**Emmanuel Etuk**

# CHECK POINT AS AN ALTERNATIVE TO ACCESS CONTROL LISTS IN MODERN NETWORK SECURITY

**Thesis**
**CENTRIA UNIVERSITY OF APPLIED SCIENCES**
**Information Technology**
**April 2016**

## ABSTRACT

| | | |
|---|---|---|
| **UNIT**<br>Kokkola-Pietarsaari | **Date**<br>April  2016 | **Author**<br>Emmanuel Etuk |
| **Degree programme**<br>Information Technology | | |
| **Name of thesis**<br>CHECK POINT AS AN ALTERNATIVE TO ACCESS CONTROL LISTS IN MODERN NETWORK SECURITY. | | |
| **Instructor**<br>Risto Passoja | | **Pages**<br>39 |
| **Supervisor**<br>Risto Passoja | | |

The scope of monitoring activities on a network is not an easy task. Users constantly try to retrieve information and documents while hackers try every minute to gain access. Protection, being the keyword, is what is needed in both private and public networks to safeguard relevant information from being stolen or misused because no network is truly or completely safe. This project is about modern Network Security using CheckPoint as against Access Control List (ACL). The research focuses more on devices embedded on WAN and used in many network scenarios, including implementation using CheckPoint security.

ACLs are used to filter traffic in parts of the network by denying or allowing flow of traffic to and from these parts. The list has an entry for each system user with access privileges. This is useful as a means of security from both internal and external attacks. Modern networks require a more dependable form of data security.

The research will focus on Check Point as a modern security tool, which makes use of Stateful inspection firewall system. Comparisons will be made on the benefits of depending solely on packet filtering and the combination of both stateful inspection and packet filtering in today's firewall architecture deployment in large and small companies.

**Keywords:**
Security, firewall, checkpoint, gateway, network, communication, list, server.

## CONCEPT DEFINITIONS

**Advanced Encryption Standard -128 bit key (AES-128):** An advanced encryption standard containing 128-bit key size.

**Advanced Encryption Standard -256 bit key (AES-256):** An advanced encryption standard containing 256-bit key size.

**Demilitarized zone (DMZ):** In computer security, a DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet.

**Graphical User Interface (GUI):** A means of interacting with a desktop environment like windows operating systems and statistical software such as JMP, a software for analyzing statistical data.

**Hypertext Transfer Protocol Secure (HTTPS):** This is a secure version of HTTP, which is a safe protocol for communication over a network. It also means data transfer between a user and an accessed website is encrypted.

**Internet Control Message Protocol (ICMP):** A protocol used by network devices to send error messages.

**Internet Key Exchange (IKE):** A protocol used to set up a security association (SA) in the IPsec protocol suite.

**Internet Protocol (IP):** The method or protocol by which data is sent from one computer to another on the Internet through unique identifiers called addresses by different computers.

**Internet Security Association and Key Management Protocol (ISAKMP):** A protocol for establishing Security Associations (SA) and cryptographic keys in an Internet environment.

**Internet Service Provider (ISP):** An organization that provides access to the internet, often times for a fee.

**Local Area Network (LAN):** A computer network that covers a relatively small area.

**Network Interface Cards (NIC):** This is a circuit board or card that is installed on a computer in order to allow it connect to a network.

**Open Systems Interconnection model (OSI model):** A model, which describes how applications can communicate over a network.

**Telecommunication Service Priority (TSP):** A program that approves national security and crisis ready organizations to get needed treatment for critical voice and data circuits or related telecommunications services.

**Transmission Control Protocol (TCP):** A network communication protocol designed to send data packets over the Internet.

**Triple Data Encryption Standard (3DES):** Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block.

**Wide Area Network (WAN):** A computer network that covers a large area.

## CONTENTS

## GRAPHS

## TABLES

# 1 INTRODUCTION

The globalization of the internet has precipitated the need for a more effective and reliable security infrastructure. Organizations and businesses are more dependent on the internet as vaults for private data and information. Just as there is an increase in this regard, security breaches also are on the increase. The common excuse for breaches, when they occur, is that some security defense mechanism somehow fails to provide the needed prevention from intrusion.

Today, many businesses and organizations still depend on packet filtering. This is a way of controlling access to a network by analyzing incoming and outgoing packets. It is achieved by filtering them based on the IP addresses of their sources and destinations. Without a firewall, a network is open to anyone connected through a private or public network. A wide area network is a network that exists within a large geographical area. A Telecommunication Service Provider (TSP) interconnects LANs at their different locations. The providers manage large area networks that can span long distances.  TSPs transports voice and data communications on separate networks. Those networks that connect LANs in geographically separated locations are referred to as Wide Area Networks (WANs). The need to secure a wide area network can be aided and achieved with Checkpoint, a modern security software that uses Stateful inspection by gathering, storing and manipulating traffic relevant to all communication layers and other applications.

This thesis aims to look into the types of threats individuals, organizations and institutions face while using the network as a form of information and data transfer medium. To guarantee a safe working environment for users, an effective mode of network security must be put in place. Access control lists as a firewall solution will be analyzed in relation to large networks and organizations. The period and length of the list in relation to how it translates into more workload for the routers main CPU, will also be analyzed.

The use of Check Point as a tool for effective network security will be looked into concerning large and small organizations. Its use of Stateful inspection will be discussed. Its architecture, firewall modes and relevant component tools will also be analyzed alongside their proper installation procedures.

## 2 SECURITY

Threat level is based on two critical elements, which are the potential impact of the security violation on functional operations (severity of the hazard) and the probability that the violation will occur. The severity of the risk is classified into four categories: Critical, Severe, Moderate, and Low. The probability ranking is also categorized as Frequent, Probable, Occasional, and Possible.

Critical is the exploitation of the vulnerability, which would result in a total system compromise, which may include complete loss of management control and/or use of the compromised system to launch attacks or intrusions against other companies. In addition to direct costs, there may be significant indirect financial loss, due in part to litigation or damaged reputation. An example of vulnerabilities of this nature would be installation of remote control software that would permit a remote intruder full access to the machine. (Danielyan & Knipp 2002, 63-64.)

Severe implies the exploitation of the vulnerability would result in a partial system compromise, potentially losing control over a delivered service or prompting unauthorized distribution of sensitive information. The primary impact of this sort of vulnerability is the direct cost associated with loss of service or information. An example of vulnerabilities of this nature would be a weakness in Web server configuration that allowed for Web page defacement. (Danielyan 2002, 63-64.)

Moderate describes when exploitation of the vulnerability would result in degraded performance and loss of system integrity. Primary impact of this sort of vulnerability is the indirect cost associated with event normalization. An example of vulnerabilities of this nature would be a server subject to a Denial of Service attack. (Danielyan 2002, 63-64.)

Low is considered when exploitation of the vulnerability results in degraded performance without loss of integrity, or which prompts an inability to control integrity in a functioning host. The primary impact of this sort of vulnerability is the indirect cost associated with higher maintenance. An example of vulnerabilities of this nature would be user-controlled desktops. (Danielyan 2002, 63-64.)

The level of probability for the aforementioned include frequent, which is the probability of the event happening again. This might occur if the vulnerability has been widely publicized, automated tools are available, or if a worm, using the exploit is available. The probability level, which is considered probable, is when the event is likely to happen several times during the life cycle of the host system. This might occur because the vulnerability is well known, but “user friendly” exploit tools are not available, and thus require a higher level of skill to compromise the system. Likewise, occasional level implies the event is likely to occur again sometime during the host system’s life cycle. This would occur when the vulnerability is not well known, or when specific circumstances would be required for a breach (such as a maintenance window when certain protections are not in place). Finally, possibility level is when it is unlikely but possible to occur in the system’s lifecycle. A classification may be such when the vulnerability is of a theoretical nature and no exploit code is known, or specific circumstances of low probability are required, or when the vulnerability is of a theoretical nature whereby no methods exits to exploit the vulnerability as it is currently known. (Danielyan 2002, 63-64.)

## 2.1 Attacks

Due to the ever-increasing expansion of the internet, many organizations are fully focused on providing protection against attackers, which can be both internal and external. Various information security studies have found that the majority of attacks actually come from inside the organization. The internal threat can include authorized users attempting to exceed their permissions or unauthorized users trying to go where they should not be at all. The insider is potentially more dangerous than the outsider is because they have level of access than the outsider. (Vitaly 2002, 8.)

According to Lammle (2014), the most common forms of attacks are in the category of Application-layer attacks, which is a kind of denial of service attack achieved by attacking the OSI model. The assault creates more activities in particular functions or components of a site with the aim to cripple those capacities or features. Also described is Auto-rooters, which is a toolkit made by hackers to infiltrate particular shortcomings in PCs particularly with most recent point and click PC users. (Sumit  & Elliot. 2011.). Another form of attack is the Backdoor attack, which refers to a situation where access can be gained to a network in order to create pathway through a programme for easy access by hackers. (Emmet 2011, 150.) Similarly, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks works by flooding and creating more workload in network resources in order to meddle with typical operations of network administrations, depleting and overpowering the assets of the focused on system.  A distributed denial-of-service (DDoS) attack occurs when different systems surge the data transmission on a focused system, generally one or more web servers. Such an assault is regularly the aftereffect of different compromised multiple systems (for instance a botnet) flooding the focused system with activity. (Ghorbani, Wei, & Tavallaee 2009, 11.)

Tribe Flood Network (TFN) and Tribe Flood Network 2000 (TFN2K) are sets of computer program aimed at conducting various DDoS attacks like ICMP, SYN, UDP floods including Smurf attacks. TFN2K is a device allowing clients to exploit others' resources to facilitate a cyber-attack against one or numerous objectives, bringing about a Distributed Denial of Service (DDoS) attack. It is made of two components namely a user-controllable interactive client program on the master and a server process operating on an agent. (Lammle 2014.)

Other examples such as Stacheldraht, IP spoofing, Man-in-the-middle attacks, Network reconnaissance, Packet sniffers, Password attacks, Brute-force attack, Port redirection attacks, Trojan horse attacks and viruses and Trust exploitation attacks, according to Lammle (2014), are classified under Reconnaissance, Access and DoS attacks. Reconnaissance attacks involves Hackers attempting to discover vulnerable systems in order to gather information. In most cases, these attacks are used to gather information to set up an access or a DoS attack. A typical reconnaissance attack might consist of a hacker pinging IP addresses to discover what is alive on a network. The hacker might then perform a port scan on the systems to see which applications are running as well as to determine the operating system and version on a target machine. Access attacks involves one in which an intruder attempts to gain unauthorized access to a system to retrieve information. Sometimes the attacker needs to gain access to a system by cracking passwords or using an exploit. At other times, the attacker already has access to the system but needs to escalate his or her privileges. DoS attacks are used by Hackers to disable or corrupt access to networks, systems, or services. The intent is to deny authorized or valid users access to these resources. DoS attacks typically involve running a script or a tool, and the attacker does not require access to the target system, only a means to reach it. In a distributed DoS (DDoS) attack, the source consists of many computers that are usually spread across a large geographic boundary. (Vitaly 2002, 8.)

## 2.2 Firewall Solutions

Access Control Lists as a Firewall Solution is a list containing access control entries, which identifies a user by allowing or denying access rights. Although ACLs does not serve the same purpose as a complete firewall, it serves majorly in controlling the IP network. Grout, Mcginn & Davies (2007), describe an access list, or Access Control List (ACL), as a sequence of rules designed to implement a given objective or set of objectives. ACLs can be used simply to pass or block packets or as filters for more sophisticated policies such as traffic shaping, address translation, queuing or encryption.

ACLs consists of two types namely, Standard and Extended ACLs. Deepak & Prasad (2015), describe Standard ACLs as a simple IP ACL that filters based on source address only, that is, source network or source host. It cannot filter based on the destination of a packet wherein the protocol being used like Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), or on the port number.

Deepak (2015) explains that for Extended ACLs, the list checks both the source and destination addresses. In addition, checks are carried out for specific protocols, port numbers and other parameters. They can also be used in enforcing network policies. Deepak. A packet may be matched against several ACLs on a single router and many on its complete journey from source to destination. A rule can consist of different parts such as permit or deny type, the protocol, source address, destination address and flag function. Colton (2002), gives a typical example in the syntax of the Cisco Internetwork Operating Systems (IOS) as follows:

```
access-list 101 deny icmp any 10.0.0.0 0.255.255.255
echo-reply
```

This implies that the parameter above matches all source addresses whilst the 0.255.255.255 parameter matches destination addresses in the 10.0.0.0 network. It states that the Internet Control Message Protocol (ICMP) echo-reply packets from any source to the 10.0.0.0 network will be blocked. (Grout, McGinn & Davies 2007.)

The rules are processed one after the other. This means that each rule is tried against the first control rule. If it matches, it is passed. If not, it is blocked accordingly without further test. This is because there is a specific (deny all) rule at the end of each ACL. (Grout et al. 2007.)

Cisco explicitly explains that traffic coming into a router is compared to entries in the ACL. This determines the action of the router, whether to keep looking until it finds a match or deny all after reaching the end of the list in the event there is no match. This means that there must be at least one permit entry in ACL, else all traffic is denied. (Cisco Systems, Inc. 2007.) According to Cisco Systems, Inc. (2007), Table 1 below correctly describes ACL commands and their functions.

TABLE 1. ACL Commands and Functions (Cisco 2007).

| ACL Command | Function |
|---|---|
| `access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255` | This command permits IP traffic from 10.1.1.0 network to 172.16.1.0 network. Any packet with a source address not in this range is rejected or denied. |
| `access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255`<br>`access-list 102 deny ip any any` | In this example, IP traffic from 10.1.1.0 network is granted permission to network 172.16.1.0. Likewise, packets with a source address not in this range is denied. |
| `access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet` | For this example, the command permits Telnet Traffic from machine 10.1.1.2 to machine 172.16.1.1. |
| `access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1` | Here, the command is used to permit TCP Traffic from 10.1.1.2 host machine to 172.16.1.1 host machine. |

| | |
|---|---|
| `access-list 101 permit udp host 10.1.1.2 host 172.16.1.1` | In this example, the command permits UDP Traffic from 10.1.1.2 host machine to 172.16.1.1 host machine. |
| `access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255` | The command here permits IP Traffic from 10.1.1.0 network to 172.16.1.10 network. |

Access list statements are entered one line at a time and the list is scanned for a match in that same order. Once entered, the list must be associated with the interface on the router where filtering will occur. One can apply the list to incoming packets, (an "in" access list) or outgoing packets (an “out” access list). In most cases, either list will work. For out access lists, one needs to set up the filter only on the one outgoing interface rather than on the individual incoming interfaces.  This improves performance because only the network you are protecting will force a lookup on the access list. (Morrissey 1998.)

The time to process an ACL is then the total time taken to test a packet against each rule up to and including the one it matches. This brings to question the issue of performance. Router effectiveness is altered by access list filters despite Cisco’s inbuilt performance enhancing features. Features such as fast switching, autonomous switching, distributed switching and optimal switching is not utilized during packet filtering, hence forcing the packets to be processed switched. The ultimate outcome of this effect creates a burden for the router’s main CPU. (Morrissey 1998.)

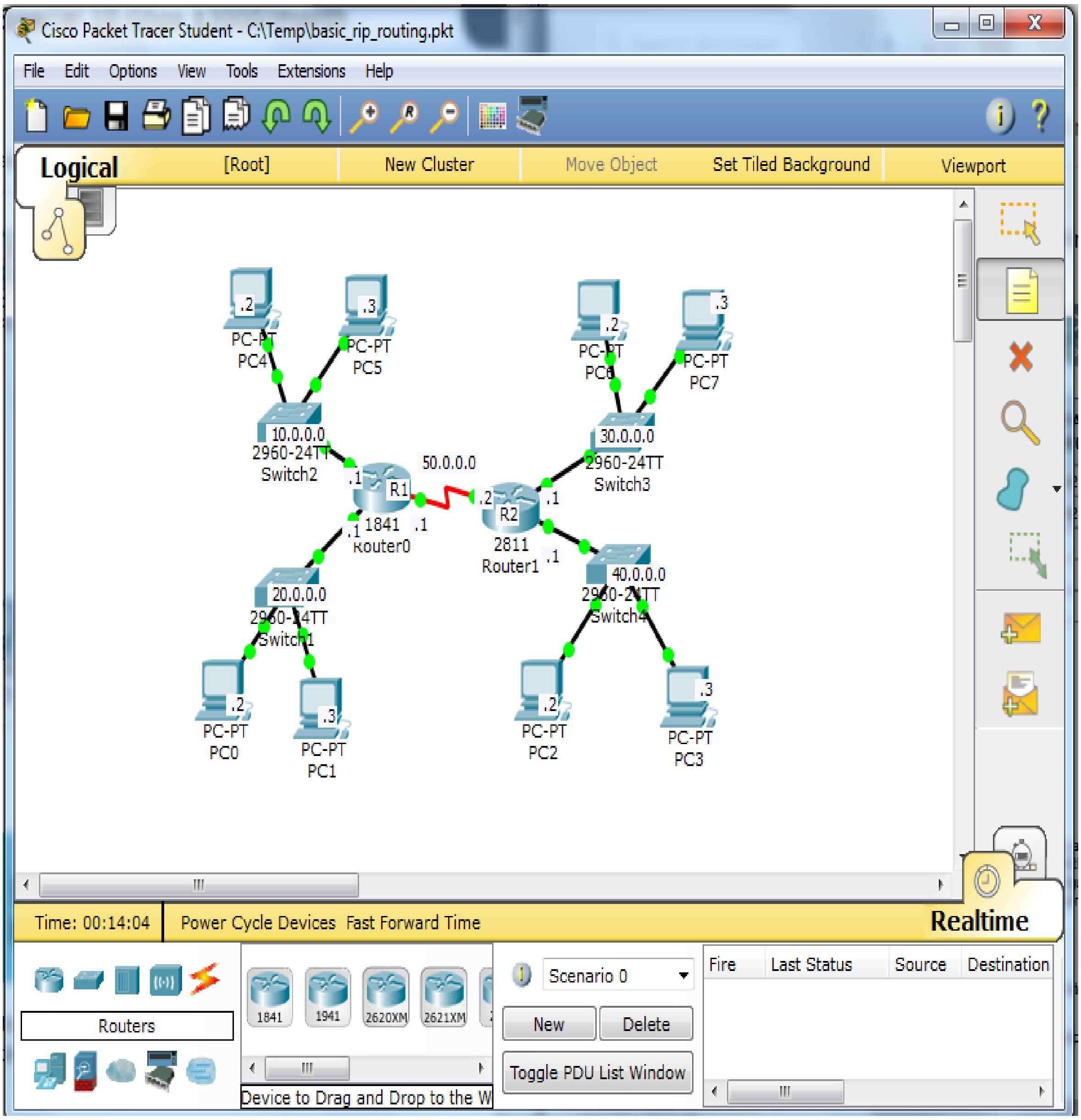
Another problematic issue is the length of the access lists. The more the lists the more the work done by the router to process each packet. The solution to reduce this is to locate the most likely matches at the top of the list. This is achieved by placing a rule that allows all TCP established or ACK (acknowledged) packets. The following statements at the top of the access lists allows all established packets.

```
access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.0
established
```

Access Control is an integral part of securing the network especially in WANs with lots of locations and systems. Data protection and packet filtering at this level reduces the success and manifestation of threats and attacks. Access controls at both the network and system level, are often not as strong as they should be. All users may share drives with read/write access. The typical user has a greater level of access than he or she needs to do a job. Tightening up access controls can result in substantial improvements in a company's security posture. Some technological solutions include firewalls, router access lists, and policy enforcement tools that validate and perhaps control file system access. (Vitaly 2002, 13.)

A typical example for configuring a standard access list can be shown using a Routing Information Protocol (RIP) topology as in Graph 1. The Packet Tracer, a cross platform simulation tool, will be made use of in this instance. All that is needed at this point is the IP addresses of the hosts (PC5) and the subnet to permit or deny, relative to which direction. This is because standard ACLs filters traffic based on traffic coming from the source.

In this case, an attempt will be made to block 10.0.0.3 from gaining access to 40.0.0.0 whilst being able to communicate with other networks. In addition, network 10.0.0.0 should be able to receive packets from 40.0.0.0. In order for our host to be able to communicate with others except 40.0.0.0., the list will be placed on FastEthernet 0/1 of Router 2 (R2) despite being connected to 40.0.0.0.



GRAPH 1 Packet Tracer RIP Topology

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 deny 10.0.0.3 0.0.0.0
R2(config)#access-list 1 permit any
R2(config)#interface fastEthernet 0/1
R2(config-if)#ip access-group 1 out
```

As seen above in the commands, the router is configured and the list is applied to match every device in the network. In order to test, ping from 10.0.0.3 to 40.0.0.3. As the packet is filtered by the ACL, it requests time out. Nevertheless, pinging 30.0.0.3 is successful as shown below.

```
PC>ping 40.0.0.3
Pinging 40.0.0.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 40.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 30.0.0.3

Pinging 30.0.0.3 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.3: bytes=32 time=140ms TTL=126
Reply from 30.0.0.3: bytes=32 time=156ms TTL=126
Reply from 30.0.0.3: bytes=32 time=112ms TTL=126

Ping statistics for 30.0.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 112ms, Maximum = 156ms, Average = 136ms
```

Just as the list is applied to a specific host, other networks connected to 10.0.0.0 should be able to connect to 40.0.0.0 network. This will be tried by pinging from 10.0.0.2 to 40.0.0.3. The result is as shown below.

```
PC>ipconfig

IP Address......................: 10.0.0.2
Subnet Mask.....................: 255.0.0.0
Default Gateway.................: 10.0.0.1

PC>ping 40.0.0.3

Pinging 40.0.0.3 with 32 bytes of data:

Request timed out.
Reply from 40.0.0.3: bytes=32 time=141ms TTL=126
Reply from 40.0.0.3: bytes=32 time=140ms TTL=126
Reply from 40.0.0.3: bytes=32 time=125ms TTL=126

Ping statistics for 40.0.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 125ms, Maximum = 141ms, Average = 135ms
```

In order to match everyone and anyone, the following list is implemented.

```
access-list 1 permit any
```

Or

```
access-list 1 permit 0.0.0.0 255.255.255.255
```

A good example of where a packet filter fails is with the File Transfer Protocol (FTP). The FTP protocol requires a dynamic high TCP port opened back to the server. Since a packet filter does not understand protocols, it would have to have all TCP high ports opened back to the server to support the FTP protocol. Any protocol that uses dynamic ports would require all the ports opened through a packet-filtering firewall. (Stiefel, Stephens & Watkins 2005, 5.)

Packet filtering comes with a few advantages and disadvantages. The advantages include compatibility, which allows the packet filters to work with any protocol as far as the packet stream is not altered by the packet filters. So also is Performance whereby the packet filters work swiftly since they only depend on headers. Lastly is Scalability. This is due to the simplicity of the packet filters. Disadvantages include low security whereby the packet filters ignore the data portion through which attacks can come through. Furthermore, there is a lack of support for dynamic protocols because the filters do not keep track of connections.  In all it is advisable not to depend solely on packet filtering as firewalls because attacks can pass through them easily. (Danielyan 2002.)

CheckPoint VPN-1/Firewall-1 is a new generation firewall Solution that analyzes traffic through Stateful inspection. This technology stores and allows all traffic to be checked and manipulated as they pass through the firewall. This gives traffic a more robust protection whilst taking into account high performance, application awareness, security, transparency and extensibility.VPN-1 is a Stateful firewall which filters traffic by inspecting the application layer. It is designed to prevent unauthorized access to data to or from the networks linked with the firewall. Firewall-1 is usually considered the same but in fact, both have different functions. (Simonis 2002, 5.)

According to Noble, Maxwell, Hourihan, Stephens, Stiefel, Amon & Tobkin (2003), FireWall-1 provides the data filtering, logging, and access control as expected of any firewall gateway. VPN-1 integrates tightly into FireWall-1 to add virtual private networking tools alongside the firewall. Combining VPN-1 with FireWall-1 has allowed Check Point to provide firewall and VPN products that not only leverage each other's strengths, but

Check Point provides, in the NG suite, the tools required to manage VPN1/FireWall-1 in a distributed environment, allowing security managers to define and enforce a single Security Policy across the entire enterprise. (Simonis 2002, 5.)

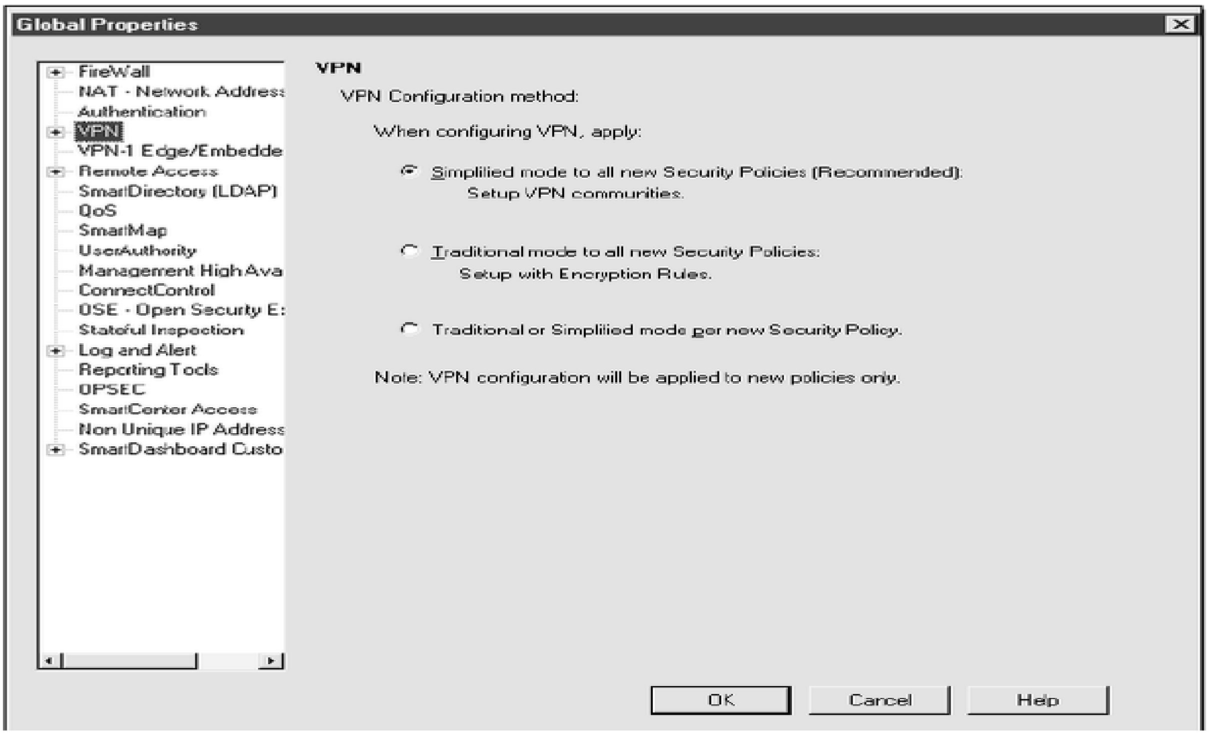
## 3 CHECKPOINT

Check Point Software Technologies Ltd is a pioneer in securing the Internet. It is a market pioneer in enterprise firewall, personal firewall and VPN markets. Check Point Software Technologies sets up a perimeter around networks. It provides security tools and devices for large networks and service providers. Check Point's products verify remote users, incoming traffic alongside virus protection. Its products enable companies to set up virtual private networks (VPNs) for secure internal and remote connections, alongside devices for bandwidth management, network performance, and availability applications. (Checkpoint 2009.)

The Check Point Next Generation (NG) Suite is composed of several different products bundled to create a complete enterprise security solution. The combination of these specialized tools allows the NG suite to address the major security and network management challenges facing today’s security managers. Rather than look at network security solely from the firewall or Virtual Private Network (VPN) solution, Check Point set out with its Secure Virtual Network (SVN) architecture, to encompass all areas of Enterprise security into a single, easy-to-use product offering. Until recently, many enterprise security managers believed that simply firewalling their network at the Internet connection provided all the security they needed. In today’s network world, there are Intra and Extranet connections to secure, not to mention remote dial and VPN access to worry about. The SVN architecture looks at the entire enterprise network, encompassing not only Local Area Network (LAN) and Wide Area Network (WAN) connections, but extending right down to the individual VPN connected user. This new enterprise level view of security defines a complete, scalable, and secure architecture that requires the integration of several products to achieve. (Noble et al. 2003, 3.) According to Morrissey (1998), CheckPoint Software Technologies Router Management Module, available with its Firewall-1 product allows the central management of the configuration of access list on Bay, Cisco, and 3Com Routers via GUI.

### 3.1 CheckPoint NGX

Checkpoint NGX supports varied number of encryption algorithms such as Digital Encryption Standard (DES), Triple Digital Encryption Standard (3DES), Advanced Encryption Standard -128 bit key (AES-128), Advanced Encryption Standard -256 bit key (AES-256), and finally Cast Encryption. VPN-1 primarily uses the traditional and simplified approach to configure Virtual Private Networks (VPN) between sites. The traditional method requires configuring the access rules, which specify what traffic should be encrypted. The simplified method requires the specification of the devices, which should have their communication encrypted. Setting up VPN between sites using these methods is quite easy. Selection of the desired approach can be made easily by going through Policy - global properties – VPN, as shown in Graph 2. ( Stiefel, Stephens & Watkins 2005.)



VPN

VPN Configuration method:

When configuring VPN, apply:

● Simplified mode to all new Security Policies (Recommended):
Setup VPN communities.

○ Traditional mode to all new Security Policies:
Setup with Encryption Rules.

○ Traditional or Simplified mode per new Security Policy.

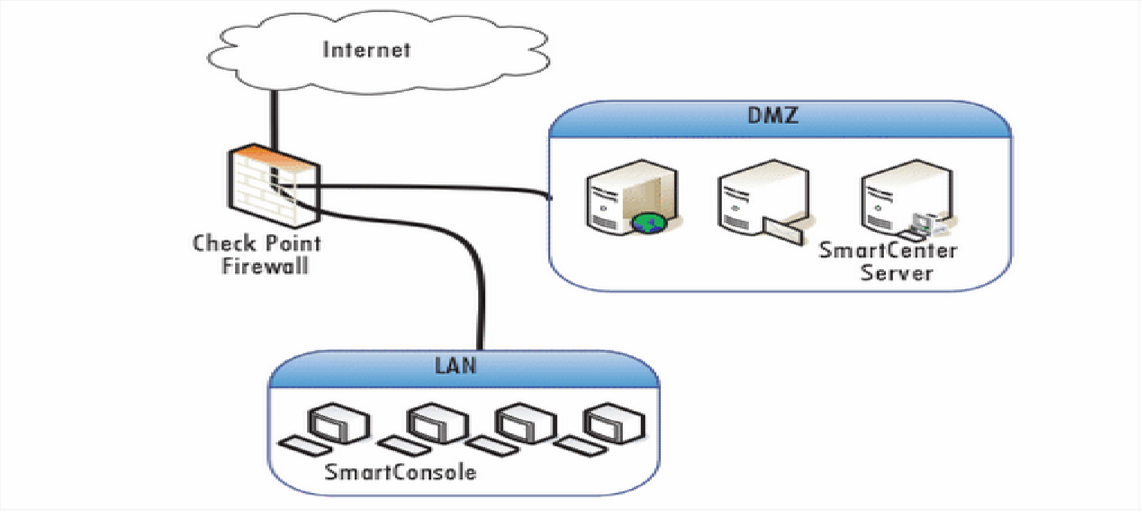
Note: VPN configuration will be applied to new policies only.

GRAPH 2. VPN Configuration Method Selection (Stiefel et al. 2005, 367).

According to Bonnell & Desmeules (2008), there have been significant improvements in VPN functionality with the new addition of SecurePlatform pro, which offers dynamic routing and support for remote authentication Dial-in User service (RADIUS) for enterprise security solution managers. The product is available to larger organizations interested in incorporating the router in their Checkpoint firewalls into their current dynamic routing configuration.

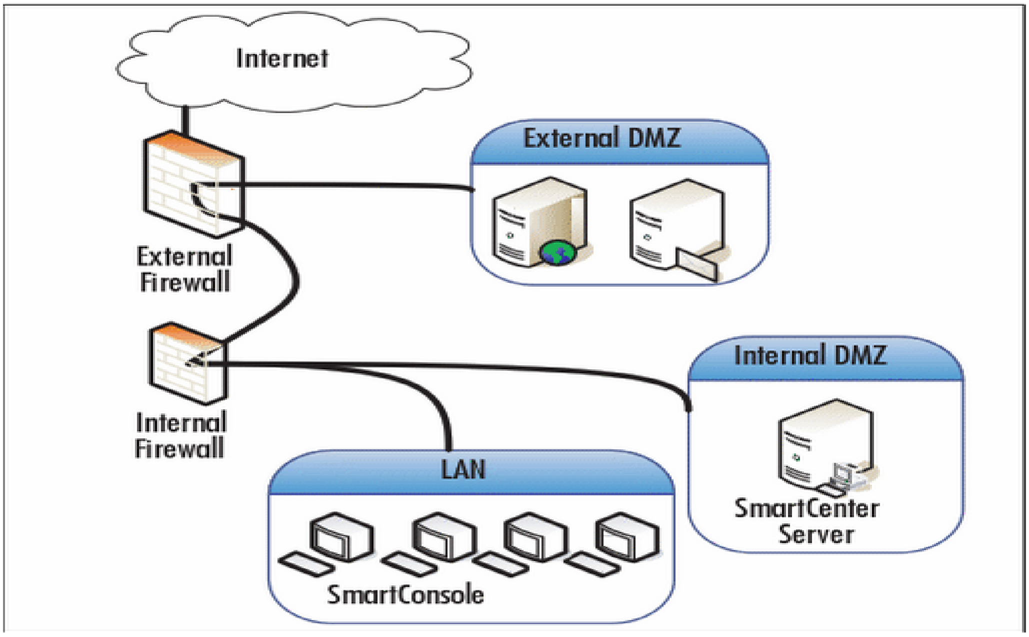
### 3.2 Firewall Modes

Check Point firewalls can be utilized as a part of any possible DMZ setup, including the conventional "three-legged" configuration, a multi-DMZ setup, and the dual-firewall "sandwich" or "back-to-back" design, where separate firewalls shield the external and internal networks from one another (Flynn 2006 321.) Graph 3 illustrates a typical “three-legged firewall design” having SmartConsole and SmartCenter separate from the gateway. The SmartCenter server is located in the DMZ but could serve the same purpose even if located inside the LAN. Essence of the SmartCenter in the DMZ is to allow the user use the SmartConsole GUI in the internal LAN to manage other firewalls located on external, Internal or third party networks. When limited to managing firewalls on the local network, it would be more useful placed on the internal LAN. This ensures extra security since it cannot be accessed by unknown networks. (Flynn, 2006.)



GRAPH 3. “Three-legged” firewall with distributed CheckPoint Architecture (Flynn 2006, 322).

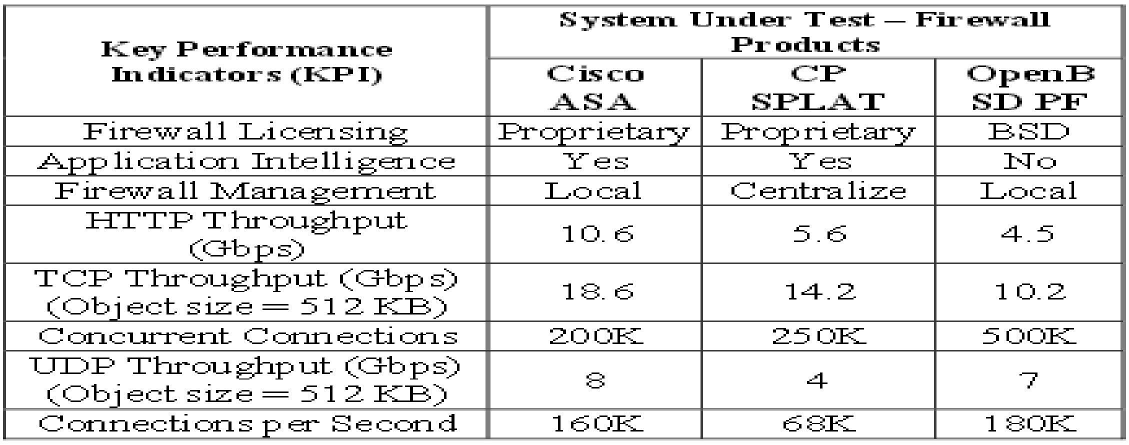
“Sandwich” or “Back-to-Back” combines two firewalls to separate internal resources from external resources, which could be accessed from outside the infrastructure. The two firewalls serve to boost up security at the gateway. The primary disadvantage to the three-legged firewall is the additional complexity. Access to and from the DMZ and to and from the internal network is controlled by one large set of rules. This is illustrated in Graph 4.



GRAPH 4. “Sandwich” or “Back-to-Back” firewall with distributed CheckPoint architecture (Flynn 2006, 323).

Performance test results using curl loader, an open source tool, indicates, as shown in Table 2, describes the various performance levels for various firewalls. The results were arrived at using Key Performance Indicators (KPI). Test were performed on Cisco ASA, CheckPoint SPLAT and OpenBSD PF. The results show CheckPoint firewall as most suitable for large networks alongside greater functionality. (Chirag & Thakker 2011.)

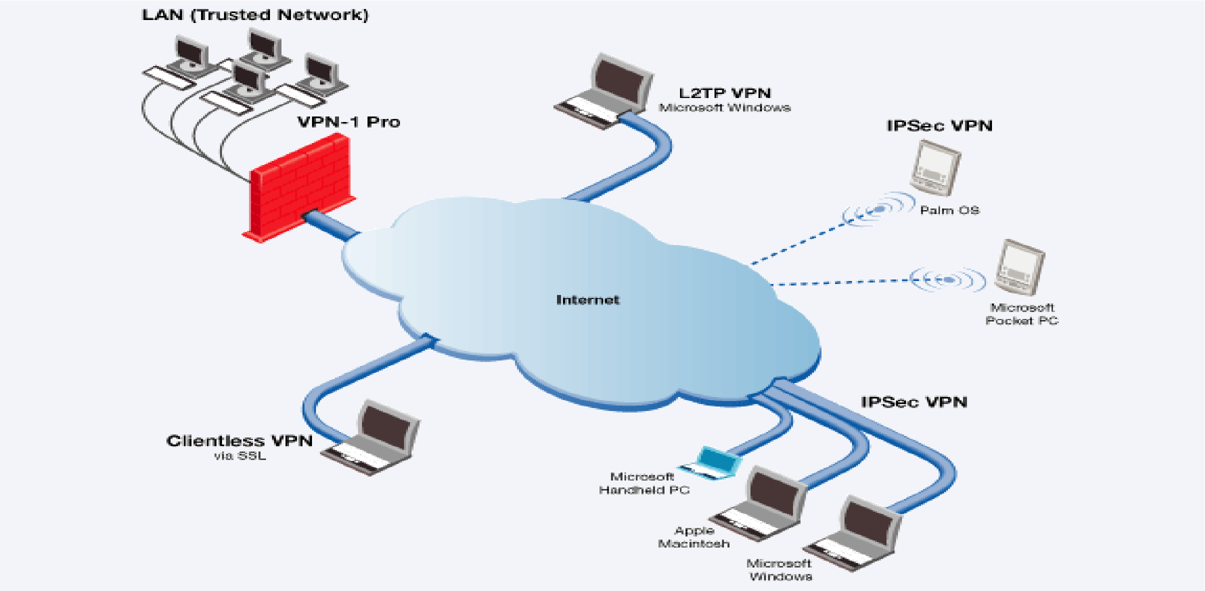
TABLE 2. Performance Test Results (Chirag 2011).



| Key Performance Indicators (KPI) | System Under Test – Firewall Products | | |
|---|---|---|---|
| | Cisco ASA | CP SPLAT | OpenBSD PF |
| Firewall Licensing | Proprietary | Proprietary | BSD |
| Application Intelligence | Yes | Yes | No |
| Firewall Management | Local | Centralize | Local |
| HTTP Throughput (Gbps) | 10.6 | 5.6 | 4.5 |
| TCP Throughput (Gbps) (Object size = 512 KB) | 18.6 | 14.2 | 10.2 |
| Concurrent Connections | 200K | 250K | 500K |
| UDP Throughput (Gbps) (Object size = 512 KB) | 8 | 4 | 7 |
| Connections per Second | 160K | 68K | 180K |

### 3.3 SecuRemote and SecureClient as Gateway tools

SecuRemote and SecureClient are great tools provided by Checkpoint for VPN remote connections. Both make use of AES-128 and AES-256 encryption alongside SmartDashboard, which add new functionality with dual routing rules to the SecureClient Device. Ultimately, this enables applications to connect to VPN hosts through existing encrypted tunnels. Both tools also support rapid and fixed IP addressing for all ISP's such as dial-up, cable, and digital subscriber lines DSL. All VPN functionality, including key negotiation and data encryption, is very meaningful to the client. Every time a user requests a connection, VPN-1 SecuRemote/SecureClient intercepts the request and figures out whether the destination resource is linked to a known VPN-1 gateway as illustrated in the diagram below. Once identified, the VPN-1 client is instantly invoked and authentication is requested. (Stiefel 2005.) VPN-1 SecuRemote/SecureClient likewise resolves both internal unregistered domains and external domain names. This described in Graph 5.



GRAPH 5. Secure VPN Connectivity (Checkpoint 2009).

#### 3.3.1 SecuRemote

SecuRemote is Check Point's VPN-1 Client item. It is a specialist tool located on the customer machine, allowing encrypted secure access to an organization's private network. It makes use of an easy to use Graphical User Interface (GUI) VPN customer. It uses the IKE

(ISAKMP) key exchange protocol to set up an encoded passage between the desktop machine and the VPN-1 Firewall gateway thereby enabling desktops to be connected to any internet connection and allowing users to safely access an organizations internal network resources like email and internal web applications. (Stiefel et al. 2005, 399.)

Features in the CheckPoint NGX SecuRemote include NAT-T Support, which conforms to the industry standard Network Address Translation (NAT) transversal. Office Mode, which is utilized to allow access to other gateways within the private network using an assigned address and Multiple Entry Point MEP, which centralizes a connection profile by providing a backup gateway irrespective of a MEP decision. General Connectivity in terms of encryption domains are now specified from site to site VPN and for remote access VPN. (Stiefel et al. 2005, 399.)

### 3.3.2 SecureClient

SecureClient takes into account increased desktop security. As an enterprise, it is essential to guarantee that the mobile workforce has access to data to and from the organization's private network. Nonetheless, once data is downloaded to a client's portable PC or remote machine, the information is helpless against attack. Upon connecting to the VPN-1 gateway, SecureClient downloads the most recent, applicable Desktop Security policy and enforces it on the end user’s machine. SecureClient are located at the kernel level, inspecting all network traffic to and from the machine to protect the end user from malicious traffic and attacks. This way it protects the end user from attacks as well as the internal network. (Stiefel et al. 2005, 429.)

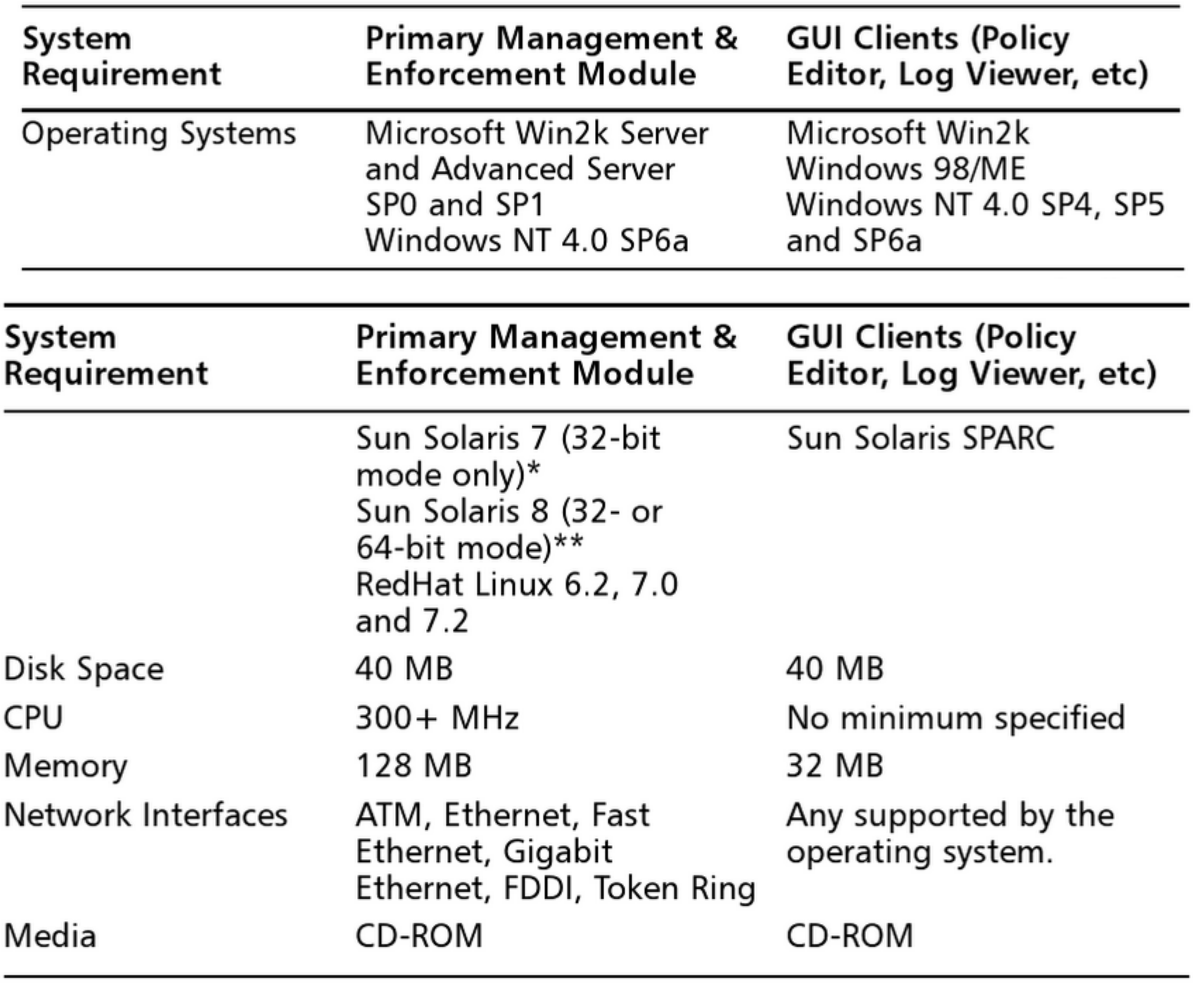
New features of the CheckPoint SecureClient include Policy Expiration, which happens after connection. SecureClient attempts to download and update the policy in half the expiration time. If unsuccessful, it does not revert to the default policy. As will be discussed later during the installation process, there is not much difference between the installation of SecuRemote and SecureClient. Preferences can be made by selection when installing the package. (Stiefel et al. 2005, 429.)

### 3.4 System Requirements

CheckPoint earliest releases defines a list of minimum requirements as shown in Table 3 below. Current versions, which include Checkpoint Splat, R65, R70 and R77, come with added features and have updated system requirements. Clients can upgrade from the older versions to the newer ones with ease. Table 4 & 5 describe the latest requirements by platform basis.

For Windows platform, Ultimate, Professional and Enterprise Editions are supported by Windows 7 while for Windows 8, it is true for Professional and Enterprise editions only. Just as indicated below, all the marked consoles and platforms are true for 32-bit and 64-bit, unless shown otherwise. (Checkpoint Software Technologies Ltd. 2016.)

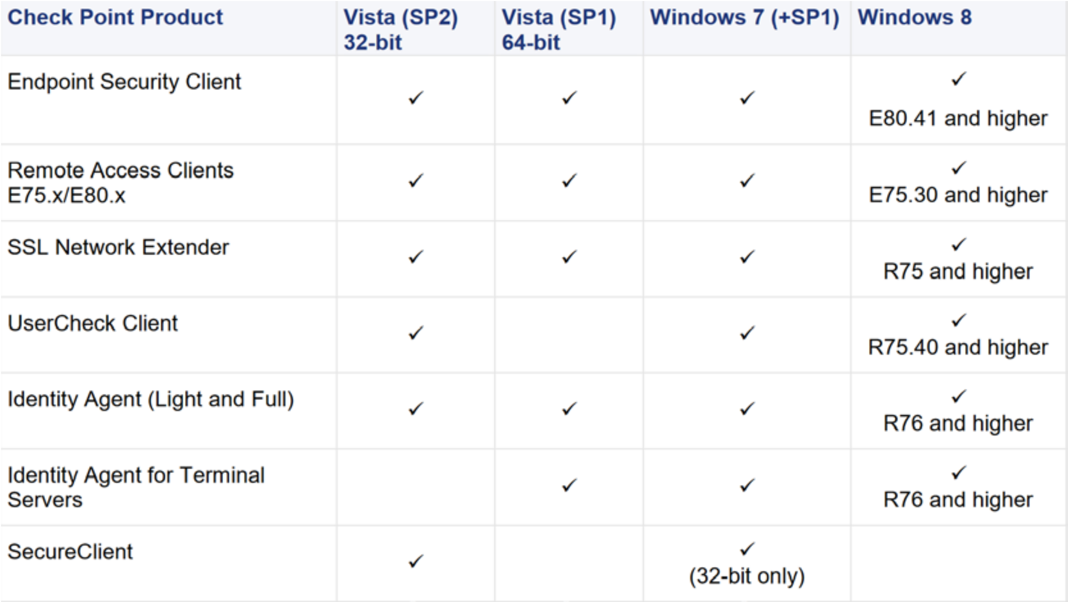
TABLE 3. Minimum System Requirements (Amon et al. 2002).



| System Requirement | Primary Management & Enforcement Module | GUI Clients (Policy Editor, Log Viewer, etc) |
|---|---|---|
| Operating Systems | Microsoft Win2k Server and Advanced Server SP0 and SP1<br>Windows NT 4.0 SP6a<br>Sun Solaris 7 (32-bit mode only)*<br>Sun Solaris 8 (32- or 64-bit mode)**<br>RedHat Linux 6.2, 7.0 and 7.2 | Microsoft Win2k<br>Windows 98/ME<br>Windows NT 4.0 SP4, SP5 and SP6a<br>Sun Solaris SPARC |
| Disk Space | 40 MB | 40 MB |
| CPU | 300+ MHz | No minimum specified |
| Memory | 128 MB | 32 MB |
| Network Interfaces | ATM, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, Token Ring | Any supported by the operating system. |
| Media | CD-ROM | CD-ROM |

Below (TABLE 4), is the requirements by Windows platform for current Checkpoint products. From Windows Vista 32-bit to Windows 8, all products are supported except for SecureClient that supports only 32-bit platform for Windows 7.

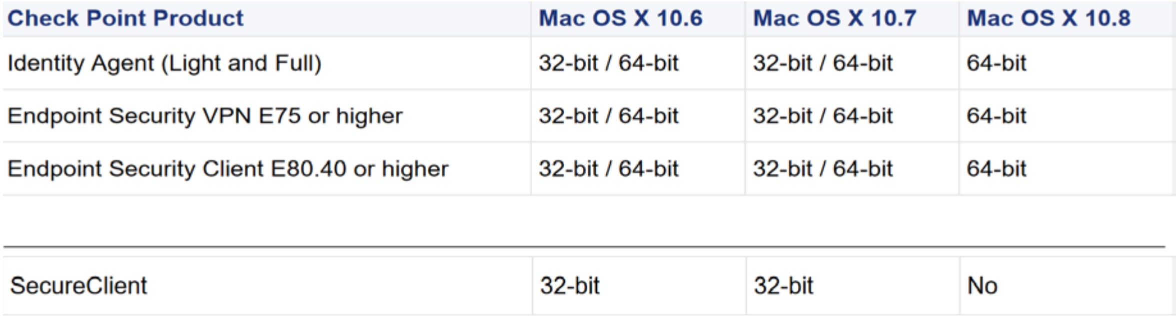
TABLE 4. Clients by windows platform (Checkpoint Software Technologies Ltd. 2016).



| Check Point Product | Vista (SP2)<br>32-bit | Vista (SP1)<br>64-bit | Windows 7 (+SP1) | Windows 8 |
|---|---|---|---|---|
| Endpoint Security Client | ✓ | ✓ | ✓ | ✓<br>E80.41 and higher |
| Remote Access Clients E75.x/E80.x | ✓ | ✓ | ✓ | ✓<br>E75.30 and higher |
| SSL Network Extender | ✓ | ✓ | ✓ | ✓<br>R75 and higher |
| UserCheck Client | ✓ |  | ✓ | ✓<br>R75.40 and higher |
| Identity Agent (Light and Full) | ✓ | ✓ | ✓ | ✓<br>R76 and higher |
| Identity Agent for Terminal Servers |  | ✓ | ✓ | ✓<br>R76 and higher |
| SecureClient | ✓ |  | ✓<br>(32-bit only) |  |

Table 5 below shows the current requirements by Mac platform. Products like Identity Agent, Endpoint Security VPN E75 and Endpoint Security client E80 retain similar configuration requirements for Mac OS. SecureClient requires 32-bit for both Mac OS X 10.6 and Mac OS X 10.7. It does not support Mac OS X 10.8.

TABLE 5. Clients by Mac Platform (Checkpoint Software Technologies Ltd. 2016).



| Check Point Product | Mac OS X 10.6 | Mac OS X 10.7 | Mac OS X 10.8 |
|---|---|---|---|
| Identity Agent (Light and Full) | 32-bit / 64-bit | 32-bit / 64-bit | 64-bit |
| Endpoint Security VPN E75 or higher | 32-bit / 64-bit | 32-bit / 64-bit | 64-bit |
| Endpoint Security Client E80.40 or higher | 32-bit / 64-bit | 32-bit / 64-bit | 64-bit |
| SecureClient | 32-bit | 32-bit | No |

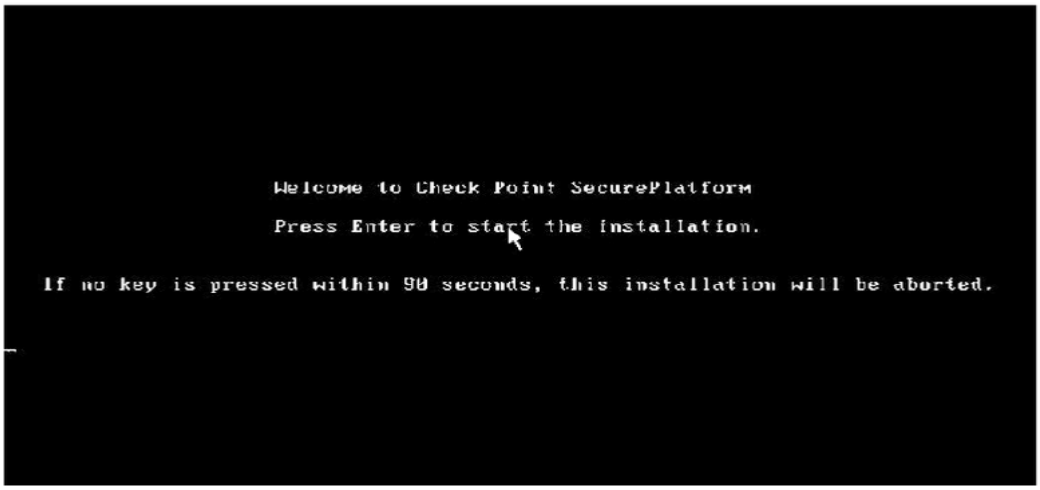
# 4 INSTALLING CHECKPOINT NGX

CheckPoint NGX can be installed in two ways namely, distributed installation, which requires the separation of the SmartCenter server (management server) from the Firewall-1/VPN-1 gateway. The other type of installation is the Stand Alone installation. Here, the security management server (SmartCenter) and the security gateway are installed on the same computer or appliance. For distributed deployment, the gateway allows or rejects traffic based on security policies, user databases, logs, objects and so on that it receives from the SmartCenter. (Shinder, Amon & Shimonski 2007, 2.)

Rather than go through with the installation of CheckPoint NGX in a distributed environment with its entire component products, emphasis will be placed more on installation and configuration procedures for VPN-1/Firewall-1 NG. Before installation, it is important to strengthen the current operating system. This is to ensure that the OS is not running unwanted services that could leave the gateway open to risk. Ping the remote devices from the OS that will host the CheckPoint installation to make sure packets are forwarded to the right destinations. (Stiefel et al. 2005, 47.)

## 4.1 SecurePlatform

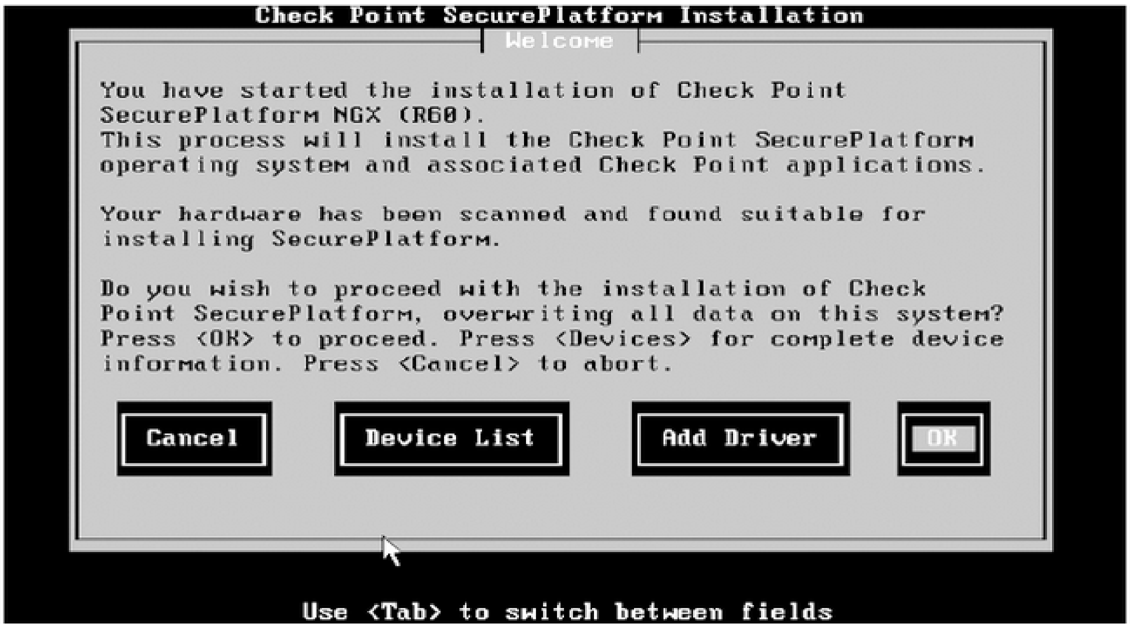
This is installed first from CheckPoint media kit. It requires Intel or AMD based systems with CD-ROM. First step involves inserting the NGX CD1 and rebooting the system. After reboot, a welcome screen appears, prompting the user to press enter to commence installation as shown in Graph 6 below.



```
Welcome to Check Point SecurePlatform

Press Enter to start the installation.

If no key is pressed within 90 seconds, this installation will be aborted.
```

GRAPH 6. SecurePlatform Welcome Screen (Stiefel et al. 2005, 47).

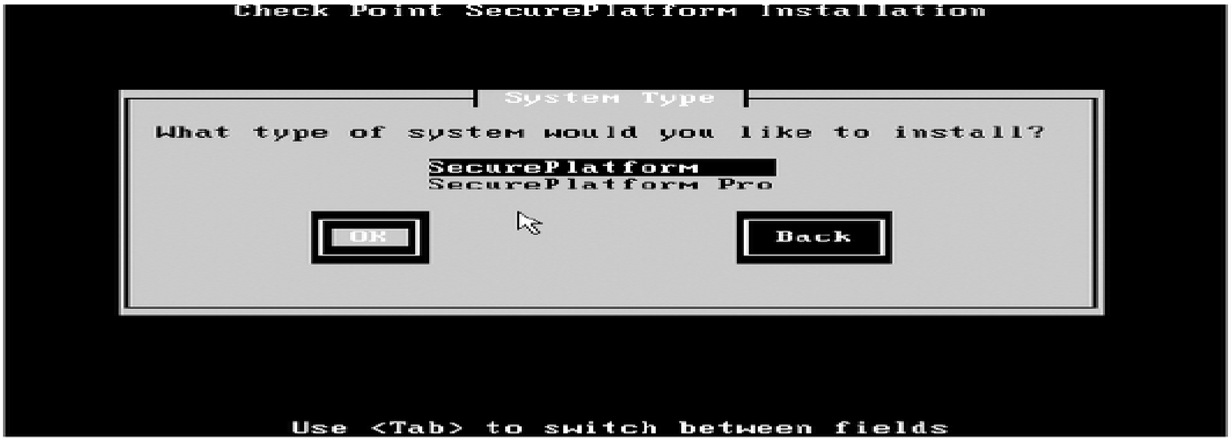
As indicated on the welcome screen, if no key pressed within ninety seconds, the installation aborts without affecting the system. This applies also when “cancel” is selected in the next screen. The device list shows hardware devices detected by SecurePlatform. Compatibility of connected hardware is important in order not to cause problems later. To add a hardware device, select Add Driver. This action prompts a selection for the path to the new driver. Select OK to continue the installation, as shown in Graph 7.



```
Check Point SecurePlatform Installation
Welcome

You have started the installation of Check Point
SecurePlatform NGX (R60).
This process will install the Check Point SecurePlatform
operating system and associated Check Point applications.

Your hardware has been scanned and found suitable for
installing SecurePlatform.

Do you wish to proceed with the installation of Check
Point SecurePlatform, overwriting all data on this system?
Press <OK> to proceed. Press <Devices> for complete device
information. Press <Cancel> to abort.

Use <Tab> to switch between fields
```

GRAPH 7. Options in welcome screen (Stiefel et al. 2005, 48).

Next, the “System Type” screen comes on (GRAPH 8). Simply select SecurePlatform and press OK. This pops a screen prompting selection of keyboard type, depending on the region of the gateway as shown below (GRAPH 9). Click OK to continue to language selection.



Check Point SecurePlatform Installation

System Type

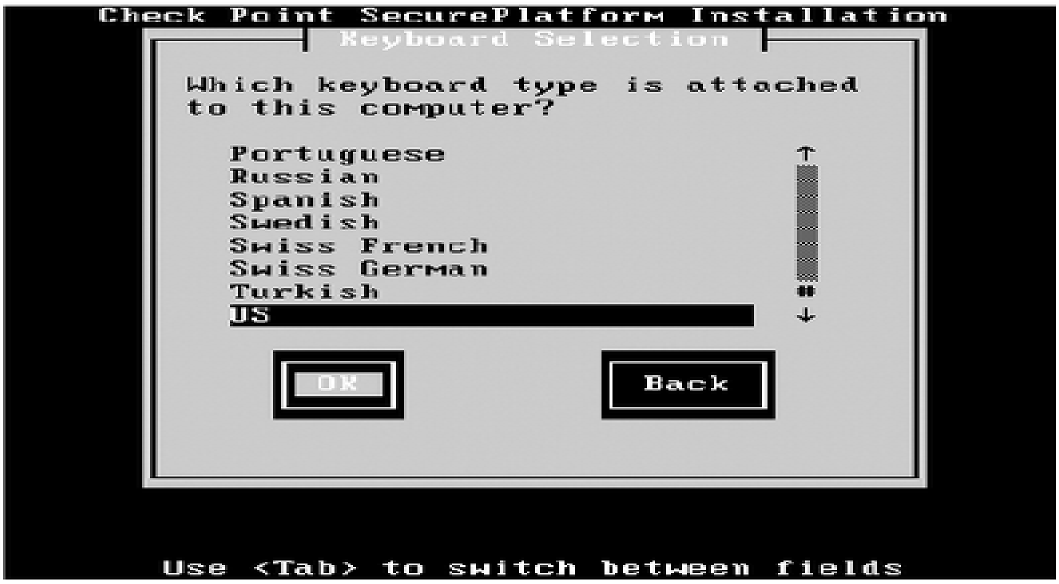
What type of system would you like to install?

SecurePlatform
SecurePlatform Pro

Use <Tab> to switch between fields

GRAPH 8. System Type (Stiefel et al. 2005, 49).

The keyboard type is not optional, meaning that selecting any type because it suits the user more, would cause an error eventually in the installation. It is mandatory to select the type of keyboard attached to the computer based on the region detected. Notwithstanding this, language selection is optional.



Check Point SecurePlatform Installation

Keyboard Selection

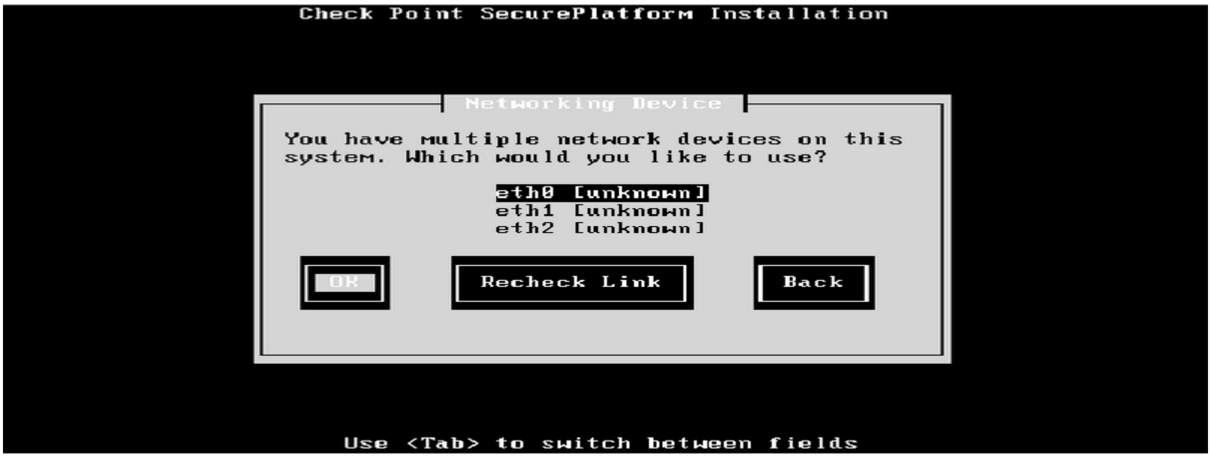
Which keyboard type is attached to this computer?

Portuguese
Russian
Spanish
Swedish
Swiss French
Swiss German
Turkish
US

Use <Tab> to switch between fields

GRAPH 9. Keyboard Selection (Stiefel et al. 2005, 50).

Graph 10, which comes next, displays the Network Interface Cards (NIC) attached to the system. The screen also indicates a Link, No Link, or Unknown, if the interface does not support Secure Platform’s link detection protocol. It is recommended for initial installation of FireWall-1/VPN-1, to be on the interface that is facing the Internet, as this will be automatically listed in the operating system host’s file. Select the external interface and then select OK to continue.



Check Point SecurePlatform Installation

Networking Device

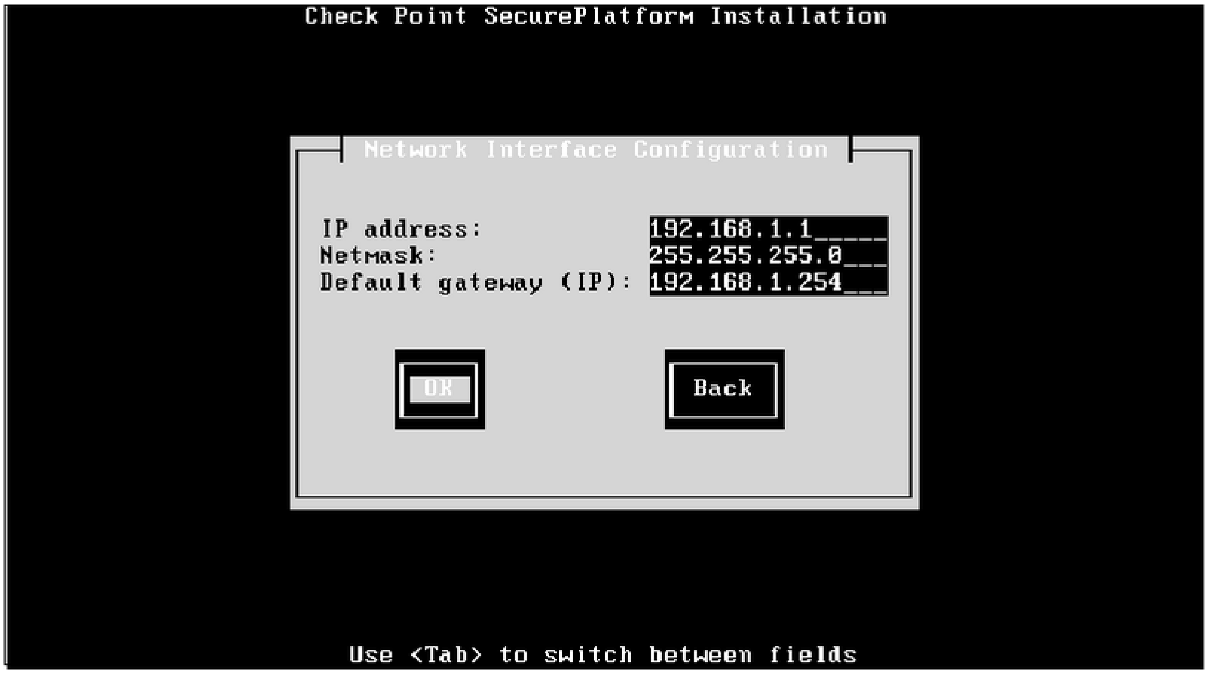
You have multiple network devices on this system. Which would you like to use?

```
eth0 [unknown]
eth1 [unknown]
eth2 [unknown]
```

Use <Tab> to switch between fields

GRAPH 10. Network Device (Stiefel et al. 2005, 50).

As shown in Graph 11, which comes next, it is required to use routable internet protocol addressing provided by the ISP in use, but for installation instruction purposes, private addressing is used. Note that the internet protocol addressing used here is a sample for installation instructions only. Select ok to continue after the configuration.



Check Point SecurePlatform Installation

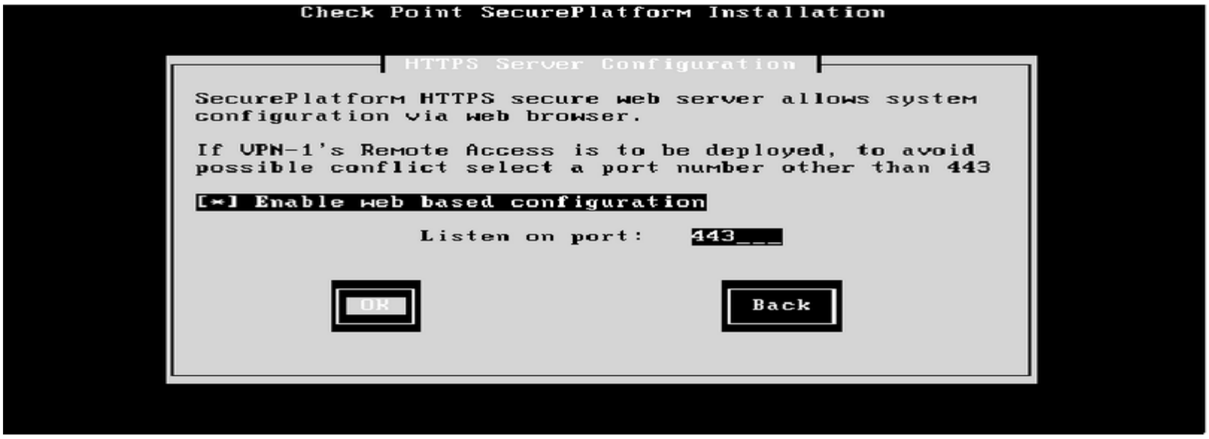
Network Interface Configuration

```
IP address:               192.168.1.1_____
Netmask:                  255.255.255.0___
Default gateway (IP):     192.168.1.254___
```

Use <Tab> to switch between fields

GRAPH 11. Network Interface Configuration (Stiefel et al. 2005, 51).

SecurePlatform has a distinct feature, which allows it to configure the OS directly from a web-based browser like Internet Explorer. Graph 12 displays the HTTPS server configuration screen prompting the user to enable web-based configuration or not and which port it should be listed on. By default, it is enabled but it may be better to change the default HTTPS sockets port 443 to another port. Click OK to continue after configuration.



Check Point SecurePlatform Installation

HTTPS Server Configuration

SecurePlatform HTTPS secure web server allows system configuration via web browser.

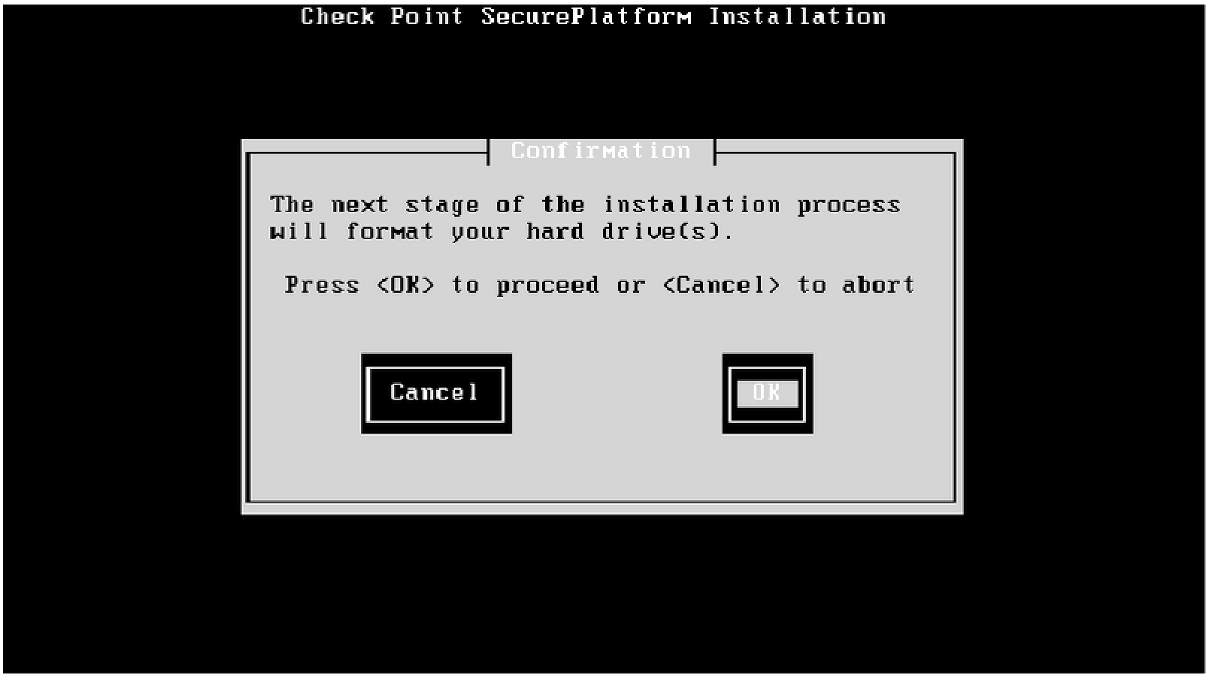
If VPN-1's Remote Access is to be deployed, to avoid possible conflict select a port number other than 443

[*] Enable web based configuration

Listen on port: 443___

GRAPH 12. HTTPS Server Configuration (Stiefel et al. 2005, 52).

Following this process is the confirmation screen (GRAPH 13). Selecting ok commences the disk format process, which allows CheckPoint SecurePlatform to install a pre-hardened OS in minutes. Stopping the formatting process is impossible unless the computer is switched off. This is not advisable since it may cause unwanted issues.



Check Point SecurePlatform Installation

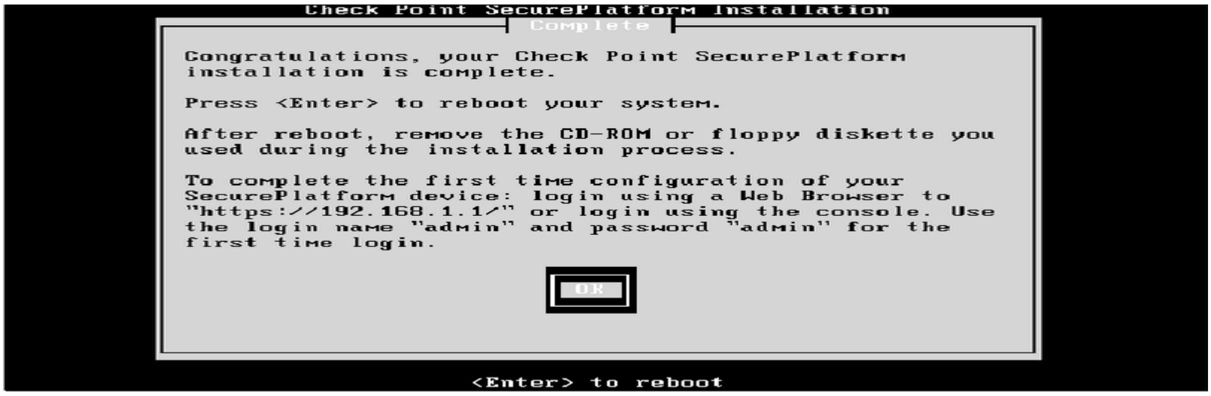
Confirmation

The next stage of the installation process
will format your hard drive(s).

Press <OK> to proceed or <Cancel> to abort

GRAPH 13. Confirmation (Stiefel et al. 2005, 52).

After completion, pressing OK ejects the CD and reboots the system. A login screen requesting username and password follows this. By default, the username and password are both admin.  (Stiefel et al. 2005, 53.)



Check Point SecurePlatform Installation

Complete

Congratulations, your Check Point SecurePlatform
installation is complete.

Press <Enter> to reboot your system.

After reboot, remove the CD-ROM or floppy diskette you
used during the installation process.

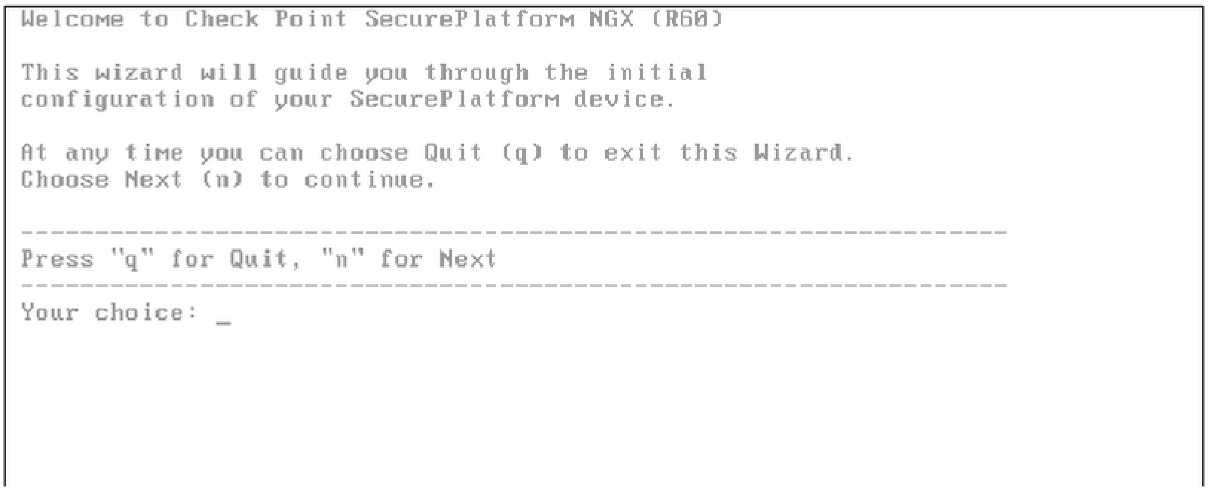
To complete the first time configuration of your
SecurePlatform device: login using a Web Browser to
"https://192.168.1.1/" or login using the console. Use
the login name "admin" and password "admin" for the
first time login.

<Enter> to reboot

GRAPH 14. Complete Check Point SecurePlatform Installation (Stiefel et al. 2005, 53).

The installation can be completed via the command line (using serial connections, ssh connection, or keyboard and monitor) or via a web browser. The simplest being via a Web User

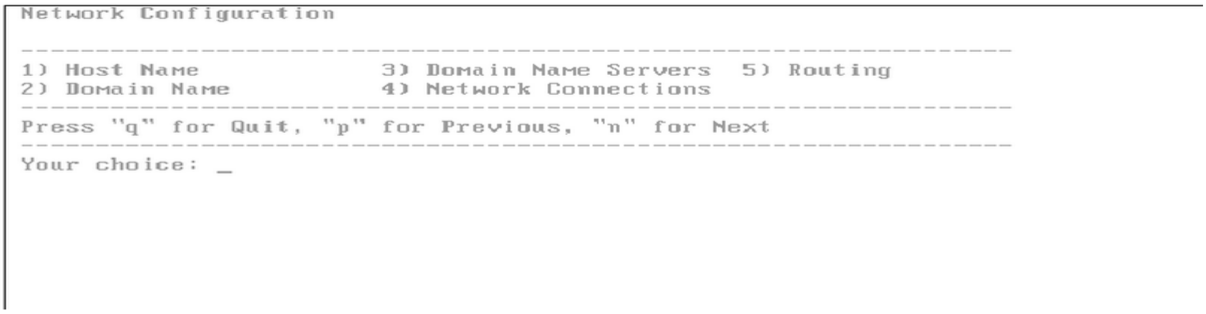
Interface (WebUI). Open the browser and connect to https://<IP address used during installation>. It opens up a license agreement prompting you to accept. After this comes the login screen where you use the default username and password. A new screen will appear requesting you change the password. (Stiefel et al. 2005, 55.) On completion of this, log into secure platform either by the website or by using the sysconfig utility provided as in the graph below.



```
Welcome to Check Point SecurePlatform NGX (R60)

This wizard will guide you through the initial
configuration of your SecurePlatform device.

At any time you can choose Quit (q) to exit this Wizard.
Choose Next (n) to continue.

-------------------------------------------------------------------
Press "q" for Quit, "n" for Next
-------------------------------------------------------------------
Your choice: _
```

GRAPH 15. Welcome wizard (Stiefel et al. 2005, 55).

Selecting the option for next produces a screen where all the components required for configuration is required for selection. Each option comes with its own configuration screens to enable the user properly configure the components. Be sure to select all the components by going through their configuration screens. This is shown in Graph 16.

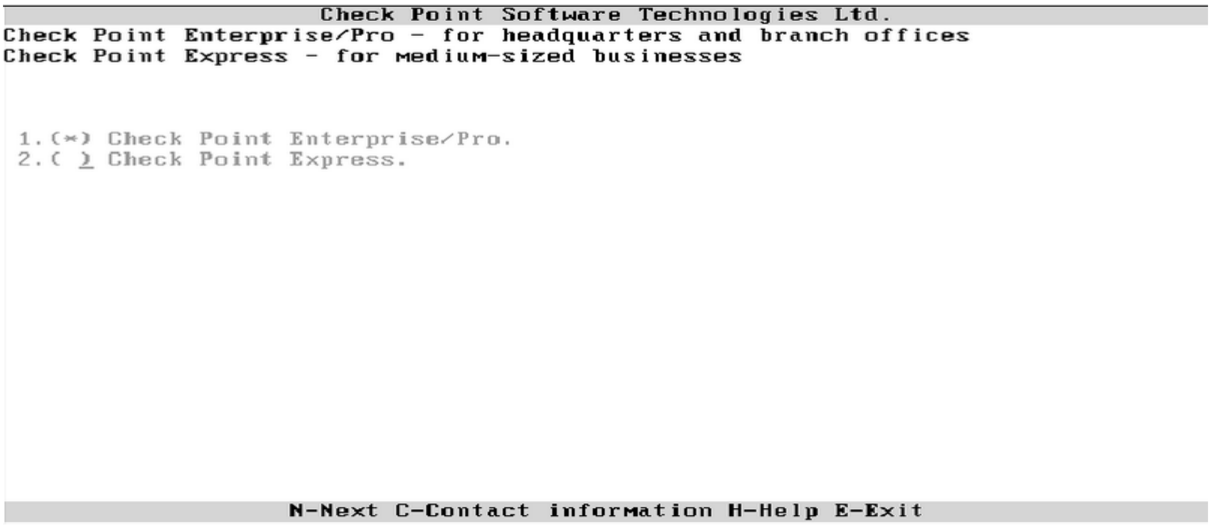


```
Network Configuration

-------------------------------------------------------------------
1) Host Name            3) Domain Name Servers   5) Routing
2) Domain Name          4) Network Connections
-------------------------------------------------------------------
Press "q" for Quit, "p" for Previous, "n" for Next
-------------------------------------------------------------------
Your choice: _
```

GRAPH 16. Initial Configuration screen (Stiefel et al 2005, 55).

### 4.2 FireWall-1/VPN-1 Installation

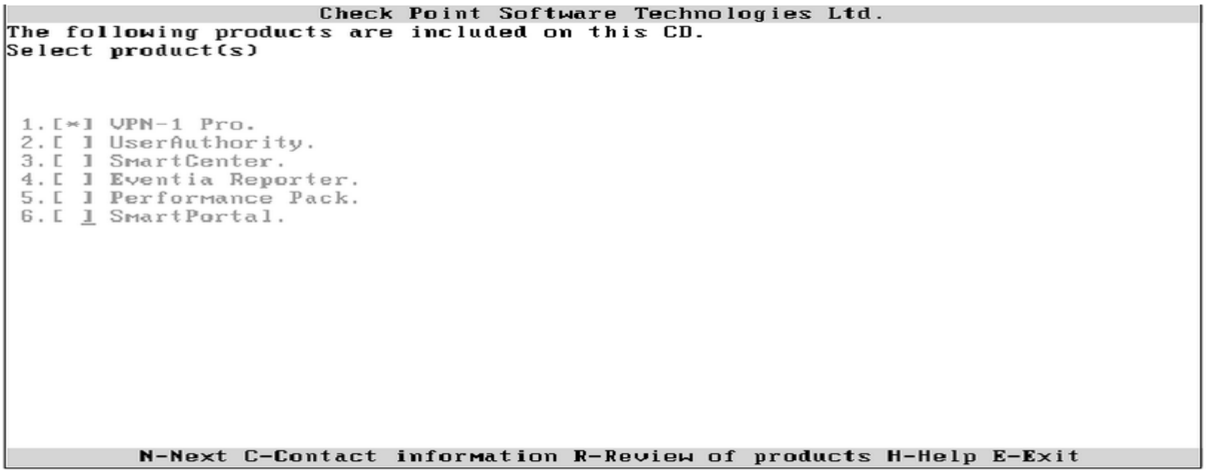
From the welcome screen, make sure the license agreement is read and accepted. This prompts the next screen, (GRAPH 17), where by a selection must be made between Enterprise and Express. The difference being the number of IPs that can be protected. Express is smaller with less than 500 IPs, which makes it more suitable for medium sized businesses. Select “1” and click on “next” to starts the installation of the Enterprise/Pro product. (Stiefel et al. 2005, 57.)



```
                     Check Point Software Technologies Ltd.
Check Point Enterprise/Pro - for headquarters and branch offices
Check Point Express - for medium-sized businesses


 1.(*) Check Point Enterprise/Pro.
 2.( ) Check Point Express.









                   N-Next C-Contact information H-Help E-Exit
```

GRAPH 17. Enterprise/Express Selection (Stiefel et al. 2005, 57).

Selecting Enterprise prompts a screen (GRAPH 18) that asks which products to install. Since a distributed architecture is needed, select VPN-1 Pro. This action also automatically installs FireWall-1 because both products are now merged.

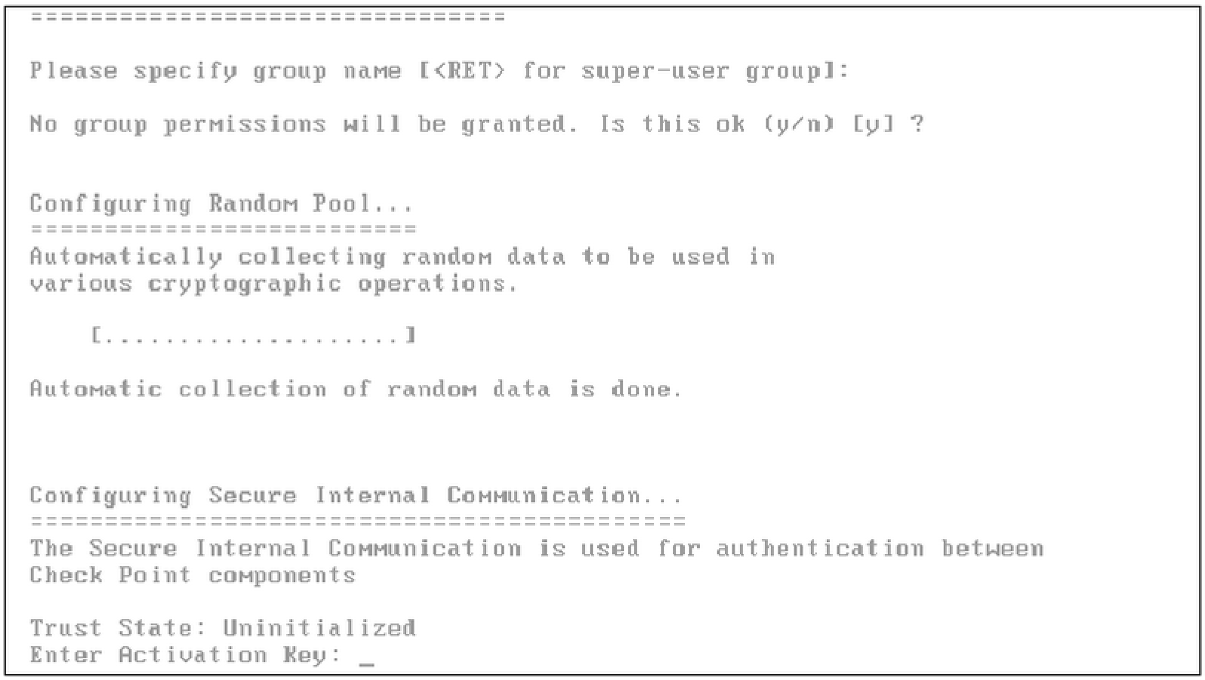


```
                    Check Point Software Technologies Ltd.
The following products are included on this CD.
Select product(s)


 1.[*] VPN-1 Pro.
 2.[ ] UserAuthority.
 3.[ ] SmartCenter.
 4.[ ] Eventia Reporter.
 5.[ ] Performance Pack.
 6.[ ] SmartPortal.

        N-Next C-Contact information R-Review of products H-Help E-Exit
```

GRAPH 18. Select Products (Stiefel et al. 2005, 57).

A validation screen pops up anytime a product is selected. In case of any errors, one can always go back to the selection screen. OS questions regarding whether or not the gateway has a Dynamically Assigned IP (DAIP) address and if there is a ready installed clustering product like ClusterXl, pop up on the next screen after confirmation. Select yes for both because Check Point supports DAIP in order to create a certificate to send to the SmartCenter Server for management, logging and VPN services. At the same time, it will disable IP forwarding, harden the OS security and generate the default filter for the gateway. The default filter being a “drop all” rule with the exception of some CheckPoint communication protocols. These are done after reboot. (Stiefel et al. 2005, 59.)

After completion of the installation, configure the product after the prompt. Installing a license could be done at the same time, though easier through SmartUpdate. Also important in the configuration of a distributed installation is the SIC, an activation key which is a one-time pass phrase that must be entered in any CheckPoint product installation. This is done by entering the pass phrase when prompted, install the policies and send. Once through, a prompt will suggest a reboot for server as illustrated in Graph 19 below.

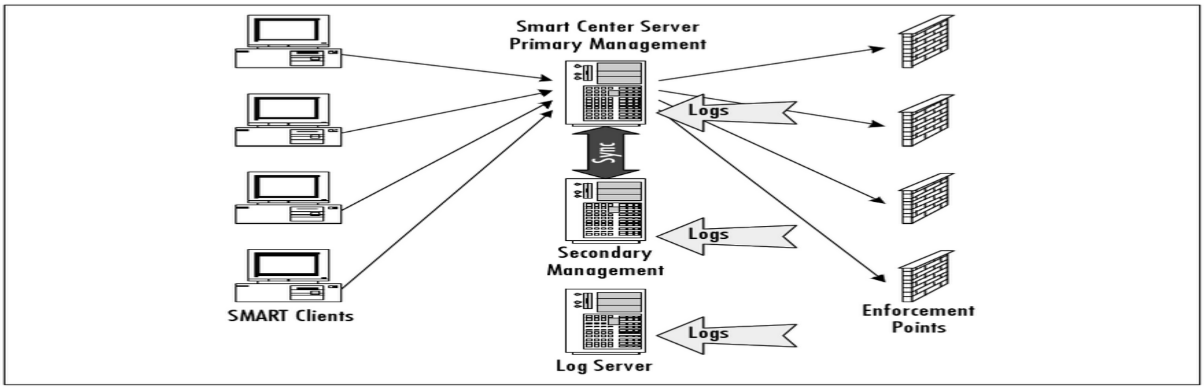


```
==================================
Please specify group name [<RET> for super-user group]:

No group permissions will be granted. Is this ok (y/n) [y] ?


Configuring Random Pool...
==========================
Automatically collecting random data to be used in
various cryptographic operations.

    [....................]

Automatic collection of random data is done.



Configuring Secure Internal Communication...
============================================
The Secure Internal Communication is used for authentication between
Check Point components

Trust State: Uninitialized
Enter Activation Key: _
```

GRAPH 19. Product Configuration (Stiefel et al. 2005, 60).

### 4.3 SmartCenter Server Installation

This is the most crucial system in all Check Point FireWall-1 configuration especially in a distributed environment. Notwithstanding the type of deployment, standalone or distributed, all FireWall-1 comes with a SmartCenter Server. The server handles important functions of the firewall requirement point and gives all availability to the SMART Clients. It also provides connectivity and data to all SMART Client connections whilst storing enforcement point logs, enforcement point configuration, and every single other part of the firewall building design. This is illustrated in Graph 20 below. (Noble et al. 2003, 350.)



GRAPH 20. Check Point Architecture (Noble et al. 2003, 350).

# 5 CONCLUSION AND RECOMMENDATIONS

As technological innovations change for the better, its overall effect changes the way people work, live, play and even share information. Network firewalls are designed to protect a trusted network from an untrusted one. This is achieved through packet filtering with regard to special security policies. ACLs as a form of firewall contains sets of rules that are multi-dimensional, that is, containing source addresses, destination addresses and ports. The more complex the rule sets are, the less effective they become concerning large organizations. Although different firewalls are deployed in various markets, there is still no standard evaluation process for comparison, which is due largely to different implementation methods per organization.

The cur loader test as discussed in Chapter three, replicated behavior of http/https clients using their unique IP addresses. The results from the test are indicative of the fact that Cisco ASA gives better performance while Checkpoint SPLAT’s functionality is unparalleled. It provides better firewall and centralized policy management an alongside a great user interface than the rest. This uniquely makes it stand out and definitely more suitable for complex networks.

As a firewall, Checkpoint is important because Stateful inspection allows for a deeper scrutiny or filtering unlike in ACLs. This mostly because ACLs found on routers, filter packets based on information given in the command. Moreover, Checkpoint firewalls, which perform Stateful inspection, also scrutinize the packets payload alongside the application protocol.

Every three to four years CheckPoint upgrades its products to suit the rising needs of the dynamic network industry. Some of its latest products and the year of release include the CheckPoint NGX R65 (2007-2009), R70 (2009-2011), R75 (2011-2013). Most of the current versions come with new features such as SmartDefense (IPS), Quality of Service (Floodgate-1) and Content Inspection.

## REFERENCES

Amon, C, Kligerman, D, Simonis, D. 2002. Check Point Next Generation Security Administration. Rocland, MA, USA: Syngress Publishing.

Bonnell, R & Desmeules, S. 2008. CheckPoint NGX R65 Security Administration. Burlington, MA, USA: Syngress Publishing Inc.

Checkpoint. 2009. Data Center & Enterprise Security Platforms. Available: https://www.checkpoint.com/products-solutions/next-generation-firewalls/enterprise-firewall/index.html. Accessed: 10th October, 2015.

CHECK POINT SOFTWARE TECHNOLOGIES LTD. 2016. Next Generation Threat Prevention. Available: http://dl3.checpoint.com/paid/d2/d21e464b03722d07253c57cf6de3a1ea/CP_R77_Release-Notes.pdf?HashKey=1460464946_0e8e789fca3f9013b342366ef197a1d2&xtn=.pdf Accessed: 12th April, 2016.

CHECK POINT: Check point VPN-1 edge NGX extends security protection with advanced intrusion prevention and anti-virus. (2006, Jan 19). M2 Presswire. Available: http://search.proquest.com/docview/443620664?accountid=10007
Accessed: 15th October, 2015.

CHECK POINT SOFTWARE TECHNOLOGIES LTD. 2016. Hoover's Company Records. Austin: Dun and Bradstreet, Inc. Available: http://search.proquest.com/docview/230586356?accountid=10007.
Accessed: 15th October, 2015.

Chirag, S & Thakker, R. 2011. "Performance Evaluation and Comparative Analysis of Network Firewalls." International Conference on Devices and Communications (ICDeCom). Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5738566&tag=1. Accessed: 8th January, 2016.

Colton, A. 2003 Cisco IOS for IP Routing. London: Rocket Science.

Cisco Systems, Inc. 2007. Configuring IP Access Lists. Available: http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccess-lists.html. Accessed: 14th March, 2016.

Danielyan, E & Knipp, E. 2002. Managing Cisco Network Security. Rockland, Mass: Syngress Media.

Deepak, S & Prasad K. 2015. Enhancing the Performance and Security of Network. International Journal of Science, Engineering and Technology, Volume 3 Issue 6. Accessed: 15th March 2016.

Emmet D. 2011. CompTIA Security+ Deluxe Study Guide Recommended Courseware: Exam SY0-301, Wiley Publishing Inc.

Flynn, H. 2006. Designing and Building Enterprise DMZs. Rockland, MA, USA: Syngress Publishing.

Ghorbani, A, Wei L, & Tavallaee, M. 2010. Network Intrusion Detection and Prevention: Concepts and Techniques. New York: Springer.

Grout, V, Mcginn, J, & Davies, J. 2007. "Real-time Optimisation of Access Control Lists for Efficient Internet Packet Filtering." Journal of Heuristics J Heuristics. Available: http://dx.doi.org/10.1007/s10732-007-9019-1. Accessed: 25th August 2015.

Lammle, T. 2014. Todd Lammle's CCNA/CCENT IOS Commands Survival Guide: Exams 100-101, 200-101, and 200-120 (2nd Edition). Somerset, NJ, USA: John Wiley & Sons, Incorporated.

Morrissey, P. 1998. Demystifying cisco access control lists. Network Computing, 9(7), 116. Available: http://search.proquest.com/docview/215429009?accountid=10007. Accessed 29th August, 2015.

Noble, J, Maxwell, D, Hourihan, K, Stephens, R, Stiefel, B, Amon, C & Tobkin, C. 2003. Check Point NG VPN-1/FireWall-1 Advanced Configuration and Troubleshooting. United States: Syngress Publishing, Inc.

Shinder, T, Amon, C, & Shimonski, R. 2007.  Best Damn Firewall Book Period. Rockland, MA, USA: Syngress Publishing.

Simonis, D. 2002. Check Point NG: Next Generation Security Administration. Rockland, MA: Syngress Media.

Stephens, R, Stiefel, B & Watkins, S. 2005. Configuring Check Point NGX VPN-1/Firewall-1. Rockland, MA: Syngress.

Sumit G & Elliot T. 2010. Cybercrimes: A Multidisciplinary Analysis. Springer Science & Business Media.

Vitaly, O. 2002. Cisco Security Specialist's Guide to PIX Firewall. Rockland, MA: Syngress.