# European International Virtual Congress of Researchers

## EIVCR
## May 2015

**Progressive Academic Publishing, UK**

www.idpublications.org

# CHECK-POINT WITH VPN THE OPPORTUNITIES AND SECURITY THAT OFFERS: PRACTICAL IMPLEMENTATION OF THE CHECK POINT AS AN INTERNAL NETWORK IN A COMPANY

**Esmeralda Hoxha**
Department of Informatics Engineering/
SHPAL Pavaresia, Vlore
**ALBANIA**

## ABSTRACT

Increasingly as a result of new services and new technologies, intranets, different institutions or companies are exposed to malevolent attacks which often exceed the limit of attempted causing losses in a specified grade of service offered, destruction of information even greater monetary loss. Such a thing makes the security one of the main factors to be taken into consideration during the design and implementation of an intranet and the resources to be provided by it. Therefore in this topic will submit the opportunities and security that offers the use of Check Point VPN as a security policy and critical step towards securing the network of an organization or institution. Network security should not be seen under individual perspectives of installation of a firewall or the configuration of a VPN connection. SVN architecture (Secure Virtual Network) provided by Checkpoint includes all aspects of the network security in a single product and easy way to use, further with a GUI interface. Package Check Point Next Generation (NG) consists of several products designed to create a total solution on the security issue. After the analysis that will do on functionality and services provides us Checkpoint NG AI packages on implement in the network, after this will see its practical implementation. For this will choose the network, which may be internal network of a company or any sort business and therefore the implementation of security could be a practical example from daily life.

**Keywords:** Security, Check Point, VPN, Network.

## INTRODUCTION

As already we all know, the Internet is making the world we live increasingly "smaller". As a result of its vigorous development the geographical position of people is no longer a fundamental problem because we can talk and play, we buy even and perform business transactions with a person on the other side of the globe in the same way as if he were facing of us. That which before a decade was considered impossible or a miracle of technology today has become a routine process where everyone is invited to participate. All this cannot be achieved, in no way without network security and the tools that provide it which make up the only true measure of security to the "curious" who want to know everything. Check Point has supplied us with a solution to our digital dilemma. Their excellent VPN-1/FireWall-1 security product can go a long way towards soothing the fears associated with connecting your little neck of the woods to the rest of the world. In its latest incarnation, the market leading VPN-1/FireWall-1 eschews a version number for the term “Next Generation.” [1].

First in this topic we will talk about, in general, for security in Nets and security policies, then short information for Firewalls, what is a Firewall and what we are trying to protect using a Firewall. Will handle below with Check-Point as VPN Firewall Package, opportunities and security which Offers, and completing this topic then with Implementation in a Practical Network of Check Point.

## LITERATURE REVIEW

### Security In Nets, General Concepts

To project a much more secure system should first become acquainted with the persons from whom should be wary, the types of attacks and the target of these attacks thus understanding the critical points and more exposed of our system. Threatening of the security in the network can be categorized as follows:

- Script Kiddies Threats
- Expert Threats; External Attackers
- Internal Attackers

Starting from this division of the types of attackers, then the attacks in the network include the following processes:

- Reconnaissance (the disclosure of as much as information about the victime);
- Exploitation (infiltrating in the network); DoS (Denial of Service).

Security in itself constitutes a cycle that comprising many processes and not a single activity. Security phases are divided into:

- Prevention :The stoppage of threats
- Detection :The process of determining that an attack is happening
- Evaluation and response: Assessment of the problem and of situation
- The correction:Fixing the problem

Once corrective action is performed, prevention is concerned with the application of the new rules in the firewall security or an new ACL (access control list) in router. IDS (intrusion detection systems) help us identify attacks that may occur. As firewalls and IDS also keep records (logs) which help us evaluating possible problems. Security tools are as follows:

- Prevention → Firewall and router ACL-s
- Detection → IDS
- Evaluation → Logging

Security Policies: A security policy is a critical first step towards securing the network of an organization or institution. Based on all the way this organization deals with issues of security and resources who offered what are the most important. Besides the usage of acceptable security policies, and encryption a good management policy is needed for the application-specific firewall. These policies guide the configuration for an operating system as independently from mistakes and strengthen (by disabling non-essential services and leaving only those indispensable), for the gates to be opened and the procedure to open the new gate. Always it is useful to apply the principle of minimum privilege which states that only the resources that are necessary to do the job should be accessible.

In addition, an information security policy is also extremely beneficial to the security manager because it provides, at an executive level, a mandated framework for ensuring the confidentiality, integrity, and availability of an organization's information assets.What this means is that the security manager has some weight in his or her corner for budget requests when he or she has an approved information security policy.[1] Finally, for the security administrator, having a written and approved policy can ensure that you are able to deploy Check Point NG in a way that it minimizes disruption to business.[1]

## FIREWALLS AND THEIR CHARACTERISTICS

### What is a firewall?

In general terms a firewall is a software or a hardware ASIC which assesses and analyzes the network traffic and filters it based on a set of rules defined by the security policy. In this sense Firewalls are similar to the router because routers serve to control the traffic of packets TCP / IP. For each packet firewall compares known components of the package with set of security rules and decides whether packets will be allowed to pass.

As it said a firewall can be a hardware device or a software program that runs on a secure host computer. In each case must have at least two interfaces, one for internal network that will protect, considered secure, and one for the external public network considered not secure. Figures below are two cases where the firewall is a hardware ASIC or simply a software which runs on a normal computer.

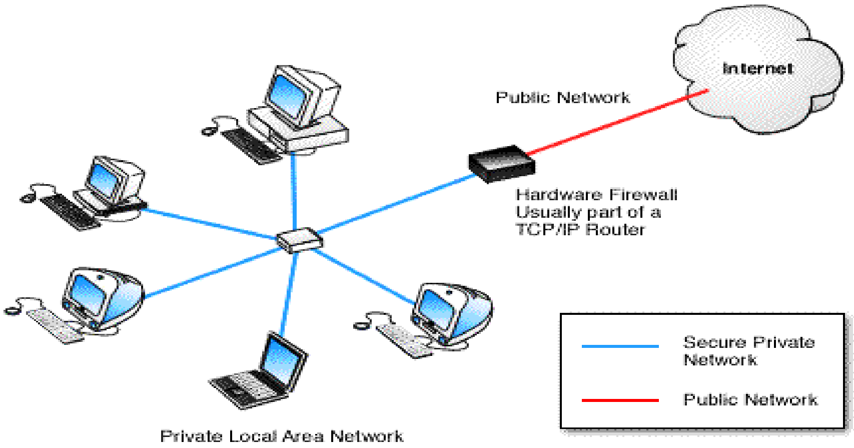

Internet
Public Network
Hardware Firewall Usually part of a TCP/IP Router
Secure Private Network
Public Network
Private Local Area Network

Figure 1. VPN

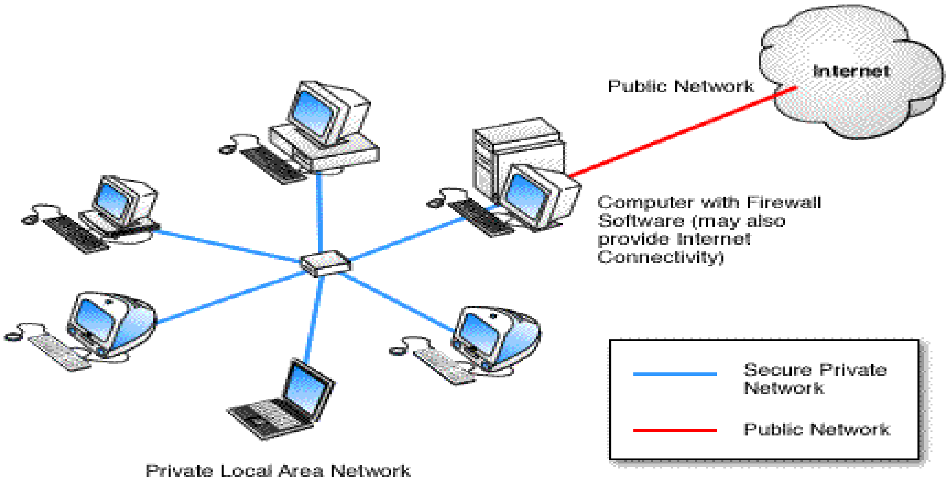

Internet
Public Network
Computer with Firewall Software (may also provide Internet Connectivity)
Secure Private Network
Public Network
Private Local Area Network

Figure 2. VPN with Firewall Software

### What do a Firewall

A firewall examines all packages that routing between two or more networks connected to interfaces of the firewall to see if these packages fulfill the specified criteria. If this condition is completed packets allowed to pass, otherwise they are rejected (Discard). So the main purpose of using the firewall is imposition of network security in communication between the internal and external. A firewall can make the authentication of users who are authorized to communicate through it, according to a predefined security policy.

### Check-Point As VPN Firewall Package, Opportunities And Security Which Offers

### Introduction

Once we treated in general firewall and their functioning and the services offered is the moment to focus on a specific product that will make the final solution of our problems regarding network security. Package Check Point Next Generation (NG) consists of several products designed to create a total solution on the security issue. SVN architecture (Secure Virtual Network) provided by Checkpoint includes all aspects of network security in a single product and easy to use, further with a GUI interface. SVN architecture looks across the enterprise network in general not just the local network including LAN and its WAN connections, but by handle and the VPN user connected to the distance.

Check Point products Package Next Generation (NG) is designed to fulfill the needs of security and management required by SVN architecture. Thus the use of Firewall 1 / VPN first as internal network protection and as secure terminal point for all VPN traffic meets the priority needs of security for all companies. Secure Client is designed to build SecuRemote functionality allowing security managers to set and impose security policies for client platforms associated with VPN services. To assist in the management of the network, two new tools were integrated in the product suite NG. Meta IP allows management of DNS and DHCP servers, while the floodgate-1 provides management Quality of Service (QoS) very necessary on the Internet and VPN connections. Finally to provide detailed information on security checkpoint has integrated Reporting Module. By combining the eight such products in a single suite, NG gives us all security managers and network together with appropriate tools so essential in today's networks in a single package, integrated and scalable.

### Architecture Checkpoint Firewall-1 / VPN-1 NG

Package Check Point Firewall-1 / VPN-1 includes the following products:

1. **SmartClient:** Is a GUI application that allows the system administrator to configure and monitor the Enforcement Module. He is the main application that contains tools for configuration of firewall or and the VPN connections. SmartCenter Server: Called differently in previous versions of Check Point management server is the central point of architecture Check Point. He used to distribute security policies to the Enforcement Modules and to maintain log files which then were upload to management stations (SmartClient). Well Management Server takes over the functions of maintenance policies and of files log by facilitated work to the inspection modules which are responsible for the implementation of access control, authentication of clients and sessions and of address translation by means of NAT. In the center of Check Point architecture stands precisely Management Module. This module is configured by using GUI clients (SmartClient) which

can be installed on the same platform where is installed the SmartCenter or in another platform.

2. **Enforcement Module:** Summary the module inspection and the security servers Firewall-1 and VPN-1. It is installed in an Internet gateway or in network access points. By definition an access point is the point where the local network is connected so is accessible to the external network. Security policies defined by the administrator of firewall generates a script which is written in INSPECT language that is the native language of checkpoint suite. The code which compiled from this script is loading to enforcement module that protects the network.

3. **SVN** foundation: is considered as Check Point operating system (CPOS). SVN has the ability to configure and manage firewall security, VPN networks, allocation of bandwidth, IP in addressing etc.

4. **OPSEC:** Nothing can be considered perfect, so Check Point created a program to allow other developer and manufacturing firms to meet the standard package with additional products and services. So OPSEC provides Check Point package compatibility with other applications of the third party.

## Installation Of Check Point

Choosing the platform and configuration is the main problem that must be solved before starts installing the module Checkpoint. Accurate installation of Firewall-1 at the proper platform reflects directly in the success of security designed infrastructure. Firewall-1 is the main problem that must be solved before starts installing of the Checkpoint module. As we know Firewall-1 is compatible with many platforms including those Solaris, Unix, Windows, but also in Nokia or Nortel modules specially designed for this work. Another option that can be used is Checkpoint SecurePlatform comprising an operating system and software Checkpoint Firewall-1/ VPN 1. In the table below are provided minimum standards hardware and software that are required to install management modules and GUI clients of the package Check Point NG.

Table.1 Minimum Hardware Requirements.

| **System Requirements** | **Enforcement module and Server Management** | **Clients GUI (SmartClient)** |
|---|---|---|
| Operating System | Microsoft Win2000 Server, Advanced Server<br>Windows NT 4.0 + SP6a<br>Sun Solaris 7.0 (32 bit )<br>Sun Solaris 8.0 (32 ose 64 bit)<br>Red Hat Linux (6.0, 7.0, 7.2, 8.0 - )<br>CheckPoint SecurePlatform | Microsoft Win2000,<br>Windows 98/ME<br>Windows NT 4.0 +SP4, SP5, SP6a<br>Sun Solaris Sparc |
| Disc Space | 40 MB | 40 MB |
| CPU | 300 MHZ + | 300 MHZ + |
| RAM | 128 MB | 32 MB |
| Network Interface | ATM,Ethernet,Fast Ethernet, Gigabit Ethernet, FDDI, Token Ring | All supported by the operating system |

Firewall's performance will depend more on the type of hardware that will choose. It is recommended that the hardware settings used to be at least the double of minimal parameters specified in Table 1 above. Thus the Management Server will save the log files to each of the modules that will control so that must have enough free space on disk, memory and CPU to manage all connections.

## METHODOLOGY

Analysis of the functionality and services that offers us the Checkpoint NG AI packages at implementation on network and the establishment of the base of rules for the security policy constitute the main methodology that configures the advantage of this paper. The Package Check Point Next Generation (NG) consists of Several Products Designed to create a total solution on the issue of security. With the Next Generation software, you can manage multiple firewalls from a central management server, and can now centrally manage licenses and software upgrades with the SecureUpdate application. [1] SVN architecture (Secure Virtual Network) offered by the Checkpoint includes all aspects of network security in a single product and easy to use, further with a GUI interface. Having addressed the firewall and user VPN capabilities most companies are looking for, NG turned to address the user management problems identified by the SVN. Two products were added to the suite to enable security managers to easily manage users and accounts.[1] Finally to provide detailed information on safety and the use not only of the products of NG package but and other applications of the third party (third-party), Checkpoint has integrated Reporting Module. Combining these eighth products in a single suite, NG gives us all security managers and network together with appropriate tools so essential in today's networks in a single package, integrated and scalable.

## RESULTS

### Implementation In A Practical Network Of Check Point

### Introduction

Once we analyzed the functionality and services provides us the Checkpoint NG AI packages to the network implementation, now is the moment to see its practical implementation. For this we have chosen network, the infrastructure of which is given in the figure below. This may be the internal network of a company or business and therefore whatever the implementation of safety could be a practical example from everyday life. The implementation is done in Bunkie Company’s network that operates in Albania.

### Network Infrastructure

The network is designed to be built according to the following schema. For security reasons servers which are accessible from the Internet Web Server such as Apache, SMTP Relay which manages the inbound and outbound emails and DNS Sever are placed in a DMZ are located in a DMZ thus isolated from the internal subnet of the company where are located the most important servers as DB server that may have confidential information that should not get out of company are located in a DMZ thus isolated from the internal subnet of the company where are located the most important servers as DB server that may have confidential information that should not get out of company. In internal network is located the Management Server of SmartCenter firewall and also the SmartClient GUI that will administer firewall and will be at the center of our attention. Let's look in more detail the integral parts of internal network:

- **Internal MailServer:** Is the server that manages the system's internal electronic mail of the company. There is installed the Microsoft Exchange 2000

- **PDC, DHCP Server:** The Domain Controller of the company. It is installed in Active Directory where are specified all computers and user accounts of the company.
- **Database Server:** It maintained the database of the company that contains all information about its operation. There are also saved all the documents used by the employees of the company.
- **SmartCenter Server:** Is the server that manages firewall and that stores log data recorded by the reinforcement module.
- **Web Server**: Server that manages the company's Web site.
- **SMTP Relay:** It is the server that manages inbound and outbound traffic to e-mail so that manages e-mails that are run inside and outside of the internal network to company.
- **DNS Server:** The server that provides DNS service for the company's internal computers.

The Internet in Internal network is provided by ISP through a dedicated DSL line. With the help of VPN the internal network resources will be accessed by several remote users which may be partners of the company or mobile employees.

3.

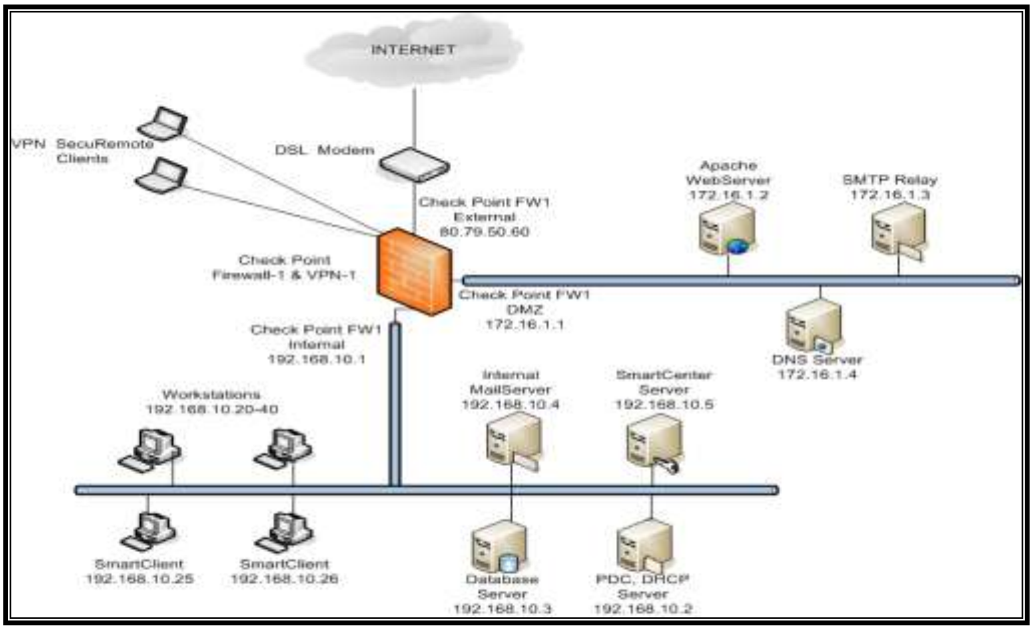

INTERNET
VPN SecuRemote Clients
DSL Modem
Check Point FW1 External 80.79.50.60
Apache WebServer 172.16.1.2
SMTP Relay 172.16.1.3
Check Point Firewall-1 & VPN-1
Check Point FW1 DMZ 172.16.1.1
Check Point FW1 Internal 192.168.10.1
DNS Server 172.16.1.4
Internal MailServer 192.168.10.4
SmartCenter Server 192.168.10.5
Workstations 192.168.10.20-40
SmartClient 192.168.10.25
SmartClient 192.168.10.26
Database Server 192.168.10.3
PDC, DHCP Server 192.168.10.2

Figure Internet

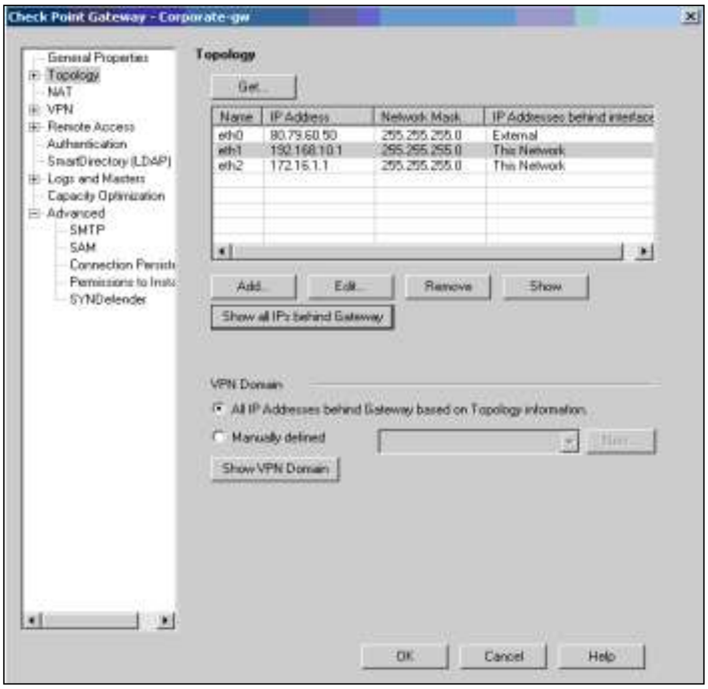
Infrastructure

For simplicity, we chose the case when this module is a Windows 2000 platform where are active only necessary services for its operation as a firewall. Must have three network interfaces configured as in the figure. The mask used shall be that default 24 corresponding to the subnet mask 255.255.255.0. Once we set up all three network interfaces reinforcement module and activate IP forwarding we can then begin installing Firewall-1 & VPN-1 to the computer, the SmartClient to the management server and GUI clients. During installation of SmartClient shall be asked to make registration of licenses for our product Check Point, determining the GUI clients by giving the IP addresses to computers on the network where we installed SmartClient respectively 192.168.10.25 and 192.168.10.26 and the creation of entities with the administrative rights on SmartCenter management server. At the end will be and Initialization internal certification authority. All these procedures are explained in chapter three for the installation and configuration of Check Point NG.

## Creation Of Network Objects

Before configuring the Base of Rules must to create network objects in the server management. To realize this we follow the following steps associated with the respective figures:

Choose corporate-gw object representing our network firewall and give Edit. We will create two objects Networks which will be named Internal and DMZ as in figures below



Check Point Gateway - Corporate-gw

Topology

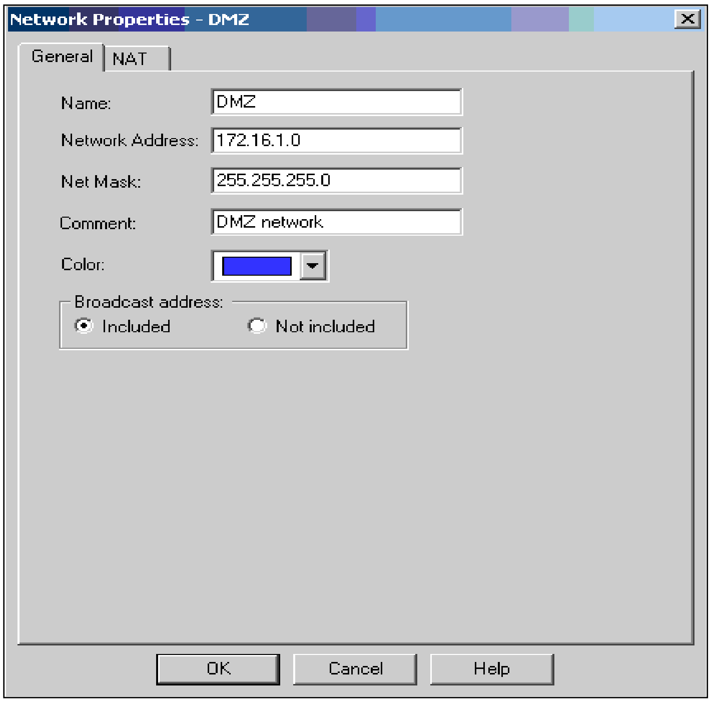
| Name | IP Address | Network Mask | IP Addresses behind interface |
|---|---|---|---|
| eth0 | 80.79.60.50 | 255.255.255.0 | External |
| eth1 | 192.168.10.1 | 255.255.255.0 | This Network |
| eth2 | 172.16.1.1 | 255.255.255.0 | This Network |

VPN Domain

● All IP Addresses behind Gateway based on Topology information

○ Manually defined

Figure 4. Corporate-gw



Network Properties - DMZ

Name: DMZ

Network Address: 172.16.1.0

Net Mask: 255.255.255.0

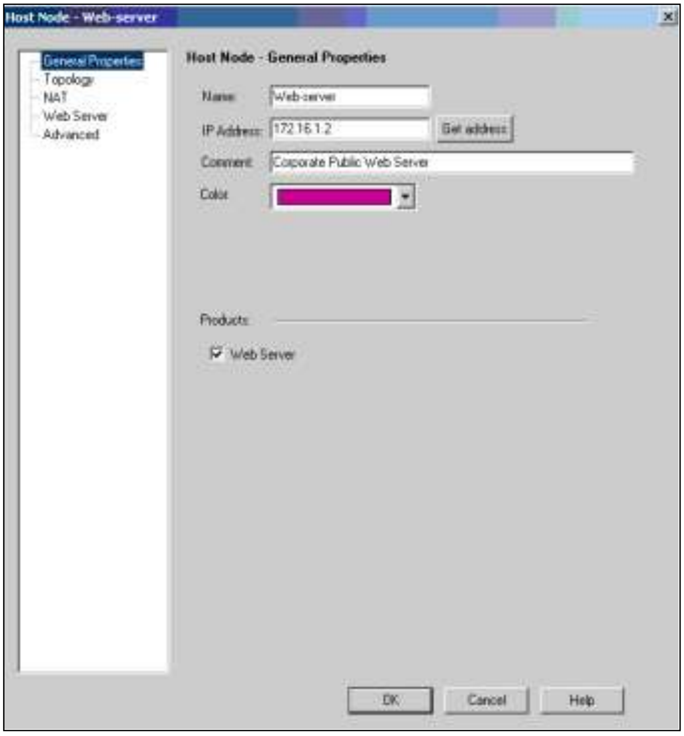
Comment: DMZ network

Color: 🟦

Broadcast address: ● Included ○ Not included

Figure 5. Creation of a DMZ

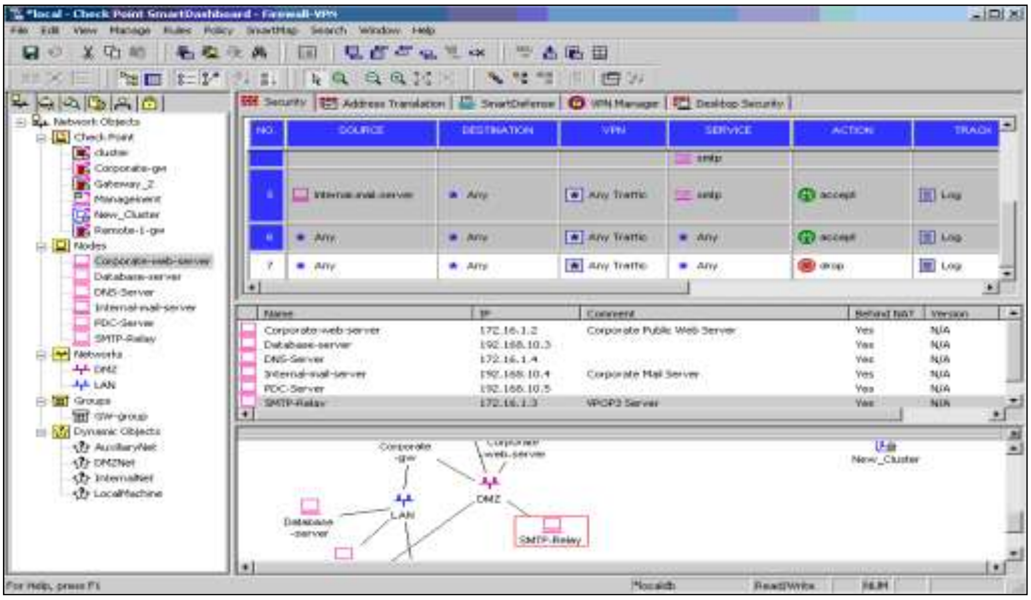
At the two objects have allowed NAT to hide modality and all internal addresses are hidden behind the IP address of external interface. The example of the creation of the object that represents WebServer is given in figure below.



Name: Web-server
IP Address: 172.16.1.2
Comment: Corporate Public Web Server
Color:
Products:
☑ Web Server

Figure 6. Object that represents WebServer

To General Properties we will give the WebServer's name and its IP address. On Topology will create network interface Web Server by marking once again the IP address and Subnet Mask. We will apply the NAT mechanism. To Web Server menu we choose the Enforcement Module that will serve as protection and which in our case is called Corporate_gw firewall. The same procedure will follow also for other hosts that are part of our network and to be included in the security policy. At the end the view of the tree of objects in the main window of SmarDashboard will be like this:



| NO. | SOURCE | DESTINATION | VPN | SERVICE | ACTION | TRACK |
|---|---|---|---|---|---|---|
| | | | | smtp | | |
| 5 | Internal-mail-server | Any | Any Traffic | smtp | accept | Log |
| 6 | Any | Any | Any Traffic | Any | accept | Log |
| 7 | Any | Any | Any Traffic | Any | drop | Log |

| Name | IP | Comment | Behind NAT | Version |
|---|---|---|---|---|
| Corporate-web-server | 172.16.1.2 | Corporate Public Web Server | Yes | N/A |
| Database-server | 192.168.10.3 | | Yes | N/A |
| DNS-Server | 172.16.1.4 | | Yes | N/A |
| Internal-mail-server | 192.168.10.4 | Corporate Mail Server | Yes | N/A |
| PDC-Server | 192.168.10.5 | | Yes | N/A |
| SMTP-Relay | 172.16.1.3 | VPOP3 Server | Yes | N/A |

Figure 7. Tree of objects of the SmartDashboard

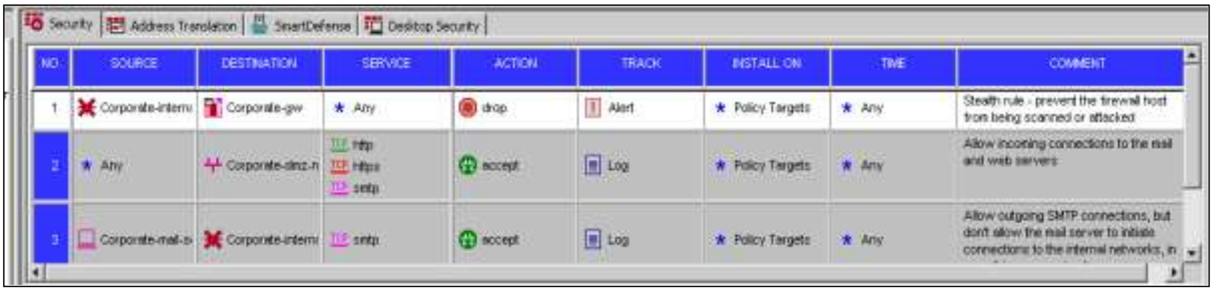
## Creation of Base Of Rules

The first thing to be done is to identify the allowed traffic and then everything else will be disallowed. Such thing depends on many factors such as the services that will offer the company, the IT operations staff etc. In the following table is defined allowed traffic.

Table.2 Allowed traffic

| Source | Source Location | Destination | Location of Destination | Number of Gates |
|---|---|---|---|---|
| X | X | ***SMTP Relay*** | DMZ Net | 25 TCP |
| X | X | ***Web Server*** | DMZ Net | 80 TCP (http)<br>443 TCP(https) |
| X | X | ***DNS Server*** | DMZ Net | 53 TCP<br>53 UDP |
| SMTP Relay | Internal Net | ***Internal Mail Server*** | Internal Net | 25 TCP |
| Internal Mail Server | Internal Net | ***SMTP Relay*** | DMZ Net | 25 TCP |
| X | Internal Net | ***X*** | X | 80 TCP<br>443 TCP |
| Web Server | Internal Net | ***X*** | X | 53 TCP<br>53 UDP |
| IT sector | Internal Net | ***X*** | X | 20 TCP<br>21 TCP |
| IT sector | Internal Net | ***X*** | X | 23 TCP |
| IT sector | Internal Net | ***X*** | X | 23 TCP |
| IT sector | Internal Net | ***X*** | X | 161 UDP |

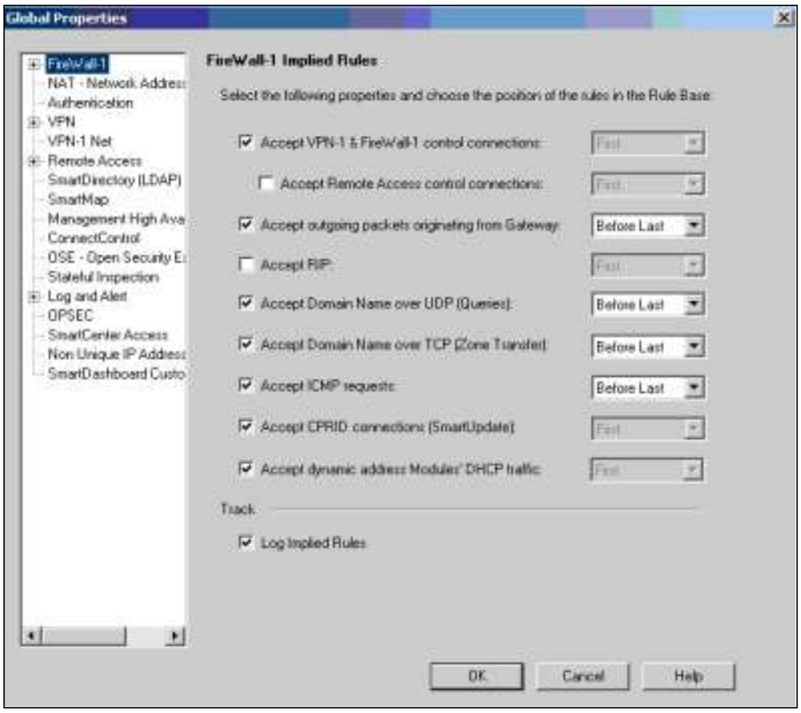
Configuring the Base of Rules. Initially will establish Stealth and Clean Up rules which will be respectively the first and last rules at the Base. The Stealth rules is the rules that rejects and record in the log files the traffic that is destined for Firewall-1. While the rules Clean-Up is the last rules of the Base of Rules and rejects all traffic that is not allowed in the rules above.



| NO | SOURCE | DESTINATION | SERVICE | ACTION | TRACK | INSTALL ON | TIME | COMMENT |
|---|---|---|---|---|---|---|---|---|
| 1 | Corporate-interna | Corporate-gw | Any | drop | Alert | Policy Targets | Any | Stealth rule - prevent the firewall host from being scanned or attacked |
| 2 | Any | Corporate-dmz-n | http<br>https<br>smtp | accept | Log | Policy Targets | Any | Allow incoming connections to the mail and web servers |
| 3 | Corporate-mail-s | Corporate-interna | smtp | accept | Log | Policy Targets | Any | Allow outgoing SMTP connections, but don't allow the mail server to initiate connections to the internal networks, in |

Figure 8. Base of Rules

All the rules must be saved at the database server that is located in management server: Policy menu, Global Properties Command, Accept ICMP requests check option, both options Accept Domain Name Domain over UDP to allow the DNS server to perform its function and be connected to other DNS servers, To the right of each option specify the respective Rule rankings involved on the basis of the rules. We can provide three values First, Before Last and Last. Choose the Before Last option, click Ok, the Install command to the Policy menu.



**FireWall-1 Implied Rules**

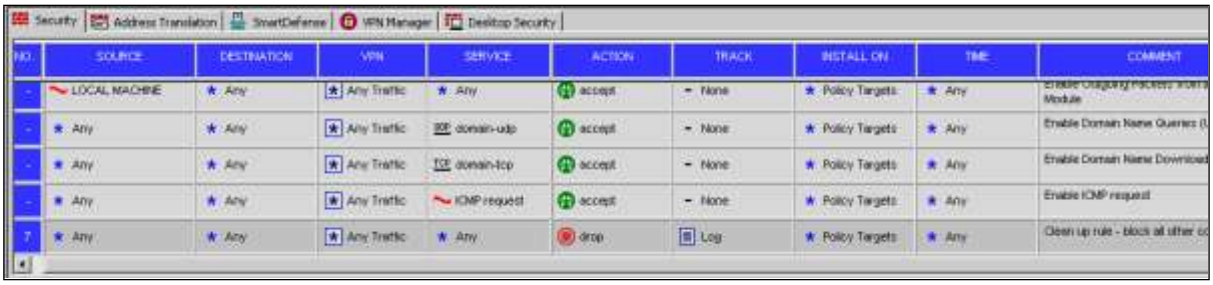
Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept VPN-1 & FireWall-1 control connections: First
☐ Accept Remote Access control connections: First
☑ Accept outgoing packets originating from Gateway: Before Last
☐ Accept RIP: First
☑ Accept Domain Name over UDP (Queries): Before Last
☑ Accept Domain Name over TCP (Zone Transfer): Before Last
☑ Accept ICMP requests: Before Last
☑ Accept CPRID connections (SmartUpdate): First
☑ Accept dynamic address Modules' DHCP traffic: First

Track

☑ Log Implied Rules

Figure 9. Global Properties

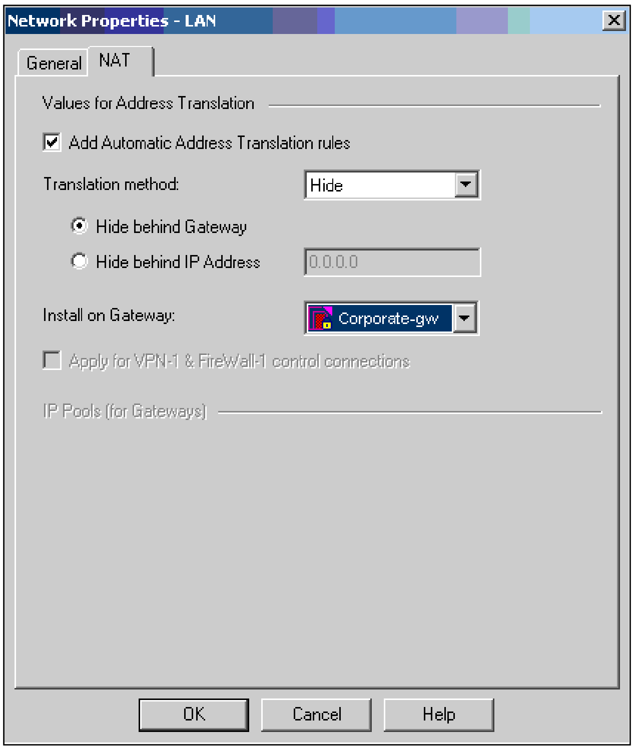


| NO. | SOURCE | DESTINATION | VPN | SERVICE | ACTION | TRACK | INSTALL ON | TIME | COMMENT |
|---|---|---|---|---|---|---|---|---|---|
| - | LOCAL MACHINE | ★ Any | ★ Any Traffic | ★ Any | accept | - None | ★ Policy Targets | ★ Any | Enable Outgoing Packets from<br>Module |
| - | ★ Any | ★ Any | ★ Any Traffic | domain-udp | accept | - None | ★ Policy Targets | ★ Any | Enable Domain Name Queries (U |
| - | ★ Any | ★ Any | ★ Any Traffic | domain-tcp | accept | - None | ★ Policy Targets | ★ Any | Enable Domain Name Download |
| - | ★ Any | ★ Any | ★ Any Traffic | ICMP request | accept | - None | ★ Policy Targets | ★ Any | Enable ICMP request |
| 7 | ★ Any | ★ Any | ★ Any Traffic | ★ Any | drop | Log | ★ Policy Targets | ★ Any | Clean up rule - block all other co |

Figure 10. Base of Rules

## The Application Of Automatic NAT

NAT mechanism will apply in the internal subnet and at the DMZ. We will use the Hide modality and all the packages that go out of our network will be hidden to address of external interfaces of firewall. To realize the NAT mechanism, choose objects that represent the internal network and the DMZ and give the command Edit. If we choice the Hide Behind Gateway option will be used the external interfaces of firewall. Then we look at the base effects of the rules.



Values for Address Translation

☑ Add Automatic Address Translation rules

Translation method: Hide

● Hide behind Gateway

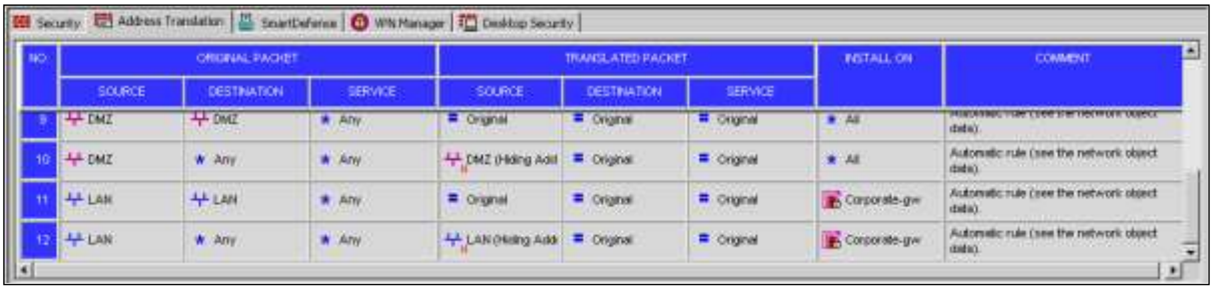
○ Hide behind IP Address 0.0.0.0

Install on Gateway: Corporate-gw

□ Apply for VPN-1 & FireWall-1 control connections

IP Pools (for Gateways)

Figure 11. Hide Behind Gateway

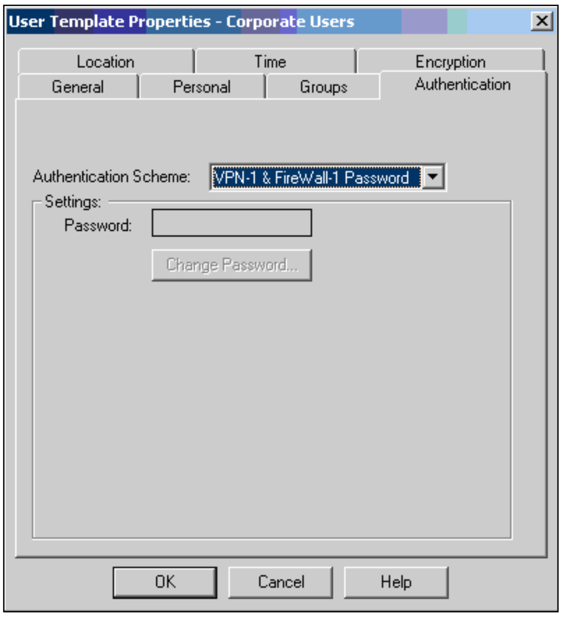


| NO. | ORIGINAL PACKET | | | TRANSLATED PACKET | | | INSTALL ON | COMMENT |
|---|---|---|---|---|---|---|---|---|
| | SOURCE | DESTINATION | SERVICE | SOURCE | DESTINATION | SERVICE | | |
| 9 | DMZ | DMZ | Any | Original | Original | Original | All | Automatic rule (see the network object data). |
| 10 | DMZ | Any | Any | DMZ (Hiding Add | Original | Original | All | Automatic rule (see the network object data). |
| 11 | LAN | LAN | Any | Original | Original | Original | Corporate-gw | Automatic rule (see the network object data). |
| 12 | LAN | Any | Any | LAN (Hiding Add | Original | Original | Corporate-gw | Automatic rule (see the network object data). |

Figure 12. Base of Rules

## Authentication of Users

After we applied NAT-in automatic is the time to configure the user authentication process. We have chosen to use the authentication of the user type since it is independent of the client's computer that is used but is oriented toward the user's profile. Such a thing is very suitable for domain user accounts which can log on at any computer that takes part in the domain. Authentication can be used for many purposes. For example, we may use authentication to restrict user access to various network resources by dividing by departments. Being that the rules of authentication using user groups and not individual user environments we must first define the groups that will use and then create users in them. We can create a specific template for users. In this way the creation of new user becomes simple. For creating users, templates or users groups go to **User** icon in the tree of objects or to the **Manage menu**, **Users** and **Administrators**, **New**. We create a template for Users firewall.
At **General** menu we give the template's name that we are creating. While at **Groups** menu we specify in which of group will be parts the users that will be created from this template.



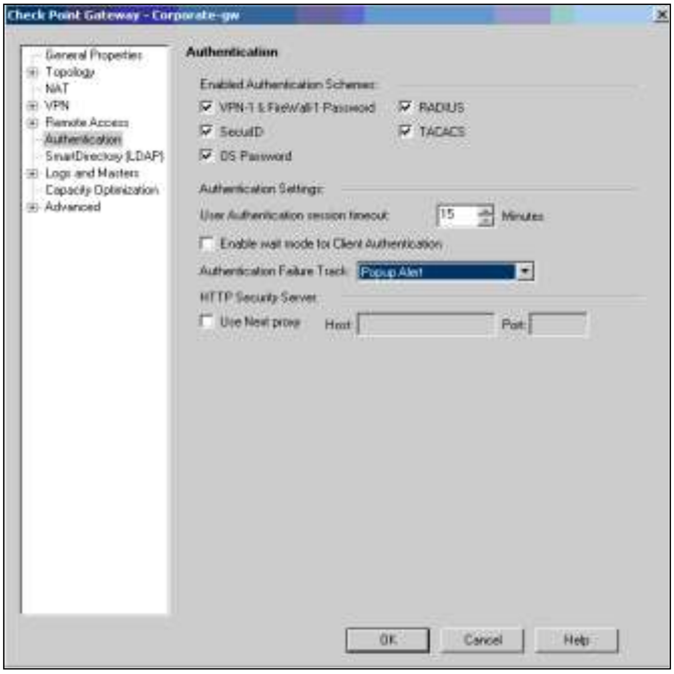
Authentication Scheme: VPN-1 & FireWall-1 Password

Settings:

Password:

Figure 13. Corporate Users

For Users we have created two groups: Local_Users representing the company's internal employees and Mobile_Users representing mobile Users that access the network by VPN connections. Of special importance for us is the Authentication menu because there is specified the authentication schema to be used. A preferred schema would be RADIUS but in the absence of a RADIUS server we have chosen the schema which realizes the authentication with the help of Firewall-1 module password as shown in the figure. At the end we give the menu command **Install Database** at **Policy** menu so all the changes that are made to be saved to the user database. In **Authentication** select the authentication scheme that will use. While other options do not changes.



Authentication

Enabled Authentication Schemes:

☑ VPN-1 & FireWall-1 Password ☑ RADIUS

☑ SecurID ☑ TACACS

☑ OS Password

Authentication Settings:

User Authentication session timeout: 15 Minutes

□ Enable wait mode for Client Authentication

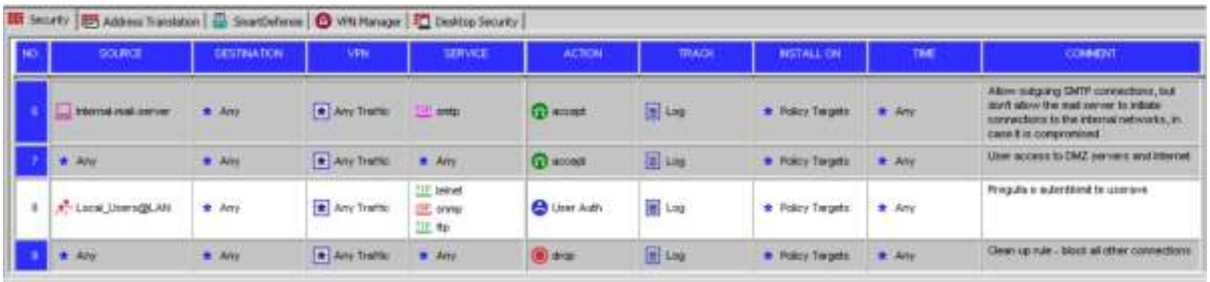
Authentication Failure Track: Popup Alert

HTTP Security Server:

□ Use Next proxy Host: Port:

Figure 14.Check Point Gateway

To Service field we specify the services we wish to authentify while to Action field will choose User_Auth which represents user authentication action. The last step is the establishment of the rule of the authentication on the basis of rules. To Service field we specify the services we wish for  authentication while to Action field will choose User_Auth which represents user authentication action. The last step is the establishment of the rule of the authentication on the basis of rules.



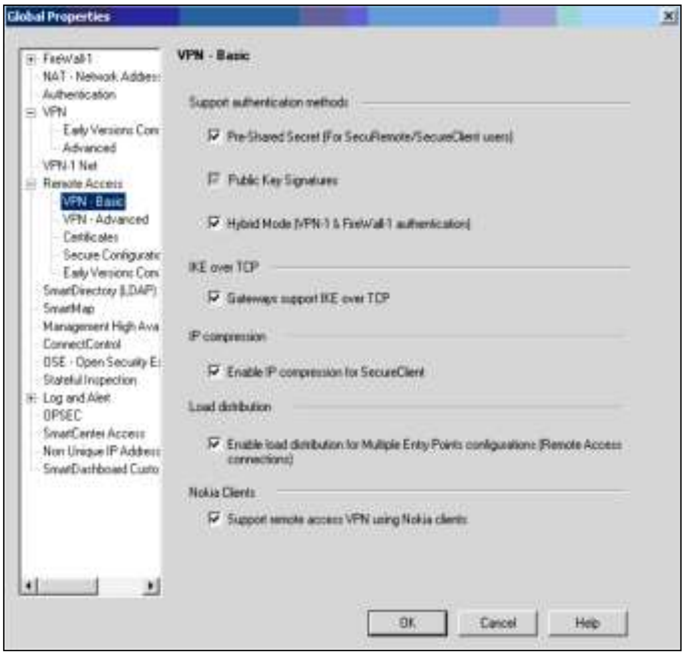
| NO | SOURCE | DESTINATION | VPN | SERVICE | ACTION | TRACK | INSTALL ON | TIME | COMMENT |
|---|---|---|---|---|---|---|---|---|---|
| 6 | Internal-mail-server | Any | Any Traffic | smtp | accept | Log | Policy Targets | Any | Allow outgoing SMTP connections, but don't allow the mail server to initiate connections to the internal networks, in case it is compromised |
| 7 | Any | Any | Any Traffic | Any | accept | Log | Policy Targets | Any | User access to DMZ servers and Internet |
| 8 | Local_Users@LAN | Any | Any Traffic | telnet<br>snmp<br>ftp | User Auth | Log | Policy Targets | Any | Rregulla e autentikimit te userave |
| 9 | Any | Any | Any Traffic | Any | drop | Log | Policy Targets | Any | Clean up rule - block all other connections |

Figure 15. Base of Rules

## The Realization of VPN

Now is the time to configure the VPN connection for remote Users who may be partners of the company or its mobile agents. VPN connection type will be client-gateway. First must be configured the enforcement module of our company and must be installed the VPN client software: SecuRemote or SecureClient.

Give the command **Edit**, at **General Properties** chooce **SecureClient Policy Server,** at **VPN** menu click to **Traditional Mode Configuration, Exportable** option **for SecuRemote/ SecureClient, Ok.** Now we need to configure the **Global Properties** to **Policy** menu**.**



VPN - Basic

Support authentication methods

☑ Pre-Shared Secret (For SecuRemote/SecureClient users)

☐ Public Key Signatures

☑ Hybrid Mode (VPN-1 & FireWall-1 authentication)

IKE over TCP

☑ Gateways support IKE over TCP

IP compression

☑ Enable IP compression for SecureClient

Load distribution

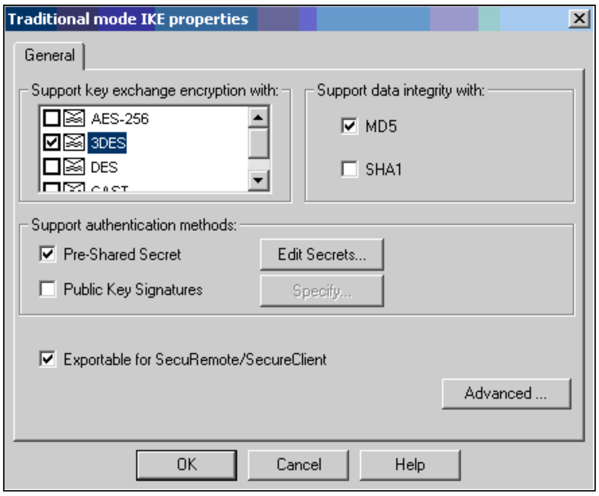
☑ Enable load distribution for Multiple Entry Points configurations (Remote Access connections)

Nokia Clients

☑ Support remote access VPN using Nokia clients

Figure 16. Global Properties

**Remote Access, VPN-Basic** menu, **Pre-Shared Secret** option and other option show in the figure. The **Pre-Shared Secret** option allows the usage of a common password for client authentication. Thus the exchange of keys will be realized with 3DES encryption schema because we use symmetrical switch while to verify the integrity of the data we will use the MD5 hash function.



Traditional mode IKE properties

General

Support key exchange encryption with:
- □ AES-256
- ☑ 3DES
- □ DES
- □ CAST

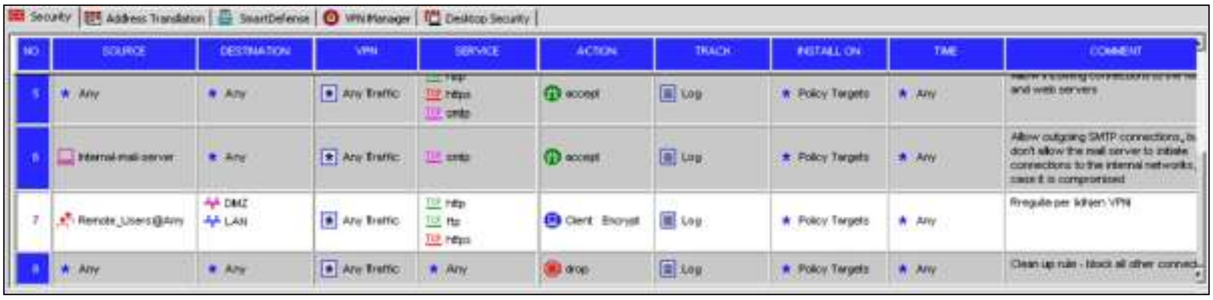
Support data integrity with:
- ☑ MD5
- □ SHA1

Support authentication methods:
- ☑ Pre-Shared Secret — Edit Secrets...
- □ Public Key Signatures — Specify...

☑ Exportable for SecuRemote/SecureClient

Figure 17. 3DES encryption scheme

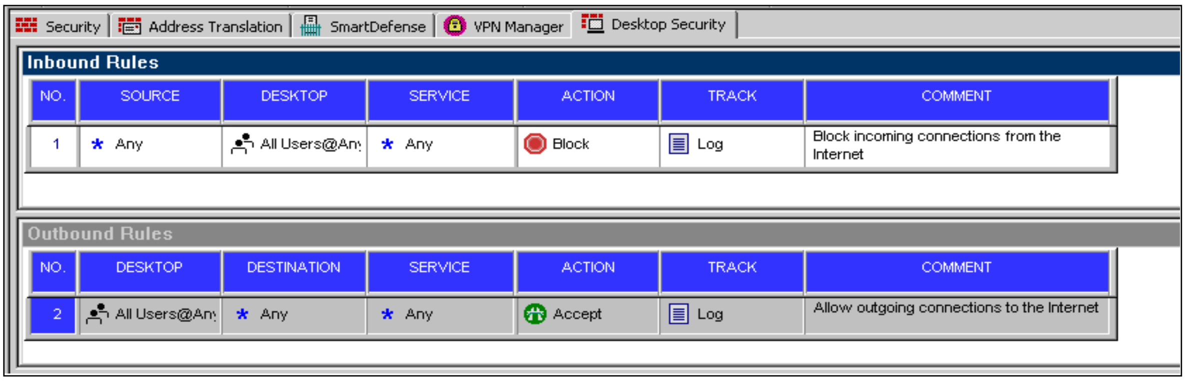
In the Rule of VPN connectivity the field Source will contain the group of remote users while the Destination field may contain a network, a server or servers group. Service field will be completed as needed while the field Action will contain the Encrypt Client action.



| NO | SOURCE | DESTINATION | VPN | SERVICE | ACTION | TRACK | INSTALL ON | TIME | COMMENT |
|---|---|---|---|---|---|---|---|---|---|
| 5 | Any | Any | Any Traffic | http<br>https<br>smtp | accept | Log | Policy Targets | Any | Allow incoming connections to the mail and web servers |
| 6 | Internal-mail-server | Any | Any Traffic | smtp | accept | Log | Policy Targets | Any | Allow outgoing SMTP connections, but don't allow the mail server to initiate connections to the internal networks, case it is compromised |
| 7 | Remote_Users@Any | DMZ<br>LAN | Any Traffic | http<br>ftp<br>https | Client Encrypt | Log | Policy Targets | Any | Rregulle per klient VPN |
| 8 | Any | Any | Any Traffic | Any | drop | Log | Policy Targets | Any | Clean up rule - block all other connect... |

Figure 18. Rules of VPN connectivity

Respectively the Inbound rules will block the connections coming from Internet into computer where is installed the SecureClient while Outbound rules will allow connections that the Internet are addressed.



Inbound Rules

| NO. | SOURCE | DESKTOP | SERVICE | ACTION | TRACK | COMMENT |
|---|---|---|---|---|---|---|
| 1 | Any | All Users@Any | Any | Block | Log | Block incoming connections from the Internet |

Outbound Rules

| NO. | DESKTOP | DESTINATION | SERVICE | ACTION | TRACK | COMMENT |
|---|---|---|---|---|---|---|
| 2 | All Users@Any | Any | Any | Accept | Log | Allow outgoing connections to the Internet |

Figure 19. Outbound Rule

After we finish with VPN module configuration must continue with the installation and configuration of clients SecuRemote /SecureClient. Both these programs are found in the CD packet checkpoint and will install on the computers that will be used by the mobile Users to connect to our network. We need to add the VPN module to which the connection will be realized. For this go to the File menu, Name, IP and give the IP address of the external interfaces to our firewall. Finally we have to create a new security rule which would allow users to have access on the network. This rule will be the same with the security rule we created to firewall At this point VPN connection is ready and can control the log data to see if the tunnel is created.

## CONCLUSIONS

Many organizations and companies use Check Point VPN technologies on the Internet to have a sure channel so that remote offices or mobile user accounts have access to their internal network. For many of them the VPN have replaced perfectly dedicated point-to-point connections, which are very expensive to install and maintain. While a VPN connection using an existing Internet connection and establish a secure communication channel. VPN use different cryptographic procedures to authenticate user and to ensure that the data will remain private. VPNs use authentication to ensure that only authorized persons are allowed to access network resources. That is to say VPN is an encrypted tunnel. Check Point has supplied us with a solution to our digital dilemma. Their excellent VPN-1/FireWall-1 security product can go a long way towards soothing the fears associated with connecting your little neck of the woods to the rest of the world.

The functionality and services that offers us the Checkpoint NG AI packages to the network implementation are very important when it comes to its practical implementation in a real network. This may be the internal network of a company or business and therefore whatever the implementation of safety could be a practical example from everyday life.

## REFERENCES

**Books**

1. Cherie Amon , Allen V.Keele, Daniel Kligerman, Drew Simonis , Corey Pincock (March, 2002) Check Point NG Security Administration – Syngress.

**Journals**

2. *SC Magazine Awards 2014, Feb. 25, 2014* • San Francisco, Barracuda Firewall, Check Point NG Firewall -1 Administration Guide – Check Point Technologies

**Manuals**

3. Check Point Firewall -1 VPN Manual – Check Point Technologies. *Manuals are taken from Bankers Company, operate in Albania.*

**Website**

4. *Learn more about Computer Security*. Available from World Wide Web: www.syngress.com
5. *Syngress IT Security Project Management Handbook*. Available from World Wide Web: www.syngress.com
6. www.checkpoint.com
7. www.globalknowledge.com