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

The Topics

- INTRODUCTION
- SECURITY IN NETS, GENERAL CONCEPTS
- FIREWALLS AND THEIR CHARACTERISTICS
- CHECK-POINT AS VPN FIREWALL PACKAGE, OPPORTUNITIES AND SECURITY WHICH OFFERS
- METHODOLOGY
- RESULTS
- CONCLUSIONS
- REFERENCES REFERENCES

INTRODUCTION

- Internet is making the world we live increasingly "smaller".
- 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
- 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 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.

SECURITY IN NETS, GENERAL CONCEPTS

Threatening of the security in the network can be categorized as follows:

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

Security phases

Securety 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

Security Policies

- A security policy is a critical first step towards securing the network of an organization or institution.
- 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.
- 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 confiden, integrity, and availability of an organization’s information assets.
- 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.

FIREWALLS AND THEIR CHARACTERISTICS

What is a firewall?

- Firewalls are similar to the router because routers serve to control the traffic of packets TCP / IP.
- 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.

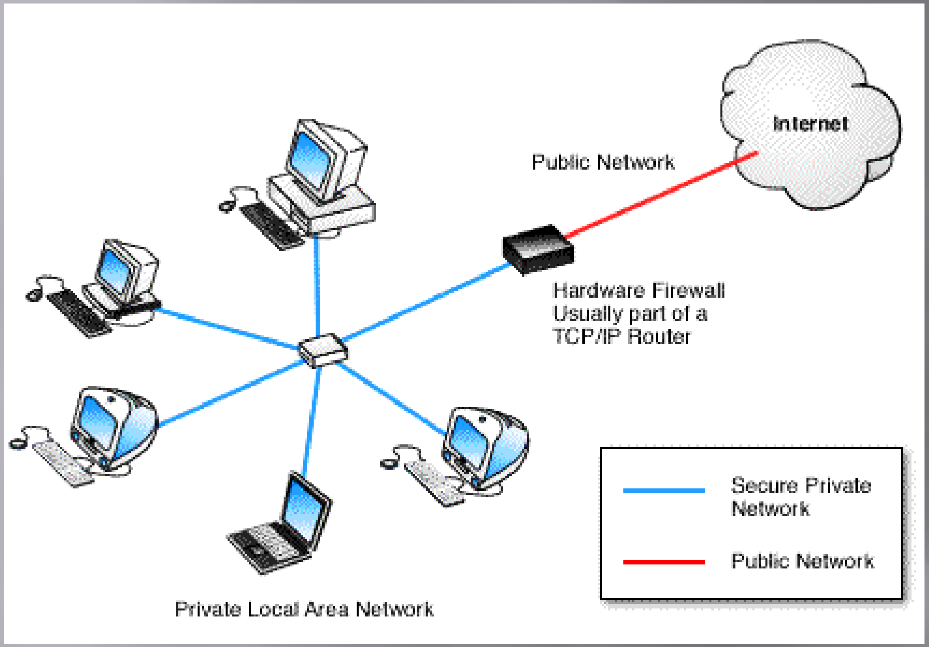


Figure 1. VPN

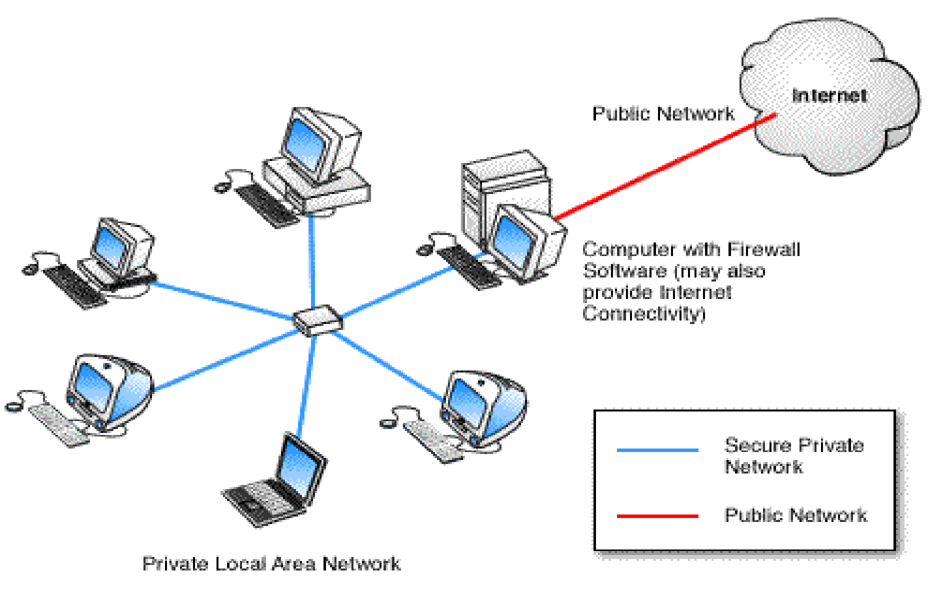


Figure 2. VPN with Firewall Software

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.
- 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.

Introduction

- 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.
- Check Point products Package Next Generation (NG) is designed to fulfil 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

Architecture Checkpoint Firewall-1 / VPN-1 NG

- **SmartClient:** Is a GUI application that allows the system administrator to configure and monitor the Enforcement Module.
- **Enforcement Module:** Summary the module inspection and the security servers Firewall-1 and VPN-1. **Enforcement Module:** Summary the module inspection and the security servers Firewall-1 and VPN-1.
-

- **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.
- **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

System Requirements	Enforcement module and Server Management	Clients GUI (SmartClient)
Operating System	Microsoft Win2000 Server, Advanced Server Windows NT 4.0 + SP6a Sun Solaris 7.0 (32 bit) Sun Solaris 8.0 (32 ose 64 bit) Red Hat Linux (6.0, 7.0, 7.2, 8.0 -) CheckPoint SecurePlatform	Microsoft Win2000, Windows 98/ME Windows NT 4.0 +SP4, SP5, SP6a 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

METHODOLOGY

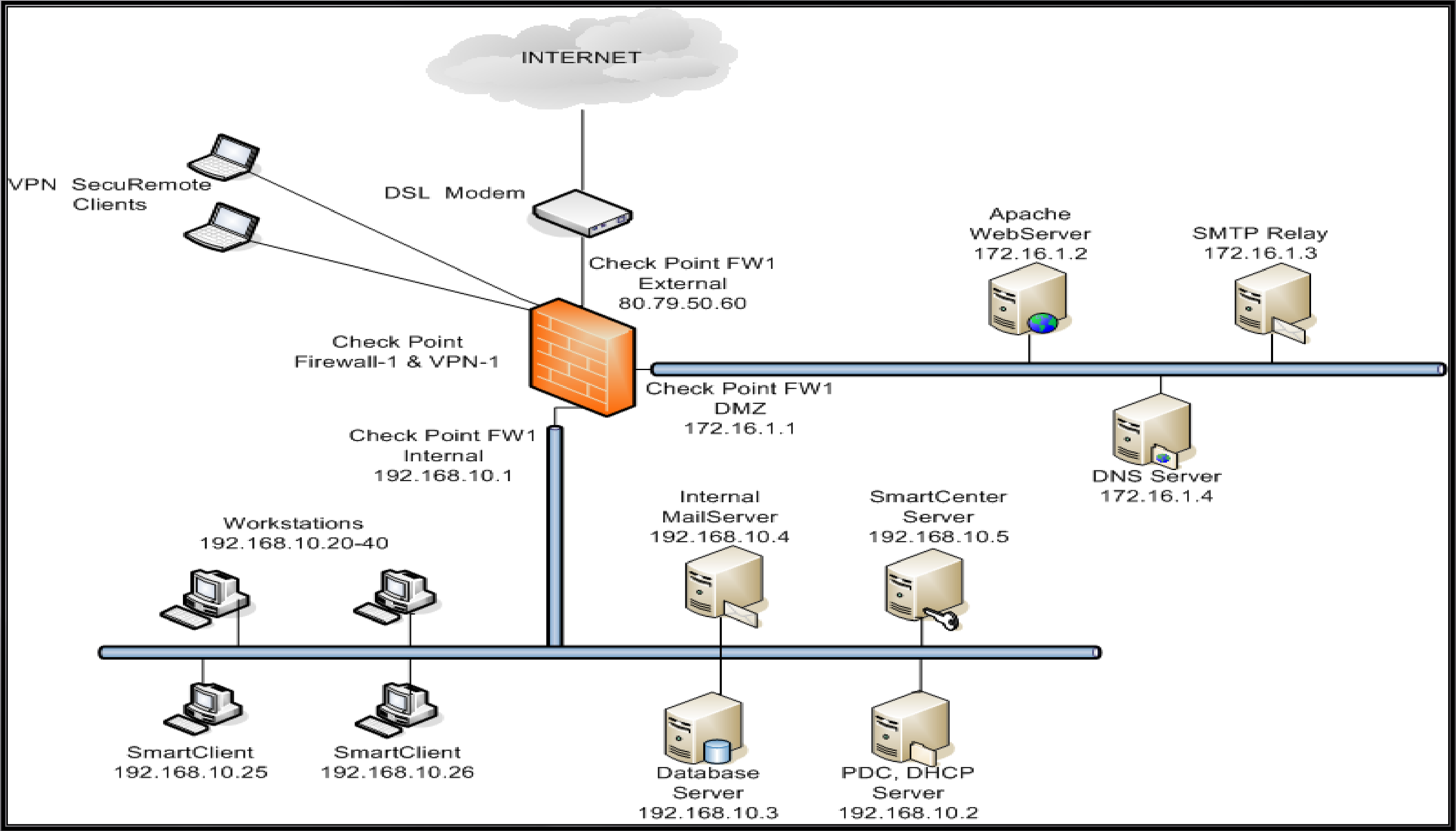
- Analysis of the functionality and services that offers us the Checkpoint NG AI packages at implementation on network and the establishment of the base of rules for the security policy constitute the main methodology that configures the advantage of this paper.
- The Package Check Point Next Generation (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.

RESULTS

Implementation In A Practical Network Of Check Point

- 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.
- 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

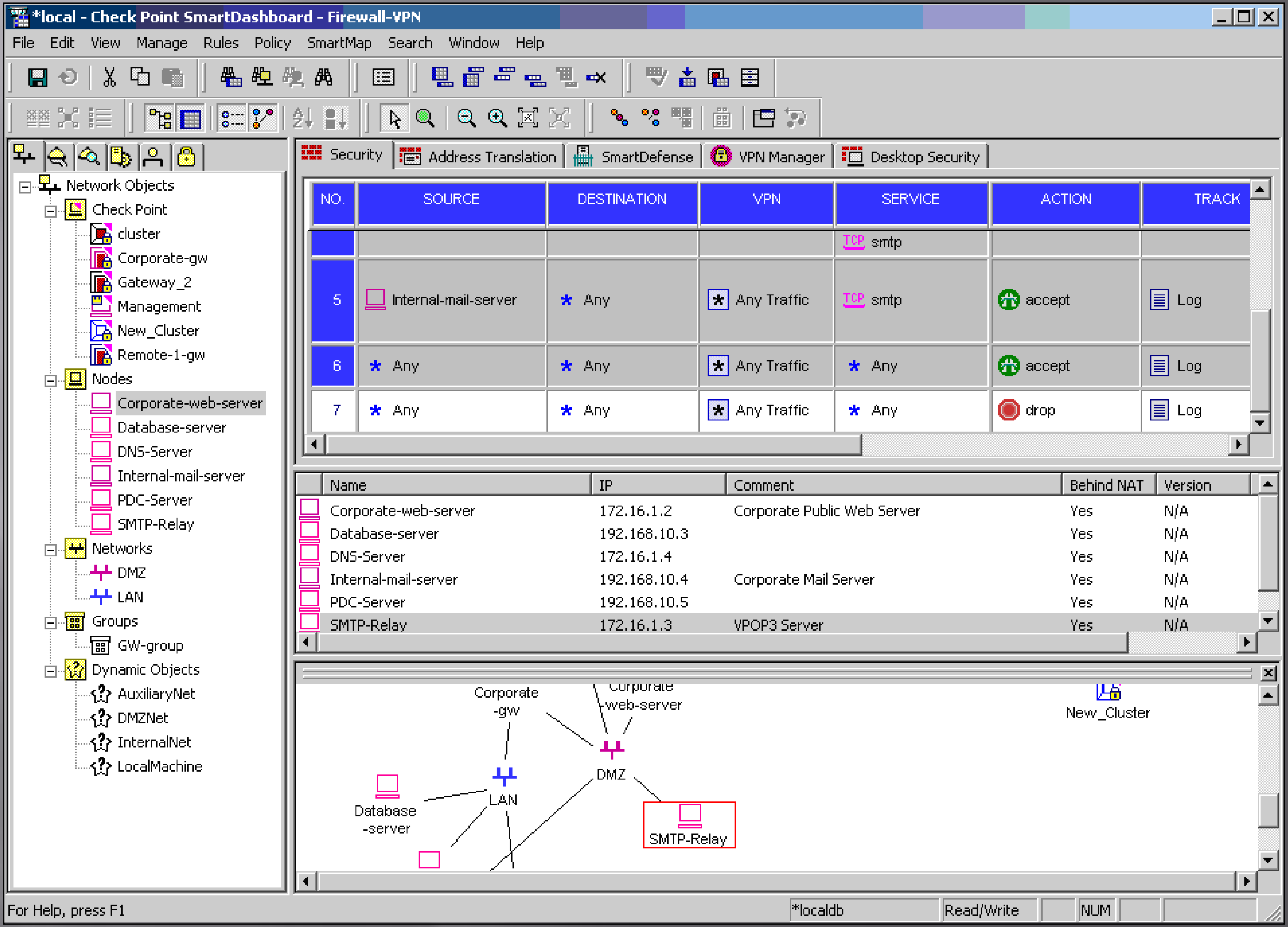
Figure 3. Internet Infrastructure


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

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
-

Tree of objects of the SmartDashboard



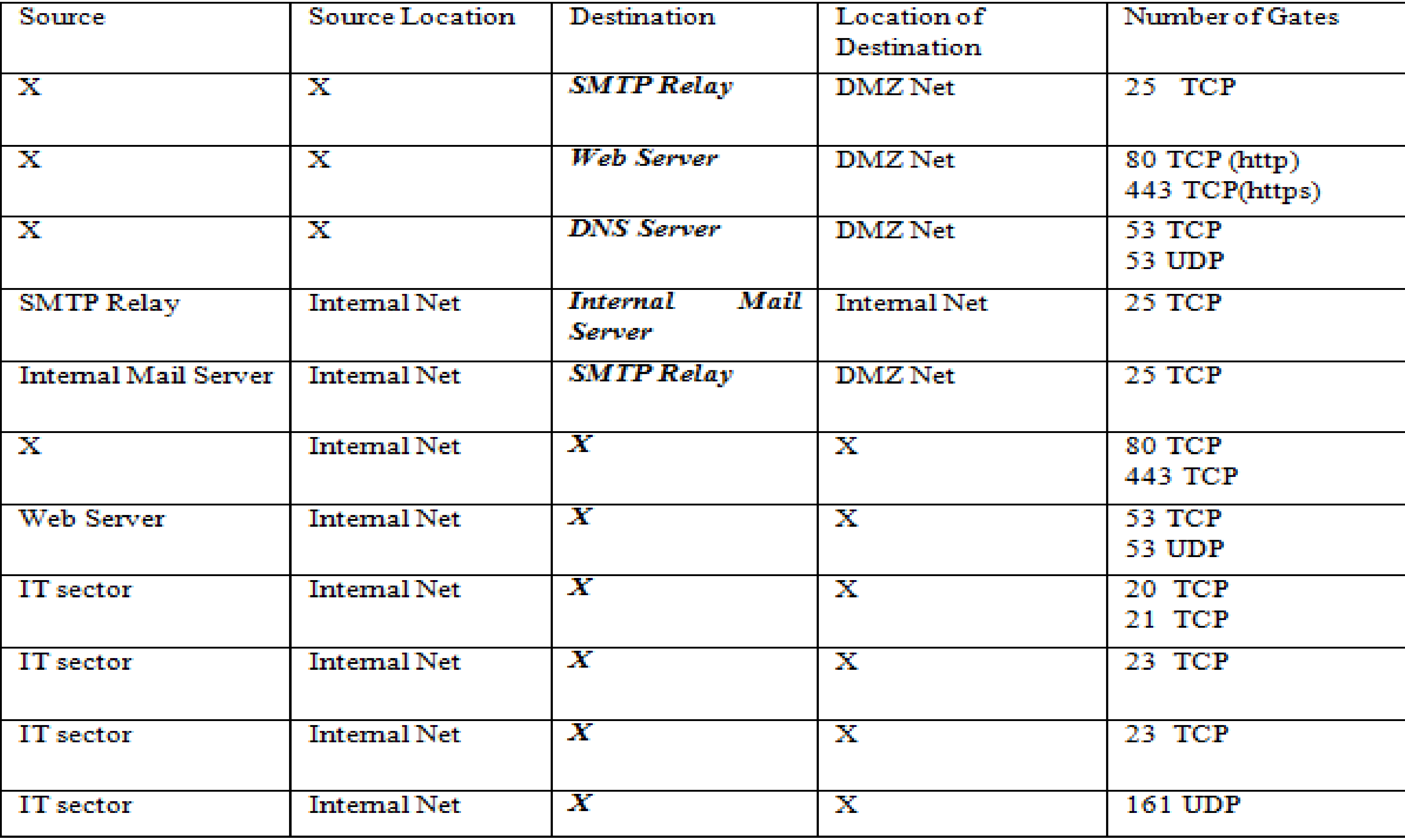
NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
				TCP smtp		
5	Internal-mail-server	Any	Any Traffic	TCP smtp	accept	Log
6	Any	Any	Any Traffic	Any	accept	Log
7	Any	Any	Any Traffic	Any	drop	Log

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

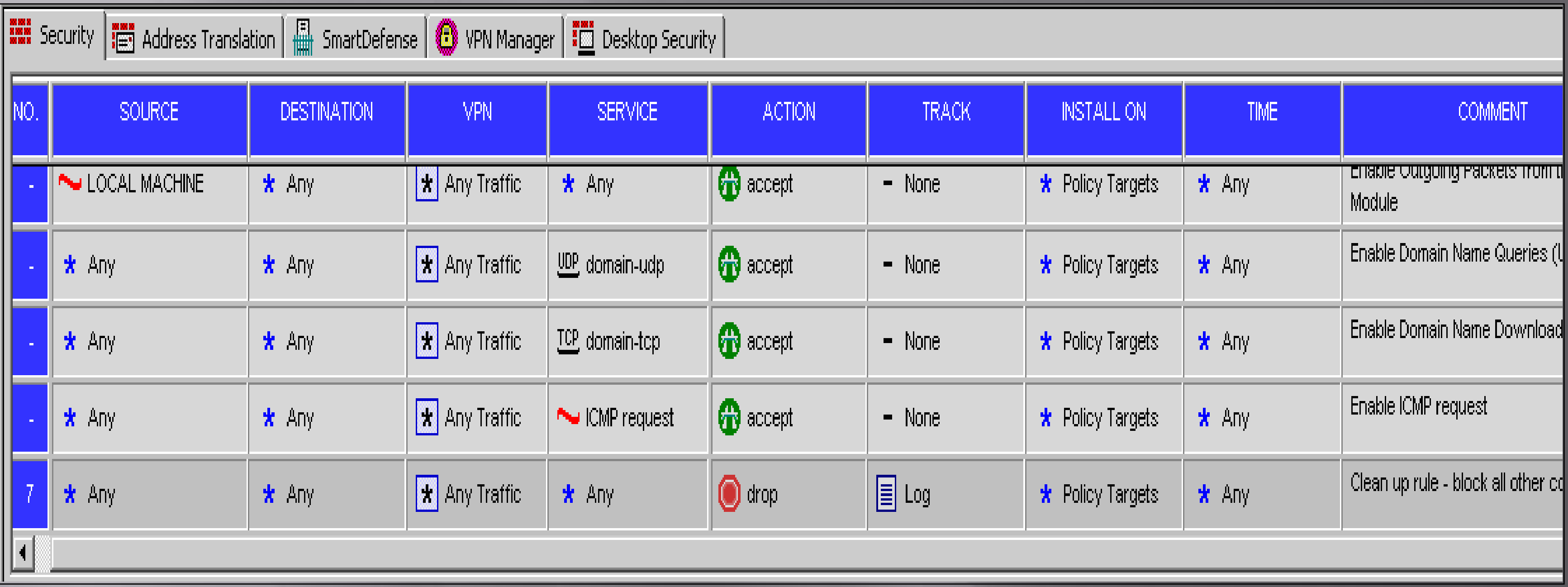
Creation Of Base Of Rules

- 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) 443 TCP(https)
X	X	*DNS Server*	DMZ Net	53 TCP 53 UDP
SMTP Relay	Intemal Net	*Internal Mail Server*	Intemal Net	25 TCP
Intemal Mail Server	Intemal Net	*SMTP Relay*	DMZ Net	25 TCP
X	Intemal Net	*X*	X	80 TCP 443 TCP
Web Server	Intemal Net	*X*	X	53 TCP 53 UDP
IT sector	Intemal Net	*X*	X	20 TCP 21 TCP
IT sector	Intemal Net	*X*	X	23 TCP
IT sector	Intemal Net	*X*	X	23 TCP
IT sector	Intemal Net	*X*	X	161 UDP

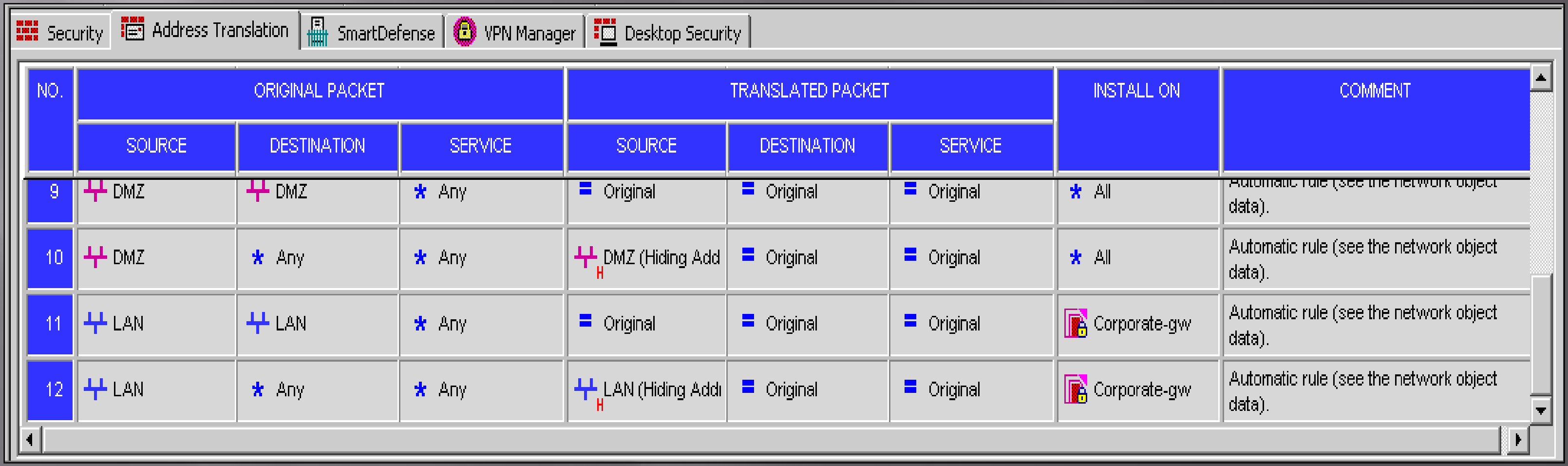


NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
-	LOCAL MACHINE	* Any	* Any Traffic	* Any	accept	- None	* Policy Targets	* Any	Enable Outgoing Packets from t Module
-	* Any	* Any	* Any Traffic	UDP domain-udp	accept	- None	* Policy Targets	* Any	Enable Domain Name Queries (U
-	* Any	* Any	* Any Traffic	TCP 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

Base of Rules
All the rules must be saved at the database server that is lercated in management server

The Application Of Automatic NAT

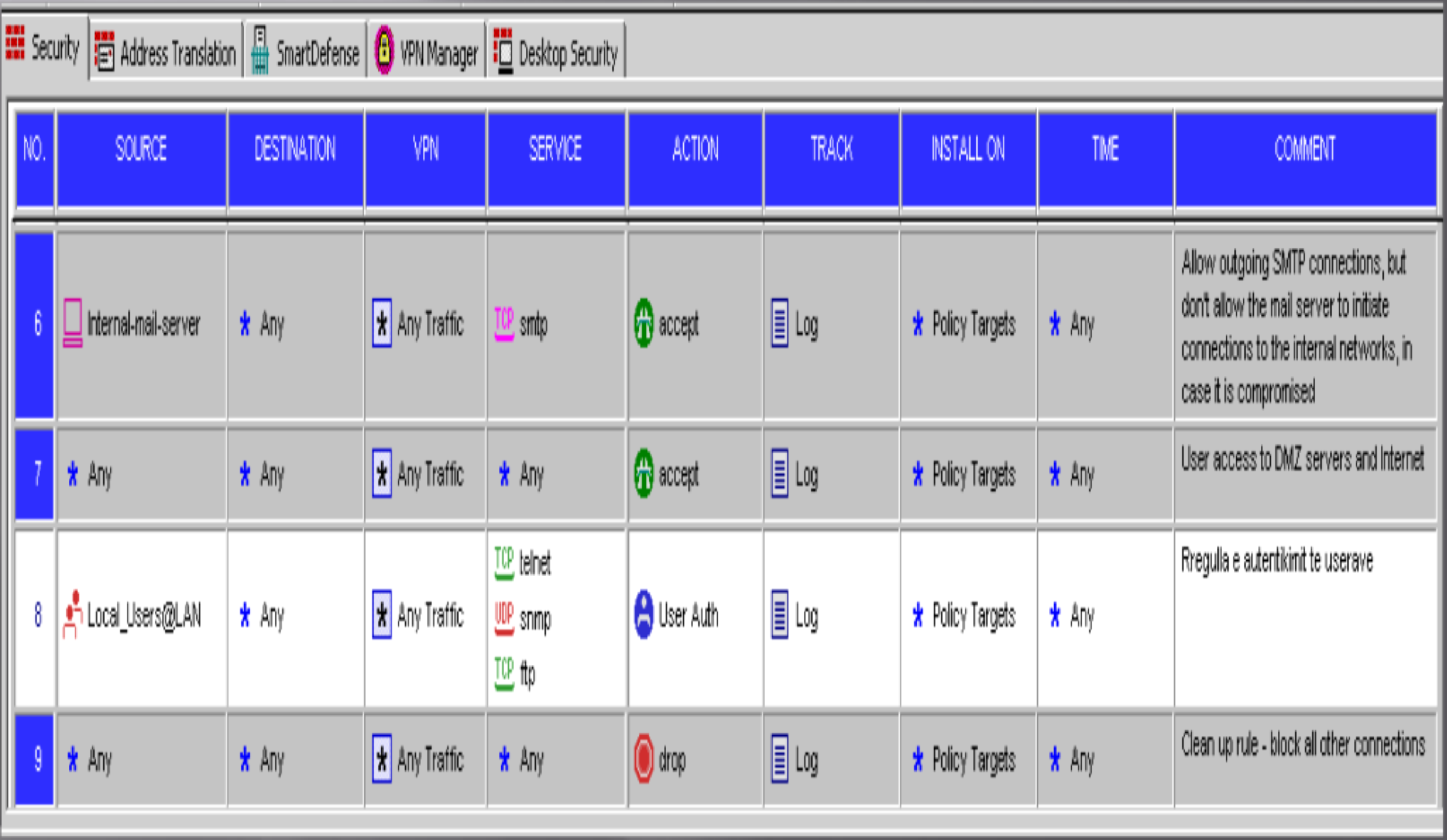
- NAT mechanism will apply in the internal subnet and at the DMZ. We will use the Hide modality and all the packages that go out of our network will be hidden to address of external interfaces of firewall.



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).

Authentication Of Users

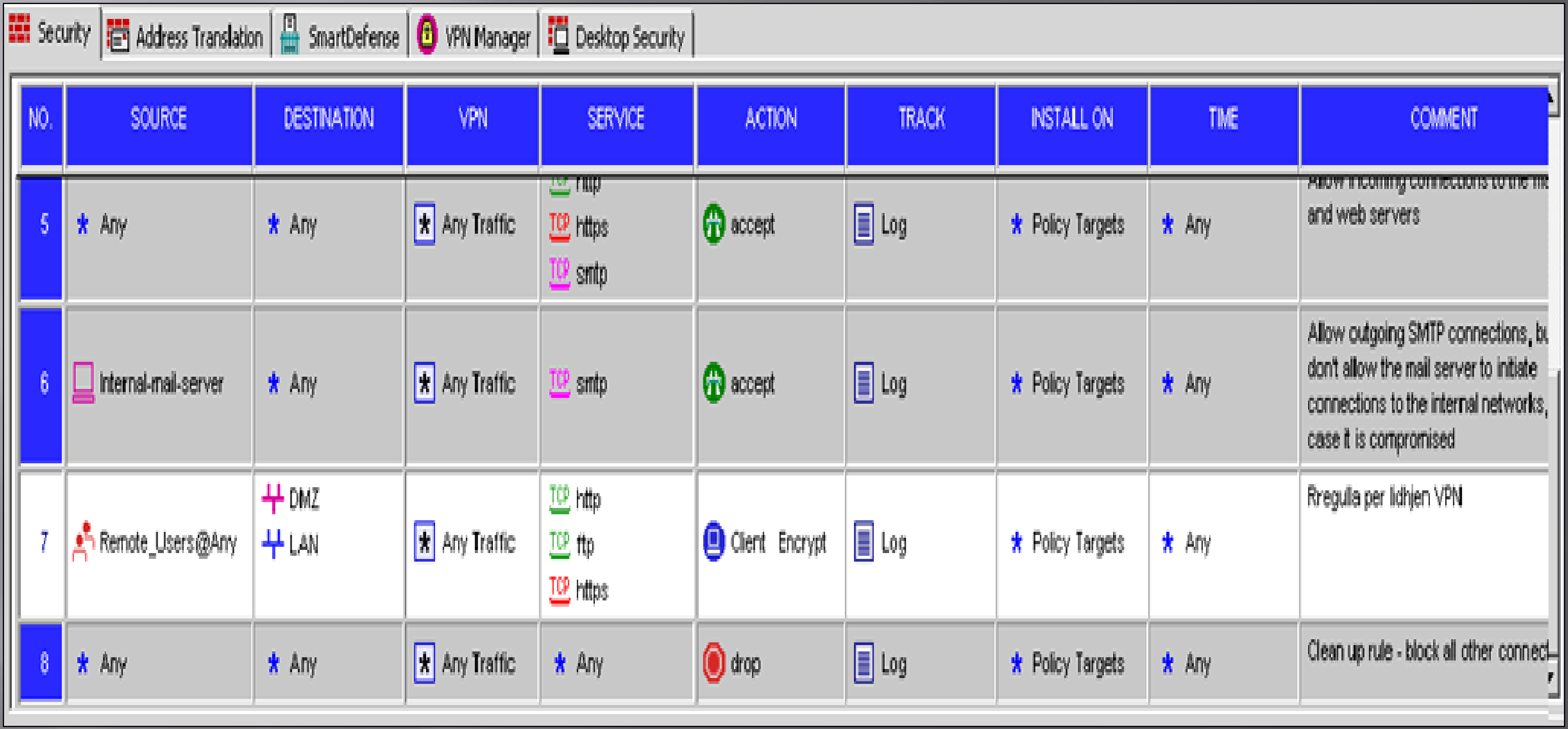
- After we applied NAT-in automatic is the time to configure the user authentication process
- We may use authentication to restrict user access to various network resources by dividing by departments.
- Being that the rules of authentication using user groups and not individual user environments we 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



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
6	Internal-mail-server	* Any	* Any Traffic	TCP 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	TCP telnet UDP snmp TCP 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

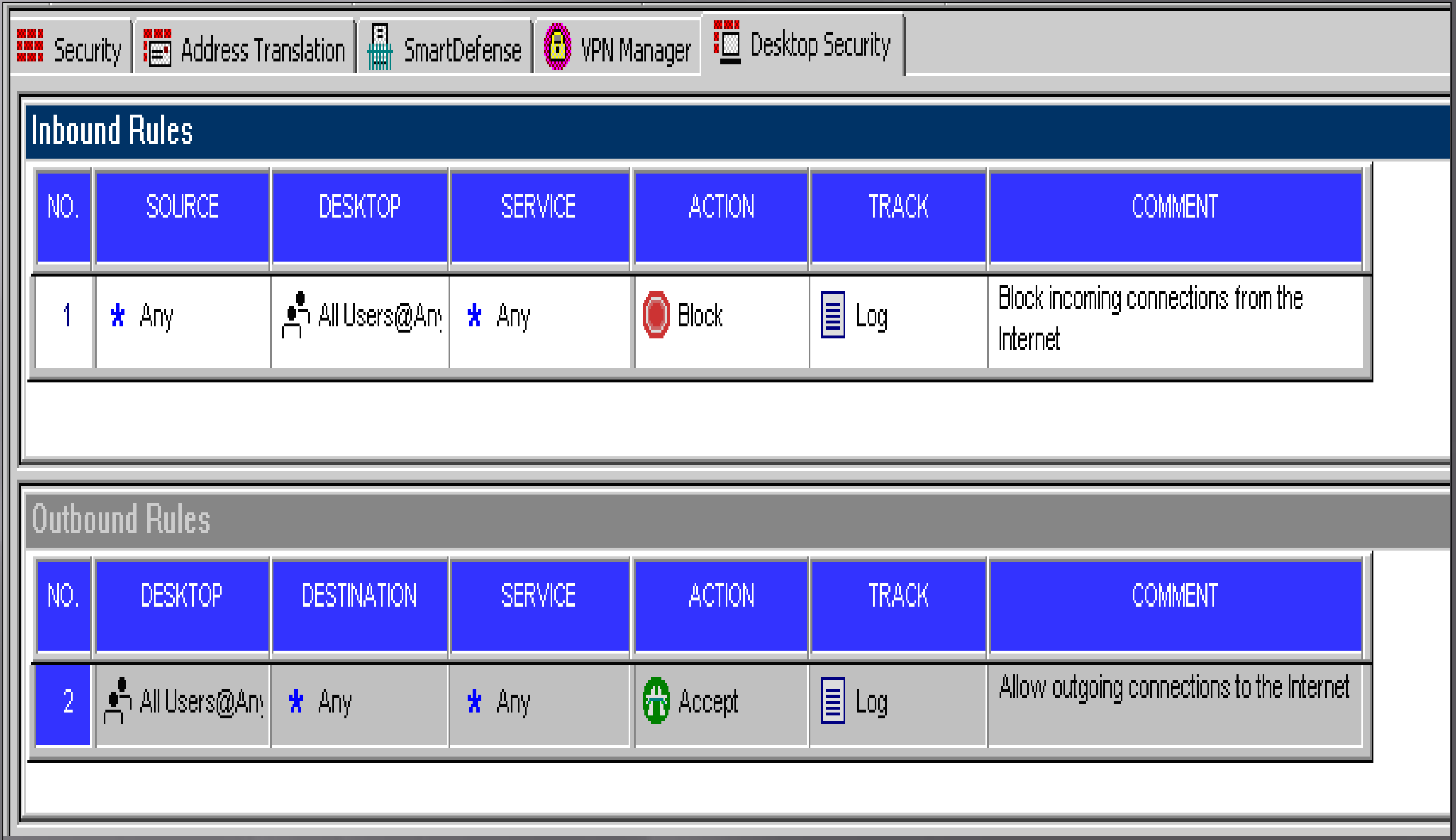
The Realization Of VPN

- 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.**



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
5	Any	Any	Any Traffic	http https smtp	accept	Log	Policy Targets	Any	Allow incoming connections to the m and web servers
6	Internal-mail-server	Any	Any Traffic	smtp	accept	Log	Policy Targets	Any	Allow outgoing SMTP connections, bu dont allow the mail server to initiate connections to the internal networks, case it is compromised
7	Remote_Users@Any	DMZ LAN	Any Traffic	http ftp https	Client Encrypt	Log	Policy Targets	Any	Rregulla per lidhjen VPN
8	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Clean up rule - block all other connect

- Outbound Rule



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

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.
- 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**
- Cherie Amon , Allen V.Keele, Daniel Kligerman, Drew Simonis , Corey Pincock (March, 2002) Check Point NG Security Administration – Syngress.
- **Journals**
- *SC Magazine Awards 2014, Feb. 25, 2014* • San Francisco, Barracuda Firewall, Check Point NG Firewall -1 Administration Guide – Check Point Technologies
- **Manuals**
- Check Point Firewall -1 VPN Manual – Check Point Technologies. *Manuals are taken from Bankers Company, operate in Albania.*
- **Website**
  - *Learn more about Computer Security*. Available from World Wide Web: www.syngress.com
  - *Syngress IT Security Project Management Handbook*. Available from World Wide Web: www.syngress.com
  - www.checkpoint.com
  - www.globalknowledge.com