UJI COBA TEKNOLOGI SECURITY FIREWALL
PADA SYSTEM NETWORKING DENGAN MENGGUNAKAN MICROSOFT FOREFRONT THREAT MANAGEMENT GATEWAY

ABSTRAK

Firewall atau tembok-api adalah sebuah sistem atau perangkat yang mengizinkan traffic networking yang dianggap aman untuk melaluinya dan mencegah traffic network yang tidak aman. Umumnya, sebuah firewall diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara dan jaringan lainnya. Firewall umumnya juga digunakan untuk terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah lazim yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan berbadan hukum di dalamnya, maka perlindungan terhadap modal digital perusahaan tersebut dari serangan para , pemata-mata, ataupun pencuri lainnya, menjadi hakikat. Penerapan Thread Management Gateway merupakan salah satu cara untuk mendukung pembentukan mekanisme firewall pada Microsoft Forefront.

ABSTRACT

Firewall or wall-fire is a system or device that allows networking traffic that is considered safe for network traffic through it and prevent unsafe. Generally, a firewall is implemented in a dedicated machine, running on the gateway (gateway) between the local network and other networks. Firewalls are generally also used to control access to anyone who has access to a private network from outside parties. Today, the term firewall became prevalent that the term refers to systems that manage communication between two different networks. Given today many companies that have access to the Internet and also of course the network incorporated in it, then the protection of digital capital of the company from attacks by hackers, pemata-eye, or other data thieves, into nature. Application of Thread Management Gateway is one way to support the establishment of mechanisms a firewall on Microsoft Forefront.

Kata Kunci : Firewall, Thread Management Gateway, Microsoft Forefront

Dhian Sweetania

Jurusan Sistem Informasi
Universitas Gunadarma
Jl. Margonda Raya 100 Pondok Cina Depok 16424
dhian_sweetania@staff.gunadarma.ac.id

PENDAHULUAN

Internet merupakan sebuah jaringan komputer yang sangat terbuka di dunia, konsekuensi yang harus di tanggung adalah tidak ada jaminan keamanan bagi jaringan yang terkait ke Internet. Artinya jika operator jaringan tidak hati-hati dalam menset-up sistemnya, maka kemungkinan besar jaringan yang terkait ke Internet akan dengan mudah dimasuki orang yang tidak di undang dari luar. Adalah tugas dari operator jaringan yang bersangkutan, untuk menekan resiko tersebut seminimal mungkin. Pemilihan strategi dan kecakapan administrator jaringan ini, akan sangat membedakan apakah suatu jaringan mudah ditembus atau tidak.

Firewall merupakan alat untuk mengimplementasikan kebijakan security (security policy). Sedangkan kebijakan security, dibuat berdasarkan perimbangan antara fasilitas yang disediakan dengan implikasi security-nya. Semakin ketat kebijakan security, semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan semakin banyak fasilitas yang tersedia atau sedemikian sederhananya konfigurasi yang diterapkan, maka semakin mudah orang orang 'usil' dari luar masuk kedalam sistem (akibat langsung dari lemahnya kebijakan security).

TINJAUAN PUSTAKA

Pengertian Firewall

Firewall adalah istilah yang biasa digunakan untuk menunjuk pada suatu komponen atau sekumpulan komponen jaringan, yang berfungsi membatasi akses antara dua jaringan, lebih khusus lagi, antara jaringan internal dengan jaringan global Internet. Firewall mempunyai beberapa tugas :

- Pertama dan yang terpenting adalah: harus dapat mengimplementasikan kebijakan security di jaringan (site security policy). Jika aksi tertentu tidak diperbolehkan oleh kebijakan ini, maka firewall harus meyakinkan bahwa semua usaha yang mewakili operasi tersebut harus gagal atau digagalkan. Dengan demikian, semua akses ilegal antar jaringan (tidak diotorisasikan) akan ditolak.
- Melakukan filtering: mewajibkan semua traffik yang ada untuk dilewatkan melalui firewall bagi semua proses pemberian dan pemanfaatan layanan informasi. Dalam konteks ini, aliran paket data dari/menuju firewall, diseleksi berdasarkan IP-address, nomor port, atau arahnya, dan disesuaikan dengan kebijakan security.
- Firewall juga harus dapat merekam/mencatat even-even mencurigakan serta memberitahu administrator terhadap segala usaha-usaha menembus kebijakan security.

Merencanakan Jaringan Dengan Firewall

Merencanakan sistem firewall pada jaringan, berkaitan erat dengan jenis fasilitas apa yang akan disediakan bagi para pemakai, sejauh mana level resiko-security yang bisa diterima, serta berapa banyak waktu, biaya dan keahlian yang tersedia (faktor teknis dan ekonomis). Firewall umumnya terdiri dari bagian filter (disebut juga screen atau choke) dan bagian gateway (gate). Filter berfungsi untuk membatasi akses, mempersempit kanal, atau untuk memblok kelas trafik tertentu. Terjadinya pembatasan akses, berarti akan mengurangi fungsi jaringan. Untuk tetap menjaga fungsi komunikasi jaringan dalam lingkungan yang ber-firewall, umumnya ditempuh dua cara :

- Pertama, bila kita bayangkan jaringan kita berada dalam perlindungan sebuah benteng, komunikasi dapat terjadi melalui pintu-pintu keluar benteng tersebut. Cara ini dikenal sebagai packet-filtering, dimana filter hanya digunakan untuk menolak trafik pada kanal yang tidak digunakan atau kanal dengan resiko-security cukup besar, sedangkan trafik pada kanal yang lain masih tetap diperbolehkan.
- Cara kedua, menggunakan sistem proxy, dimana setiap komunikasi yang terjadi antar kedua jaringan harus dilakukan melalui suatu operator, dalam hal ini proxy server. Beberapa protokol, seperti telnet dan

SMTP(Simple Mail Transport Protocol), akan lebih efektif ditangani dengan evaluasi paket (packet filtering), sedangkan yang lain seperti FTP (File Transport Protocol), Archie, Gopher dan HTTP (Hyper-Text Transport Protocol) akan lebih efektif ditangani dengan sistem proxy. Kebanyakan firewall menggunakan kombinasi kedua teknik ini (packet filtering dan proxy).

Tujuan utama dari firewall adalah untuk menjaga (prevent) agar akses (ke dalam maupun ke luar) dari orang yang tidak berwenang (unauthorized access) tidak dapat dilakukan.

Konfigurasi dari firewall bergantung kepada kebijaksanaan (policy) dari organisasi yang bersangkutan, yang dapat dibagi menjadi dua jenis: Apa-apa yang tidak diperbolehkan secara eksplisit dianggap tidak diperbolehkan (prohibitted), Apa-apa yang tidak dilarang secara eksplisit dianggap diperbolehkan (permitted).

Firewall bekerja dengan mengamati paket IP (Internet Protocol) 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 berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu, sehingga pemakai (administrator) tinggal melakukan konfigurasi dari firewall tersebut. Firewall juga dapat berupa perangkat lunak yang ditambahkan kepada sebuah server (baik UNIX maupun Windows NT), yang dikonfigurasi menjadi firewall. Dalam hal ini, sebetulnya perangkat komputer dengan prosesor Intel 80486 sudah cukup untuk menjadi firewall yang sederhana. Firewall biasanya melakukan dua fungsi; fungsi (IP) filtering dan fungsi proxy.

Keduanya dapat dilakukan pada sebuah perangkat komputer (device) atau dilakukan secara terpisah. Beberapa perangkat lunak berbasis UNIX yang dapat digunakan untuk melakukan IP filtering antara lain: ipfwadm: merupakan standar dari sistem Linux yang dapat diaktifkan pada level kernel , ipchains: versi baru dari Linux kernel packet filtering yang diharapkan dapat menggantikan fungsi ipfwadm

Fungsi proxy dapat dilakukan oleh berbagai software tergantung kepada jenis proxy yang dibutuhkan, misalnya web proxy, rlogin proxy, ftp proxy dan seterusnya. Di sisi client sering kali dibutuhkan software tertentu agar dapat menggunakan proxy server ini, seperti misalnya dengan menggunakan SOCKS. Beberapa perangkat lunak berbasis UNIX untuk proxy antara lain: Socks: proxy server oleh NEC Network Systems Labs , Squid: web proxy server.

Microsoft ForeFront adalah sebuah jajaran produk komprehensif yang dibuat oleh untuk klien Microsoft (, , atau) dan sistem operasi . Menurut Microsoft, jajaran ForeFront akan menyediakan perusahaan dengan beberapa lapisan keamanan terhadap ancaman yang datang dari luar maupun dari dalam.

Microsoft ForeFront sendiri mencakup produk-produk berikut:

1. Kategori Client Security
   - Microsoft ForeFront Client Security (sebelumnya dikenal sebagai Microsoft Client Protection)
     Produk ini merupakan produk dan yang dimiliki oleh Microsoft. *Scan engine* yang digunakan oleh produk ini sama dengan scan engine yang digunakan oleh , dan menggunakan *signature* yang sama dengan dalam hal pendeteksian . Tampilan pun juga mirip dengan Windows Defender. Versi terbaru sekarang adalah versi 1.5. Versi yang akan datang akan memiliki nama Microsoft Forefront Endpoint Protection, yang merupakan bagian dari Forefront Protection Suite.
2. Kategori Server Security
   - Microsoft ForeFront Security for (sebelumnya dikenal sebagai Antigen for Exchange)
   - Microsoft ForeFront Security for (sebelumnya dikenal dengan sebutan Sybari Antigen for SharePoint)
   - Microsoft ForeFront Security for (sebelumnya dikenal dengan sebutan Antigen for Instant Messaging)
   - Microsoft Forefront Security Management Console
3. Kategori Edge Security
   - (ISA Server) 2006
   - Microsoft Intelligent Application Gateway 2007
   - Microsoft ForeFront Threat Management Gateway (versi selanjutnya ISA Server)
   - Microsoft ForeFront Unified Access Gateway (versi selanjutnya IAG)

METODE PENELITIAN

Metodologi penelitian yang digunakan adalah sebagai berikut:

1. Melakukan penginstalan Microsoft forefront
2. Selanjutnya melakukan penginstalan thread gateway
3. Menyimpan Microsoft ForeFront TMG pada salah satu directory folder. Lalu mulai melakukan Run Preparation Tools.

Dalam pembuatan program ini digunakan seperangkat computer dengan spesifikasi sebagai berikut :

1. 4 GB RAM
2. 1024x768 display
3. 260 GB hard disk

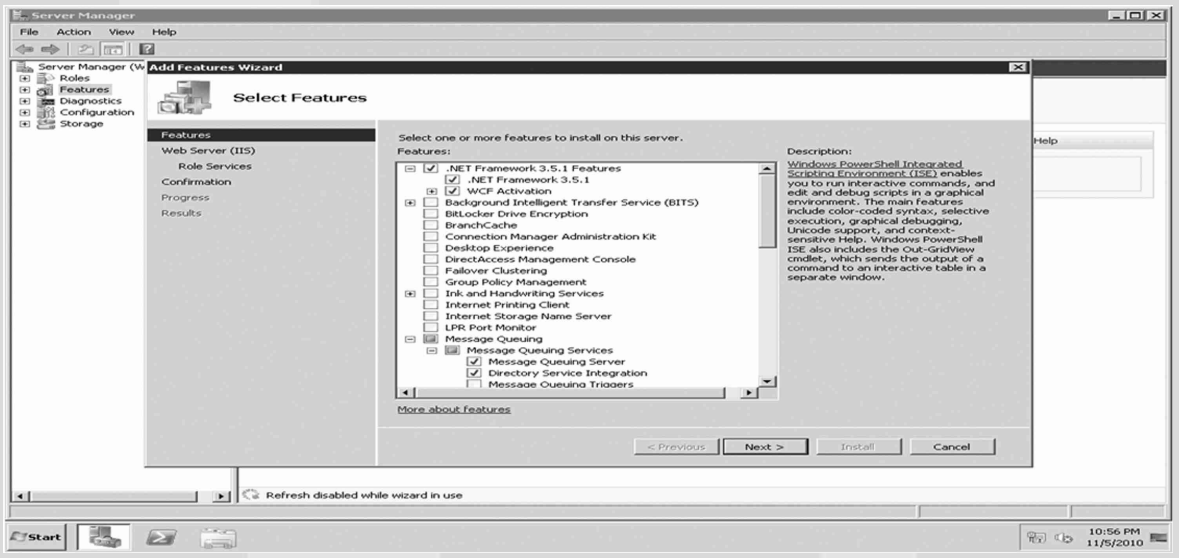
Sedangkan software-software yang digunakan dalam pembuatan program ini adalah sebagai berikut:

1. Windows server 2010
2. Microsoft windows 7

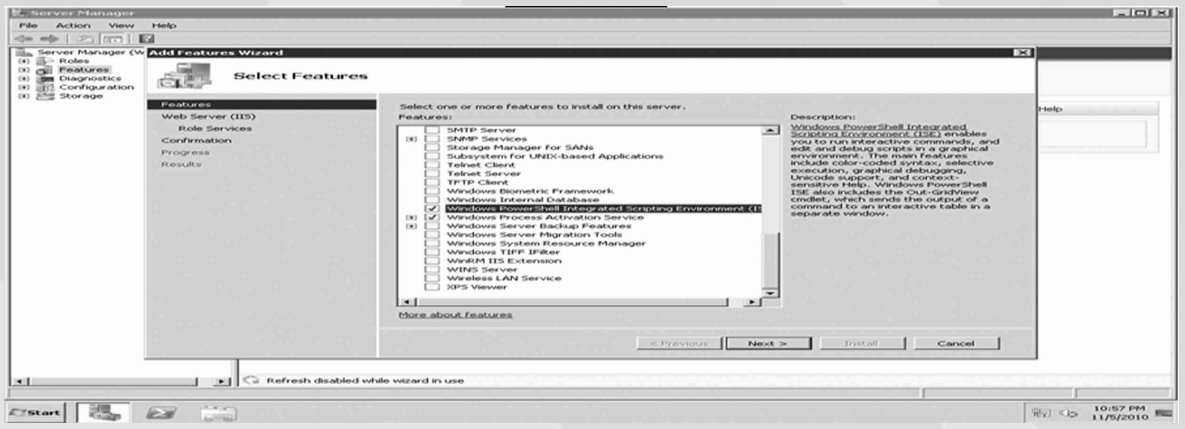
PEMBAHASAN

Langkah awal dalam membuat firewall adalah dengan menginstal forefront terlebih dahulu, berikut adalah langkah penginstalan forefront :

Masukkan CD software forefront, jika sudah muncul tampilan seperti dibawah ini pilih Net FrameWork 3.5.1 Feature, Net FrameWork 3.5.1, WCF Activion, Message Quire Server, Directory Service Integration, Windows Power Shell, Windows Process Active Process seperti pada gambar 1, 2, 3.

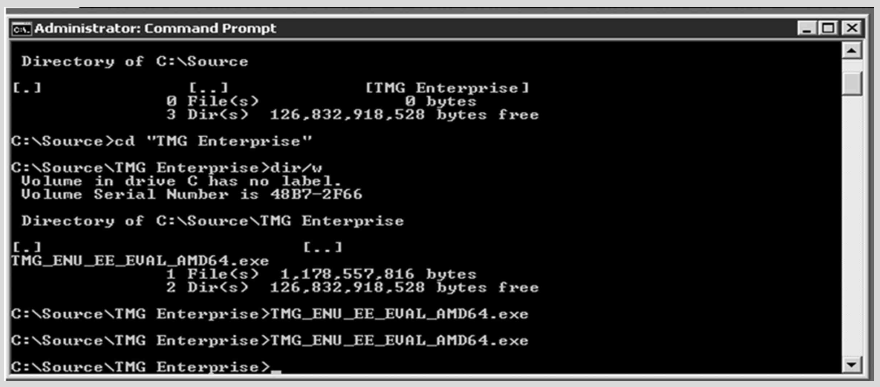


Gambar 1



Gambar 2.

2. Setelah proses instalasi selesai maka akan muncul command prompt



Gambar 3

3. Ini adalah tampilan utama untuk menginstal Thread Gateway

Gambar 4

4. Ini adalah tampilan untuk menyimpan microsoft Forefront TMG.seperti gambar 5.

Gambar 5

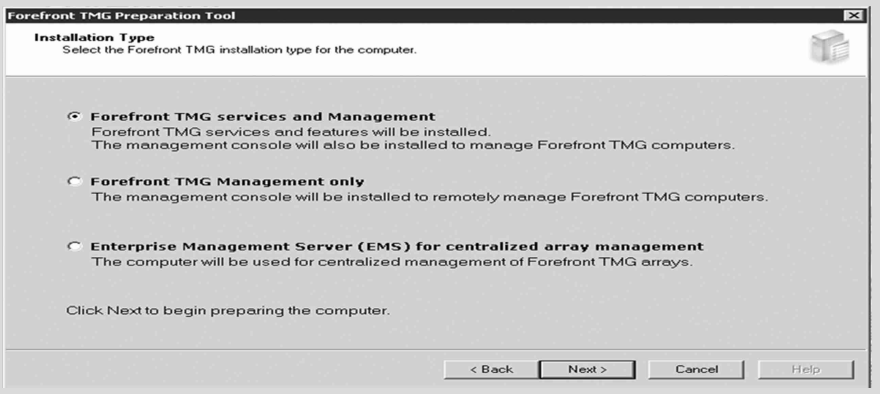
5. Tampilan ini adalah tampilan awal Forefront Threat Management Gateway 2010. Lalu pilih Run Preparation Tool seperti gambar 6.

Gambar 6

6. Lalu pilih Next, pada gambar 7

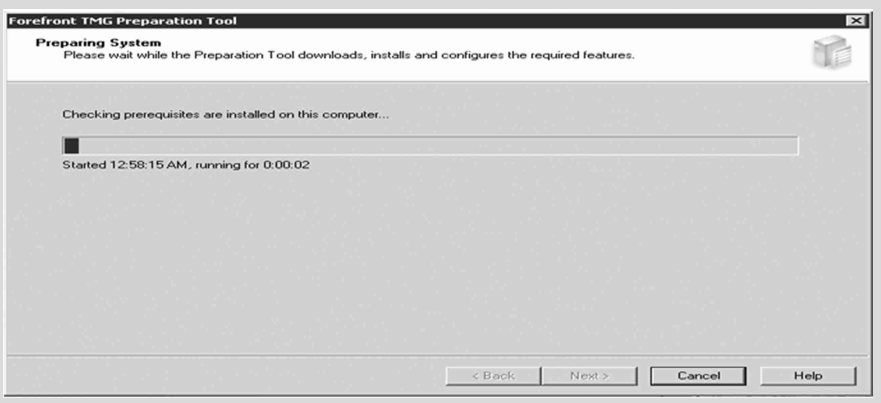
Gambar 7

7. Lalu akan muncul tampilan Installation Type, lalu pilih Forefront TMG service and Management, pilih Next. Seperti gambar 8.



Gambar 8

8. Berikut proses instalasi



Gambar 9

9. Installation Wizard selesai lalu klik next. Gambar 10

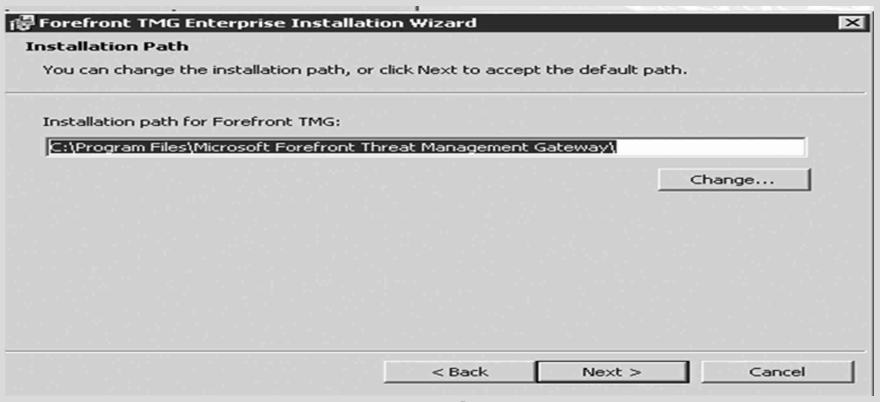
Gambar 10

10. License Installation Wizard seperti gambar 11

Gambar 11

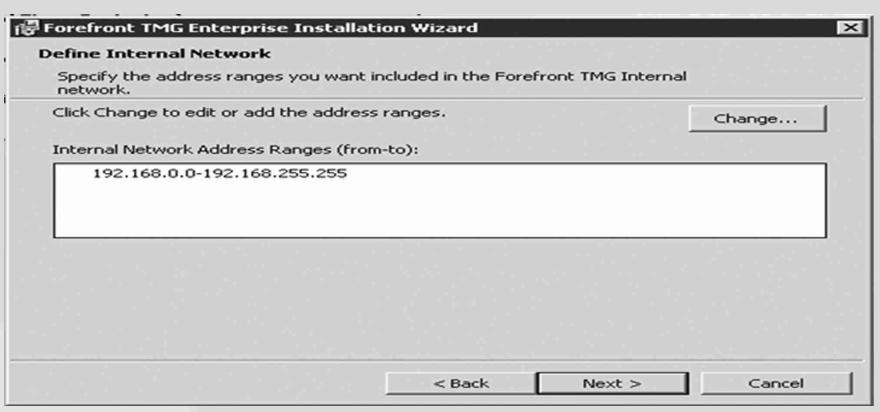
11. Pada user name masukkan windows user, pada Organization MSI, lalu klik next. Seperti gambar 12.

Gambar 12



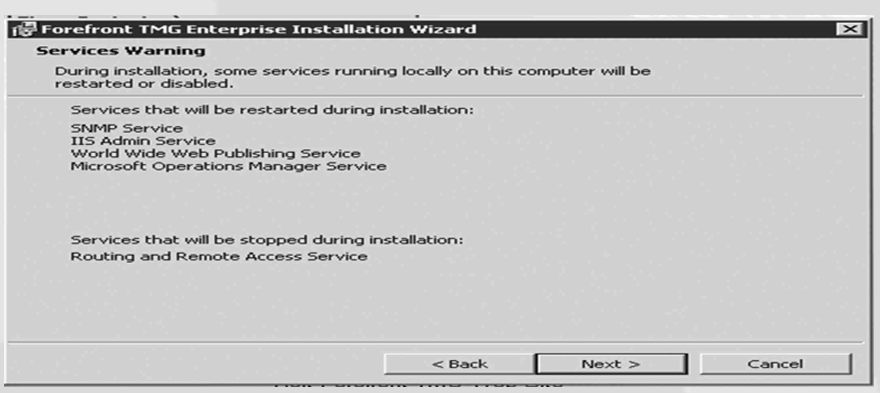
Gambar 13

12. Pada jaringan internal masukkan ip tersebut, seperti gambar 14



Gambar 14

13. Pilih Next



Gambar 15

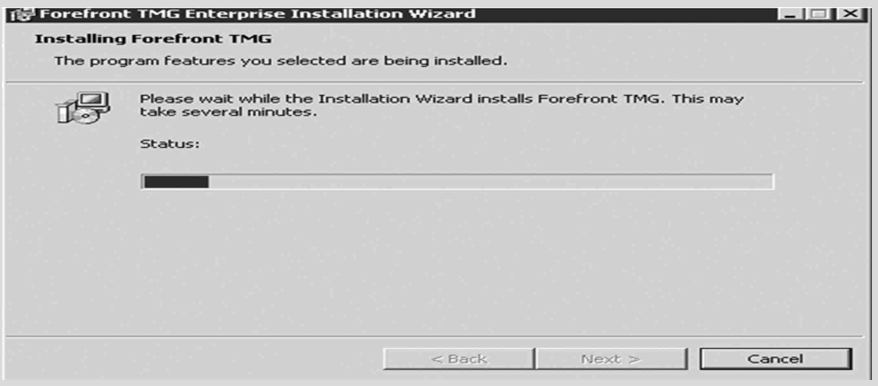
14. Pada tampilan ini pilih install. Gambar 16

Gambar 16

15. Berikut adalah tampilan installing Forefront TMG. Seperti 17.

Gambar 17

16. Ini adalah proses installasi forefront TMG. Seperti gambar 18.

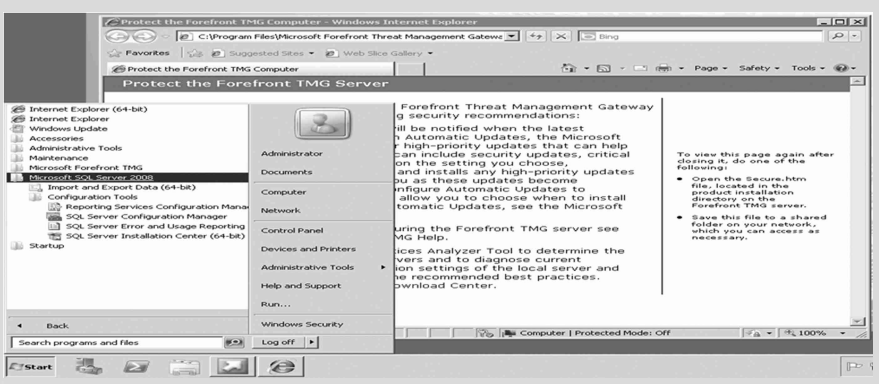


Gambar 18

17. Tampilan ini adalah proses selesai lalu tekan finish

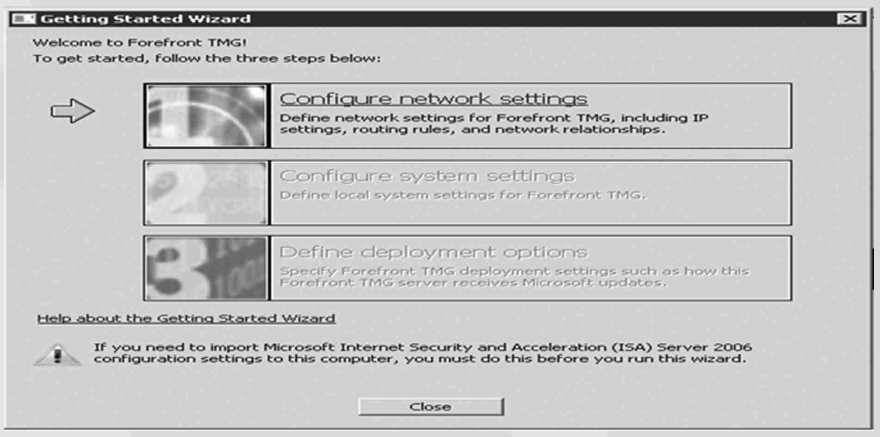
Gambar 19

Setelah selesai melakukan instalasi Forefront, maka komputer yang telah terinstal akan terprotect dengan ForeFront TMG Server, untuk mengetahui apakah komputer tersebut telah terprotect dengan melihat melalui internet Explorer. Seperti pada gambar 20.



Gambar 20

18. Ini adalah beberapa tahap jika sudah selesai instalasi forefront TMG.

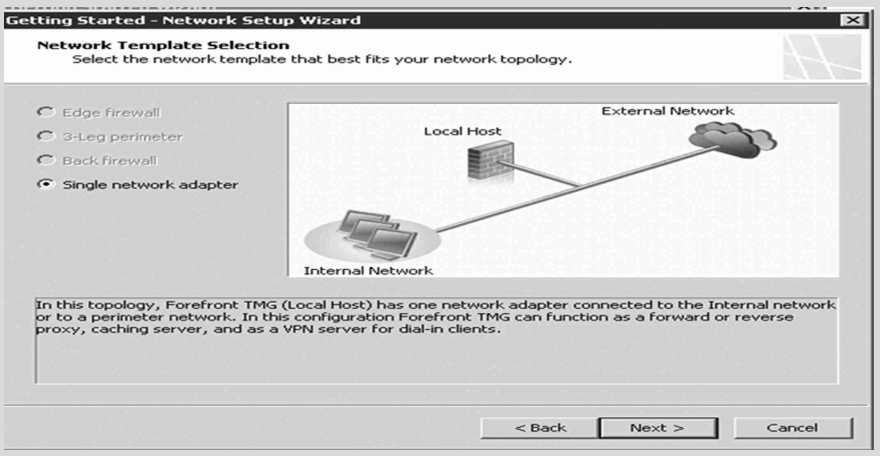


Gambar 21

19. Berikut adalah tampilan awal meu Wizard, lalu klik next. Seperti gambar 22.

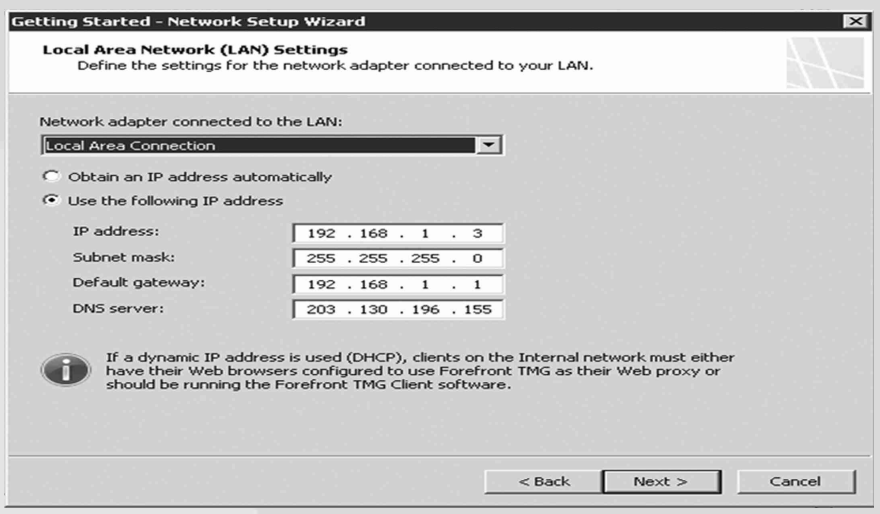
Gambar 22

20. Berikut adalah struktur jaringan single network adapter. Seperti gambar 23.



Gambar 23

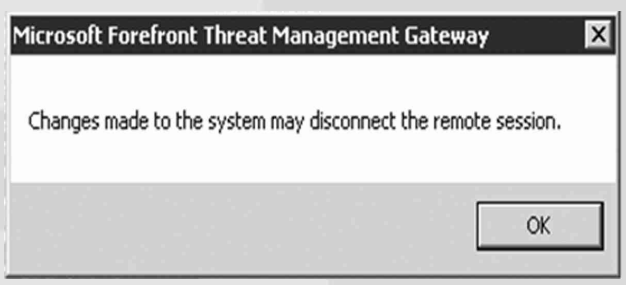
21. Pada tampilan IP address, subnet mask, default gatewaye, DNS server, usahakan no IP tersebut satu segmen. Seperti gambar 31.



Gambar 24

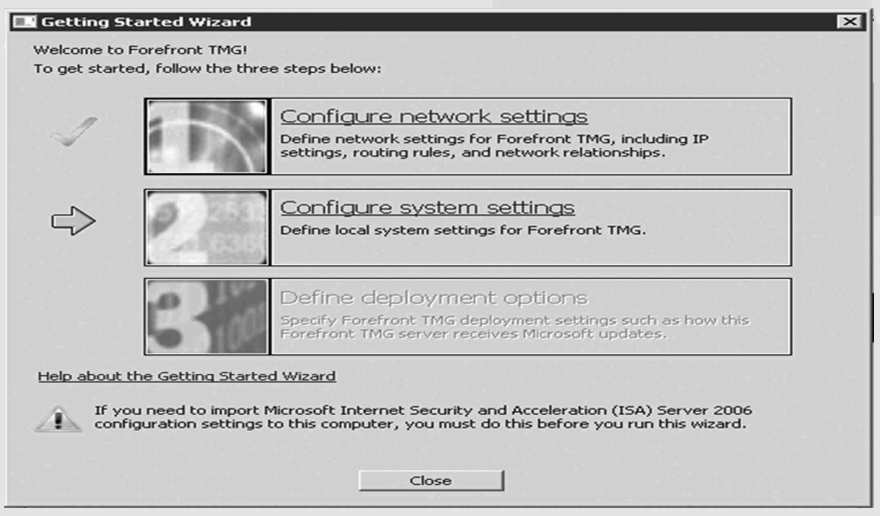
22. Pilih Finish,seperti gambar dibawah ini.

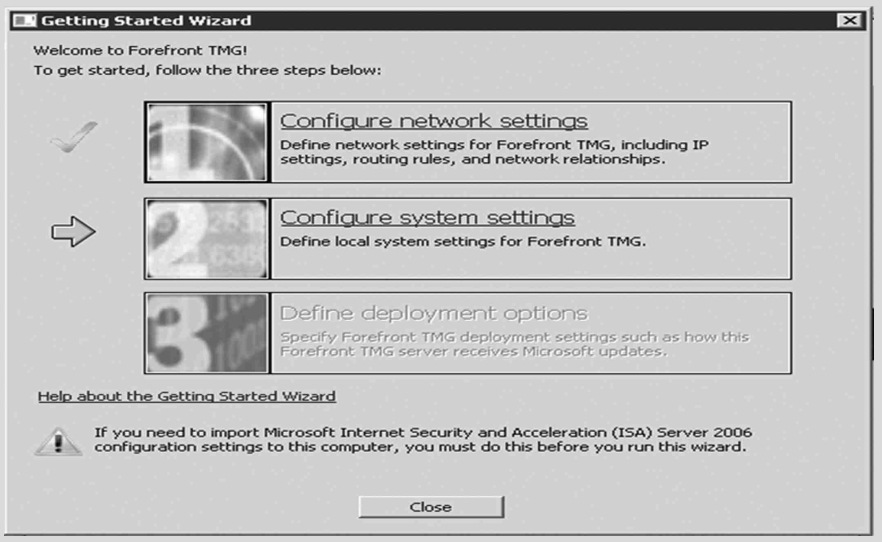
Gambar 25



Gambar 26

23. Tampilan ini adalah tahap yang akan diselesaikan kembali. Seperti gambar 27.



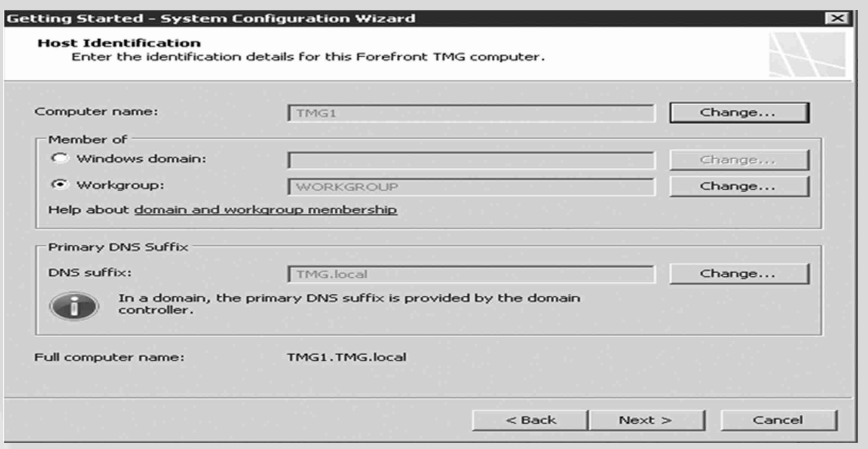


Gambar 27

24. Tekan next seperti pada gambar 28.

Gambar 28

25. Pilih workgroup untuk menjadi host, seperti gambar 36.



Gambar 29

26. Pilih Finish untuk selesai .

Gambar 30

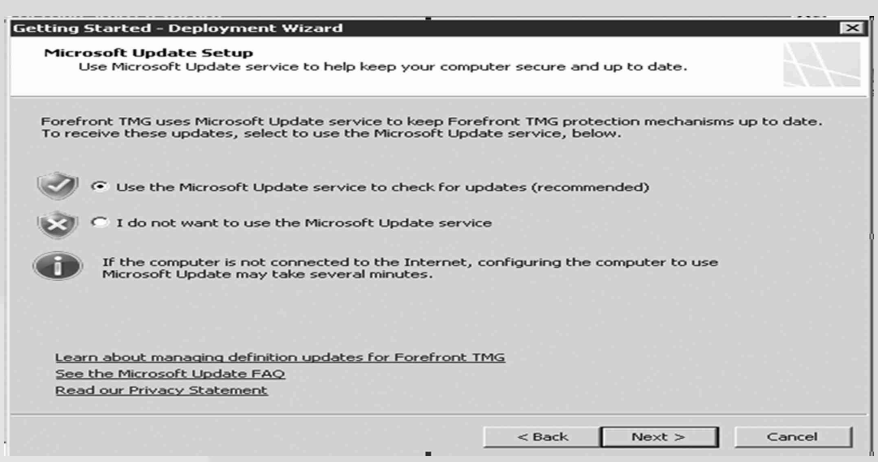
27. Masukkan pada tahap 3, untuk proses instalasi

Gambar 31

28. Pilih next seperti gambar 32.

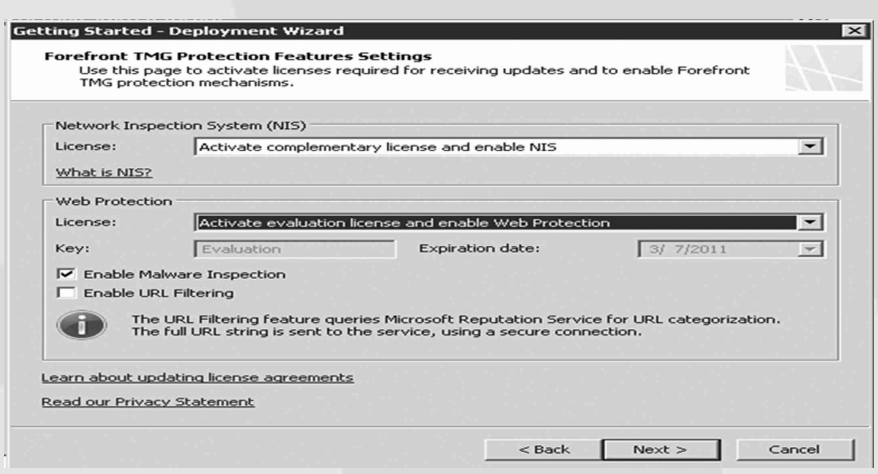
Gambar 32

29. Pilih next untuk melanjutkan, seperti gambar 33.

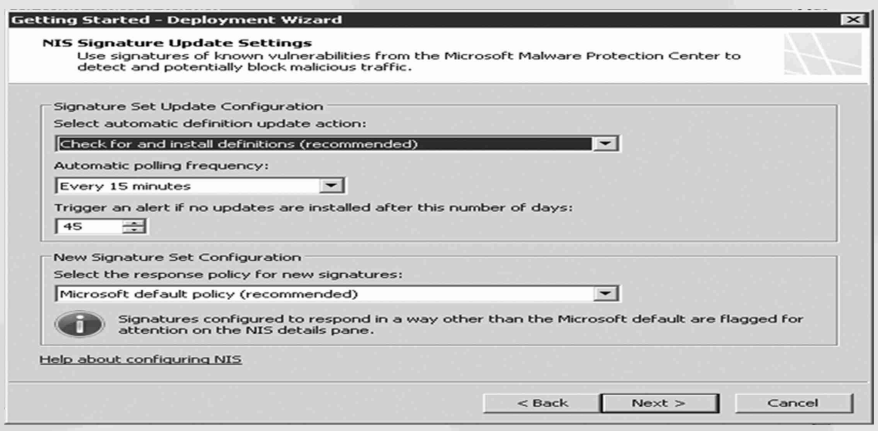


Gambar 33

30. Pilih next untuk melanjutkan. Seperti gambar 34 dan 35.

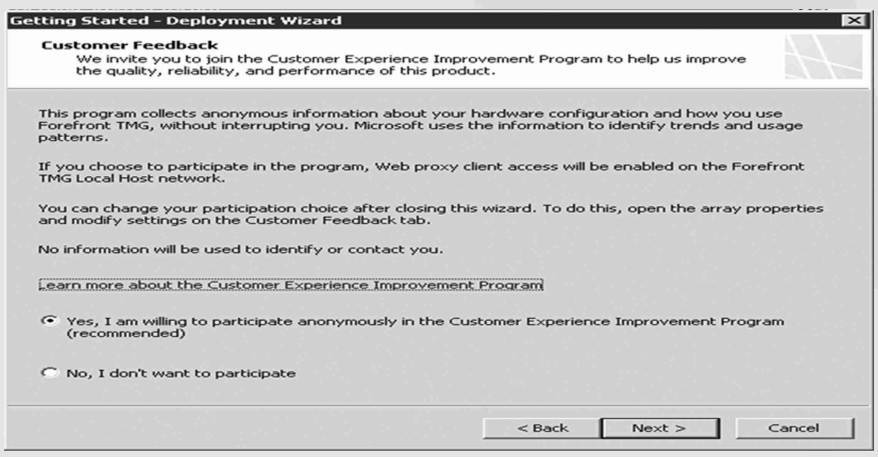


Gambar 34



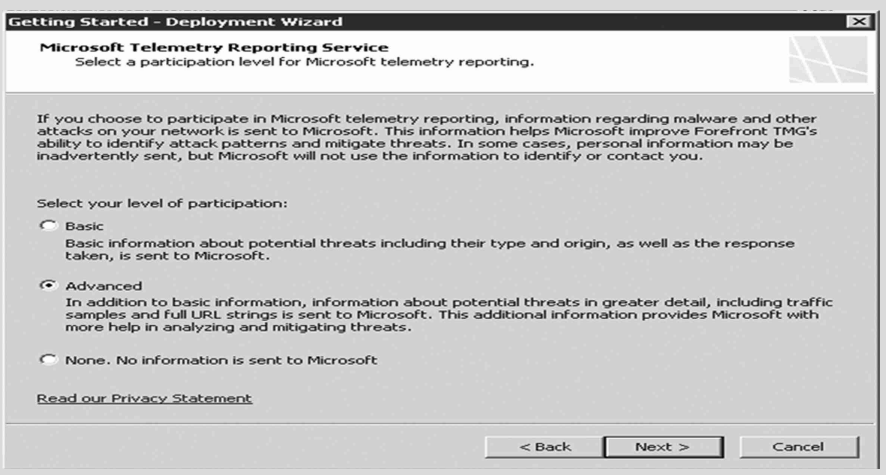
Gambar 35

31. Pilih yes, lalu klik next , seperti gambar 36



Gambar 36

32. Pilih Advanced, lalu klik next

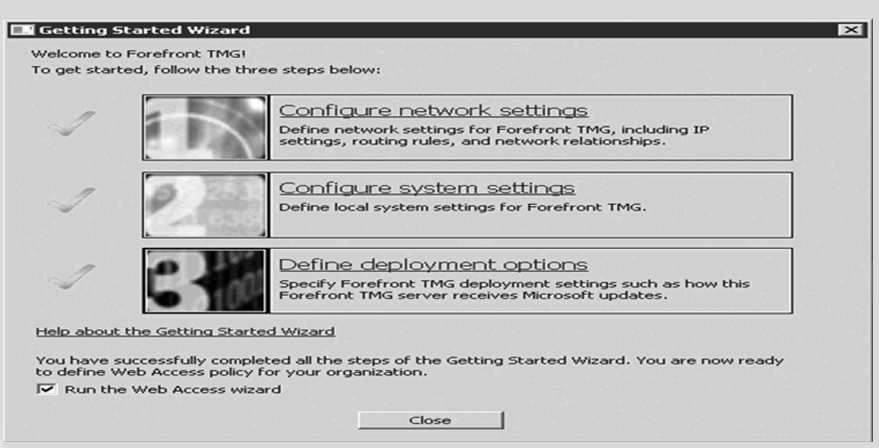


Gambar 37

33. Berikut adalah tampilan selesai.

Gambar 38

34. Semua tahap telah selesai dilakukan, seperti gambar 39.

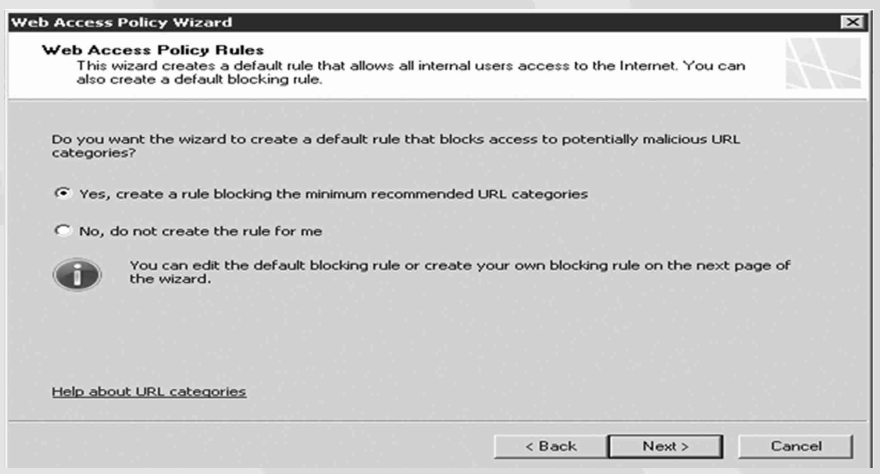


Gambar 39

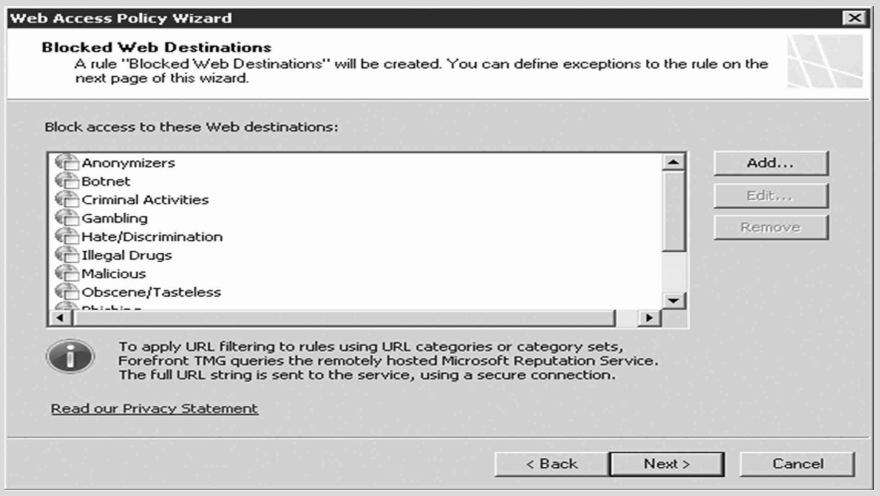
35. Setelah penginstalan selesai akan tampil tahap penginstalan Web Access Policy Wizard.

Gambar 40

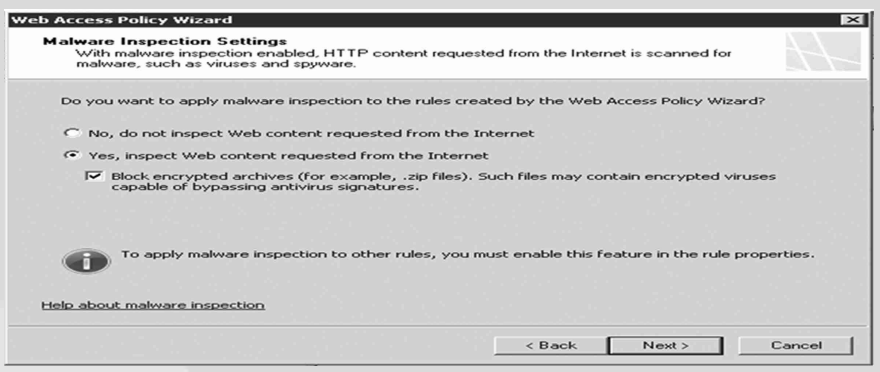
36. Pilih yes, lalu tekan next untuk melanjutkan. Seperti gambar 41.



Gambar 41

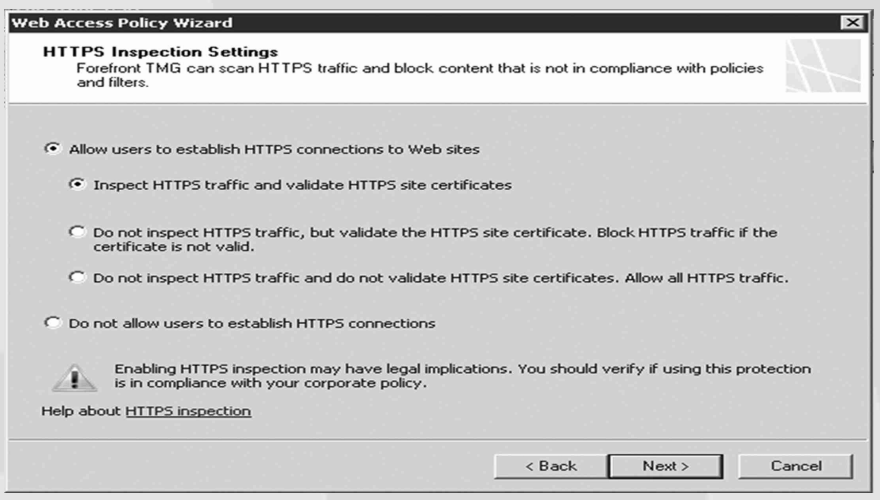


Gambar 42



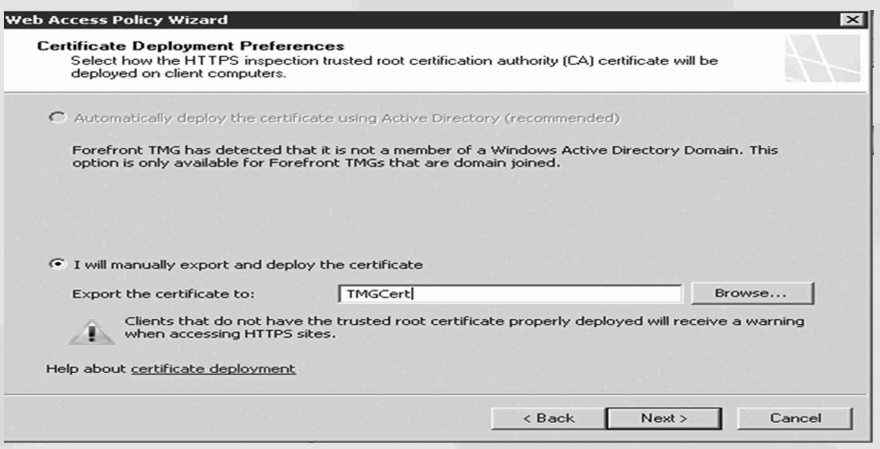
Gambar 43

37. Pilih allow users to establish HTTP dan inspect HTTPS



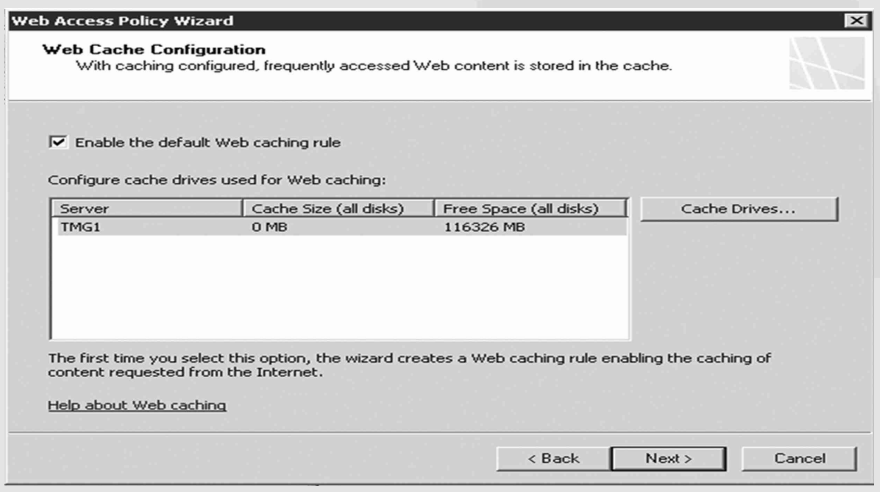
Gambar 44

38. Memilih cara manual dengan mengisikan TMGCert



Gambar 45

39. Status space yang ada di web acces policy



Gambar 46

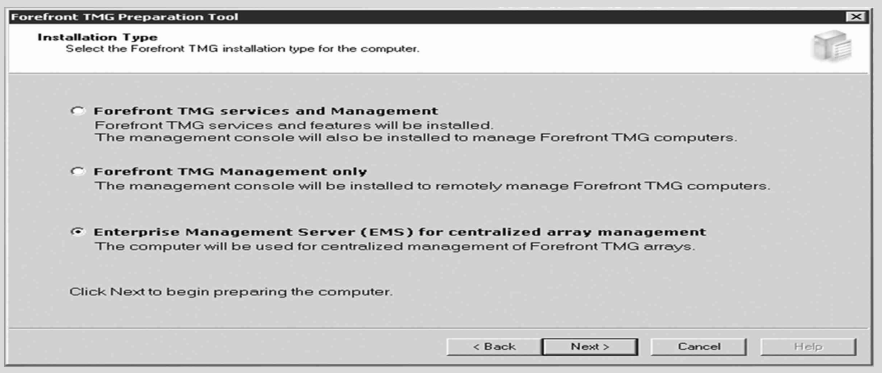
1. Selesai penginstalan web acces policy, lalu lunch TMG dan menampilkan dashboard TMG.
2. Create TMG EMS didalam server lain

Gambar 47

42. Halaman awal persiapan penginstalan

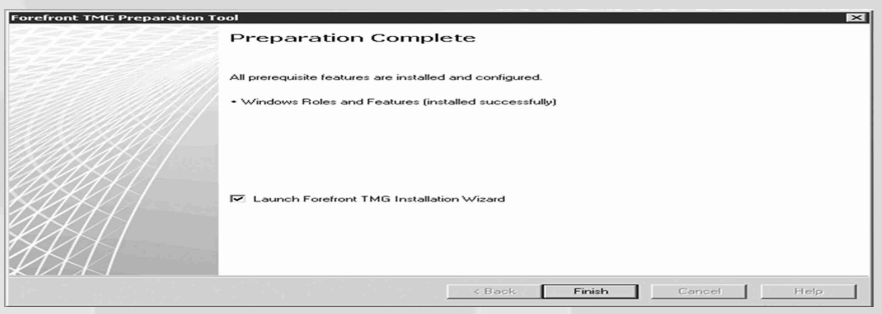
Gambar 48

43. Membuat EMS



Gambar 49

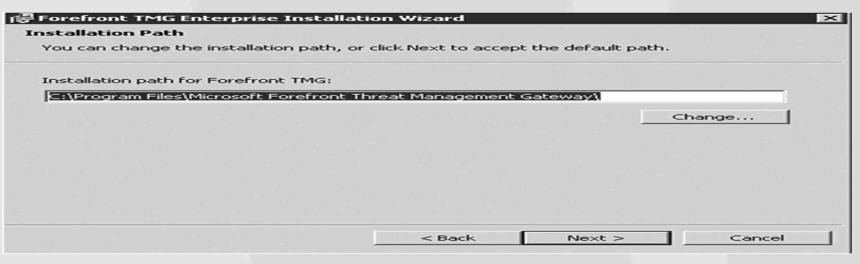
44. Progres penginstalan
45. Tahap persiapan selesai



Gambar 50

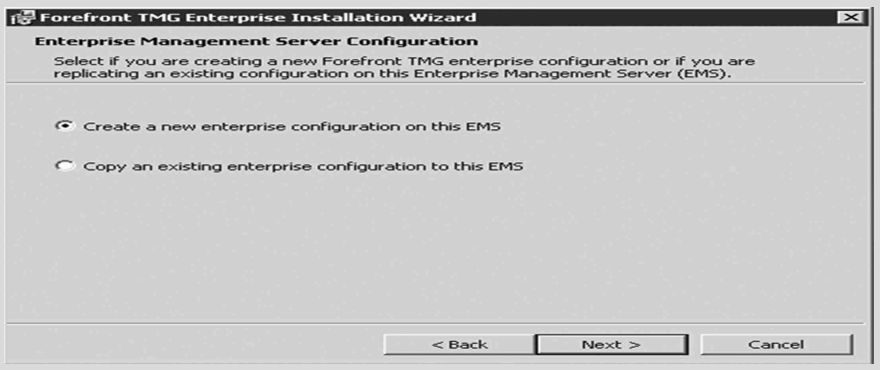
1. Lisensi
2. User name dan organization serta product key

Gambar 51



Gambar 52

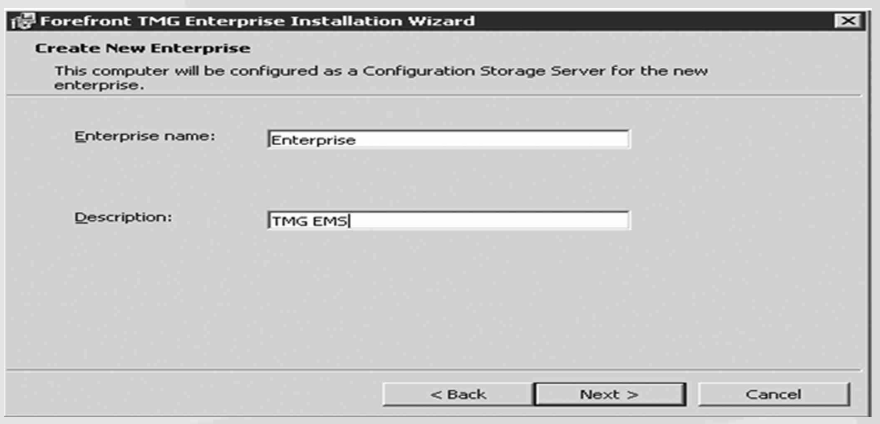
49. Membuat enterprise didalam EMS



Gambar 53

50. Peringatan enterprise baru

Gambar 54



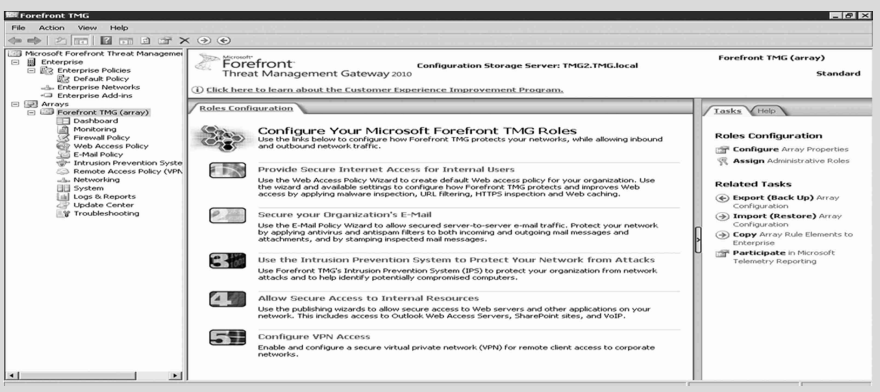
Gambar 55

52. Pilih apakah akan single atau workgroup

Gambar 56

53. Progres instalasi
54. Selesai instalasi

Gambar 57



Gambar 58

KESIMPULAN

Suatu keamanan merupakan suatu hal yang penting dalam system networking. Pembuatan konfigurasi keamanan yang baik pada firewall dalam suatu jaringan menunjang tingkat proteksi yang tinggi terhadap suatu server dan database di dalamnya dari user yang tidak memiliki hak akses.

Penerapan Thread Management Gateway pada Microsoft Forefront memberikan beberapa fitur yang memberikan beberapa fungsi, diantaranya melakukan filterisasi terhadap IP address dari suatu web ataupun IP Server, serta melakukan setting server untuk membuat konfigurasi server networking yang diinginkan.

DAFTAR PUSTAKA

http://www.klik-kanan.com/fokus/firewall.shtml

http://krisgeto.blogspot.com/2008/05/penjelasan-tentang-firewall.html

http://id.wikipedia.org/wiki/ Firewall

(http://www.microsoft.com/forefront/threat-management-gateway/en/us/product-documentation.aspx)