INSTALLAZIONE CHECKPOINT SECUREPLATFORM NG FIREWALL R55 HFA 15

Inserire il CD-ROM di Checkpoint all'interno del Server.
Avviare la macchina, ci apparirà la seguente schermata
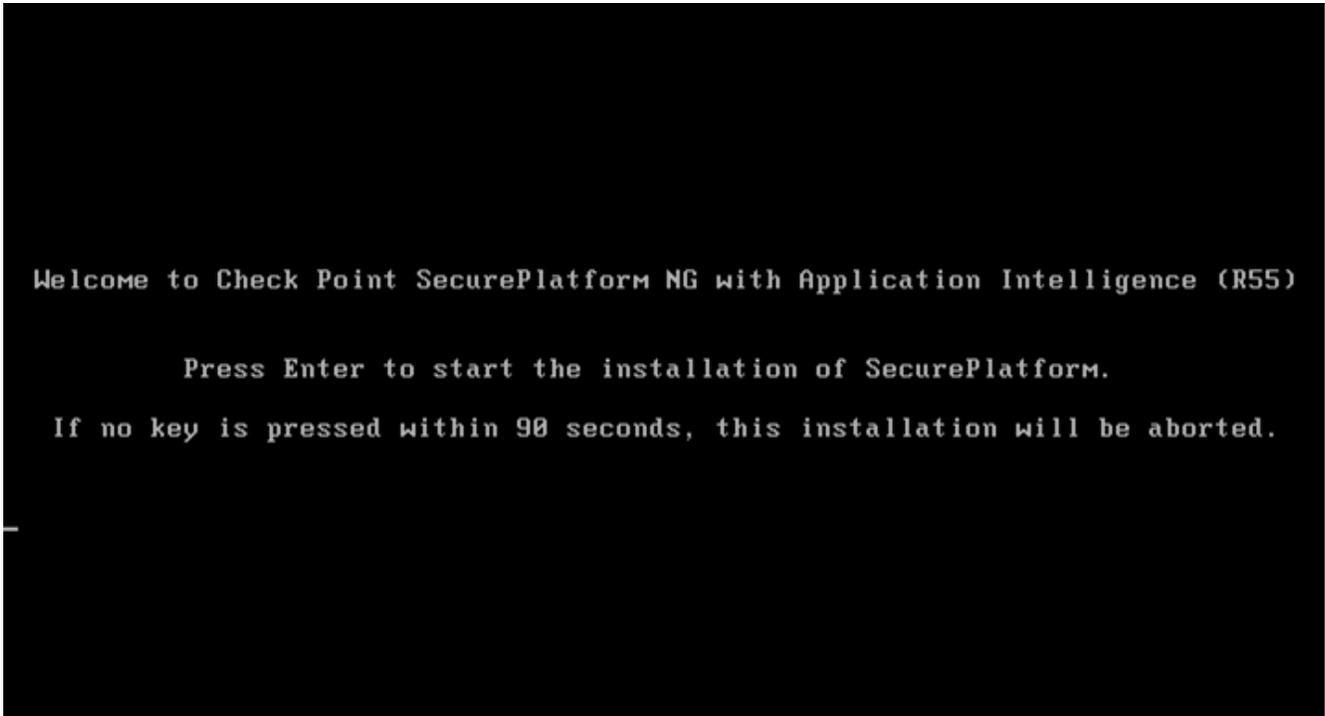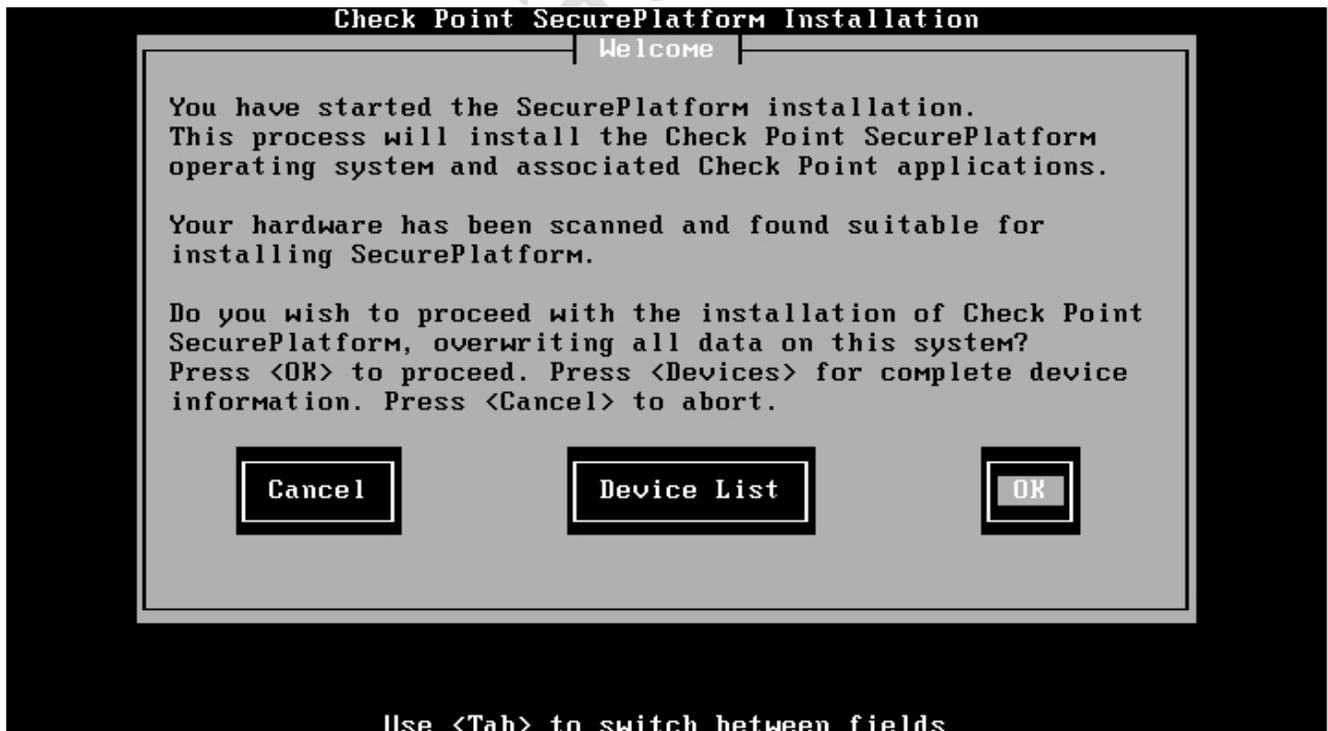

Fig.1

Premere **INVIO**.

Fig.2

Selezionare **OK** e premere **INVIO**

Fig.3

Selezionare **Italian** e premere **INVIO**

Fig.4

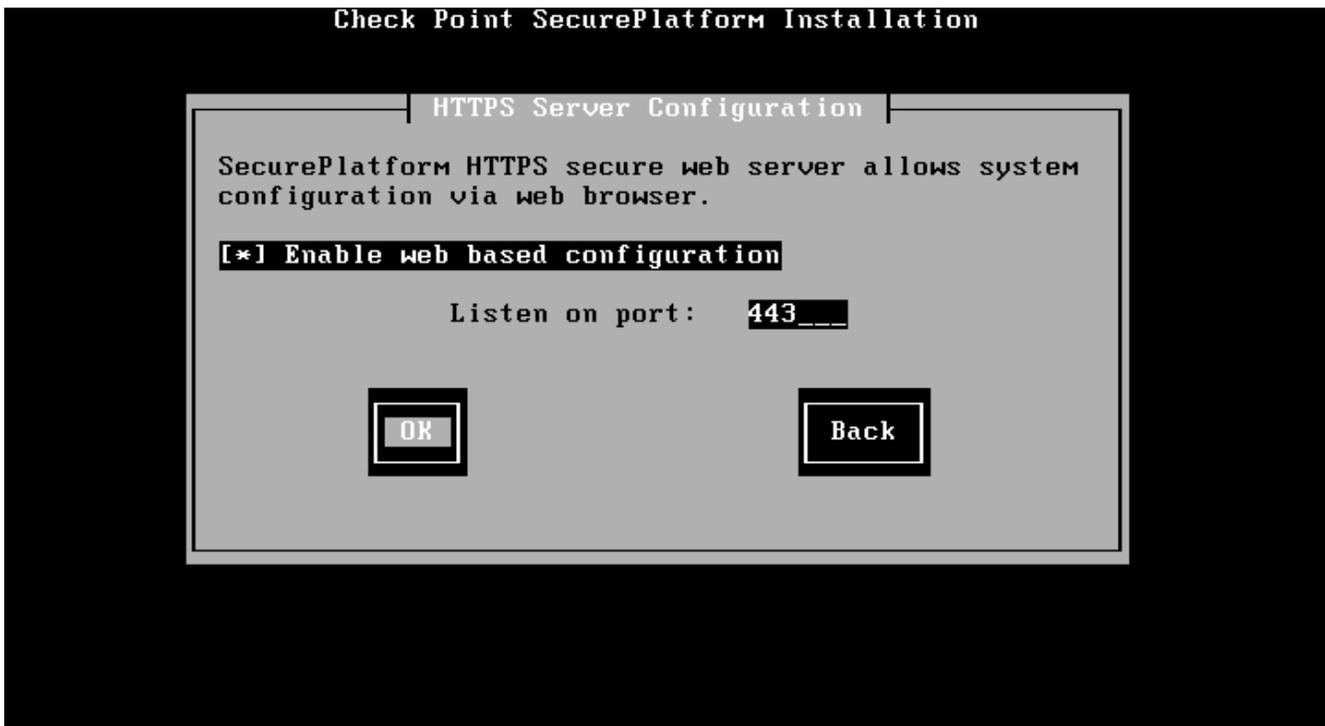Assegnare l'indirizzo IP, la Subnet Mask e il Default Gateway quindi premere **INVIO**

Fig.5

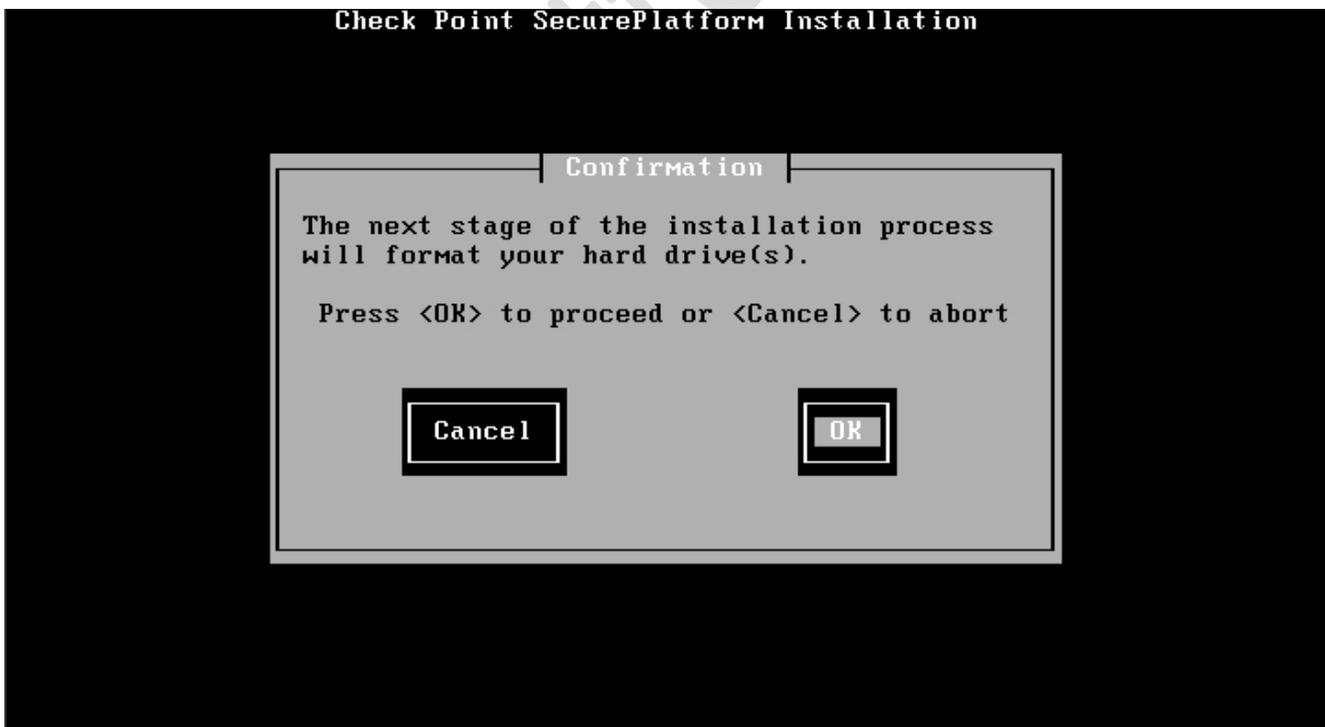Lasciare tutto invariato e premere **INVIO**
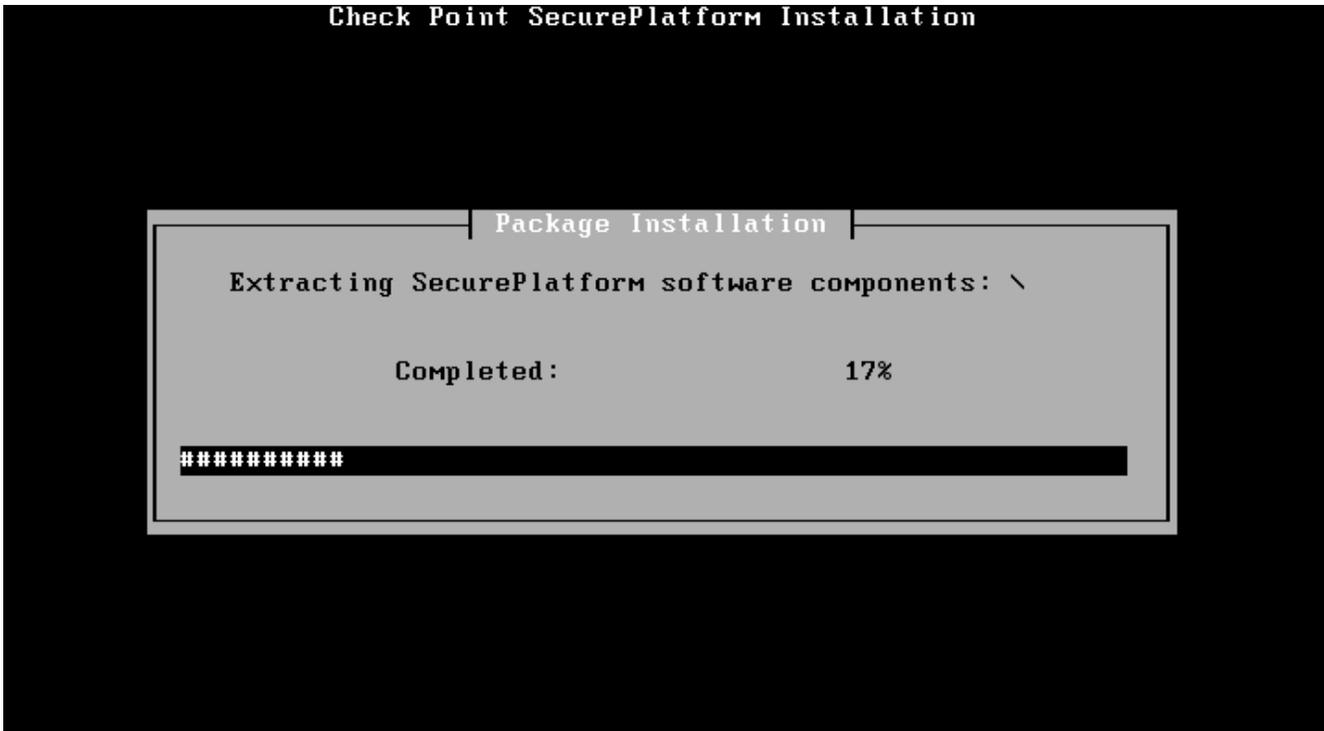

Fig.6

Selezionare **OK** e premere **INVIO**

Check Point SecurePlatform Installation

Package Installation

Extracting SecurePlatform software components: \

Completed: 17%

##########

Fig.7

Attendere l'installazione del prodotto

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.

OK

<Enter> to reboot

Fig.8

Selezionare **OK** e premere **INVIO**
Adesso verrà espulso il CD ROM e verrà riavviato il sistema.

```
Check Point SecurePlatform NG with Application Intelligence (R55)
For Web User Interface access connect to https://192.168.1.1

login: admin
Password: _
```

Fig.9

Inseriamo le seguenti credenziali :

User: admin
Password: admin

```
Check Point SecurePlatform NG with Application Intelligence (R55)
For Web User Interface access connect to https://192.168.1.1

login: admin
Password:

You must change the default password.

Enter new password: _
```

Fig.10

Adesso ci verrà richiesto di cambiare la password,inseriamo la nuova password e premiamo **INVIO**.

!!!ATTENZIONE!!! Bisogna inserire una password che abbia almeno un carattere maiuscolo, di almeno 8 caratteri alfanumerici e un carattere speciale.

```
Check Point SecurePlatform NG with Application Intelligence (R55)
For Web User Interface access connect to https://192.168.1.1

login: admin
Password:

You must change the default password.

Enter new password:
Enter new password (again):
Passwords do not match, try again.
Enter new password:
Enter new password (again):

You may choose a different user name.

Enter new user name: _
```

Fig.11

Premere **INVIO**

```
Check Point SecurePlatform NG with Application Intelligence (R55)
For Web User Interface access connect to https://192.168.1.1

login: admin
Password:

You must change the default password.

Enter new password:
Enter new password (again):
Passwords do not match, try again.
Enter new password:
Enter new password (again):

You may choose a different user name.

Enter new user name:
User name was not changed.

? for list of commands
sysconfig for system and products configuration

[cpmodule]# _
```

Fig.12

Scrivere expert e premere **INVIO**


```
Check Point SecurePlatform NG with Application Intelligence (R55)
For Web User Interface access connect to https://192.168.1.1

login: admin
Password:

You must change the default password.

Enter new password:
Enter new password (again):
Passwords do not match, try again.
Enter new password:
Enter new password (again):

You may choose a different user name.

Enter new user name:
User name was not changed.

? for list of commands
sysconfig for system and products configuration

[cpmodule]# expert
Enter current password:
```

Fig.13

Adesso bisogna inserire la password per la **modalità expert** (si consiglia di inserire sempre la medesima password per evitare confusioni).


```
Enter new password (again):
Passwords do not match, try again.
Enter new password:
Enter new password (again):

You may choose a different user name.

Enter new user name:
User name was not changed.

? for list of commands
sysconfig for system and products configuration

[cpmodule]# expert
Enter current password:

This is the first time you enter the expert mode.
Expert password must be changed.

Enter new expert password:
Enter new expert password (again):

You are in expert mode now.

[Expert@cpmodule]# _
```

Fig.14

Dalla figura sovrastante possiamo vedere che siamo in modalità expert.

7

Adesso bisogna configurare i settaggi minimi del firewall.
Entrare con modalità expert e digitare il comando **sysconfig** e premere **INVIO**.

```
Welcome to Check Point
SecurePlatform NG with Application Intelligence

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: _
```

Fig.15

Premere "**n**" per andare avanti nella configurazione, quindi **INVIO**

```
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: _
```

Fig.16

Come prima operazione settiamo l'host name.
Premiamo "**1**" quindi **INVIO**. Ripremiamo **1** per settare l'Host Name

```
Choose an action ('e' to exit):
---------------------------------------------------------------
1) Set host name
2) Show host name
---------------------------------------------------------------
Your choice: 1
Enter host name: _
```

Fig.17

Inseriamo il nome da assegnare al firewall e premiamo **INVIO**


```
Choose an action ('e' to exit):
---------------------------------------------------------------
1) Set host name
2) Show host name
---------------------------------------------------------------
Your choice: 1
Enter host name: prova_firewall
Enter IP of the interface to be associated with
this host name (leave empty for automatic assignment): _
```

Fig.18

Premiamo **INVIO**

```
Choose an action ('e' to exit):
---------------------------------------------------------------
1) Set host name
2) Show host name
---------------------------------------------------------------
Your choice: 1
Enter host name: prova_firewall
Enter IP of the interface to be associated with
this host name (leave empty for automatic assignment):

The host name is set.

Press Enter to continue..._
```

Fig.19

Premere **INVIO** per continuare

Quindi premere "**e**" e poi **INVIO** per tornare al menù principale.

Adesso dal menù principale selezioniamo l'opzione 2) Domain Name

```
Choose an action ('e' to exit):
---------------------------------------------------------------
1) Set domain name
2) Show domain name
---------------------------------------------------------------
Your choice: _
```

Fig.20

Inseriamo il nome del DNS.

```
Choose an action ('e' to exit):
----------------------------------------------------------------
1) Set domain name
2) Show domain name
----------------------------------------------------------------
Your choice: 1
Enter domain name: lab1.prv_
```

Fig.21

Quindi ritorniamo al menù principale.

Adesso selezioniamo l'opzione 3) Domain Name Server e inseriamo l'indirizzo IP del DNS.

Ritornando al menù principale selezioniamo l'opzione 4) Network Connections e procediamo alla configurazione delle interfacce di rete.

Sempre nel menù principale selezioniamo l'opzione 5) Routing per settare le rotte statiche.

Adesso in corrispondenza del menù principale premere "n" per passare al menù successivo.

```
Choose a time and date configuration item:
----------------------------------------------------------
1) Set time zone                    3) Set local time
2) Set date                         4) Show date and time settings
----------------------------------------------------------
Press "q" for Quit, "p" for Previous, "n" for Next
----------------------------------------------------------
Your choice: _
```

Fig.22

Premere "**1**" per settare il Time Zone (Scelgiere quello Europeo)

Premere "**2**" e quindi **INVIO**

```
Choose a time and date configuration item:
----------------------------------------------------------
1) Set time zone                    3) Set local time
2) Set date                         4) Show date and time settings
----------------------------------------------------------
Press "q" for Quit, "p" for Previous, "n" for Next
----------------------------------------------------------
Your choice: 2
Enter date in format MM-DD-YYYY: _
```

Fig.23

Inserire la data corrente e premere **INVIO** per confermare le modifiche

12

Quindi una volta ritornati al menù principale premere "**3**" per settare l'ora corrente.

```
Tue May 24 10:17:22 UTC 2005

Choose a time and date configuration item:
----------------------------------------------------------------
1) Set time zone              3) Set local time
2) Set date                   4) Show date and time settings
----------------------------------------------------------------
Press "q" for Quit, "p" for Previous, "n" for Next
----------------------------------------------------------------
Your choice: 3
Enter time in format HH:MM: _
```

Fig.24

Inserire l'ora e premere **INVIO** per confermare.

Adesso per confermare che i settaggi fatti siano stati salvati, dal menù principale premere "**4**" ci apparirà la seguente schermata

```
Tue May 24 10:19:05 UTC 2005

Choose a time and date configuration item:
----------------------------------------------------------------
1) Set time zone              3) Set local time
2) Set date                   4) Show date and time settings
----------------------------------------------------------------
Press "q" for Quit, "p" for Previous, "n" for Next
----------------------------------------------------------------
Your choice: _
```

Fig.25

13

Completati i settaggi di configurazione di date e ora ritorniamo al menù principale e clicchiamo "**n**" quindi **INVIO**.

Fig.26

Clicchiamo ulteriormente "**n**" fino ad arrivare alla schermata seguente

Fig.27

Clicchiamo "**n**" per proseguire senza l'inserimento della licenza

```
Check Point Software Technologies Ltd.
License Agreement V.NG.2

This End-user License Agreement (the "Agreement") is an agreement between you (b
oth the individual installing the Product and any legal entity on whose behalf s
uch individual is acting) (hereinafter "You" or "Your") and Check Point Software
 Technologies Ltd. (hereinafter "Check Point").
TAKING ANY STEP TO SET-UP, USE OR INSTALL THE PRODUCT CONSTITUTES YOUR ASSENT TO
 AND ACCEPTANCE OF THIS END USER LICENSE AGREEMENT. WRITTEN APPROVAL IS NOT A PR
EREQUISITE TO THE VALIDITY OR ENFORCEABILITY OF THIS AGREEMENT AND NO SOLICITATI
ON OF ANY SUCH WRITTEN APPROVAL BY OR ON BEHALF OF YOU SHALL BE CONSTRUED AS AN
INFERENCE TO THE CONTRARY. IF YOU HAVE ORDERED THIS PRODUCT SUCH ORDER IS CONSID
ERED AN OFFER BY YOU, CHECK POINT'S ACCEPTANCE OF YOUR OFFER IS EXPRESSLY CONDIT
IONAL ON YOUR ASSENT TO THE TERMS OF THIS AGREEMENT, TO THE EXCLUSION OF ALL OTH
ER TERMS. IF THESE TERMS ARE CONSIDERED AN OFFER BY CHECK POINT, YOUR ACCEPTANCE
 IS EXPRESSLY LIMITED TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH A
LL THE TERMS OF THIS AGREEMENT, YOU MUST RETURN THIS PRODUCT WITH THE ORIGINAL P
ACKAGE AND THE PROOF OF PAYMENT TO THE PLACE YOU OBTAINED IT FOR A FULL REFUND.
1.      DEFINITIONS:
1.1     "Product" means the object code copy of the software program provided to
 You in association with this Agreement, together with the associated original e
lectronic media and all accompanying manuals and other documentation, and togeth
er with all enhancements, upgrades, and extensions thereto that may be provided
--More--(9%)
```

Fig.28

Teniamo premuta la barra spaziatrice fino all'arrivo della seguente schermata

```
s of the State of Israel shall govern all issues arising under or relating to th
is Agreement, without giving effect to the conflict of laws principles thereof.
All disputes arising under or relating to this Agreement shall be resolved exclu
sively in the appropriate Israeli court sitting in Tel Aviv, Israel. This Agreem
ent will not be governed by the United Nations Convention on Contracts for the I
nternational Sales of Goods, the application of which is expressly excluded. Thi
s Agreement sets forth the entire understanding and agreement between You and Ch
eck Point and may be amended only in writing signed by both parties.
9.2     Third Party Software. The provisions of this Agreement shall apply to al
l Third Party Software Providers and to Third Party Software as if they were the
 Product and Check Point, respectively.
9.3     Government Restricted Rights. This provision applies to Product acquired
 directly or indirectly by or on behalf of any Government. The Product is a comm
ercial product, licensed on the open market at market prices, and was developed
entirely at private expense and without the use of any Government funds. Any use
 modification, reproduction, release, performance, display, or disclosure of the
 Product by any Government shall be governed solely by the terms of this Agreeme
nt and shall be prohibited except to the extent expressly permitted by the terms
 of this Agreement, and no license to the Product is granted to any government r
equiring different terms.
9.4      Questions? Should You have any questions concerning this Agreement conta
ct the manufacturer at Check Point Software Technologies Ltd., 3a Jabotinsky St.
, Ramat-Gan, Israel 52520.

Do you accept all the terms of this license agreement (y/n) ?  y_
```

Fig.29

Accettiamo la licenza e premiamo **INVIO**

```
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
```

Fig.30

Selezioniamo la prima opzione e clicchiamo "**n**" per andare avanti

```
Installation Options.
Please select one of the following options:


 1.(*) New Installation.
 2.( ) Advanced Upgrade.



















                    N-next E-exit H-help
```

Fig.31

Selezionare l'opzione **1 (New Installation)** e clicchiamo "**n**" per andare avanti

```
The following products are included on this CD.
Select product(s)


  1.[*] VPN-1 Pro.
  2.[ ] SmartCenter.
  3.[ ] FloodGate-1.
  4.[ ] VPN-1 SecureClient Policy Server.
  5.[ ] UserAuthority.
  6.[ ] SmartView Monitor.
  7.[x] SmartView Reporter.
  8.[ ] Performance Pack.

    _




       N-Next C-Contact information R-Review of products H-Help E-Exit
```
Fig.32

Selezionare l'opzione **1 (VPN-1 Pro)** e in automatico verrà selezionata l'opzione **7 (SmartView Reporter)**

```
Validation



  You have selected the following products for installation:
  * VPN-1 Pro_













       N-next B-go Back H-help E-exit
```
Fig.33

Clicchiamo su "**n**" per andare alla schermata successiva

Clicchiamo su "**n**" per andare avanti.
Attendiamo qualche minuto fino alla fine dell'installazione dei pacchetti selezionati.

Premiamo **INVIO** per non accettare la prima opzione, quindi **INVIO** per non accettare la seconda opzione.

17

Adesso ci verrà richiesta di nuovo di aggiungere la licenza clicchiamo "**n**" quindi **INVIO** per andare avanti.

```
Configuring Licenses...
========================
Host              Expiration  Signature                    Features


Note: The recommended way of managing licenses is using SmartUpdate.
cpconfig can be used to manage local licenses only on this machine.

Do you want to add licenses (y/n) [y] ? n


Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used in
various cryptographic operations.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

    [.....              ] *
```
Fig.34

Adesso clicchiamo lettere a caso fino al completamento dell'inserimento del Random Pool

```
Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used in
various cryptographic operations.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

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

Thank you.


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

Trust State: Uninitialized
Enter Activation Key: _
```
Fig.35

Inseriamo **l'Activation Key** (ci verrà richiesta due volte)

18

```
IMPORTANT: Don't forget to reboot in order to complete the installation.

Press Enter to continue..._
```

Fig.36

Premiamo **INVIO**
Adesso facciamo un bel riavvio della macchina.

Adesso doppiamo applicare la PATCH R55-HFA-15.
Inseriamo il CD ROM contenente la Patch e copiamo la cartella contenente la fix all'interno della cartella var/patch.
Una volta inserito il CD editare il seguente comando

mount /dev/cdrom /mnt/cdrom

Adesso andiamo all'interno della cartella /mnt/cdrom e copiamo il file SHF_HFA_R55_15.linux.22 della cartella /var/patch.

Quindi scomapattiamo il file SHF_HFA_R55_15.linux.22.tgz con il seguente comando
tar xvzf SHF_HFA_R55_15.linux.22.tgz

Ed infine lo lanciamo con il comando ./install.

Alla fine dell'installazione riavviamo il sistema.

ALTRE OPERAZIONI DA EFFETTUARE

- Per aggiungere le licenze definitive dalla modalità expert lanciare il comando cpconfig e selezionare 1 quindi procedere seguendo le istruzioni. Per caricare il file bisogna installare un server TFTP sulla macchina sorgente
- Se abbiamo dimenticato l'Activation Key sempre all'interno del menù di cpconfig selezioniamo 5 e reinseriamo la chiave
- Abilitare il cluster selezionando l'opzione 6 seguire le istruzioni e riavviare il checkpoint
- Settare l'NTP con il seguente comando
  - ntp –n 300 time1.augustanet.prv time2.augustanet.prv (CONVIENE METTERE AL POSTO DEL NOME DNS DEL SERVER IL SUO INDIRIZZO IP NEL CASO NON VIENE LOGGATO IL TRAFFICO NTP-UDP SUL FIREWALL)

19

COMANDI UTILI

1. Per restartare il web server andare in /etc/init.d/cpwm.d e aggiungere l'opzione start,stop o restart
2. Per verificare quale macchina è il master del cluster utilizzare il seguente comando dalla modalità expert cphaprob stat
3. Per settare le velocità delle schede di rete della macchine andare lanciare il comando ethtool

UTILITY DA CONFIGURARE

Per testare il FAILOVER creiamo due script.
Ad esempio all'interno della cartella /usr/sbin

I due script sono :

fw_offline.sh

```
#!/bin/sh
/opt/CPfw1-R55/bin/cphaprob -d faildevice -s ok -t 0 register
/opt/CPfw1-R55/bin/cphaprob -d faildevice -s problem report
```

fw_online.sh

```
#!/bin/sh
/opt/CPfw1-R55/bin/cphaprob -d faildevice -s ok report
/opt/CPfw1-R55/bin/cphaprob -d faildevice unregister
```

Dopo aver creato i due script bisogna dargli i permessi di esecuzione quindi eseguimao il seguente comando :

chmod 777 fw_offline.sh
chmod 777 fw_online.sh

Naturalmente su entrambe i nodi del firewall.

Vanno lanciati in ordine cronologico prima fw_offline.sh e poi fw_online.sh