RANCANG BANGUN KEAMANAN TRANSFER DATA VOIP MENGGUNAKAN VPN PADA TRIXBOX DI UNIVERSITAS SATYA NEGARA INDONESIA

Meri Kristina Br Sinuraya, Berlin S
merysinuraya158@gmail.com, sitorus1970@gmail.com
Fakultas Teknik, Universitas Satya Negara Indonesia

ABSTRAK

Universitas Satya Negara Indonesia (USNI) berdiri sejak 1989 dan di naungi oleh Yayasan Abdi Karya (YADIKA). Sebagai salah satu perguruan tinggi, sistem komunikasi yang di gunakan karyawan, staff dan pegawai di USNI masih menggunakan telepon kabel untuk alat komunikasi di lingkungannya. Dalam penggunaan telepon kabel biaya setiap panggilan masih terbilang mahal, dan tidak seperti penggunaan VoIP. Penggunaan VoIP sangat menguntungkan, namun keamanan pada sistem ini kurang diperhatikan, karena transfer data pada VoIP berbasis IP maka mudah di sadap dan dapat dilakukan perekaman data VoIP. Jika data yang ditangkap ternyata rahasia maka akan sangat merugikan, bahkan bisa disalahgunakan. Hal ini menyebabkan kurangnya kemanan dan privasi pengguna VoIP. Dari Masalah tersebut penulis tertarik untuk melakuan penelitian dengan merancang dan membangun jaringan VoIP ini dengan menggunakan TrixBox berikut juga pengamanannya dengan menggunakan jaringan VPN
Kata kunci : VOIP, VPN, Transfer Data, Trixbox

ABSTRACT

Satya Negara Indonesia University (USNI) was founded in 1989 and is under the auspices of the Abdi Karya Foundation (YADIKA). As a tertiary institution, the communication system used by employees, staff and employees at USNI is still using landlines for communication tools in their environment. In the use of landline telephony the cost of each call is relatively expensive, and unlike the use of VoIP. The use of VoIP is very profitable, but the security of this system has not been given attention, because the data transfer on VoIP is IP-based, it is easy to tap and VoIP data recording can be done. If the data captured is classified as confidential, it will be very detrimental, it can even be misused. This results in a lack of security and privacy for VoIP users. From this problem the authors are interested in conducting research by designing and building this VoIP network using TrixBox along with its security using a VPN network
Keywords: VOIP, VPN, Data Transfer, Trixbox

PENDAHULUAN

Latar Belakang

VoIP (Voice Over Internet Protocol) merupakan suatu sistem yang menggunakan jaringan internet untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan media protokol IP. VoIP bekerja dengan mengubah sinyal analog menjadi sinyal digital. Penggunaan jaringan IP menghemat biaya karena tidak perlu membangun infrastruktur baru untuk komunikasi suara dan penggunaan bandwidth lebih kecil dibanding telepon konvensional.

Universitas Satya Negara Indonesia (USNI) berdiri sejak 1989 dan di naungi oleh Yayasan Abdi Karya (YADIKA). Sebagai salah satu perguruan tinggi, sistem komunikasi yang di gunakan karyawan, staff dan pegawai di USNI masih menggunakan telepon kabel untuk alat komunikasi di lingkungannya. Dalam penggunaan telepon kabel biaya setiap panggilan masih terbilang mahal, dan tidak seperti penggunaan VoIP. Penggunaan VoIP sangat menguntungkan, namun keamanan pada sistem ini kurang diperhatikan, karena transfer data pada VoIP berbasis IP maka mudah di sadap dan dapat dilakukan perekaman data VoIP. Jika data yang ditangkap ternyata rahasia maka akan sangat merugikan, bahkan bisa disalahgunakan. Hal ini menyebabkan kurangnya kemanan dan privasi pengguna VoIP.

Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka penulis merumuskan beberapa pokok masalah yang diteliti adalah Bagaimana membangun system komunikasi VoIP menggunakan server Trixbox ?

Batasan Masalah

Agar lebih mengarah dan tidak menyimpang dari penelitian, maka penelitian ini dibatasi sebagai berikut :

1. System komunikasi VoIP dibangun menggunakan server Trixbox
2. Rancangan Keamanan Transfer Data VoIP ini, hanya menggunakan jalur VPN (Virtual Private Network).
3. Pengujian QoS pada system VoIP yang dibangun

Tujuan Penelitian

Tujuan dilakukannya Penelitian Tugas Akhir ini adalah Melakukan Rancang Bangun Keamanan Transfer Data *VoIP* Menggunakan *VPN* Pada *Trixbox* di Universitas Satya Negara Indonesia

Manfaat Penelitian

Adapun manfaat yang dapat diambil dari penelitian ini adalah :

1. Dapat membangun komunikasi system VoIP dengan server Trixbox
2. Mengamankan jalur komunikasi antar client dengan VPN (Virtual Privat Network)
3. Dapat menghemat biaya panggilan komunikasi

Metode Penelitian

Dalam penyusunan penelitian Tugas Akhir ini, penulis menggunakan beberapa metode penulisan yaitu :

1. Metode Observasi
   Metode observasi merupakan metode pengumpulan data dengan melakukan pengamatan langsung terhadap obyek yang diteliti dengan instansi terkait dengan mengumpulkan data dan informasi yang berkaitan dengan permasalahan yang ada.
2. Metode Wawancara
   Metode pengumpulan data dengan melakukan Tanya jawab kepada kepala bagian IT server di USNI, untuk memperoleh data dan informasi yang diperlukan, khususnya yang berhubungan komunikasi VOIP yang digunakan sehingga akan memperoleh data dan informasi yang lebih akurat. Jenis

wawancara yang digunakan adalah wawancara tidak terstruktur, dengan susunan pertanyaan dan susunan kata – kata dalam setiap pertanyaan dapat diubah pada saat wawancara

Tinjauan Pustaka

Pada penelitian ini diperlukannya tinjauan pustaka sebagai pendukung dalam penelitian ini, beberapa topik yang berkaitan dengan penulisan penelitian ini adalah:

1. "Rancang Bangun Keamanan Transfer Data VoIP Over VPN Pada Sistem Opensource Trixbox". VoIP merupakan suatu sistem yang menggunakan jaringan internet untuk mengirimkan paket data suara dari suatu tempat ke tempat yang lain menggunakan protokol IP. VoIP dapat mengurangi biaya panggilan hingga 70%. Namun terdapat beberapa masalah yang dialami ketika menggunakan VoIP, salah satunya transfer data yang lewat pada jaringan dapat disalahgunakan, dan dibajak. Oleh karenanya untuk mengamankan paket yang lewat maka digunakan teknologi VPN (Virtual Privat Network). VPN mempunyai dua teknik pengamanan yaitu IPSec dan Cripto IP Encapculation. Untuk mengatasi penyadapan pada penggunaan VoIP maka dilakukan penambahan VPN server pada Trixbox, serta penambahan VPN client pada sisi client VoIP, sehingga trafik VoIP dilewatkan melalui jaringan VPN. Penggunaaan VPN ini menjadikan sistem VoIP aman karena adanya enkripsi dan autentikasi antara client dan server.
2. (Azhar, Badrul, & Akmaludin, 2018) "Penerapan Voice Over Internet Protokol (VoIP) Untuk Optimalisasi Jaringan Pada Badan Kependudukan dan Keluarga Berenca Nasional". BKKBN merupakan lembaga pemerintah yang bertugas untuk mewujudkan keluarga berencana dan keluarga sejahtera. Dalam melaksanakan tugasnya salah satu hal yang menunjang keberhasilan program ini adalah kelancaran komunikasi. Adapun masalah yang dialami oleh BKKBN adalah kurang optimalnya jaringan komunikasi dari pusat BKKBN dengan wilayah Indonesia bagian timur, yaitu Maluku Utara dan Papua Barat. Hal ini di sebabkan karena wilayah tersebut masih menggunakan telepon konvensional sebagai alat komunikasinya.Untuk melakukan optimalisasi jaringan tersebut maka BKKBN harus menerapkan implementasi jaringan VoIP. Dan untuk keamanannya BKKBN Pusat menggunakan teknologi VPN (Virtual Privat Network). Dengan begitu semua percakapan yang dilakukan BKKBN akan terjamin keamanannya.

VOIP (Voice Over Internet Protocol)

VoIP dikenal juga dengan sebutan IP Telephony didefinisikan sebagai suatu sistem yang menggunakan jaringan internet sebagai media transport informasi/data. Informasi VoIP dibawa melalui media IP, bukan media telephony (Kristalina, 2015).

Sejarah VoIP

Sejarah Perkembangan teknologi VoIP dimulai dari penemuan telepon pada tahun 1876 oleh Alexander Graham Bell. Kemudian dikembangkan lagi teknologi PSTN (Public Switched Telephone Network) yang sudah berkembang sampai sekarang. Beberapa tahun kemudian mulai berkembang teknologi yang baru. Pembuatan Personal Computer (PC) secara massal, system komunikasi telepon selular dan system berdasarkan jaringan internet.

Teknologi VoIP diperkenalkan setelah internet mulai berkembang sekitar tahun 1995. Ini dimulai dengan perusahaan seperti Vocaltech dan kemudian pada akhirnya diikuti oleh Microsoft dengan program Netmeeting-nya.

Untuk di Indonesia komunitas pengguna dan pengembang VoIP di masyarakat, berkembang di tahun 2000. Komunitas awal pengguna dan pengembang VoIP adalah "VoIP Merdeka" yang dicetuskan oleh pakar internet Indonesia, Onno W. Purbo. Teknologi yang digunakan adalah H.323 yang merupakan teknologi awal VoIP. Sentral VoIP Merdeka di hosting di Indonesia Internet Exchange (IIX) atas dukungan beberapa ISP dan Asossiasi Penyelenggara Jaringan Internet (APJII). Di tahun 2005, Anton Raharja dan tim dari ICT Center Jakarta mulai mengembangkan VoIP jenis baru berbasis Session

Initiation Protocol (SIP). Teknologi SIP merupakan teknologi pengganti H.323 yang sulit menembus proxy server. Di tahun 2006, infrastruktur VoIP SIP di kenal sebagai VoIP Rakyat.

Kualitas Jaringan VoIP

VoIP merupakan salah satu jenis layanan realtime yang membutuhkan QoS (Quality of Service). Beberapa faktor yang memengaruhi Qos adalah:

1. Delay

   Delay merupakan waktu yang dibutuhkan untuk mengirimkan suatu paket data dari sumber ke penerima . Berikut adalah standar delay berdasarkan ITU (International Communication Union)

Table 1 Kualitas *Delay*

Kategori Delay	Besar Delay
Sangat Bagus	< 150 ms
Bagus	150 s/d 300 ms
Jelek	300 s/d 450 ms
Sangat Jelek	> 450 ms

Semakin besar *delay* yang dihasilkan maka semakin rendah kualitas VOIP yang di hasilkan. *Delay* dapat di hitung dengan rumus sebagai berikut *:*

$$\text{Rata -rata Delay} = \frac{\text{Total Delay}}{\text{Total Paket Yang Diterima}}$$

Gambar 1. Rumus Delay

2. Packet Loss

   Packet Loss merupakan ukuran eror dari transmisi paket data. Berikut adalah standar Packet Loss berdasarkan ITU (International Communication Union)

Table 2. Kualitas Packet Loss

Kategori Packet Loss	Packet Loss
Baik	0 - 1 %
Cukup	1 - 5 %
Buruk	> 10 %

Berikut adalah rumus untuk menghitung Packet Loss :

$$\text{Packet Loss} = \frac{\text{P. Data yang dikirim - P. Data yang diterima}}{\text{Paket Yang Dikirim}} \times 100\%$$

Gambar 2 Rumus Pakcet Loss

3. Throughput

   Throghput merupakan kecepatan rata rata data dalam selang waktu tertentu. Berikut adalah standar Packet Loss berdasarkan ITU (International Communication Union)

Table 3. Kualitas Throughput

Kualitas Throughput	Throughput
Sangat Bagus	100
Bagus	75
Cukup	50
Buruk	<25

Berikut adalah rumus untuk menghitung *Throughput :*

$$\text{Throughput} = \frac{\text{Jumlah Data yang Dikirim}}{\text{Waktu Pengiriman Data}}$$

Gambar 3 Rumus *Throughput*

Protokol VoIP

Protokol jaringan yang digunakan untuk mengimplementasikan VoIP meliputi :

1. H.323

Protokol H.323 merupakan suatu standar ITU-T (International Telecomunications Union – Telecomunications) yang menentukan komponen protokol, dan prosedur yang menyediakan layanan komunikasi multimedia, yaitu komunikasi audio, video dan data real-time (waktu nyata), melalui jaringan berbasis paket (packet-based network).

2. Media Gateway Control Protocol (MGCP)
3. MGCP ialah protokol yang digunakan untuk signaling dan call control yang digunakan dalam sistem VoIP yang terdistribusi.
4. Session Initiation Protocol (SIP)
   SIP merupakan signaling protocol, banyak digunakan untuk membangun dan memutus sesi komunikasi multimedia seperti panggilan suara dan video melalui internet. Protokol ini dapat digunakan untuk membuat, mengubah dan mengakhiri sesi unicast atau multicast yang terdiri dari satu atau beberapa media stream.
5. Real-time Transport Protocol (RTP)
   Real-time Transport Protocol (RTP) didefinisikan sebagai standarisasi paket untuk mengirimkan audio dan video pada jaringan IP. RTP digunakan untuk komunikasi dan sistem entertain yang termasuk didalamnya streaming media seperti telepony, aplikasi video teleconfrence dan web yang memiliki fitur berbasis push-to-talk.
6. Session Description Protocol (SDP)
   Session Description Protocol adalah sebuah protokol yang mempunyai fungsi untuk memberikan deskripsi terhadap suatu sesi multimedia. Secara umum, protocol SDP digunakan pada saat melakukan session announcement serta session invitation. Informasi yang diberikan oleh sebuah pesan SDP antara lain adalah nama session dan tujuan penggunaan session, waktu aktif dari sebuah session, jenis media yang digunakan (audio,video), format media (3GP, MPEG4 ,dsb) dan informasi untuk menerima media tersebut (alamat, port).

VPN (Virtual Private Network)

Virtual Private Network atau biasa disebut VPN adalah Sebuah teknologi komunikasi yang memungkinkan dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. VPN merupakan koneksi virtual yang bersifat private, dikarenakan jaringan yang dibuat tidak nampak secara fisik hanya berupa jaringan virtual, dan jaringan tersebut tidak semua orang dapat mengaksesnya sehingga sifatnya private. (Oktivasari & Utomo, 2016).

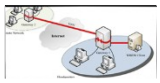
Fungsi utama VPN

Teknologi VPN menyediakan beberapa fungsi utama bagi penggunanya, diantaranya :

a. Confidentially (kerahasiaan)
   Inti utama dari penyadapan ini adalah usaha untuk menjaga informasi dari orang – orang yang tidak berhak mengakses. Privacy lebih kearah data – data yang sifatnya prifat. Serangan terhadap aspek Privacy misalnya usaha untuk melakukan peyadapan.
b. Data integrity (Keutuhan Data)
   Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan house, atau pemakai alat lain yang mengubah informasi tanpa izin. Sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.
c. Origin Autenthication (Autentikasi Sumber)
   Untuk menguji identitas dari perusahaan lain yang hendak melakukan transaksi.
d. Non- Repudiation
   Untuk mencegah adanya kecurangan di antara salah satu pihak, misalnya tidak mengakui bahwa mereka telah mengirim ataupun menerima sebuah file.
e. Kendali Akses
   Bagi yang tidak memiliki hak maka tidak akan bisa mengakses ke jaringan ini

Jenis – jenis Jaringan VPN

1. Access VPN
   Access VPN atau Virtual Private Dial-Up Network (VPDN) adalah koneksi user-to-LAN yang digunakan untuk koneksi ke jaringan dari berbagai lokasi remote. Remote Access VPN memungkinkan pekerja untuk mengakses data-data dan segala sumber daya dimanapun mereka berada.
2. Intranet VPN
   Intranet VPN atau site to site VPN merupakan VPN yang digunakan untuk menghubungkan antara kantor pusat suatu perusahaan dengan kantor cabang atau kantor pembantu melalui shared network menggunakan koneksi yang permanen (dedicated). Tujuan penggunaan intranet VPN agar administrative control berada sepenuhnya di bawah satu kendali.
3. Extranet VPN
   Extranet VPN merupakan VPN yang digunakan untuk menghubungkan antara kantor dengan pihak luar seperti pelanggan, suplier, rekan bisnis, atau suatu komunitas ke dalam jaringan internal dengan menggunakan koneksi Dedicated. Dengan adanya Extranet VPN perusahaan-perusahaan yang terlibat dapat berkomunikasi serta bertukar informasi secara cepat, mudah, tapi dalam sistem keamanan yang terjamin.



Gambar 2. Jaringan VPN

Keamanan Jaringan

Keamanan jaringan adalah proses untuk mengidentifikasi dan mencegah pengguna yang tidak sah dari suatu jaringan komputer. Tujuannya tentu saja untuk mengantisipasi resiko ancaman berupa perusakan bagian fisik komputer maupun pencurian data seseorang. (Dwiki, 2015). Dilihat dari lubang keamanan yang ada pada suatu sistem, keamanan dapat diklasifikasikan menjadi empat macam:

a. Keamanan Fisik (Physical Security)
   Keamanan yang meliputi seluruh sistem beserta peralatan, peripheral, dan media yang digunakan. Biasanya seorang penyerang akan melakukan wiretapping (proses pengawasan dan penyadapan untuk mendapatkan password agar bisa memiliki hak akses). Dan jika gagal, maka DOS (Denial Of Service) akan menjadi pilihan sehingga semua service yang digunakan oleh komputer tidak dapat bekerja.
b. Keamanan Data dan Media
   Pada keamanan ini penyerang akan memanfaatkan kelemahan yang ada pada software yang digunakan untuk mengolah data. Biasanya penyerang akan menyisipkan virus pada komputer target melalui attachment pada e-mail.
c. Keamanan Dari Pihak Luar
   Biasanya orang yang melakukan social engineering akan menyamar sebagai orang yang memakai sistem dan lupa password, sehingga akan meminta kepada orang yang memiliki hak akses pada sistem untuk mengubah atau mengganti password yang akan digunakan untuk memasuki s istem tersebut.
d. Keamanan dalam Operasi
   Merupakan salah satu prosedur untuk mengatur segala sesuatu yang berhubungan dengan sistem keamanan pasca serangan. Dengan demikian, sistem tersebut dapat berjalan baik atau menjadi normal kembali. Biasanya para penyerang akan menghapus seluruh log-log yang tertinggal pada sistem target (log cleaning) setelah melakukan serangan.

Analisis

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini. Metode yang biasa digunakan antara lain

a. Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah/operator agar mendapatkan data yang konkrit dan lengkap.

b. Survey langsung kelapangan, pada tahap analisis juga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya
c. Membaca manual atau blueprint dokumentasi, pada analysis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya.
d. Menelaah setiap data yang didapat dari data-data sebelumnya, maka perlu dilakukan analisa data tersebut untuk masuk ke tahap berikutnya

Design

Pada tahap design akan dibuat gambar desain topologi jaringan interkoneksi yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun.

Simulation Prototype

Beberapa pekerja jaringan akan membuat dalam bentuk simulasi dengan bantuan tools khusus di bidang network .Hal ini dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work lainnya.

Implementation

Dalam implementasi akan diterapkan semua yang telah direncanakan dan didesain sebelumnya. Tahap ini menentukan gagal tidaknya suatu proyek.

Monitoring

Pada tahap ini akan dilakukan monitoring terhadap sistem yang telah dibuat

Management

Pada tahap ini akan diperhatikan secara khusus jaringan yang telah dibuat

TrixBox

Trixbox adalah sebuah VoIP server yang dibuat menjadi satu dengan system operasi yaitu LINUX Centos. Trixbox bersifat open source yang artinya setiap orang dapat mengetahui source code programnya dan memperolehnya secara gratis. Trixbox cocok digunakan untuk pengguna rumahan maupun lembaga. Trixbox dapat membuat sebuah jaringan VOIP, melakukan komunikasi jarak jauh, dan jaringan jangkauan pada trixbox luas. (Firmansyah, 2018)

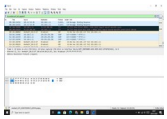
Gambar 3. Tampilan trixbox

Fungsi TrixBox

Untuk membuat jaringan VoIP , melakukan komunikasi jarak jauh serta berguna untuk jaringan yang luas dan memiliki fitur yang lengkap

Wireshark

Wireshark merupakan salah satu dari tool Network Analyzer yang biasa digunakan oleh Network Administrator pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan. Wireshark dipakai oleh network administrator untuk menganalisa kinerja jaringannya. Wireshark mampu menangkap paket-paket data atau informasi yang berjalan dalam jaringan yang terlihat dan semua jenis informasi ini dapat dengan mudah dianalisa yaitu dengan memakai sniffing , dengan sniffing diperoleh informasi penting seperti password email account lain.



Gambar 4. *Tampilan wireshark*

3CX Phone

3CX Phone adalah aplikasi pendukung VoIP yang memungkinkan untuk mengirim pesan, dan melakukan panggilan suara dan video. (Putra, 2017)

Gambar 5. *Tampilan 3CX Phone*

OpenVPN

OpenVPN merupakan salah satu aplikasi berbasis open source untuk membuat koneksi encrypted tunnels secara virtual dengan menggunkaan authenticate dengan yang lainnya menggunakan pre- shared secret - key, certificate, atau username.

Analisa Metode Pengembangan Sistem

Metode pengembangan system merupakan prosedur, cara dan aturan aturan yang digunakan untuk mengembangkan suatu system. Penulis menggunakan metode NDLC karena metode ini paling sesuai dengan penelitian ini, yaitu penelitian yang berhubungan dengan jaringan membutuhkan analisis, desain, simulasi prototyping, imlementasi, monitoring, dan management. Berikut adalah pengembangan jaringan VOIP dengan VPN sebagai keamanannya menggunakan metode NDLC (Network Development Life Cycle) pada Universitas Satya Negara Indonesia

Perangkat sistem VOIP

Dalam penelitian ini dibutuhkan beberapa perangkat sistem, yang meliputi perangkat keras, perangkat lunak dan perangkat konektifitas untuk sistem VOIP

Table 4. Perangkat Keras

No	Perangkat	Satuan	Jumlah	Spesifikasi
1	Headset	Buah	1	-
2	Router	Buah	1	tp-link TL-WR940N
3	PC Server	Unit	1	Lenovo G40, Prosesor RedHat 64bit, RAM 1249MB, VGA 16Mb , Trixbox CE 2.8.0.4
4	Pc Client	Unit	1	Lenovo G40 , prosesor AMD A8 , RAM 4gb , VGA R5 graphic 2gb, windows 7 ultimate 64bit
5	HP Client	Buah	1	Samsung Galaxy J2 Pro

Tahap berikutnya adalah simulasi prototyping pada sistem VoIP yang bertujuan untuk mengsimulasikan sistem tersebut sebelum diimplementasikan. Adapun mesin virtual yang di gunakan sebagai server adalah Trixbox CE 2.8.4.0 , dan menggunakan aplikasi 3CX Phone pada client, agar bisa saling berkomunikasi. Konfigurasi pada 3CX Phone di gunakan untuk mendaftarkan nomor telepon. Berikut adalah tampilan simulasi prototype pada cisco

Gambar 6. *Tampilan simulasi prototype VOIP menggunakan cisco*

1. Simulasi Topologi Sistem VoIP
   Simulasi topologi system VoIP menggunakan Cisco Packet Tracer 7.3.0 yang bertujuan untuk mengetahui keberhasilan masing – masing perangkat keras. Pengetesan dilakukan dengan cara melakukan ping ke komponen yang terdapat pada topologi tersebut.

2. Simulasi Sistem VoIP
   Simulasi ini dilakukan terlebih dahulu pada mesin virtual, yaitu virtual Box dengan server Trixbox. Sebelum nantinya diimplementasikan secara nyata pada perangkat keras. Pada bab ini hanya akan di jelaskan proses konfigurasi dan instalansi padamesin virtual yang akan di buat.
3. Simulasi konfigurasi softphone
   Softphone yang digunakan adalah 3CX Phone. Konfigurasi softphone untuk mendaftarkan username, password user, host, dan account name

Kesimpulan

1. System komuniakasi VOIP VPN pada USNI berhasil di buat.
2. QoS (Quality of Service) dari Komunikasi VOIP ini memperoleh nilai delay 7 ms, throughput 25,868 kbps dan packet loss 0 %. Dan kamonukasi VoIP yang telah dibuat tergolong bagus.
3. Dengan menggunakan VPN sebagai keamanan, data yang dikirim melalui VoiP tidak dapat disadap dan direkam.
4. Client yang menggunakan VoIP, harus mendaftar terlebih dahulu pada server Trixbox.
5. Komunikasi VoIP dapat dilakukan jika perangkat yang digunakan terkoneksi dalam satu jaringan

Saran

Untuk penelitian berikutnya IP Server VPN diharahapkan terkoneksi dengan internet dan dapat menggantikan IP Public agar di kenal global

DAFTAR PUSTAKA

Azhar, A., Badrul, M., & Akmaludin. (2018, Maret 1). Penerapan Voice Over Internet Ptotokol (Voip) Untuk Optimalisasi Jaringan Pada Badan Kependudukan Dan Keluarga Berencana Nasional. Penerapan Voice Over Internet Ptotokol (Voip) Untuk Optimalisasi Jaringan Pada Badan Kependudukan Dan Keluarga Berencana NasionaL, 5, 1-8.

Darmawan, I. E. (2016, February). Rancang Bangun Keamanan Transfer Data Voip Over Vpn Pada Sistem Opensource Trixbox. Rancang Bangun Keamanan Transfer Data Voip Over Vpn Pada Sistem Opensource Trixbox, 1-11.

Dwiki. (2015, December). Diambil kembali dari http://mydwiki23.blogspot.com/2015/12/definisi-keamanan-jaringan-komputer.html

Firmansyah, F. A. (2018, August 18). Diambil kembali dari https://pembelajaranteknologilayananjaringan.wordpress.com/2018/08/18/mengetahui-pengertian-trixbox-fungsikelebihandan-cara-membuat-topologi-voip-dengan-trixbox-serta-menginstal-trixbox/

Kristalina, P. (2015). VOICE INTERNET OVER PROTOKOL (VOIP) : INTERNET TELEPHONY. POLITEKNIK ELEKTRONIKA NEGERI SURABAYA, 1-42.

Purniasatam. (2017, september 28). Diambil kembali dari https://catataninetkita.wordpress.com/2017/09/28/pentingnya-firewall-dalam-jaringan-komputer/

Sukaridhoto, S., Dutono, T., Harsono, N., Sarif, I., Hadi, Z. S., & Kurniawan, D. (2017). Teknik Keamanan Pada VoIP dengan Virtual Privat Networking dan Kriptografi Pada Jaringan Wireless LAN 802.11b Serta Korelasi Terhadap Bandwidth dan Intelligibility Suara . 1-7.

Widodo, C., Yana, M., & Agung, H. (2018, April). implementasi topologi hybrid untuk pengoptimalan alpikasi EDMSpada projek office PT PHE ONJW. Jurnal Teknik Informatika, 11, 1-12.