NET Security Manager

Version 2.1

User Manual

Document Version: 1.1

Last update: 06.07.2012

www.netakod.com

Copyright

NET Security Manager

Table of contents

Product Overview

Version history

1.0 MS Office Access based initial application, using Access as database and Access Forms as user input.

2.0 Database migration from Office Access to SQL Server/Express.
New, standalone user interface built in Visual Basic.
ACL calculation extremely improved.
Added support for Cisco PIX devices.
Installation wizard is built by Windows installer.
Added detailed reports: Networks, Networks – Hosts, Network Group Membership, Network Policy, Network Group Policy, Network Group Members, Devices- Interfaces and Services.
Save device configuration to flash and TFTP server support.
Calculating and warning of the networks with specified security policy and it has no any device layer 3 interface connection.
Some bug fixes

2.1 Bug fixed when generating ACL, duplicate ACL lines.
The timeout for fetching recalculation of ACLs from database is increased to support large amount of data.
Some program cosmetic improvements.
Minor bugs fixed.

What is NET Security Manager?

NET Security Manager is program for centralized managing network security policy by implementing network access control for overall organization. Management of security access to the network services is achieved by using access control lists (ACL) on networks routers, L3 switches, VPN devices, firewalls, dialups, wireless access points interfaces or any network device capable for IP routing and filtering. It is based on graphical user interface that simplify management and applying organization security policy over all network infrastructure based on TCP/IP protocol.

Logical scheme of application is depicted on Figure 1.

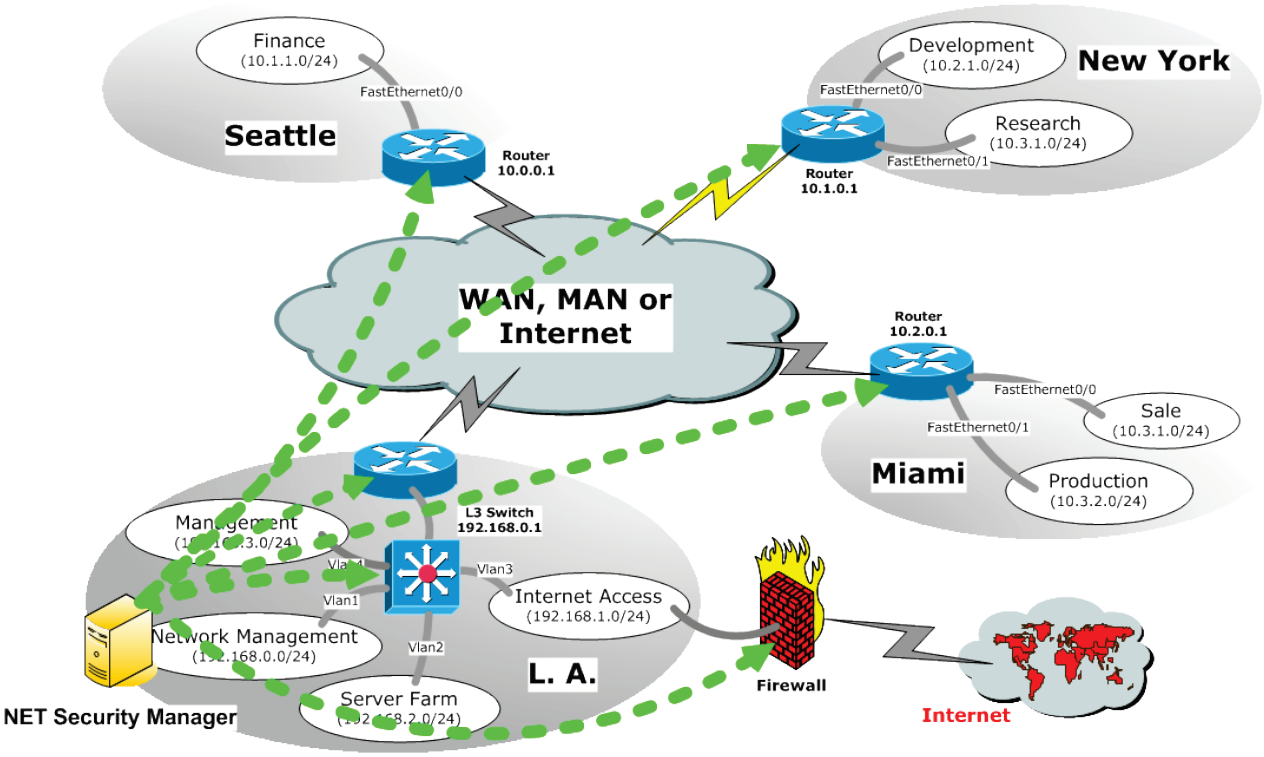

Figure 1. License Dialog

Applying security policy on network and transport layer (layer 3 and 4) of OSI communication model is powerful security mechanism that arising organization security to high level. Without network access control management each computer in any network can gain access and attack computer and server in whole organization information infrastructure, resulting in unauthorized data viewing, theft of proprietary information, data integrity changes, crashes of vital organization services, etc. This means that each computer or server (or any network device) is practically unsecured from inside intruders. Simplified, this situation leads to the system with no authorization of users in a network system, no integrated and manageable network access controls and no network access logging. The insider attack can affect all components of computer security. By accessing through a system, confidential information could be revealed. Viruses and Trojan horses are a threat to both the integrity and confidentiality of information in the system. Insider attacks can affect availability by overloading the system's processing or storage capacity, or by causing the system to crash.

Some computers or servers may hold very sensitive information or drive vital organization services, like financial, banking, strategic reports, organization structure, marketing, government, military and all other possible confidential data and services. Think about all possible damages, losing repute and other possible short and long term costs that can arise from this situation, especially when many statistic researches has showed that 70-80% of all security incidents is done from inside an organization (from insiders). That’s why it is important not to underestimate the enemy inside!

System Requirements

NET Security Manager requires the following minimum system configuration:

- **Operating System:** Microsoft Windows XP/Vista/7; Windows Server 2003/2008.
- **Database Server:** Microsoft SQL Server 2000 or Microsoft Desktop Engine 2000.
- **Memory:** 512 megabytes (MB) of RAM; 1 GB recommended.
- **Hard Disk:** 80 MB of available hard disk space.
- **Display:** VGA or higher-resolution monitor.
- **TCP/IP communication stack:** TCP/IP compliance for Internet connectivity (Windows have built-in).
- **ODBC connectivity:** 32-bit ODBC driver for SQL Server (Microsoft SQL Server/Express 2000 will install it).
- **TFTP server (optional):** To be able to backup network device configuration you need TFTP (*Trivial File Transfer Protocol*) server.
  Note that TFTP server station should not be the same computer/server where **NET Security Manager** is installed.

Network Requirements

NET Security Manager requires the following network access:

- **Telnet service:** To apply defined security policy you must ensure network telnet access (TCP port 23) from management station where NET Security Manager is installed to the network devices to which security policy is about to be applied.
- **TFTP service (optional):** To backup device configuration you must ensure network TFTP (*Trivial File Transfer Protocol*) service from network device to the TFTP station.
  Note that TFTP station should not be the same computer/server where **NET Security Manager** is installed.

Features

NET Security Manger basic features are:

- Centralized organization network security access control management over network and transport OSI layer (Layer 3 and 4).
- Vendor independent network security access control of all organization's network layer 3 devices.

- Network access control is achieved by applying ACL (*Access Control List*) on network layer 3 devices interfaces.
- Defining network security access policy for single IP (host), network, network segment or network/hosts group.
- Simplified and clarified security policy definition using Network Groups and assigning networks, hosts or network segments group membership.
- Already defined typical network services: IP, ICMP, TCP, UDP, DNS, SMTP, POP3, Telnet, HTTP, HTTPS, FTP (Active and Passive), TFTP, File Shearing, Lotus Domino, MS Exchange, NTP, ODBC, SQL Server, ODBC, SNMP, Syslog, RADIUS, …
- Custom definition of any required and specific services.
- Automatic policy appliance on redundant layer 3 network devices.
- Storing network information, network security policy and network device configuration backup - no need for additional network configuration backup & documentation.
- Managing of network objects database (NET Database).
- NET Database supports full recovery and replication features.
- Supports for multi-user environment over the network.
- Automatic calculating ACLs for all organization's network devices interfaces.
- Automatic highlighting interfaces with changed ACL due to security policy changes.
- Minimizing security policy applying time by automatic calculating interfaces ACL changes, due to security policy changes, and ability to apply changed security policy only on changed interfaces.
- Automatic highlighting networks with defined security policy and no connection to the any device interface.
- Ability to apply policy on single interface, all devices' interfaces, only changed device's interfaces, all interface for all devices or all changed interfaces for all devices.
- Applying network security policy without network interruption or need for network devices reboots to take effects.
- No network interruption or irregular security states if NET Security Manager lose network communication with device while applying security policy.
- Automatic backup network device's running configuration to flash or/and local file using TFTP file transfer.
- Unlimited number of networks/hosts - suitable for small, medium and large enterprise organizations with hundreds and thousands networks and hosts.
- Proved in a Military environment with strong security requirements and more than 500 networks and many hosts.

Database Format

NET Security Manager uses database called **NET Database** to store information about networks, network groups, network devices, interfaces, services, and all others network infrastructure objects and relevant information. NET Database is SQL Server 2000 database and you need SQL Server/Express 2000 or higher to drive this database. MS SQL Server Express edition is free.

Supports for multi-user administration over the network

NET Security Manager supports multi-user administration over the network. NET Database can be installed on one computer and **NET Security Manager** on many others. Database connection is established using TCP port **1433**. If you want to connect to remote NET Database over the network as NET Database SQL Server name enter IP address or host name of remote computer. Note that SQL Server/Express must be started on remote computer.

This can simplify your organization security management if you have two or more administrator or you want to place NET Database on server to be more secured. Any user can run NET Security Manager at its own computer and manager and apply security policy over the network concurrently. Thus, some administrators can manage network segments following geographical or logical distribution.

Supported network device manufacturers

NET Security Manager is designed to generally manage any layer 3 device (routers, layer 3 switches, dialups, firewalls, VPN concentrators, etc.) of any vendor that is capable for IP routing and interface packet filtering based on standard interface access control lists (ACL). ACL syntax varies from device vendors and **NET Security Manager** currently can work with this vendors and operating systems:

- Cisco Systems, any device with Cisco IOS capable for IP routing and IP packet filtering (IOS 10.3 and higher)
- Cisco Systems, Cisco PIX firewalls with software version 5.3 and higher

How to order and license

Trial version of NET Security Manager is available for download from **www.netakod.com**. Choose a region, and go to the Download section to download it.

For information on quantity pricing and site licenses, please visit NETAKOD web site at **www.netakod.com**, choose a region and go to the **Orders** section or you can send an e-mail message to **sales@netakod.com**.

You can purchase your registered license in following ways:

- Visit NETAKOD web site **www.netakod.com**, choose a region and go to the **Orders** section. For quicker registration, copy the **Application Reference Code(s)** (optional) and submit it with your order.
- Send an e-mail to **sales@netakod.com** with the following information: Program NET Security Manager, **Name**, **Organization** and **Application Reference Code(s)** (optional).

If **Application Reference Code(s)** is/are not supplied with your purchase, after payment process you will be contacted to get your license information.

To get your **Application Reference Code(s)** install and run NET Security Manager first. **Application Reference Code** is different for each computer and you can get it in **License Dialog** form after starting NET Security Manager, or click **Programs** and click **License** or click **About** (than click **Register)** in main program menu (see Figure 2.). Select **Application Reference Code** and copy it to your purchase.

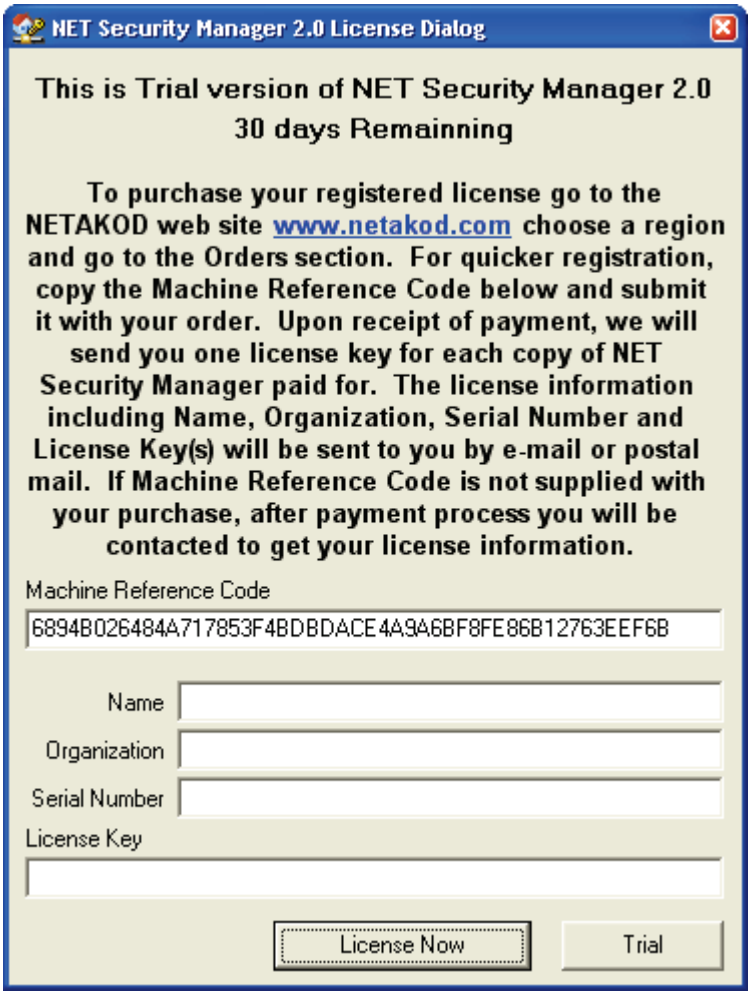

Figure 2. License Dialog

Upon receipt of payment, we will send you license key(s) for each copy of NET Security Manager paid for. The license information including **Name**, **Organization**, **Serial Number** and **License Key(s)** will be sent to you by e-mail or postal mail. Enter this information in same **License Dialog** (Figure 2.) and click **License Now** to license NET Security Manager. Enter all received license information in appropriate fields, otherwise you want be able to license NET Security Manager.

Orders will be processed within one to two business days after they are received by NETAKOD Community.

All software and software updates are available from **www.netakod.com**. Because the software is obtained by Internet download, no disk media will be mailed.

Any questions about the status of the shipment of the order, refunds, registration options, product details, technical support, volume discounts, dealer pricing, site licenses, or non-credit card orders, must be directed to NETAKOD Community (**www.netakod.com**) or to our partners.

Technical Support

Reporting problems

You can submit any problems or bug you are having with **NET Security Manager** send mail at **support@netakod.com.** Please describe the problem in as much details as possible. In your e-mail message, please include the following information:

- The version of NET Security Manager that you are using (as shown in the **About** dialog box).
- The operating system and version.
- The SQL Server or Express version.

NETAKOD Community will try to respond to all bug reports within one to two business days, and will try to resolve the problem as quickly as possible.

Feature requests and questions

We are very interested in hearing from our users. If you have a feature that you would like to see added to NET Security Manager, send e-mail to **support@netakod.com**, and specify NET Security Manager, your current program version and all your feature requirements and suggestion.

Getting Started

Program installation

Download **NETSecurityManager.exe** from www.netakod.com in Download section. Run this installation file to install **NET Security Manager** on your computer by following installation wizard. Installation will add **NET Security Manager** folder in **Programs** (click **Start** and click **All Programs** in Windows) and **NET Security Manager** shortcut on your desktop.

Database installation

When you first run **NET Security Manager** you will get form depicted in Figure 3.

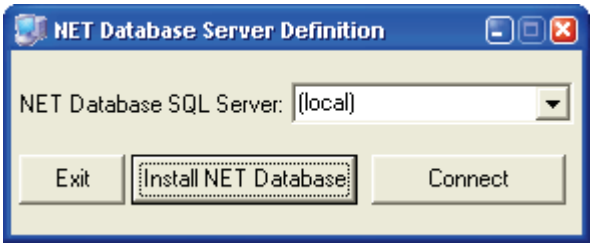

Figure 3. NET Database SQL Server definition.

Before first run of **NET Security Manager** you need to install **NET Database**. NET Database is Microsoft SQL Database and must be installed (attached) on your **SQL Server/Express**. Click **Install NET Database** to get the NET Database installation form (see Figure 4). If you already have installed NET Database on different computer you don't need to install it again, just define NET Database SQL Server name, that already has installed (attached) NET Database and click **Connect**.

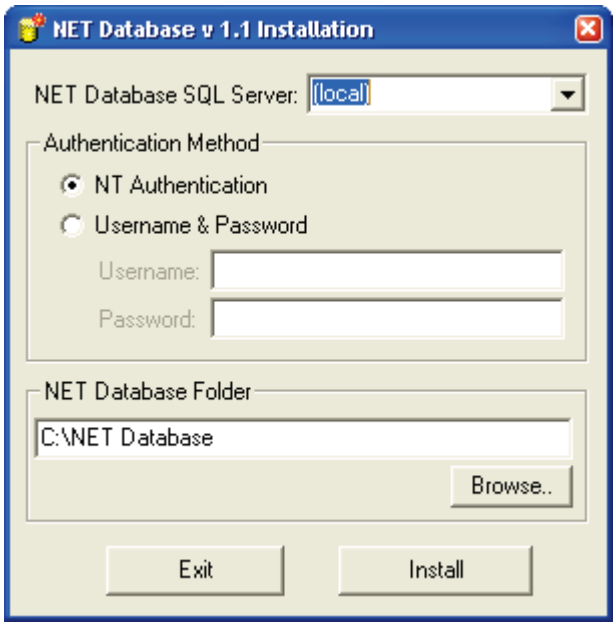

Figure 4. NET Database installation.

In **NET Database Installation** form, specify NET Database SQL Server/Express instance name. SQL Server/Express authentication mode can be NT authentication or username and password, depends on your SQL Server/Express configuration. Select NET Database folder where NET Database files (**NETDatabase.mdf** and **NETDatabase.ldf**) will be placed. Choose it carefully because it is good practice to backup this folder including NETdatabase.mdf and NETDatabase.ldf files.

NET Security Manager can work as **multi-user environment** over the network. NET Database can be installed on one computer and NET Security Manager on many others that can work concurrently. Database connection is established using SQL Server TCP port (default is 1433). If you want to connect to remote NET Database over the network as NET Database SQL Server name enter IP address or host name of the remote computer. Note, that SQL Server/Express must be started on remote computer.

Default password

NET Security Manager required user authorization. The default password after installation is **manager**. It is strongly recommended to change it and set your password. New password must be at least 5 characters long.

User's Guide

Network Design

Typically, organizations have their information infrastructure based on **LANs** (*Local Area Networks*) mutually connected over the **WANs** (*Wide Area Networks*) or **MANs** (*Metropolitan Area Network*) following geographical placement of their sites infrastructure. Logically, network infrastructure is split to small networks characterized with IP address and subnet mask. Usually, whole information infrastructure are split into logical networks like, Financial, Management, Sales, Development, Research, Marketing, Government, Agencies, Server Farm, Internet Access and any other possible segregations, following logical organization structure and requirements. Each network is connected to the layer 3 device interface. This interface is **Default Gateway** for that network. All layer 3 devices are interconnected, thus each network can access each.

With **NET Security Manager** you can manage network access security policy by controlling who can access to whom by which services; allowing users to access allowed services.

Basic Security Policy Definition

To control access to networks services access control list (ACL) should be applied on network interfaces. Generally, basic network security policy is defined by service between source and destination object, service direction and interface to apply ACL (source and/or destination) as depicted in Figure 5.

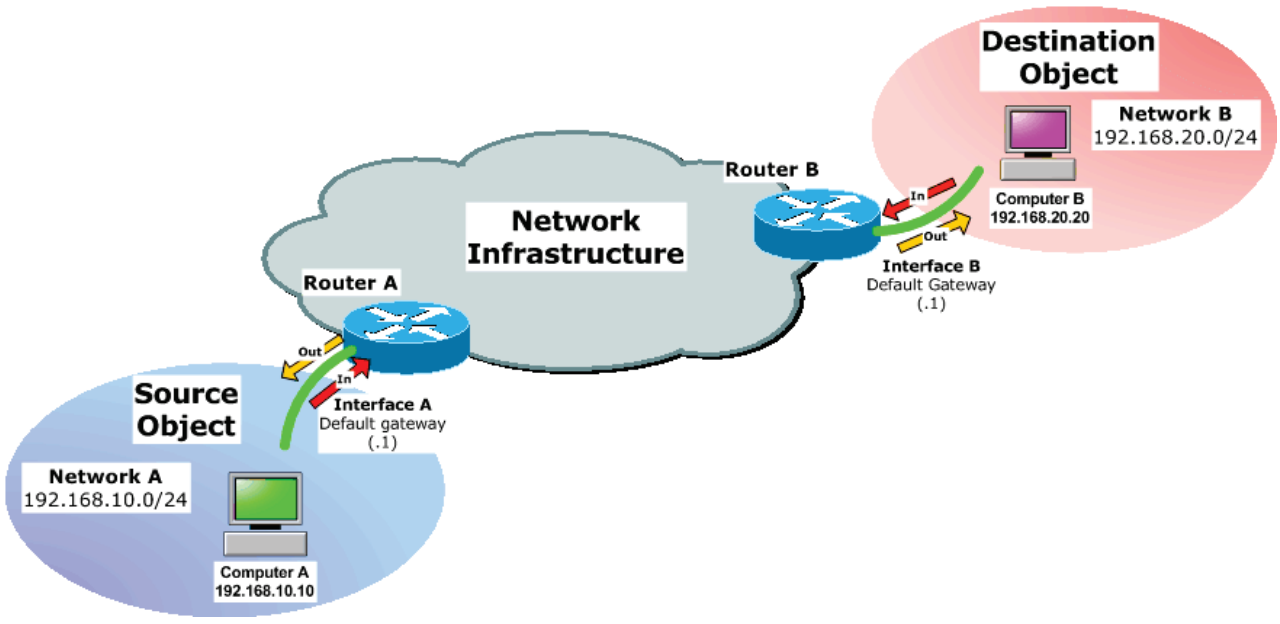

Figure 5. Source and Destination basic policy definition.

Source and destination object can be network, host, network segments or network group. Network group is a group of networks and hosts. When network group is, for e.g. source object, this means that all networks group members can access destination object by defined service.

Ones defined network groups can serve like templates that simplify security policy management. To give networks/hosts needed services, simple assign its network group membership.

User interface

Main user interfaces is illustrated in Figure 6.

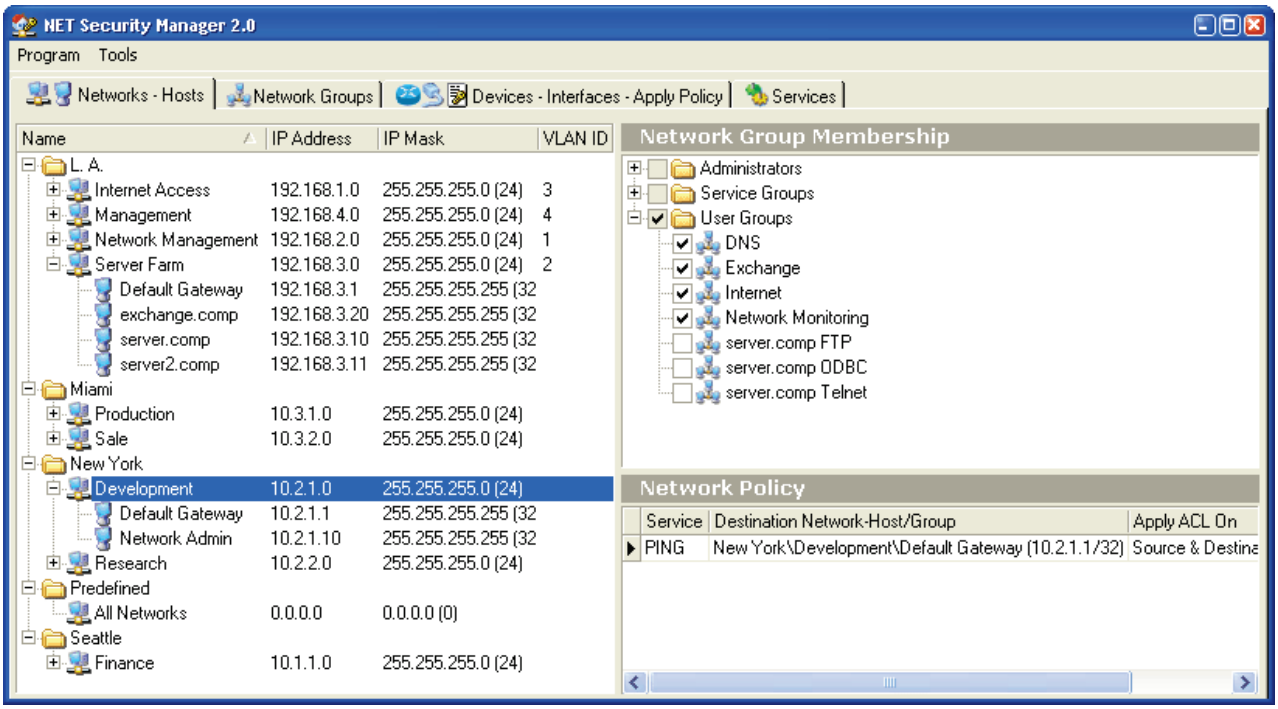

Figure 6. NET Security Manager User interface.

There are four main tabs:

- Network – Hosts,
- Network Groups,
- Devices – Interfaces – Apply Policy and
- Services.

In each tab, by right clicking mouse over the objects you'll get popup menu and you can add, delete, rename and manage objects.

Now we will start with description of each tab, starting with services as a basic policy element.

Services

To manage security policy you must define **services** between source and destination objects, first. NET Security Manager already has defined typical network services like IP, ICMP, TCP, UDP, PING, DNS, Telnet, HTTP, FTP, SMTP, POP3, File Shearing, MS Exchange and others (see Figure 7).

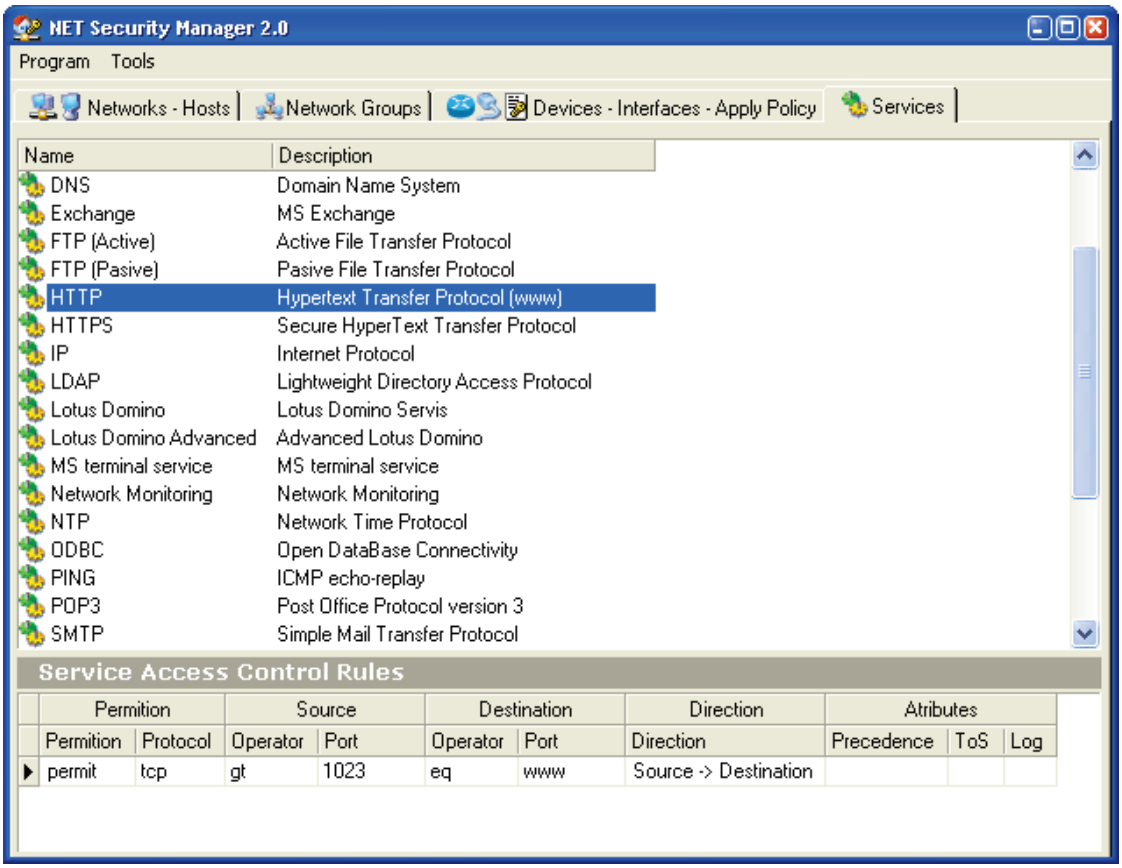

Figure 7. Services definition.

On service is composed of the **Service Control Access Rules**. Single Service Control Access Rule is defined by:

- **Permition:** permit or deny.
- **Protocol:** ip, tcp, udp, icmp, ospf, eigrp, gre, igmp, igrp, ipinip, nos, pim or type any number between 1 and 255 as ip protocol number.

- **Source Operator** (for tcp and udp protocols only): gt (greater then), lt (less then), eq (equal), neq (not equal), range (port range), or left it blank (all source ports).
- **Source Port** (for tcp and udp protocols only): choose any name in list of symbolic port names (telnet, www, smtp, pop3, snmp ...) or enter any numeric port number between 1 and 65536 or left it blank (all source ports).
- **Destination Operator** (for tcp and udp protocols only): gt (greater then), lt (less then), eq (equal), neq (not equal), range (port range) or left it blank (all destination ports).
- **Destination Port** (for tcp and udp protocols only): choose any name in list of symbolic port names (telnet, www, smtp, pop3, snmp ...) or enter any numeric port number between 1 and 65536 or left it blank (all destination ports).
- **ICMP Type** (for icmp protocol only): choose any name in list of symbolic icmp type names or enter numeric icmp type number between 1 and 255.
- **Direction:** Source->Destination, Destination->Source or Source<->Destination. For example, if source object need www service from destination object, choose Source->Destination direction. If destinations object need www service from source object choose Destination->Source direction. If source object need www service from destination object and destination object need www service from source object choose Source<->Destination direction. On Figure 5, Computer A can be source object and Computer B can be destination object in this example.
- **Log:** choose option log or left it blank.

You can go through the already defined services and see rules definition. Any new service you required simple ads them in services, assign its name and add its rules.

Networks - Hosts

Networks and **Hosts** as basic network elements are placed to folders that simplifying administration. Folders can be created to follow geographical distribution or logical grouping. **Network** is characterized by **Name**, **IP Address**, **IP Subnet Musk** and optional **VLANID** (if network is based on VLAN interface). **Host** has Name, **IP Address** and **IP Subnet Musk**.

Network must have at least one host - **Default Gateway** that will be attached to the device interface. Host can be single IP or network segment depends on IP Subnet Musk. If host is single IP host set IP Subnet Musk to 255.255.255.255 (default for hosts). If you want to add network segment enter IP Subnet Musk different then 255.255.255.255 that together with the IP Address defines the network segment.

By right-clicking mouse on selected Network or Host you'll get popup menu with **Connectionless** option as last. For a Network/Host without physical interface(s) set it to be Connectionless. Connectionless Network/Host is not verified to have unique IP Address. Network named '**All Networks**' in **Predefined** folder is an example of Connectionless

network. If you want to allow some Network or Host to access/give some service(s) to all networks use 'All Networks' as Destination Object.

Network – Host outlook is illustrated in Figure 8.

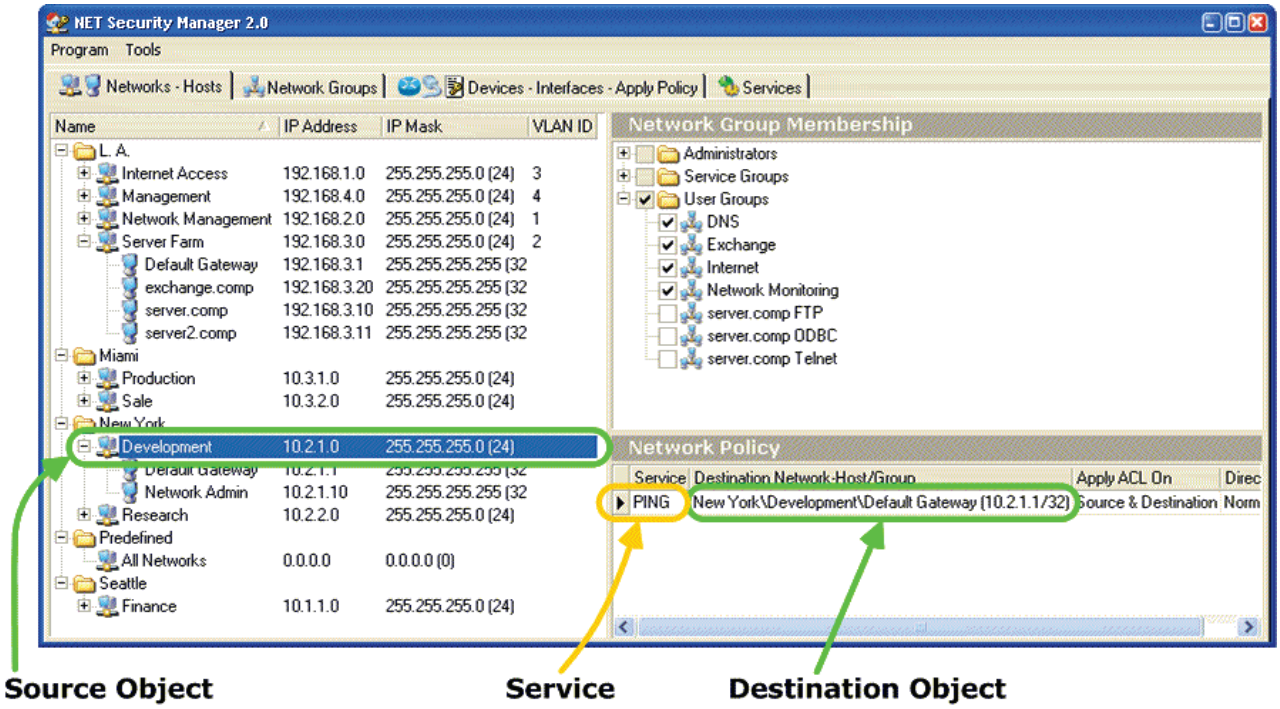

Figure 8. Networks – Hosts main outlook.

You can manage Folders, Networks and Hosts on left side. In right-top side, you can manage **Network Group Membership** for selected Network/Host. As Network Group Member Network/Host has the same rights (services) as defined in policy for this Network Group (see Network Groups). In right-down side you can define Network Policy for selected Network/Host as Source Object (see Figure 8). The fields in **Network Policy** have this meaning:

- **Service:** any service defined in Services,
- **Destination Network-Host/Group:** Destination Object; select any Network, Host or Network Group,
- **Apply ACL On:**
  - **Source Only**: this policy rule will be applied only on interface(s) attached to Source Object(s),
  - **Destination Only:** this policy rule will be applied only on interface(s) attached to Destination Object(s) and
  - **Source & Destination**: this policy rule will be applied on interface(s) attached to Source and Destination Object(s).

- **Direction:** policy rule direction. Available values are:
  - **Normal:** this policy rule will be created between Source and Destination Object with service rules direction(s) as defined in Services. If service rule direction is defined as bidirectional this rule will be applied as bidirectional.
  - **Opposite**: this policy rule will be created between Source and Destination Object with opposite service rules direction(s) as defined in Services. If service rule direction is defined as bidirectional this rule will be applied as bidirectional.
  - **Bidirectional**: this policy rule will be created between Source and Destination Object and also between Destination and Source Object no matter how service rules direction(s) is defined in Services.

Management of good defined **Network Groups** security policy can be very simple. For a new network, first add it; enter name, IP address, IP subnet musk, VLANID if it is based on VLAN. To give needed services for network simple check checkbox in **Network Group Membership** as require. To be able to send ICMP echo-request from network to its Default Gateway, add additional Network Policy; Service: ICMP, Destination Network-Host/Group (Destination Object): Network Default Gateway. If there is some hosts or group of hosts in the network that required some special services, add them as hosts in network and assign **Network Policy** for them on same way as for Network is (define Network Group Membership and/or Network Policy).

Not that any Host in Network will have access to the same services as Network has plus additional services specified for Host. Thus, you can specify common security policy for a network and for specific network users like power users, administrators, managers, specific users, etc. simple grant only them to access required services.

Network Groups

Network Groups simplifying Security Policy management. Network Groups are placed in folders, e.g. Administrators, Service Groups, User Groups, etc. Principles for defining security policy for Network Groups are the same like for Network/Host is.

Network Groups outlook is illustrated in Figure 9.

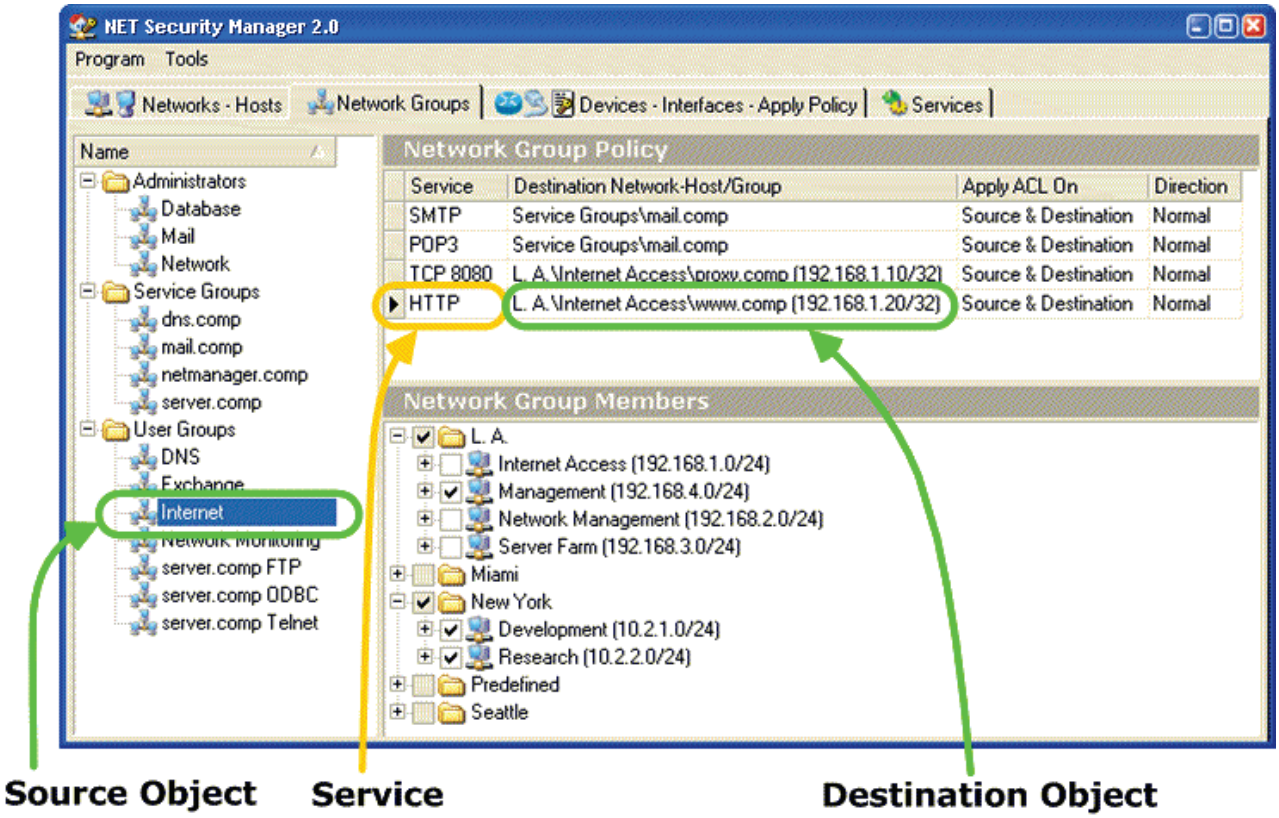

Figure 9. Network Groups main outlook.

On left side there are Network Groups. By right-clicking mouse over it you'll get navigation menu. On right-top side is **Network Group Policy** for selected Network Group. The fields in Network Group Policy; Service, Destination Network-Host/Group (Destination Object), Apply ACL On and Direction have the same meaning as described for Networks/Hosts in Network – Hosts section. Navigation is achieved by right-clicking mouse. On right-down side there are **Network Group Members**, so you can control Networks/Hosts that are members of selected Network Group.

To add/remove Network/Host from Network Group membership you can do it also in Network – Host tab by selecting specified Network/Host and assigning its Network Group Membership.

Devices – Interfaces – Apply Policy

Devices can be routers, L3 switches, VPN devices, firewalls, dialups, wireless access points interfaces or any layer 3 network devices. **Device – Interfaces – Apply Policy** outlook is depicted in Figure 10.

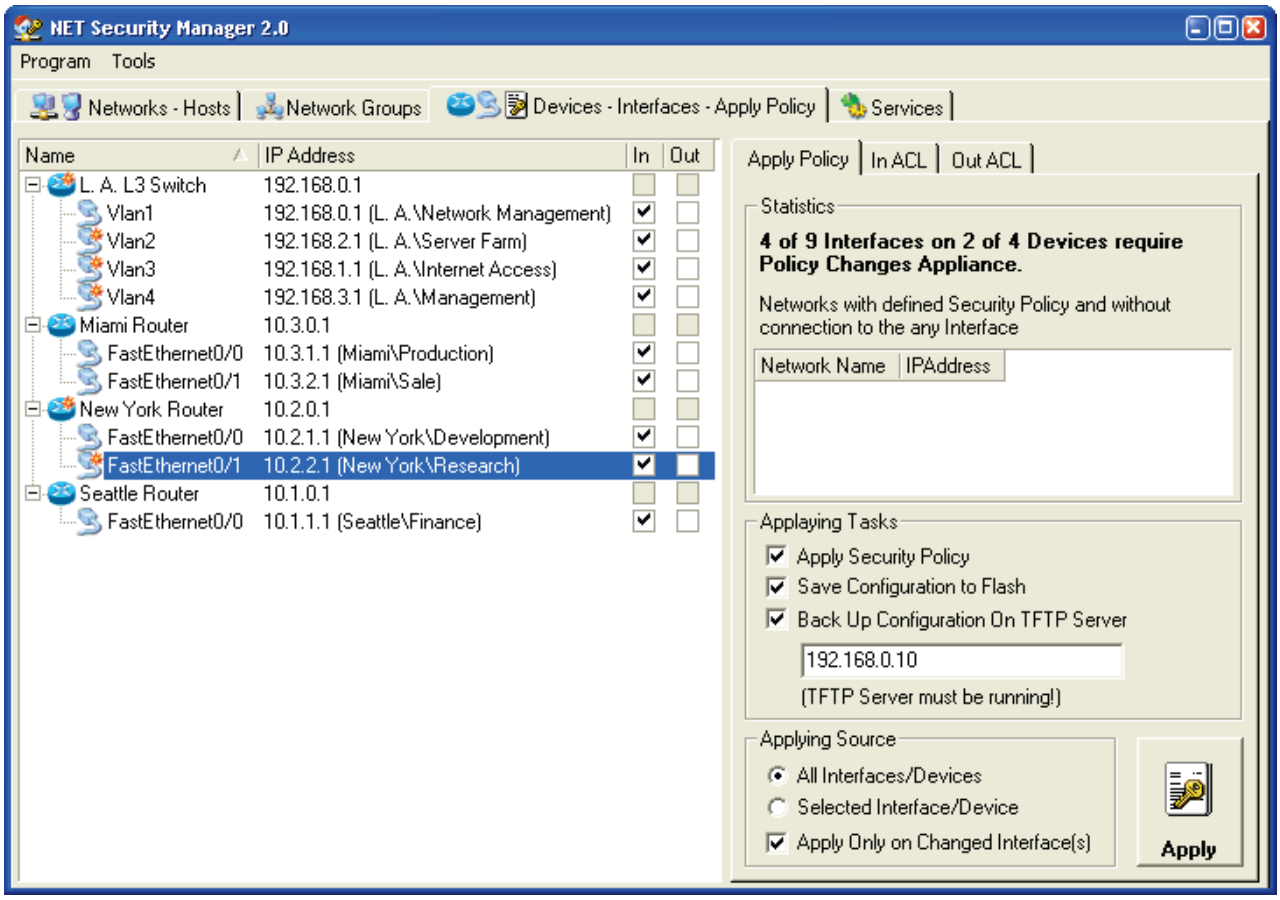

Figure 10. Devices – Interfaces – Apply Policy main outlook.

On left side, by right-clocking mouse you can manage network layer 3 devices and its interfaces. **Device** is described by **Name**, **IP Address** and **Location** (optional). To access to device in order to apply policy you must specify device **Username**, **Password** and **Cisco Enable Secret** (for device with Cisco IOS). Select device, right click mouse to get popup menu and click **Properties**. You'll get device properties form (see Figure 11.). Password and Cisco Enable Secret are typed with asterisk (*) signs.

Figure 11. Device Properties form.

Each device has interfaces as default gateways for networks. **Interface** is characterized by **Name**, **IP Address**, **In** and **Out** ACL appliance. Interface name must be the same as real device interface name is (e.g. Ethernet0, FastEthernet0/0, Vlan8, etc.). Interface IP Address defines which network is attached to the interface. Depends on defined policy for that Network, belonging hosts and Network Group Membership, access control list (ACL) has to be applied on interface. ACL is generated automatically by **NET Security Manager** and you can apply it on ingress (In) and/or egress (Out) of the interface. Input interface ACL is processed while IP packet ingress to the device interface, and output ACL while IP packet egress from device interface. It is recommended to apply policy only on input interfaces. Applying ACLs on input and output is redundant processing bat ensures strong security. It is not recommended to apply policy only on output or left interface without applying ACL on input and output.

Device – Interface – Apply Policy, on the right side, has tree tabs: Apply Policy, In ACL and Out ACL (see Figure 10.). **Apply Policy** tab has Statistics, Applying Task, Applying Source and Apply button. The **Statistics** displayed how much of the interfaces/devices required security policy appliance due to security policy definition changes. In statistics frame there is list of the networks with defined security policy and without connection to the any interface. If some network is listed there this is warning if you made mistake or if you forgot to define interface with connection to that network (interface IP address is default gateway of that network).

The **Applying Tasks** are:

- **Apply Security Policy:** Apply defined security policy on the device interfaces.
- **Save Configuration to Flash:** Save running configuration to the device flash (start up configuration) after ACL are applied on interface(s). If you save running configuration to flash, after reboot or reload device you will not lose configuration changes.

- **Backup Configuration on TFTP Server:** Save current running configuration to the text file on PC with TFTP (*Trivial File Transfer Protocol*) server started. Configuration file is one for one device and file name is device IP address plus '.cfg' extension (e.g. "10.2.0.1.cfg" for device 10.2.0.1).

Applying Source defines interface(s)/device(s) on which security policy will be applied. You can choose between **All Interfaces/Devices** and **Selected Interfaces/Devices**. If **Apply Only on Changed Interface(s)** is checked, policy will be applied only on changed interfaces. Changed interface is interface that has changed ACL from last appliance due to security policy definition changes. Changed interface has icon with red asterisk as indicator. If some device has at least one changed interface device icon also got icon with red asterisk as indicator that some its interface has been changed. Usually, you are making some security policy changes on networks, hosts, network groups, services or interfaces that will change ACL on some interfaces. You do not need to apply policy on all interfaces, but only on changed. Simple select All Interface(s)/Device(s) as Applying Source, check Apply Only on Changed Interfaces and click **Apply** button to apply policy only on changed interfaces/devices.

By clicking **Apply** button you will start applying defined Applying Tasks. Which tasks will be applied is defined by Applying Tasks and on which interfaces will be applied is defined by Appling Source. To apply tasks you must define device IP address, username, password and Cisco enable secret (for devices with Cisco IOS). Select device, right-click mouse, click on Properties and enter required device properties. Applying tasks on devices is achieved by standard telnet connection and you must ensure that station running **NET Security Manager** have access to the managed devices over telnet port (TCP port 23). Note that defined interface names must be exactly as interface names on physical device.

If network connection is broken while applying policy on device (e.g. cable connection problem, network failing out, power supply shutdown), device will continue to work with last policy definition. In and out access list on device interface is extended access list. Name of extended access list is interface name + 'In' for input and interfaces name + 'Out' for output access list. If access list with this name is already in function, '.1' is added on the end of name. After all access roles are added access list is about to attach to the interface. After attaching new access list on the interface old access list is removed. This procedure ensures immunity to connection failures.

After policy has been applied on interface it takes affects immediately while running, and no need for rebooting or reloading device.

Options

In **NET Security Manager** main menu click **Tools**, click **Options** and you'll get form **NET Security Manager Options** form (see Figure 12.).

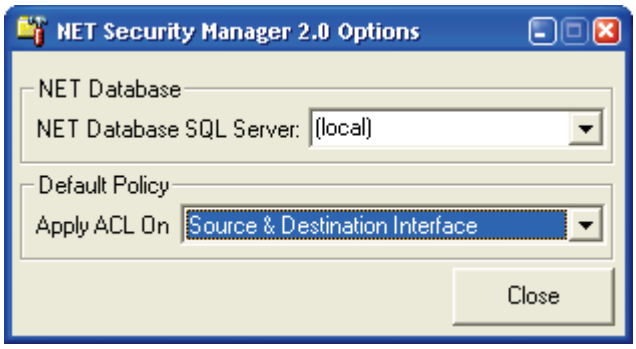

Figure 12. NET Security Manager Options.

You can define **NET Database** SQL Server name. If you change this name you must close and start again **NET Security Manager** to connect to new SQL Server. Note that SQL Server must have attached **NET Database**; otherwise you'll be prompted to install NET Database.

Default Policy defines default values when adding new policy in Network Policy (Network – Host tab) or Network Group Policy (Network Groups tab).

Reporting

In main menu click **Reports** and click on required report. You can generate the following reports:

- Networks
- Networks - Hosts
- Network Group Membership
- Networks Policy
- Network Groups Policy
- Network Groups Members
- Devices – Interfaces
- Services

Procedure for adding new network

Suppose you have already defined required network groups and services. You need to add new network in your network infrastructure, for example, Research department at the New York site (see example). Research department IP address is 10.2.2.0 with musk 255.255.255.0. Default gateway IP address is 10.2.2.1 and this network is attached to the FastEthernet0/1 interface on New York router. Research department required DNS, Exchange, Internet, server.com by telnet service and should be managed and supervised by network management stations. In research department there is database administrator 10.2.2.10 who administering database on server.comp at L. A. site.

Procedure for adding new Research network is following steps:

- On **Network – Host** tab add network in folder 'New York'. Enter network name 'Research', IP address 10.2.2.10 and IP subnet musk 255.255.255.0
- In Research network add host 'Default Gateway' with IP address 10.2.2.1 and musk 255.255.255.255
- Select Research network and assign network group membership to give Research network required services: check DNS, Exchange, Internet, server.comp Telnet and Network Monitoring in User Groups folder.
- In Network Policy add service PING and select 'New York\Research\Default Gateway (10.2.2.1/32)' as destination object. This permits all Research network hosts to use ICMP echo (PING) to check network connectivity with its default gateway.
- In Research network add host 'Database Admin' with IP address 10.2.2.10 and mask 255.255.255.255. In Network Group Membership check Database in Administrators folder.
- On physical New York router 10.2.0.1 set IP address 10.2.2.1 255.255.255.0 for FastEthernet0/1 interface.
- On **Devices – Interfaces – Apply Policy** tab add New York router (if not added before): name New York Router, IP address 10.2.0.1. Right-click mouse and click Properties. Enter username, password and Cisco enable secret (if running on Cisco IOS) to be able to access this router and apply policy on its interfaces.
- In **Applying Task** at least check **Apply Security Policy** and you might check **Save Configuration** to **Flash** and **Backup Configuration to TFTP Server** (enter IP address of TFTP server that must be running), also. As **Appling Source** select **All Interfaces/Devices** and check **Apply Only on Changed Interface(s)**.
- Click **Apply** button to apply changes in defined security policy on devices interfaces.

Capturing unknown services

If there are some services and applications in your network for which you don't know using ports and/or connection flow, you can find it in the following ways:

- Capturing traffics by the network sniffer or traffic analyzer that is attached to the appropriate network or by
- Sending traffic information to the Syslog server. For the all traffic that is explicitly denied by the interface access control list (ACL) network device is capable to send information about denied IP packets like protocol type, source and destination IP address and port to the Syslog server. Thus, you can run your unknown application and determine used ports and network flow sequences by the received Syslog

information and than you can define it in the NET Security Manager's Services section.

To activate device to send all denied traffic information to the Syslog server, first you must ensure that the Syslog server is running in the network and that the device that is about to send Syslog information is configured to send sending information in the NET Security Manager go to the **Devices – Interface – Apply Policy** section. Select Device's interface for the monitoring network, click on **In ACL** or **Out ACL** tab that will show you generated interface's access list. Right-click the mouse over access list and click on **Logging** option. The last ACL line will be changed to "deny ip any any log"; meaning that any denied packet information will be sent to the Syslog server. Than apply this ACL on this device by clicking **Apply** button on **Apply Policy** tab.

To send information to the Syslog server, network device should be configured also. Here is the example of Syslog server (192.168.0.10) configuration for the Cisco IOS compatible devices:

```
logging facility syslog
logging 192.168.0.10
```

After application discovering process is finished don't remember to switch off sending denied IP packet information to the Syslog server by clicking again on the **Logging** option and click on **Apply** (**Apply Policy** tab).

Example

The example of real network infrastructure is given in Figure 13. This can be any Community or organization that is usually spread at many sites, or can be simple Community placed at one site.

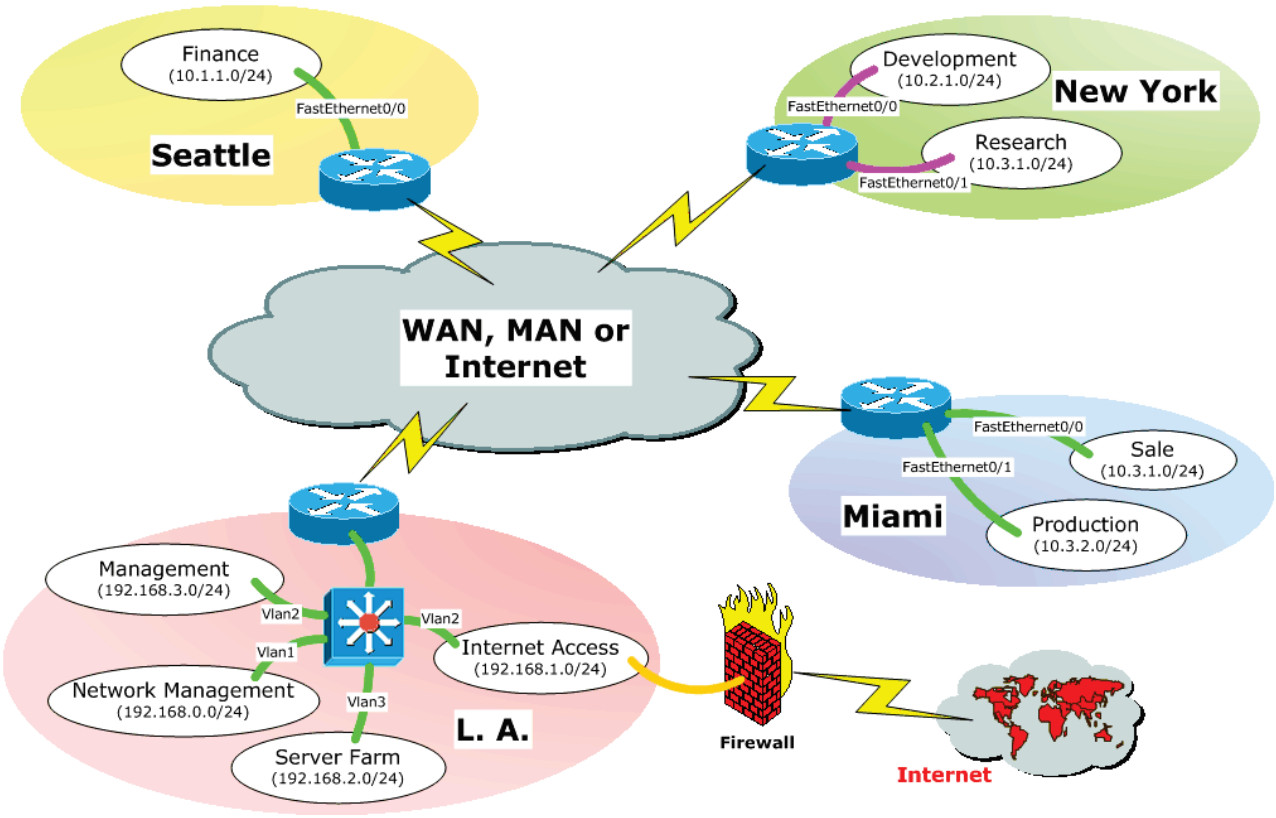

Figure 13. Network infrastructure example.

In this example network is consisted of four sites (LANs): L.A., Seattle, New York and Miami. The sites can bi interconnected using WAN (Wide Area Network), MAN (Metropolitan Area Network) or the Internet. Links can be based on gigabit Ethernet, ATM, Frame Relay, IP over SONET/SDH, PPP, etc. Connection to the Internet is centralized at L. A. site (or can be distributed). The main site is in L. A. with Internet Access, Server Farm, Network Management and Management department. Other branch offices are Seattle with Finance department, New York with Development and Research department and Miami with Sale and Production department. In this example we are using "comp" as Community domain name: dns.comp, proxy.comp, etc.

Table 1. lists Networks and Hosts and defined security policy, Table 2. lists Network Groups and defined security policy and Table 3. lists Devices and Interfaces definition.

Network – Host	IP Address	Network Group Membership Network Policy
L. A.		
Management	**192.168.4.0/24 (VLANID: 4)**	User Groups\DNS User Groups\Exchange User Groups\Internet User Groups\Network Monitoring User Groups\server.comp FTP User Groups\server.comp ODBC User Groups\server.comp Telnet
		PING: L. A.\Management\Default Gateway (192.168.4.1/32); Source & Destination; Normal
Default Gateway	192.168.4.1	
General Director	192.168.4.10	Administrators\Database Administrators\Mail Administrators\Network
Network Admin	192.168.4.20	Administrators\Network
Database Admin	192.168.4.30	Administrators\Database
Mail Admin	192.168.4.40	Administrators\Mail
Server Farm	**192.168.2.0/24 (VLANID: 2)**	User Groups\Network Monitoring
		PING: L. A.\Server Farm\Default Gateway (192.168.2.1/32); Source & Destination; Normal
Default Gateway	192.168.2.1	
server.comp	192.168.2.10	Service Groups\server.comp
server2.comp	192.168.2.11	Service Groups\server.comp
exchange.comp	192.168.2.20	
Internet Access	**192.168.1.0/24 (VLANID: 3)**	User Groups\Network Monitoring
		PING: L. A.\Internet Access\Default Gateway (192.168.1.1/32); Source & Destination; Normal
Default Gateway	192.168.1.1	
dns.comp	192.168.1.2	Service Groups\dns.comp
dns2.comp	192.168.1.3	Service Groups\dns.comp
mail.comp	192.168.1.5	Service Groups\mail.comp
mail2.comp	192.168.1.6	Service Groups\mail.comp
proxy.comp	192.168.1.10	

Network – Host	IP Address	Network Group Membership Network Policy
www.comp	192.168.1.20	
Network Management	**192.168.2.0/24 (VLANID: 1)**	
		PING: L. A.\Network Management\Default Gateway (192.168.2.1/32); Source & Destination; Normal
Default Gateway	192.168.2.1	
Management Station	192.168.2.10	Service Groups\netmanager.comp
Management Station 2	192.168.2.20	Service Groups\netmanager.comp
Seattle		
Finance	**10.1.1.0/24**	User Groups\DNS User Groups\Exchange User Groups\Network Monitoring User Groups\server.comp ODBC User Groups\server.comp Telnet
		PING: Seattle\Finance\Default Gateway (10.1.1.1/32); Source & Destination; Normal
Default Gateway	10.1.1.1	
Database Admin	10.1.1.10	Administrators\Database
New York		
Development	**10.2.1.0/24**	User Groups\DNS User Groups\Exchange User Groups\Internet User Groups\Network Monitoring
		PING: New York\Development\Default Gateway (10.2.1.1/32); Source & Destination; Normal
Default Gateway	10.2.1.1	
Network Admin	10.2.1.10	Administrators\Network
Research	**10.2.2.0/24**	User Groups\DNS User Groups\Exchange User Groups\Internet User Groups\Network Monitoring User Groups\server.comp Telnet
		PING: New York\Research\Default Gateway (10.2.2.1/32); Source & Destination; Normal
Default Gateway	10.2.2.1	

Network – Host	IP Address	Network Group Membership Network Policy
Database Admin	10.2.2.10	Administrators\Database
Miami		
Production	**10.3.1.0/24**	User Groups\DNS User Groups\Exchange User Groups\Network Monitoring User Groups\server.comp FTP
		PING: Miami\Production\Default Gateway (10.3.1.1/32); Source & Destination; Normal
Default Gateway	10.3.1.1	
Mail Admin	10.3.1.10	Administrators\Mail
Sale	**10.3.2.0/24**	User Groups\DNS User Groups\Exchange User Groups\Network Monitoring User Groups\server.comp Telnet
		PING: Miami\Sale\Default Gateway (10.3.2.1/32) Source & Destination; Normal
Default Gateway	10.3.2.1	
Network Admin	10.3.2.10	Administrators\Network

Table 1. Networks and Hosts definition.

Network Groups	Network Group Policy			
	Service	Destination Object	Apply ACL On	Direction
Administrators				
Database	ODBC	Service Group\server.comp	Source & Destination	Normal
	FTP	Service Group\server.comp	Source & Destination	Normal
	Telnet	Service Group\server.comp	Source & Destination	Normal
	HTTP	Service Group\server.comp	Source & Destination	Normal
Mail	MS terminal service	Service Group\mail.comp	Source & Destination	Normal
Network	MS terminal service	Service Group\netmanager.comp	Source & Destination	Normal
Service Groups				
dns.comp				
mail.comp				
netmanager.comp				
server.comp				
User Groups				
DNS	DNS	Service Group\dns.comp	Source & Destination	Normal
Exchange	Exchange	L. A.\Server Farm\exchange.com (192.168.2.20/32)	Source & Destination	Normal
Internet	SMTP	Service Group\mail.comp	Source & Destination	Normal
	POP3	Service Group\mail.comp	Source & Destination	Normal
	TCP 8080	L. A.\Internet Access\proxy.comp (192.168.1.10/32)	Source & Destination	Normal
	HTTP	L. A.\Internet Access\www.comp (192.168.1.20/32)	Source & Destination	Normal
Network Monitoring	Network Monitoring	Service Group\netmanager.comp	Source & Destination	Normal
server.comp FTP	FTP (Active)	Service Group\server.comp	Source & Destination	Normal
server.comp ODBC	ODBC	Service Group\server.comp	Source & Destination	Normal
server.comp Telnet	Telnet	Service Group\server.comp	Source & Destination	Normal

Table 2. Network Groups definition.

Device - Interface	IP Address (Network)
L. A. Layer 3 Switch	**192.168.0.1**
Vlan1	192.168.2.1 (L. A.\Network Management)
Vlan2	192.168.3.1 (L. A.\Server Farm)
Vlan3	192.168.1.1 (L. A.\Internet Access)
Vlan4	192.168.4.1 (L. A.\Management)
Seattle Router	**10.1.0.1**
FastEthernet0/0	10.1.1.1 (Seattle\Finance)
New York Router	**10.2.0.1**
FastEthernet0/0	10.2.1.1 (New York\Development)
FastEthernet0/1	10.2.2.1 (New York\Sale)
Miami Router	**10.3.0.1**
FastEthernet0/0	10.3.1.1 (Miami\Production)
FastEthernet0/1	10.3.2.1 (Miami\Sale)

Table 3. Devices and Interfaces definition.

