BAB III
PEMBAHASAN

3.1. Tempat dan Waktu Kerja Praktek

Kerja praktek ini dilaksanakan di :

Tempat : Pusat Data dan Informasi Departemen Pertahanan

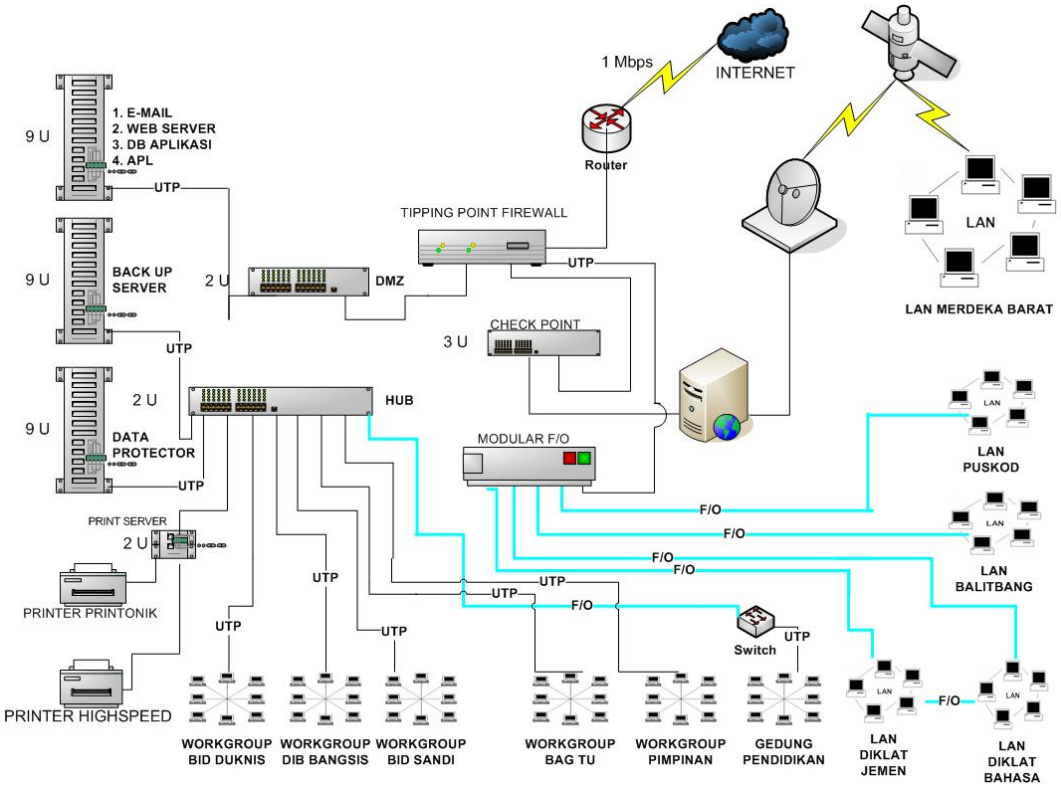
Alamat : Jln. RS. Fatmawati No. 1 Pondok Labu Jakarta Selatan

Waktu : tanggal 3 Agustus s.d 14 Agustus 2009

3.2. Job Deskripsi Kerja Praktek

Dalam melakukan kerja praktek penulis ditempatkan di Bagian Teknisi Jaringan dan konfigurasi firewall Juniper. Pada bagian teknisi jaringan ini dalam perkerjaannya adalah mengawasi jaringan pada Pusdatin Dephan ini agar selalu berjalan dengan baik tanpa ada gangguan sesuatu apapun. Selain dalam bidang jaringan penulis juga diajari bagaimana cara mensetting dan konfigurasi firewall Juniper. Firewall Juniper sendiri adalah salah satu firewall yang digunakan pada Pusdatin Dephan.

3.3. Jaringan Komputer Di Pusdatin Dephan



Gambar 3.1. Jaringan Komputer Pusdatin Dephan

Jaringan Pusat Data dan Informasi Departemen Pertahanan untuk aksesnya dilakukan dengan dua cara yaitu :

1. Dial up melalui router Dephan dengan ISP PT.Telkom dengan kecepatan ISDN 1 Mbps.
2. VPN/IP untuk komunikasi data antar jaringan LAN Dephan dari LAN Pusdatin Dephan di Pondok Labu dengan Dephan Pusat di Merdeka Barat. Kecepatan VPN/IP mencapai 1 Mbps.

Kebijakan bidang jaringan komunikasi data Pusdatin Dephan adalah Kepmen Nomor KEP/07M/XII/2004 pada tanggal 22 Desember 2004.

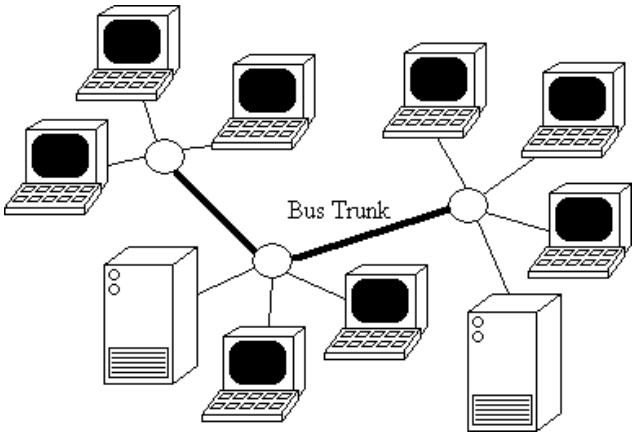
Di dalam jaringan Pusdatin Dephan juga adanya sistem pengamanan yang digunakan untuk pengamanan jaringan yaitu :

1. Fisik : antisipasi adanya petir dan antisipasi adanya kebakaran.
2. Non fisik : antivirus untuk server dan client dan anti spam.

Antivirus yang digunakan di dalam jaringan Pusdatin Dephan untuk server menggunakan Symantec dan sementara untuk client adalah sebagai berikut :

1. Mc Affe : 10%
2. Norton : 10%
3. Etrust : 20%
4. AVG : 50%
5. Interscan Antivirus : 10%

3.3.1. Topologi Yang Dipakai



Gambar 3.2. Topologi Hybrid

Pada jaringan Pusdatin Dephan topologi jaringan komputer yang dipakai adalah topologi hybrid. Di karenakan pada jaringan Pusat Data dan Informasi Departemen Pertahanan memungkinkan untuk memakai topologi hybrid karena pada tiap subnet jaringan yang memakai topologi star yang dihubungkan dengan hub/switch, topologi bus dan topologi string. Sementara itu topologi hybrid adalah gabungan dari topologi tersebut.

Dengan bentuk hubungan seperti itu, kabel yang diperlukan hanyalah sebanyak komputer dalam jaringan dan port I/O juga cukup hanya satu di setiap komputer. Sehingga banyaknya kabel link dan port I/O menjadi lebih sedikit yang berarti bahwa biaya yang dibutuhkan menjadi tidak semahal seperti pada topologi mesh.

Dalam bentuk hubungan seperti itu, kabel yang diperlukan hanyalah sebanyak komputer dalam jaringan dan port I/O juga cukup hanya satu di setiap komputer. Sehingga banyaknya kabel link dan port I/O menjadi lebih sedikit yang berarti bahwa biaya yang dibutuhkan menjadi tidak semahal seperti pada topologi mesh.

Kentungan lainnya, topologi hybrid juga memiliki sifat robustness, yaitu jika terjadi kerusakan pada satu link, maka hanya berakibat pada komputer yang berada pada jalur link itu saja, sedangkan komputer lainnya tetap aktif. Sepanjang tidak ada masalah dengan HUB, dengan sifat ini maka kerusakan link dapat segera diketahui dan diisolir.

Kelemahannya, karena topologi hybrid ini sangat bergantung kepada HUB sebagai pusat pengendali, mak HUB harus selalu berada dalam kondisi baik. Kerusakan pada HUB berakibat pada lumpuhnya seluruh link dalam jaringan komputer tidak dapat saling berkomunikasi..

3.3.2. Media Transmisi

Media transmisi yang dipakai pada Pusat Data dan Informasi Departemen Pertahanan adalah kabel UTP dan Kabel *fiber optic*. Untuk pemakaian di dalam LAN sendiri Pusdatin Dephan memakai media transmisi kabel UTP dan untuk menghubungan antar LAN Pusdatin Dephan sebagian sudah memakai kabel *fiber optic*. Pemakaian kedua kabel ini dikarenakan karena disesuaikan dengan topologi yang dipakai dan kenapa adanya penggunaan kabel *fiber optic*. Dikarenakan kabel *fiber optic* memiliki kelebihan yaitu kapasitas bandwidth yang lebih besar (gigabyte perdetik), jarak transmisi yang lebih jauh (2 sampai lebih dari 60 kilometer) dan kebal terhadap interferensi elektromagnetik.

3.3.3. Protokol

Protokol yang ada di Pusdatin Dephan yaitu TCP/IP dikarenakan protokol TCP/IP ini sangat tepat dengan jaringan komputer yang telah ada dan selain itu memiliki kelebihan sebagai berikut :

1. Perkembangan protokol TCP/IP menggunakan standar protokol terbuka sehingga tersedia secara luas. Semua orang bisa mengembangkan perangkat lunak untuk dapat berkomunikasi menggunakan protokol ini.

Hal ini membuat pemakaian TCP/IP meluas dengan sangat cepat, terutama dari sisi pengadopsian oleh berbagai sistem operasi dan aplikasi jaringan. Ini sangat tepat karena Pusdatin Dephan tidak hanya satu jenis sistem operasi saja dan juga banyak memakai aplikasi jaringan.

2. Tidak tergantung pada perangkat keras atau sistem operasi jaringan tertentu sehingga TCP/IP cocok untuk menyatukan bermacam macam network, misalnya Ethernet, token ring, dial-up line, X-25 net dan lain lain.
3. Cara pengalamatan bersifat unik dalam skala global, memungkinkan komputer dapat mengidentifikasi secara unik komputer yang lain dalam seluruh jaringan, walaupun jaringannya sebesar jaringan worldwide Internet. Setiap komputer yang tersambung dengan jaringan TCP/IP (Internet) akan memiliki address yang hanya dimiliki olehnya.
4. TCP/IP memiliki fasilitas routing dan jenis-jenis layanan lainnya yang memungkinkan diterapkan pada internetwork.

3.3.4. Kelas IP address

Pada Pusdatin Dephan ini kelas IP *address* yang dipakai adalah Kelas C. dikarenakan Kelas C sangat mungkin digunakan pada jaringan Pusdatin yang masing-masing bagiannya dibagi menjadi beberapa workgroup yang terdiri dari beberapa gedung yang terpisah dan masing-masing gedung tersebut merupakan subnet. IP Kelas C juga dapat menampung sampai 2 juta *network.*

3.4. Masalah Yang Terjadi Pada Jaringan Pusdatin Dephan

Masalah yang sering terjadi pada Jaringan komputer Pusdatin Dephan adalah adanya virus yang merusak jaringan. Untuk itu pada jaringan komputer Pusdatin Dephan di pasang Antivirus baik di server maupun clinet supaya masalah yang sering terjadi ini tidak terjadi kembali ke depannya dengan menggunakan antivirus tersebut. Dan kalaupun itu terjadi dapat ditanggulangi dengan cepat supaya jaringan yang ada tidak terganggu.

3.5. Perangkat Pendukung

Untuk mendukung sistem informasi maupun komunikasi data diperlukan perangkat-perangkat yang diperlukan untuk komunikasi tersebut supaya komunikasi berjalan dengan baik dan lancar. Adapun perangkat yang ada di Pusdatin Dephan dan informasi Departemen Pertahanan diantaranya adalah sebagai berikut :

1) Server

   a. Main Server:

      1. Xeon PIV 3Ghz
      2. Memory 2Gb
      3. VGA share
      4. 6 Harddisk SCSI 72,8Gb RAID Ultra 14400rpm
      5. DVD-RW
      6. Floppy 3,5”
      7. Double LAN Card
      8. OS Windows 2003 Server

b. Server Pendukung :

1. Xeon PIV 3Ghz
2. Memory 2Gb
3. VGA share
4. 2 Harddisk SCSI 72,8Gb RAID Ultra 14400rpm
5. DVD-RW
6. Floppy 3,5”
7. Double LAN Card
8. OS Windows 2003 server

c. Eproc :

1. Xeon PIV 3Ghz
2. Memory 2Gb
3. VGA share
4. 2 Harddisk SCSI 72,8Gb RAID Ultra 14400rpm
5. DVD-RW
6. Floppy 3,5”
7. Double LAN Card
8. OS Windows 2003 server

d. Sisfohanneg :

1. Xeon PIV 3Ghz
2. Memory 1Gb
3. VGA share
4. 6 Harddisk SCSI 72,8Gb RAID Ultra 14400rpm
5. DVD-RW
6. Floppy 3,5”
7. Double LAN Card
8. OS Windows 2003 server

e. Backup Server :

1. Xeon PIV 3Ghz
2. Memory 1Gb
3. VGA share
4. 6 Harddisk SCSI 72,8Gb RAID Ultra 14400rpm
5. DVD-RW
6. Floppy 3,5”
7. Double LAN Card
8. OS Windows 2003 server

f. Unix Server . (Dipergunakan untuk konsul untuk mengatur database yang mau di cetak di printer Printonix High Speed).

g. Server Aplikasi :

1. Processor PIV 2,8Ghz
2. Memory 1Gb
3. Harddisk 80Gb+40Gb
4. CD-RW
5. Floppy 3,5”
6. Double LAN Card
7. OS Windows 2000 server

h. Web Server :

1. Processor PIV 2,8Ghz
2. Memory 1Gb
3. Harddisk 80Gb
4. CD-RW
5. Floppy 3,5”
6. Double LAN Card
7. OS Linux Redhat 7.30

i. Email Server :

1. Processor PIV 2,8Ghz
2. Memory 1Gb
3. Harddisk 80Gb
4. CD-RW
5. Floppy 3,5”
6. Double LAN Card
7. OS Linux Redhat 7.30

j. Database Oracle untuk Linux

1. Processor PIV 2,8Ghz
2. Memory 1Gb
3. Harddisk 80Gb
4. CD-RW
5. Floppy 3,5”
6. Double LAN Card
7. OS Linux Redhat 7.30

k. Data Protektor :

1. Processor PIV 2,8Ghz
2. Memory 1Gb
3. Harddisk 93Gb
4. CD-RW
5. Floppy 3,5”
6. External HP Surestor 40Gbx6
7. Double LAN Card
8. OS Windows 2000 server

l. Network Node Management :
    1. Processor PIV 1,6Ghz
    2. Memory 1Gb
    3. Harddisk 80Gb
    4. CD-RW
    5. Floppy 3,5”
    6. Double LAN Card
    7. OS Windows 2000 server

m. Server Symantec Etrust Anti Virus
n. InterScan Anti Virus Email
o. Server Backup Aplikasi
p. Web Server Backup
q. Mail Server Bakcup
r. Printer Highspeed Printonik
s. Printer Highspeed Data Produk

2) Operating sistem untuk server yang digunakan di Pusdatin Dephan adalah sebagai berikut :

a. Windows 2003 Server
b. Fedora
c. Unix Sun Solaris V 2.7
d. Windows 2000 Server
e. Linux Redhat 7.30

3) Aplikasi server yang digunakan di Pusdatin Dephan adalah sebagai berikut :

a. Oracle 9i
b. Oracle 8.0
c. Oracle 8.0/SQL Plus
d. HP Open View Data Protector

e. HP Open View NNM
f. Etrust Anti Virus
g. InterScan Anti Virus Email
h. Foxpro

4) Perangkat jaringan yang ada :

a. Router Cisco
b. Modem
c. VPN-IP
d. Gateway
e. Firewall
f. Security Email
g. Switch Managable
h. ISP
i. ISDN
j. BRI
k. Shitara Bandwith Management
l. Kabel F/O dan Converter F/O
m. Kabel UTP
n. Penangkal Petir
o. Rak jaringan
p. Detektor kabel
q. Server
r. PC Client
s. Smart UPS Auto Shutdown

3.6. Firewall di Pusdatin Dephan

Server yang berada di Pusdatin Dephan menerapkan sistem operasi berbasis Windows 2003 Server dan linux Redhat. Adapun sistem operasi Windows 2003

Server digunakan untuk Aplikasi Web Dephan. Digunakannya Windows 2003 Server pada Aplikasi Web Dephan karena memiliki interface GUI yang baik dan tentunya hal ini akan lebih memudahkan instalasi dan pemeliharaan sistem operasi tersebut bersama Firewallnya karena lebih user-friendly. Dalam pemakaian windows 2003 Server luas dan tersedia cukup banyak pilihan perangkat pendukung lain.

Perangkat Firewall di Pusdatin Dephan dipergunakan sebagai alat untuk mengimplementasikan kebijakan sekuritas. Sedangkan kebijakan sekuritas dibuat berdasarkan perimbangan antara fasilitas yang disediakan dengan implikasi sekuritasnya. Semakin ketat kebijakan sekuritas, maka semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan semakin banyak fasilitas yang tersedia atau terlalu sederhananya konfigurasi yang di terapkan, maka semakin mudah orang-orang ”usil” dari luar masuk kedalam sistem. Itulah konsekuensi lemahnya kebijakan sekuritas.

Firewall di Pusdatin Dephan menggunakan empat produk yaitu: Nokia, Net-Screen, Juniper, 3-Com. Nokia Typing Point dan Chek Point digunakan sebagai firewall utama, sedangkan Net-Screen, Juniper, 3-Com dan Chek Point berfungsi sebagai filter dan gateway.

Piranti Nokia Tipping Point dan Check Point Firewall memiliki sistem operasi khusus keamanan yang dirancang untuk memenuhi tujuan tertentu dan

memiliki keamanan berlapis. Jaringan yang aman, handal sangat penting saat ini. Dengan piranti Tipping Point dan Check Point Firewall termasuk teknologi baru. Piranti firewall buatan Nokia Multiple Domain Security dengan Tipping Point dan Check Point Firewall dirancang untuk memberikan kemudahan dalam melindungi data dan keamanan jaringan di Pusdatin Dephan.

Koneksi yang aman serta handal sangat penting sejalan dengan makin luasnya penggunaan internet untuk konektivitas. Karena internet dipergunakan setiap hari untuk melakukan transaksi yang penting dan untuk mencari informasi. Oleh karena peranannya yang penting, jaringan IP Pusdatin Dephan harus handal dan aman. Firewall yang aman dan lega merupakan kombinasi yang tepat dalam Tipping Point dan check Point.

Dalam Platform Tipping Point dan Check Point berisi appliance firewall. Perangkat ini secara khusus dirancang fleksibel untuk mendukung aplikasi khusus seperti firewall. Sistem operasinya dikelola melalui perantara interface berbasis web. Tipping Point dan Check Point yang dipakai di Pusdatin Dephan telah memenuhi standart jaminan dan telah melewati proses pengujian secara terpadu. Dalam pengupayaan upgrade akan cenderung lebih mudah dilakukan walaupun dengan beberapa keterbatasan. Secara penempatan platform Tipping Point dan Check Point mudah di pasang dalam suatu ruang khusus yang aman dan nyaman.

Tipping point Firewall yang ada di Pusdatin Dephan salah satunya adalah seperti pada gambar berikut ini.



Gambar 3.3. Tipping Point/Firewall

3.7. Hal Yang Dilindungi Firewall

Firewall pada Pusdatin Dephan bekerja dengan cara mengamati paket IP(Internet Protokol) yang melewatinya. Berdasarkan konfigurasi dari firewall maka akses dapat diatur berdasarkan IP address, port, dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing firewall. Firewall dapat mengatasi serangan yang dilakukan dengan cara membypass Firewall, Firewall tidak bisa melindungi serangan yang dilakukan di dalam system atau internal, Firewall tidak bisa melindungi pengiriman virus yang disisipkan ke suatu program atau file. Hal itu dikarenakan Firewall tidak bisa melakukan scanning terhadap file, program, e-mail yang berisi virus. Terdapat tiga hal yang dilindungi Firewall pada Pusdatin Dephan, yaitu:

1. Data (informasi)

   Pusdatin Dephan mempunyai data yang sangat berharga dan penting kerahasiaannya untuk dilindungi. Pertukaran data di dunia maya merupakan hal yang sangat sering dilakukan oleh para pegawai Pusdatin Dephan, oleh karena itu Firewall dapat membantu mengamankan data-data yang bersifat

rahasia, intergritas dan ketersediaan agar terhindar dari pihak-pihak yang tidak bertanggung jawab. Data aplikasi, data IKN(inventaris kekayaan negara), aplikasi gaji, aplikasi personel, aplikasi SMA Taruna nusantara, aplikasi SISFOHANEG, Sistem aplikasi EPROC dll.

2. Sumber Daya

Sumber daya komputer dalam hal ini memerlukan perawatan sehingga mempunyai biaya khusus yang harus dibayar, Pusdatin Dephan mempunyai tugas melaksanakan pembinaan, pengembangan, dan standardisasi teknis serta evaluasi kebijakan di bidang sistem informasi dan persandian teknologi informasi. Untuk mencegah orang yang tidak memiliki wewenang memakai sumberdaya komputernya, maka memerlukan penanganan apabila terjadi penyusup yang memanfaatkan sumber daya komputer tersebut untuk umum.

3.Ketersediaan (Reputasi)

Hal-hal yang berhubungan dengan reputasi sering kali berhubungan dengan para hacker, yang menggunakan identitas orang lain yang tidak bersalah untuk menyusup.

3.8. Pemeliharaan Firewall

Tugas Administrator jaringan di Pusdatin Dephan sangat berperan sekali dalam mengamankan jaringan yang ada. Firewall yang baik adalah Firewall yang desainnya baik, sesuai dengan kebutuhan, ditangani oleh administrator yang ahli

dalam bidang ini dan melakukan pemeliharaan Firewallnya yang tidak kalah pentingnya. Yang sering dilakukan oleh administrator Pusdatin Dephan adalah sebagai berikut:

1. Housekeeping.

Adalah pekerjaan kecil yang rutin yang perlu dilakukan untuk memelihara satu firewall yang bersih dan aman. Ada tiga tugas utama yang harus dilakukan berulang- ulang oleh administrator jaringan, antaranya:

a. Backup Firewall

Administrator selalu melakukan backup semua bagian dari firewall

b. Management account

Administrator melakukan penambahan account baru, menghapus account yang tidak dipakai, merubah password, dan sebagainya.

c. Management disk space

Administrator melakukan pemeriksaan pada ruang kosong yang setiap waktu bertambah. Terkadang user tidak disiplin dalam memenuhi ruang kosong dengan file-file yang tidak berguna, jika tidak dilakukan pemeriksaan dapat memudahkan penyerang untuk meletakkan macilious code didalam komputer. Malicious code adalah file/data yang tidak dikenal yang memakan space diharddisk yang dapat berakibat fatal pada sistem. Management yang dilakukan Administrator untuk menghindari Malicious code adalah :

d. Melakukan checking secara dinamis

e. Membatasi file yang masuk

f. Menggunakan program antivirus dan selalu mengupdatenya

g. Membuang semua file yang tidak berguna

h. Memeriksa file log

Ini adalah contoh file log yang terdeteksi oleh sistem di Pusdatin Dephan.

```
apache   1550    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1553    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1554    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1555    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1556    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1558    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1559    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1560    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1561    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1562    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1563    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1564    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1565    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1566    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1567    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1571    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1572    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1575    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1576    1  0 06:09 ?        00:00:00 ./elf.1 ./elf.10 ./elf.2 ./elf.3
apache   1590    1 84 06:09?        01:25:37 [elf.1]
```

1. Memonitor Sistem

Dalam menangani dan mengenali sebuah serangan yang dilakukan oleh hacker atau cracker, dengan menggunakan data yang telah diperoleh. Pendekatan yang di pergunakan seorang administrator untuk mengenali serangan dengan cara

Anomaly detection (deteksi penyimpangan) dan Misuse detection (analisa aktivitas sistem).

2. Up to Date sistem

Dalam mengelola suatu sistem komputer selalu dalam kondisi up to date, administrator harus memiliki informasi maupun perkembangan yang terbaru tentang Firewall.

3.9. Kelebihan Dan Kekurangan Firewall Pusdatin Dephan

3.9.1. Kelebihan

a. Perangkat firewall yang terpasang terintegrasi penuh dengan keamanan jaringan.

b. Pemasangan firewall yang digunakan relative cepat dan mudah, karena dilengkapi dengan panduan (CD dan Modul) serta konsultan dari pemasang hardware.

c. Keunggulan dari Nokia Tipping Point adalah mudah dalam penggunaanya untuk mengkonfigurasi sistem operasi yang menggunakan perantara sistem berbasis web, akses dalam baris perintah.

d. Cukup aman karena hampir semua hal yang membuat ketidaknyamanan telah ditiadakan dalam kernel sistem operasinya.

e. Firewall di Pusdatin Dephan menggunakan empat perangkat pengaman yaitu: Nokia Tipping Point dan Check Point, Net-Screen, Juniper, 3-Com. Nokia Tipping Point dan Check Point sebagai firewall utama dan net-Screen, Juniper, 3-Com berfungsi sebagai filter dan gateway.

3.9.2. Kekurangan

a. Kemungkinan ada client di Dephan Pusat / Merdeka Barat yang menggunakan koneksi internet menggunakan dua koneksi yaitu melalui jaringan LAN dan Dial Modem (untuk Pusdatin Dephan tidak terjadi). Perangkat firewall hanya dapat melakukan pembatasan terhadap koneksi yang memang melewati parangkat ini. Firewall tidak dapat melindungi jaringan internal terhadap orang-orang yang pada saat melakukan aktifitasnya berada di sisi belakang firewall. Akses internet menggunakan dua koneksi ini biasanya dilakukan oleh pejabat tertentu yang ingin mengakses internet secara cepat.

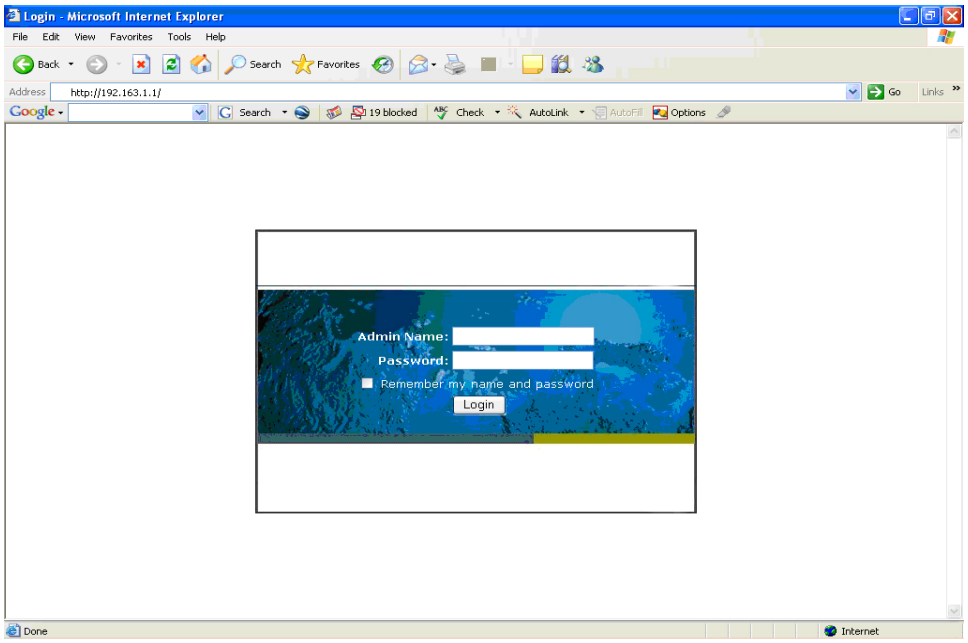
b. Rekayasa sosial. Penyusupan (spyware) yang sering terjadi disebabkan tidak adanya pembatasan akses internet, semua user di Dephan bebas mengakses internet hal ini bisa menyebabkan penyusupan/spyware masuk ke komputer client.

c. Pemakaian firewall Tipping Point dan Check Point yang memiliki banyak fitur-fitur mengakibatkan cost yang dikeluarkan sangat besar, Pusdatin Dephan sebagai bagian dari departemen pertahanan tidak

mungkin membeli perangkat tersebut secara sekaligus karena tergantung pada dana yang ada. Tidak komplitnya fitur firewall yang dibeli mengurangi keunggulan-keunggulan yang dikeluarkan produk nokia tersebut.

d. Penguasaan teknologi Pengamanan Jaringan masih terbatas pada admin Jaringan, transfer teknologi Pengamanan Jaringan ke SDM yang lain kurang diterapkan.

3.10. Seting Firewall Juniper



Gambar 3.4. Login Firewall

Untuk setting Firewall dilakukan dengan login pada alamat IP yang sudah ditetapkan .

Log in

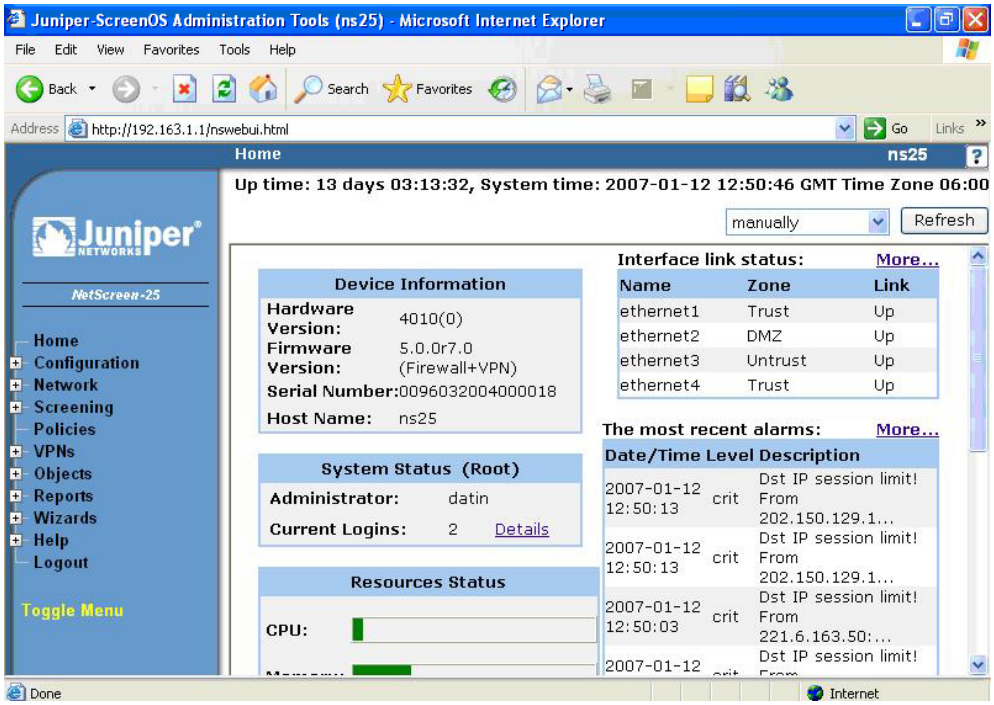
a. Alamat hardware (Firewall) yang dituju

contohnya: http://192.163.1.1 untuk Firewall Juniper.

b. Admin Name dan password untuk Login dalam Menu Firewall.

Langkah selanjutnya adalah melakukan Setting pada Toggle Menu yang terdapat pada Firewall. Adapun Togle Menu terdiri dari :

a. Home
b. Configuration
c. Network
d. Policies
e. VPNs
f. Objects
g. Report
h. Wizards
i. Help
j. Logout



Gambar 3.5. Menu Utama dari Juniper

Pada Interface link status :

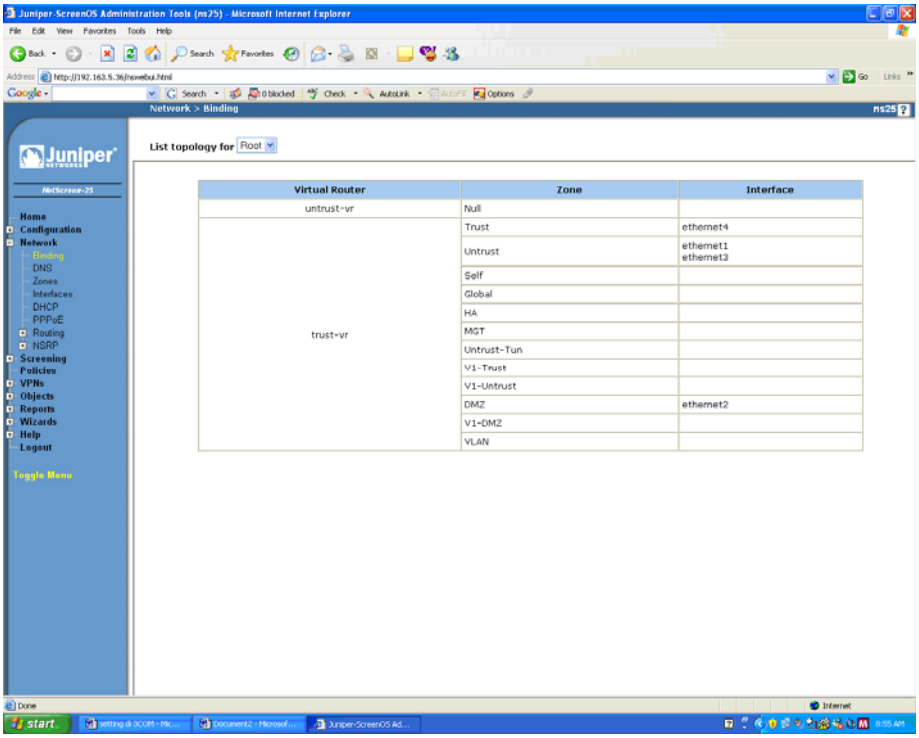
1. Trust dipergunakan untuk zone yang dilindungi

2. DMZ dipergunakan untuk zone yang lebih dilindungi

3. Untrust dipergunakan untuk zone public atau internet.

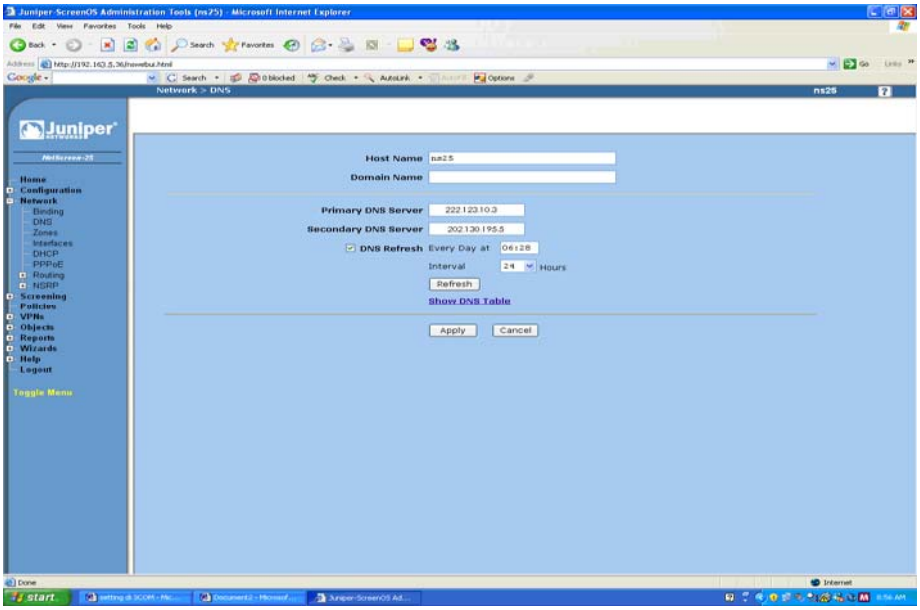
The most recent alarms:

Dipergunakan untuk mencatat semua IP yang bekerja tidak seperti biasanya/keluar dari kebijakan yang telah ditentukan oleh admin jaringan (contoh IP yang melakukan Spoofing karena terserang virus akan terdeteksi secara dini).



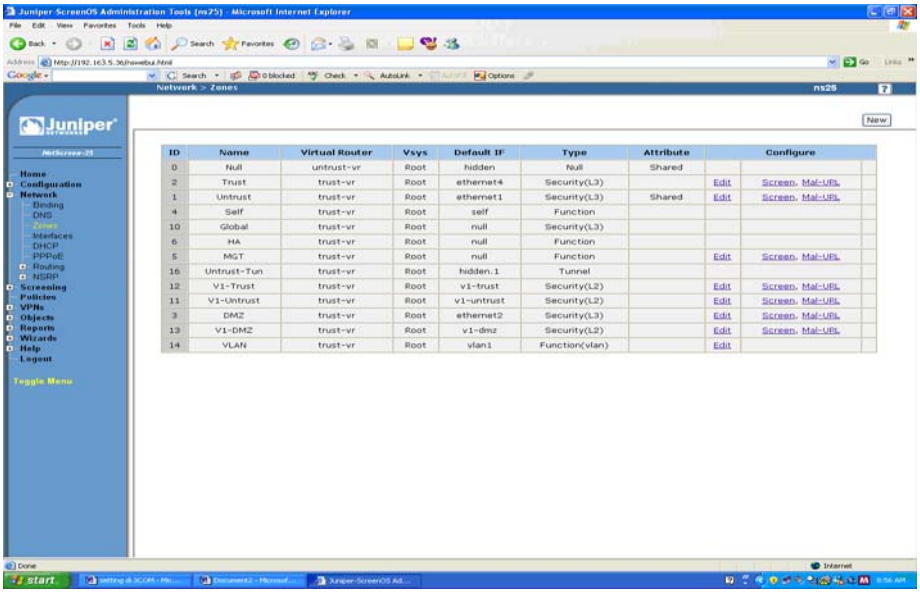
Gambar 3.6. Menu Network Binding

Pada Menu Network Binding terbentuk secara otomatis. Interfacenya tidak dapat diubah-ubah fungsinya untuk memberikan informasi Zone yang digunakan setiap interface.



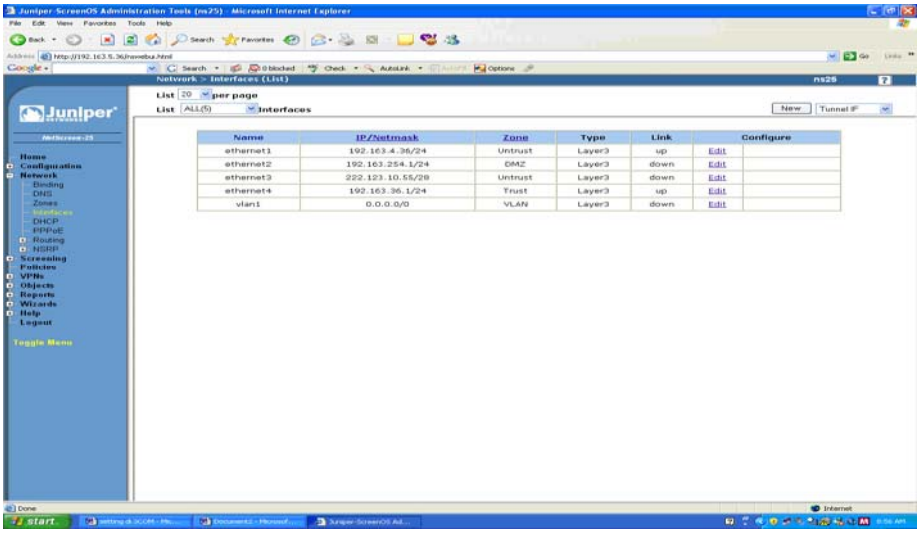
Gambar 3.7. Menu Network DNS

Pada menu Network fungsinya untuk setting Host Name, Domain Server, Primary DNS Server dan Secudary DNS Server.



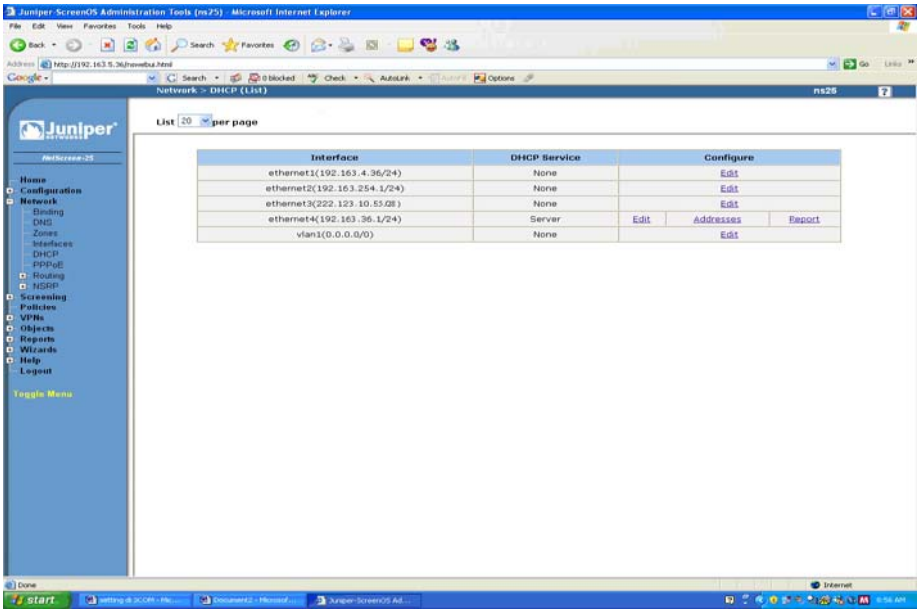
Gambar 3.8. Menu Network Zone

Pada Menu Network Zone terbentuk secara otomatis berdasarkan hasil input yang telah dilakukan sebelumnya.



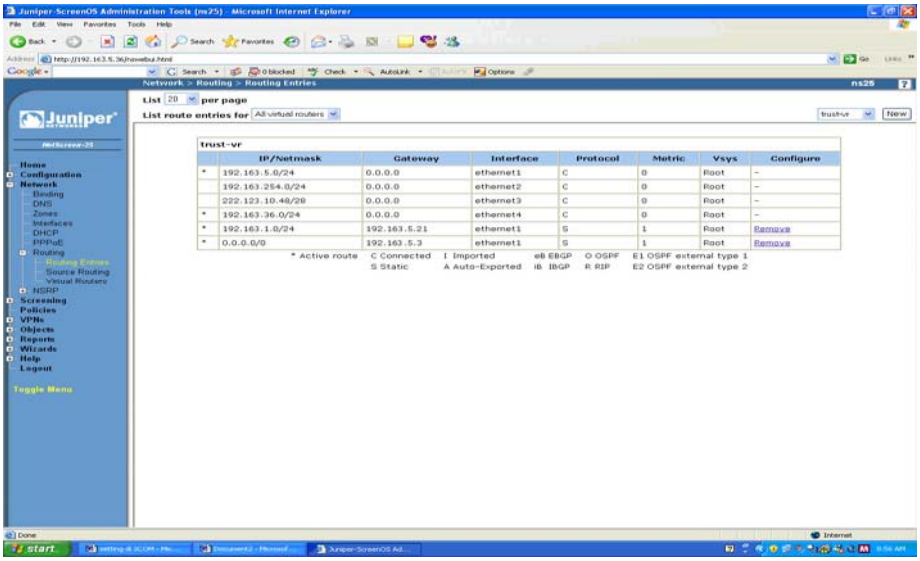
Gambar 3.9. Menu Network Interface (list)

Menu Network Interface berdasarkan dari pengalamatan IP yang ditentukan.



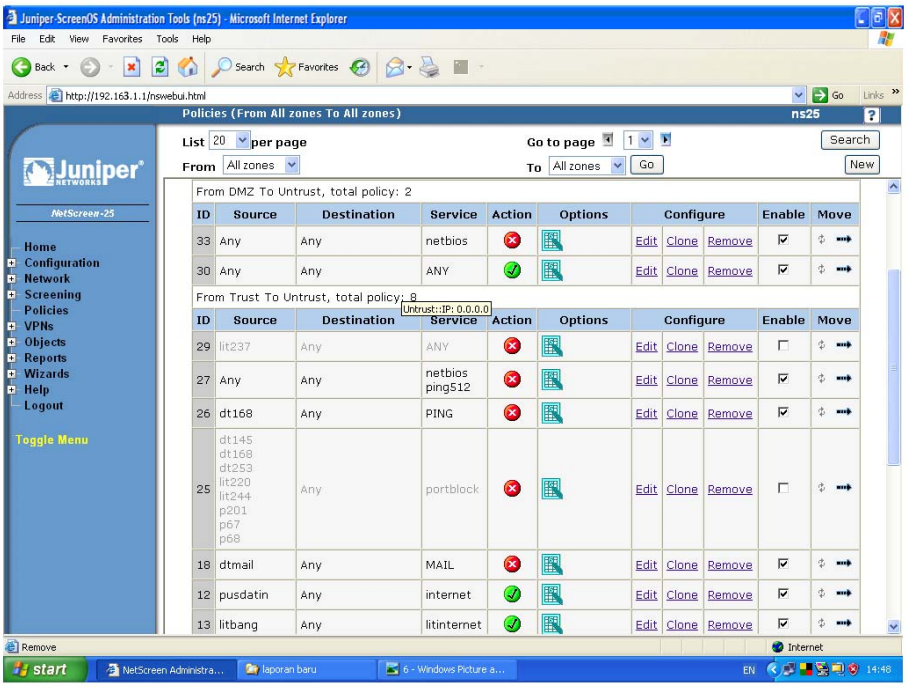
Gambar 3.10. Menu Network DHCP (list)

Menu Network DHCP adalah pengalamatan secara otomatis.



Gambar 3.11. Menu Network Routing Entries

IP yang sudah ditentukan oleh adminstator jaringan secara otomatis masuk kedalam Routing. Semua IP dari mana dan ke mana, menggunakan service apa, boleh atau tidak harus melewati Routring Entries.



Gambar 3.12. Menu Policy (From All Zone To All Zone)

Menu Policy merupakan menu pengisian untuk security policy yang harus terstruktur, security policy diperiksa secara berurut sampai yang terakhir.

3.11. Konfigurasi Juniper Untuk Membatasi Akses Internet

Berikut langkah-langkah yang diperlukan untu konfigurasi Juniper sebagai firewall untuk membatasi akses internet yaitu :

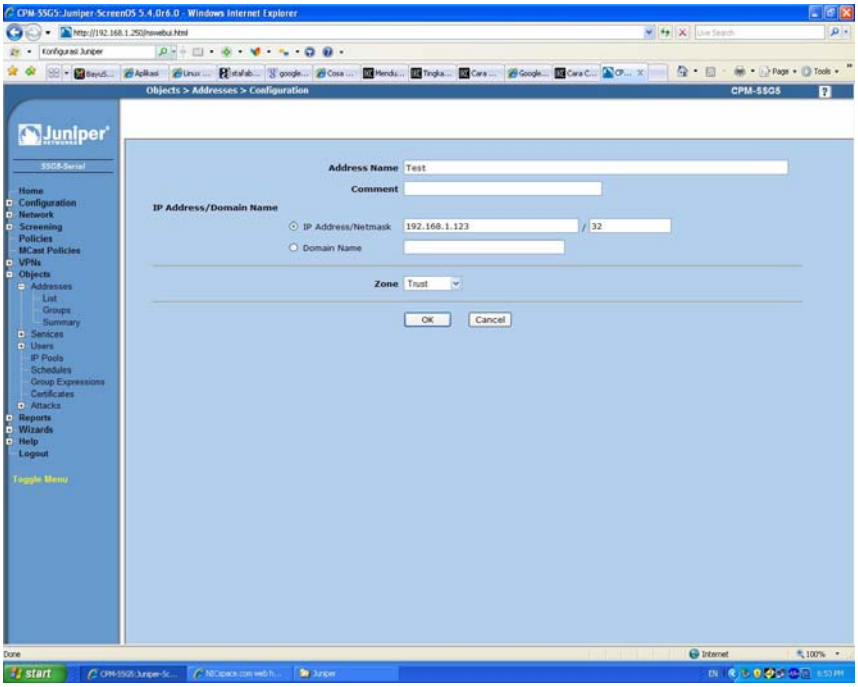
1. Menambahkan List Address pada Trust Zone (Internal Zone)

   Klik Menu **Object-Address-List**

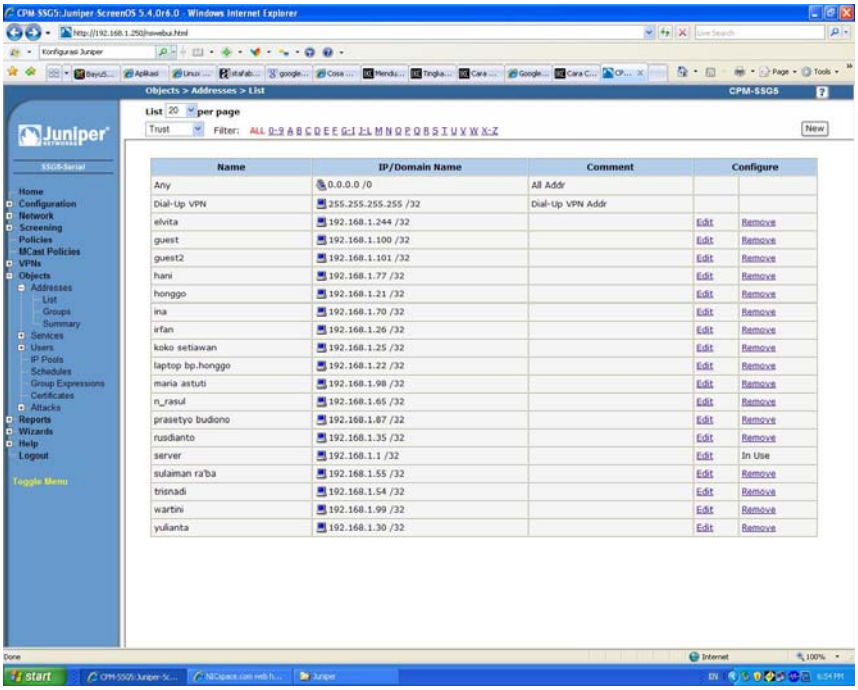
   Isikan

   Address Name, IP Address dan Netmask

   Pilih Zone : Trust (Trust Zone merupakan Zona yang ada di jaringan internal)



Gambar 3.13. Address Name



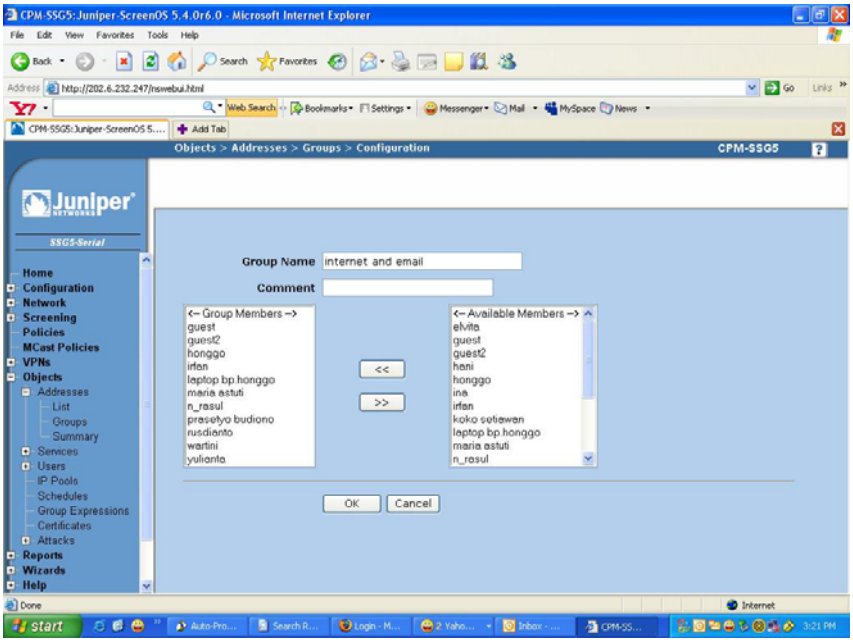
Gambar 3.14. Address List

2. Membuat Group Address List pada Trust Zone

   Pilih menu Objects > Addresses > Groups, Pilih Zone Trust lalu klik Button New.

   Isikan **Group Name** (Misal Internet dan email)

   Pilih nama di available member di kolom sebelah kanan, lalu klik tombol << untuk menambahkan ke Group (Kita akan mengkonfigurasi di policy, Member yang ada di Group ini saja yang bisa menggunaan internet)



Gambar 3.15. Membuat Group Address List

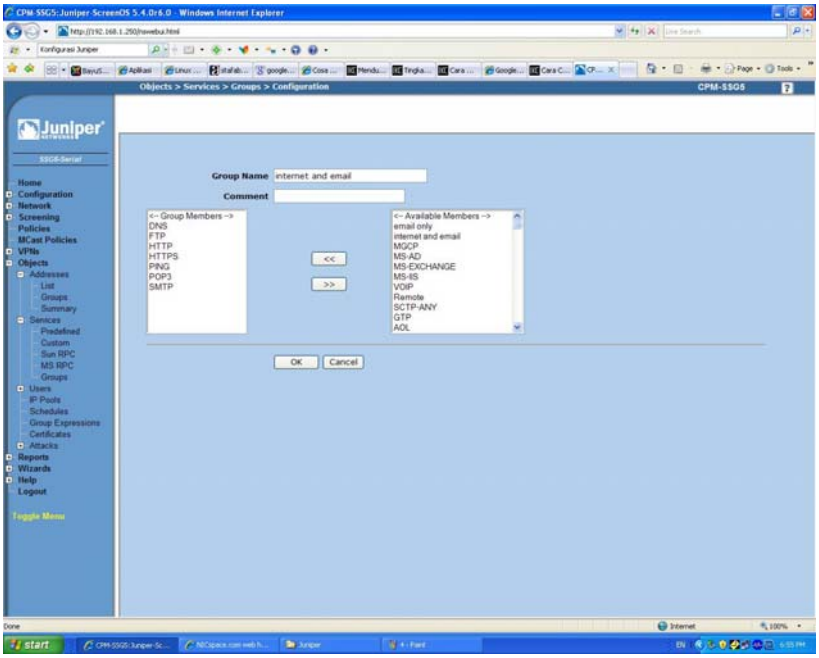
3. Mendefinisikan Group Service untuk akses internet (HTTP,FTP,DNS,PING,POP3,SMTP)

   Pilih Menu Objects > Services > Groups

Klik Tombol New untuk menambahkan Group

a. Isikan **Group Name : misal internet dan email**

b. Tambahkan DNS,FTP,HTTP,HTTPS,PING,POP3, dan SMTP di Group Service ini



Gambar 3.16. Mendefinisikan Group Service

4. Membuat Policies untuk membatasi akses internet

Pilih Menu **Policies**

Pilih zone **from Trust to Untrust**

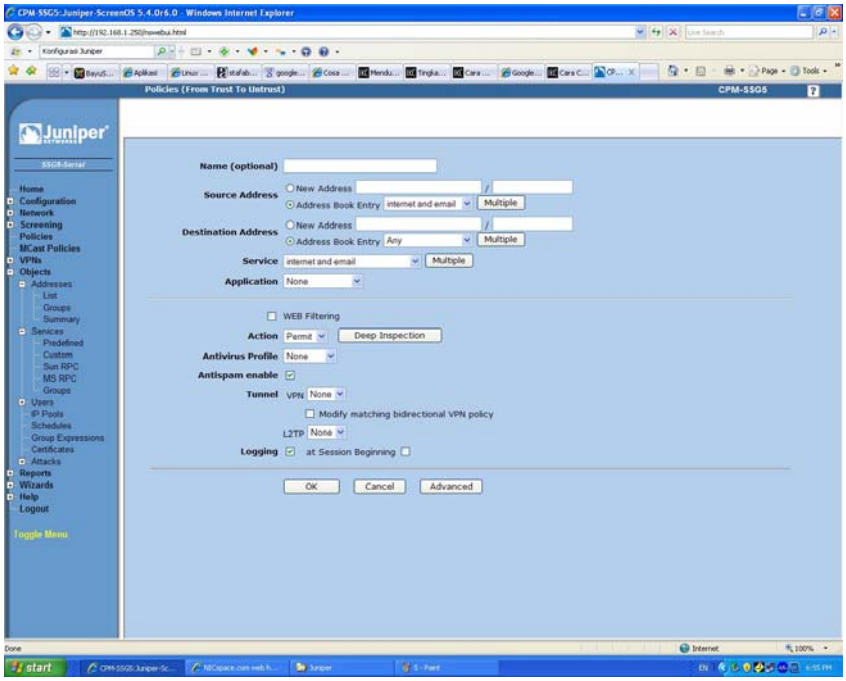
Klik tombol **New**

Pilih/Isikan Source Address “internet dan email” dari **Address Book Entry**

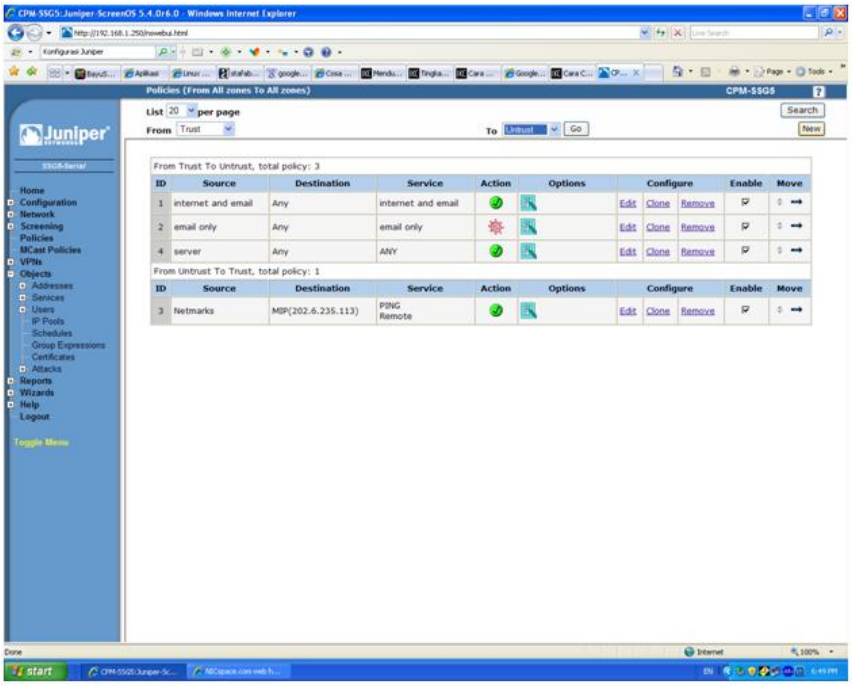
Pilih/isikan Destination Address “Any” dari **Address Book Entry**

Pilih/Isikan Service “**Internet dan Email”**

Tekan OK



Gambar 3.17. Policies (From Trust To Untrust)

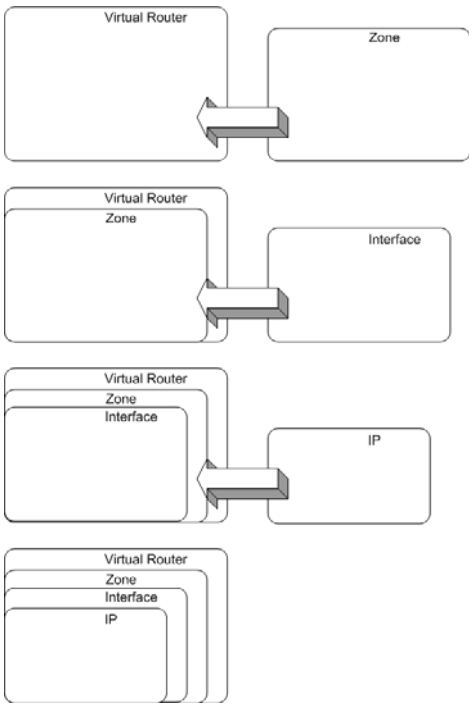


Gambar 3.18. Policies (From All zones To All Zones)

Sampai disini konfigurasi sudah selesai, dan sekarang IP Address yang ada di group **"internet dan email"** saja yang bisa mengakses internet.

3.12. Konfigurasi Firewall Juniper Untuk Jaringan

Ketika mengkonfigurasi perangkat Juniper, ada beberapa langkah yang harus dilakukan sebelum dapat berinteraksi dengan jaringan. Antarmuka fisik pertama-tama harus terikat dengan zona sebelum dapat diberikan sebuah alamat IP. Gambar di bawah menggambarkan hubungan antara zona dan sebuah antarmuka. Zona adalah orangtua untuk antarmuka fisik, dan alamat IP adalah seorang anak untuk antarmuka fisik.



Gambar 3.19. Zone Interface/IP Relationship

Mengikat Sebuah Interface Ke Zona

Pertama kita akan mengikat sebuah antarmuka untuk suatu zona. Dan kami akan mengikat zona kepercayaan untuk interface.This kepercayaan dapat dilakukan dengan menggunakan baik WebUI atau di CLI. Namun, untuk mengubah zona Anda harus terlebih dahulu menghapus alamat IP dengan menetapkan untuk 0.0.0.0 / 0. Setelah itu, Anda dapat memilih zona baru.

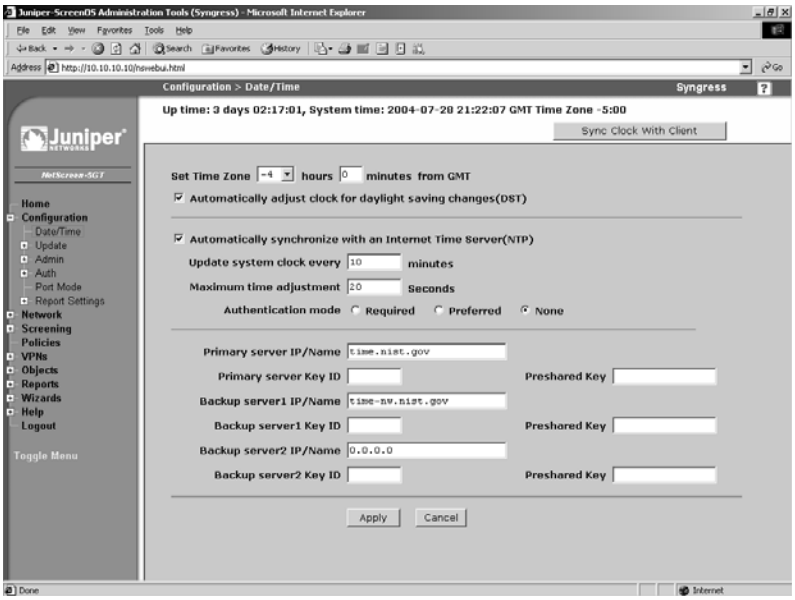
1. Access **Network | Interface**
2. Tekan Tombol **Edit**
3. Pilih **Trust** dari **zona Name drop-down list.**
4. Tekan **OK**

Untuk mengikat sebuah antarmuka untuk zona menggunakan CLI, ketik perintah set antarmuka interfacename zona zonename, di mana interfacename adalah nama dari antarmuka yang Anda inginkan untuk mengikat, dan zonename adalah nama zona Anda ingin mengikat antarmuka tertentu.

3.13. Konfigurasi Sistem Service

Pada firewall Juniper ada beberapa perangkat terkenal lainnya dikonfigurasi. Konfigurasi waktu adalah sangat penting karena dapat dihubungkan dengan informasi dalam log untuk waktu tertentu.

Seting Waktu



Gambar 3.20. Seting Waktu

1. Access **Configuration | Date/Time**
2. Gunakan **Set Time Zone** untuk menentukan perbedaan antara zona waktu Anda dan GMT (Greenwich Mean Time).
3. Aktifkan pilihan **Automatically adjust clock for daylight saving changes (DST)**.
4. Tekan **Apply**

Tekan tombol **Sync Clock with Client** dan pilih **Yes** untuk konfirmasi.