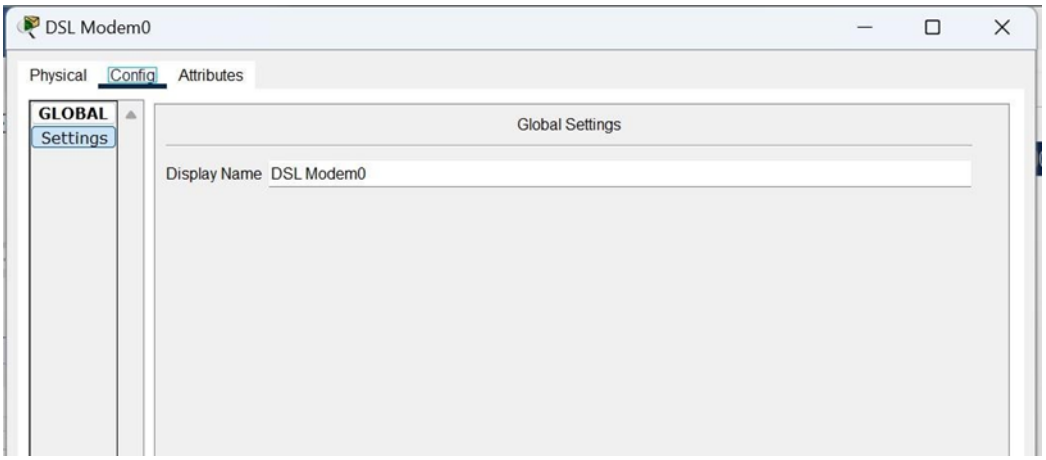
Pada DHCP ON pada Service masukkan id server
Pool 192.168.10.2, Lalu ADD



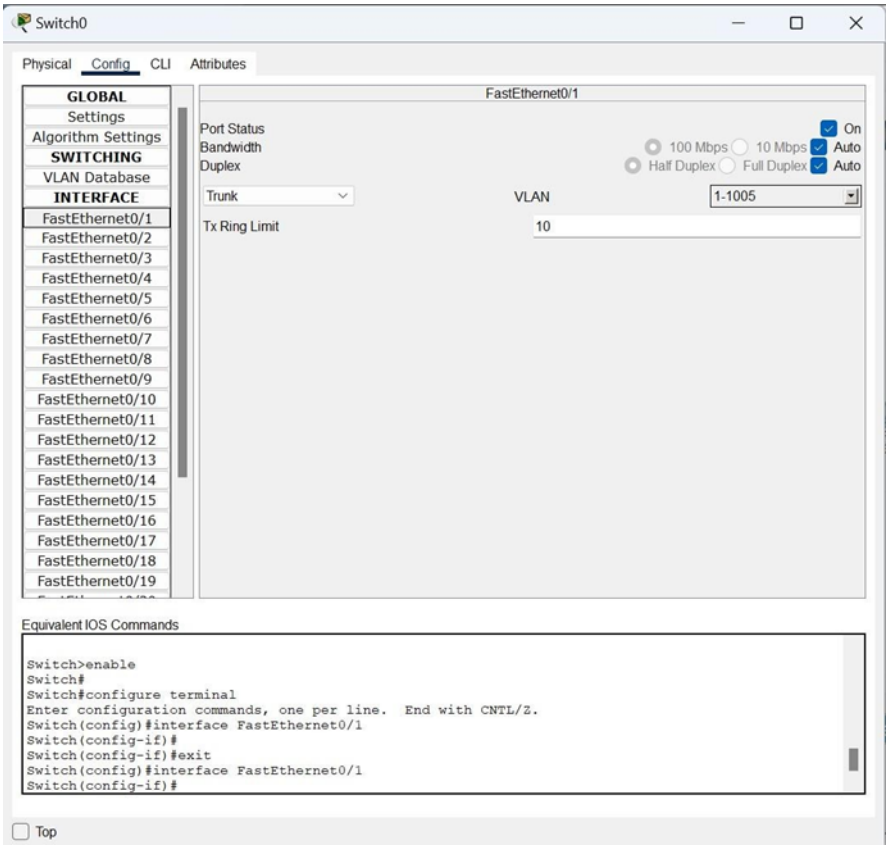
5. Cloud
   Berikut setting pada cloud:



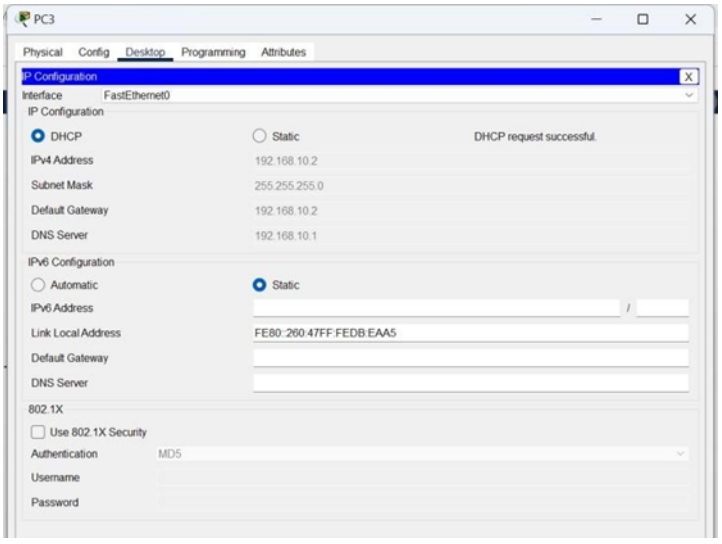
6. DSL Modem



7. Switch

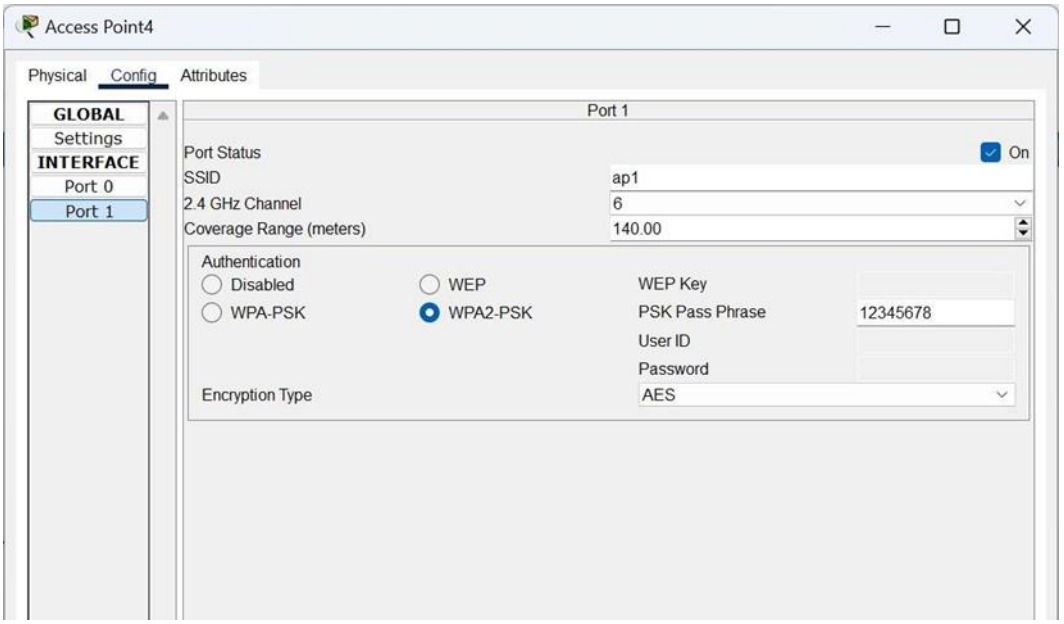


8. PC 1-3 pada Switch



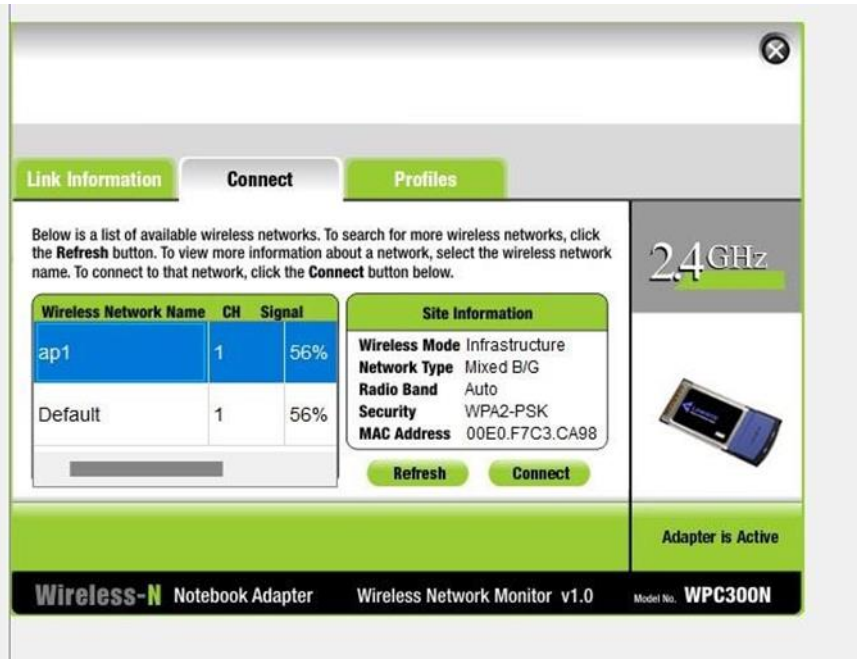
9. Acces Point Jaringan Wireles Pada PC
   Centang Auto pada Port 0

Lalu pada potr 1 centang On pada Ports Status
Pilih WPA2-PSK pada Authentication

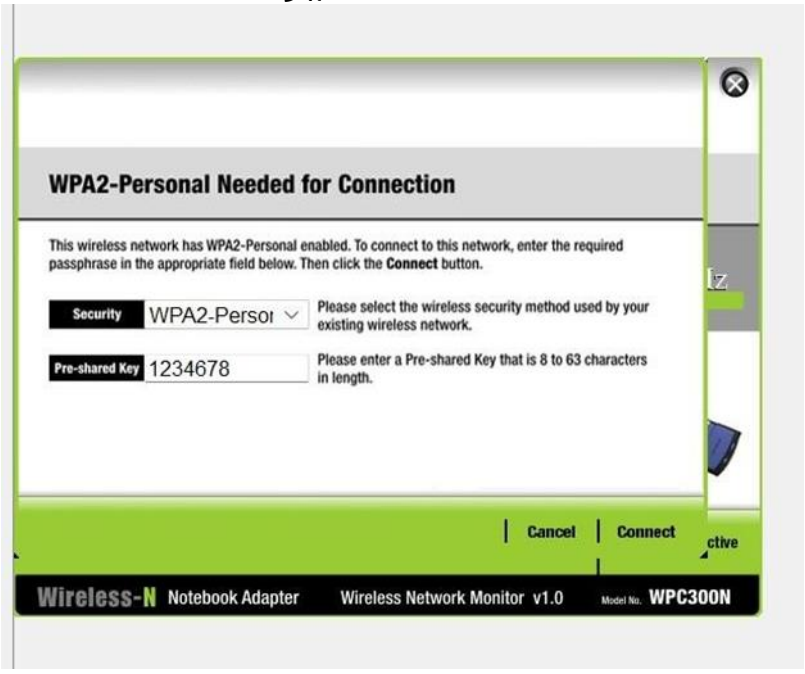


10. PC Pada Jaringan Wireles

Buka pada Desktop lalo pili WIRELES untuk mengaktifkan jaringan pada wireless lalu Refresh untuk melihat Wireles Networknya Pilih apt1 lalu Connect



Jika sudah Connect Masukan Pass 123478



Pembahasan

Hasil Penelitian ini mengeksplorasi manfaat dan pertimbangan keamanan dari mengadopsi pendekatan cloudnative untuk pengembangan dan penerapan aplikasi. Temuan ini menekankan pentingnya merancang sistem cloud-native yang tangguh, dapat diamati, dan aman untuk mendukung kebutuhan bisnis modern. Beberapa poin penting dari pembahasan ini adalah:

1. Solusi Jaringan Cloud Computing

Beberapa solusi jaringan yang umum digunakan dalam lingkungan cloud computing adalah:

- Virtual Private Cloud (VPC)
- Menyediakan jaringan virtual terisolasi di dalam cloud provider
- Memungkinkan kontrol penuh terhadap blok IP, tabel routing, dan firewall

2. Pentingnya Konfigurasi yang Tepat

   Keberhasilan Mengkonfigurasi jaringan untuk mendukung desain aplikasi cloud-native
- Memastikan konektivitas antar layanan mikro dan dengan layanan eksternal
- Menerapkan keamanan jaringan yang sesuai, seperti firewall, VPN, dan autentikasi -Otomasi dan Orchestration
- Menggunakan alat orchestration, seperti Kubernetes, untuk mengelola kontainer dan jaringan
- Mengotomasi proses deployment, scaling, dan pemulihan jaringannative.

3. Ketahanan Cloud-Native
- Mengkonfigurasi jaringan untuk mendukung desain aplikasi cloud-native
- Memastikan konektivitas antar layanan mikro dan dengan layanan eksternal
- Menerapkan keamanan jaringan yang sesuai, seperti firewall, VPN, dan autentikasi

Implikasi Praktis

Implementasi Sistem cloud-native memanfaatkan mode layanan cloud sepenuhnya. Dirancang untuk berkembang dalam lingkungan cloud virtual yang dinamis, sistem ini memanfaatkan infrastruktur komputasi dan layanan terkelola Platform as a Service (PaaS) secara ekstensif. Mereka memperlakukan infrastruktur yang mendasarinya sebagai sekali pakai - diprovisikan dalam hitungan menit dan diubah ukurannya, diskalakan, atau dihancurkan sesuai permintaan – melalui automasi.

Rekomendasi

Untuk meningkatkan efektivitas deteksi dan respon terhadap ancaman dari dalam, organisasi disarankan untuk:

1. Pengembangan Kebijakan Keamanan yang Kuat:
- Buat kebijakan keamanan yang komprehensif mencakup identifikasi aset, klasifikasi data, protokol akses, manajemen identitas dan akses, pemantauan, dan respons insiden.
- Pastikan kebijakan diselaraskan dengan standar dan regulasi industri yang relevan.
- Terapkan prinsip privilese minimum dan segregasi tugas dalam kebijakan.

2. Pelatihan dan Edukasi:
- Lakukan pelatihan keamanan secara berkala bagi staf IT dan pengguna akhir.
- Topik pelatihan dapat mencakup kesadaran ancaman, praktik keamanan terbaik, penggunaan alat keamanan, dan prosedur pelaporan insiden.
- Dorong budaya keamanan di seluruh organisasi melalui komunikasi yang konsisten dan contoh dari manajemen puncak.

3. Pemeliharaan Berkala:
- Terapkan pembaruan dan patch keamanan secara teratur pada semua komponen sistem cloud-native.
- Lakukan pengujian kerentanan dan analisis risiko secara berkala untuk mengidentifikasi dan mengatasi celah keamanan.
- Perbaharui kebijakan, prosedur, dan rencana tanggap darurat sesuai dengan perubahan ancaman dan teknologi.

4. Lapisan Keamanan Bertahap:
   - Terapkan kontrol keamanan ganda, seperti otentikasi multi-faktor, enkripsi data, dan pemantauan aktivitas.
   - Implementasikan solusi keamanan spesifik untuk komponen cloud-native, seperti WAF untuk aplikasi web, SIEM untuk pemantauan, dan firewall virtual untuk jaringan.
   - Integrasikan solusi keamanan cloud-native dengan sistem keamanan organisasi yang lebih luas.

5. Otomasi dan Orchestration:
   - Terapkan otomasi untuk proses-proses keamanan, seperti penyebaran konfigurasi aman, pembaruan, dan respons insiden.
   - Integrasikan alat keamanan dengan platform orchestration cloud-native untuk meningkatkan visibilitas dan respons yang cepat.
   - Manfaatkan kemampuan cloud-native untuk skalabilitas dan ketahanan solusi keamanan.

6. Pemantauan dan Respons Insiden:
   - Terapkan solusi SIEM (Security Information and Event Management) untuk pemantauan dan analisis aktivitas sistem cloud-native.
   - Bangun proses respons insiden yang terdefinisi dengan baik untuk mendeteksi, menganalisis, dan mengatasi insiden keamanan dengan cepat.
   - Lakukan simulasi insiden secara berkala untuk menguji dan memperbaiki rencana tanggap darurat.

Pembahasan penelitian ini mengeksplorasi manfaat dan pertimbangan keamanan dari mengadopsi pendekatan cloud-native untuk pengembangan dan penerapan aplikasi. Temuan ini menekankan pentingnya merancang sistem cloud-native yang tangguh, dapat diamati, dan aman untuk mendukung kebutuhan bisnis modern.

KESIMPULAN DAN SARAN

Kesimpulan

1. Efektivitas keamanan jaringan cloud-native merupakan suatu kebutuhan yang sangat penting dalam era digital saat ini, di mana aplikasi dan data dapat diakses dari mana saja dan kapan saja.
2. Cloud-Native memungkinkan pengembangan aplikasi yang lebih cepat dan efisien dengan menggunakan kontainer dan layanan mikro, namun hal ini juga memerlukan strategi keamanan yang lebih efektif.
3. Solusi keamanan cloud-native harus dapat menghadapi tantangan-tantangan keamanan yang terkait dengan penggunaan cloud computing, seperti manajemen identitas dan akses, keamanan jaringan, dan investigasi serta respons otomatis.
4. Keamanan jaringan cloud-native harus dapat memberikan perlindungan yang lebih baik dan fleksibel untuk aplikasi dan data yang berada di lingkungan cloud.

Saran

1. Organisasi perlu mengembangkan kebijakan keamanan yang komprehensif dan selaras dengan standar industri untuk melindungi aset dan data cloud-native.
2. Pelatihan dan edukasi keamanan secara berkala bagi staf IT dan pengguna akhir sangat penting untuk meningkatkan kesadaran dan praktik keamanan yang baik.
3. Penerapan pemeliharaan berkala, seperti pembaruan keamanan, pengujian kerentanan,

dan pembaruan rencana tanggap darurat, harus dilakukan secara disiplin.

4. Implementasi lapisan keamanan bertahap, otomasi, dan orchestration dapat meningkatkan efektivitas dan ketangguhan solusi keamanan cloud-native.
5. Pemantauan dan respons insiden yang kuat, didukung oleh solusi SIEM dan proses respons insiden yang terdefinisi dengan baik, sangat penting untuk mendeteksi dan mengatasi ancaman secara cepat.

Dengan menerapkan rekomendasi ini, organisasi dapat membangun keamanan jaringan cloud-native yang komprehensif, adaptif, dan terintegrasi untuk melindungi aplikasi dan data dari ancaman-ancaman yang ada.

DAFTAR PUSTAKA

Y. Fauziah, C. Computing, and S. S. On, "Tinjauan keamanan sistem pada teknologi cloud computing," *J. Inform.*, vol. 8, no. 1, pp. 870–883, 2014.

S. Farizy and E. S. Eriana, *Cloud Computing Komputasi Awan*, no. 1. 2011.

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

Wahono, "Penggunaan Framework Cisco," pp. 15–16, 2014, [Online]. Available: https://www.neliti.com/id/publications/170628/penggunaan-framework- ciscosebagai-kerangka-penerapan-teknologi-cloud-computing

M. Syamsu and W. Widodo, "Layanan Berbasis Cloud Untuk Infrastruktur Jaringan Mobile First – Iot – Cloud Native Versi Aruba," *J. Sist. Inf.*, vol. 2, no. 2, pp. 1–13, 2021, doi: 10.32546/jusin.v2i2.1493.