How To Install UTM-1 Appliances with Full HA

5 January 2011
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=11874
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/5/2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How To Install UTM-1 Appliances with Full HA ).
Contents

Important Information .................................................................................................................. 3
How To Install UTM-1 Appliances in Full HA ........................................................................ 5
  Objective ............................................................................................................................... 5
  Supported Versions ............................................................................................................... 5
  Supported OS ....................................................................................................................... 5
Before You Start ......................................................................................................................... 5
  Related Documentation and Assumed Knowledge .............................................................. 5
  Impact on the Environment and Warnings ............................................................................ 5
Initial Connection ....................................................................................................................... 6
First Time Configuration Wizard – Primary Firewall ............................................................. 7
First Time Configuration Wizard – Secondary Firewall ......................................................... 10
Configuring the Cluster in SmartDashboard ......................................................................... 11
Completing the Procedure ....................................................................................................... 12
Verifying ................................................................................................................................... 12
How To Install UTM-1 Appliances in Full HA

Objective

- This solution covers the first-time installation of UTM-1 appliances in a full High Availability configuration.

Supported Versions

- All

Supported OS

- All Secure Platform OSs available for the appliance.

Before You Start

Related Documentation and Assumed Knowledge

- N/A

Impact on the Environment and Warnings

- N/A
Initial Connection

1. Connect a crossover cable from a PC workstation to the Internal NIC of the Appliance.
2. Set the IP of the workstation at: 192.168.1.x / 24 – use any IP except ".1", which is the default for the appliance.
   If you have a pop-up blocker, you’ll need to disable it or add an exception for 192.168.1.1.
   If presented with a dialog similar to the following, choose the option to "Continue to this website...":

![Certificate Error: Navigation Blocked - Windows Internet Explorer](image)

4. Log in with the default account information: user admin, password admin.
5. Follow the prompts to change the default password.
First Time Configuration Wizard – Primary Firewall

1. Follow the prompts to work through the First Time Configuration Wizard.
2. Review the Welcome screen, and click Next.
3. Set the Date and Time manually or configure an NTP server, then click Apply, then click Next. Remember to set the Time and Time Zone accurately.
4. Configure your network connections:

Click on an interface name to set the IP address, netmask, and Link Speed/Duplex properties for that interface:
5. Configure your routing table.
   
   Click **New**, enter the route, and click **Apply**, which returns you to the previous screen.
   
   When all routes are entered, click **Next**.

6. Enter the firewall’s host name, domain name, and DNS servers, then click **Next**.

7. Configure the management type. For both Primary and Secondary firewalls, choose "Locally Managed":

8. Configure clustering. Mark the checkbox to indicate the appliance is part of a cluster, and then select the appropriate option button indicating if it is the primary or secondary member:

9. Configure allowed SSH and GUI client IP addresses, then click Next.

10. If needed, click Start Download to download the SmartConsole application to the workstation, then click Next.

11. The wizard presents a summary of the installation and offers the options to go back to make any changes, quit, or finish the configuration wizard. If there are any changes necessary, use Back/Next to navigate to the page where you need to make the change, and return to the summary screen.

   Once all parameters are correct, click Finish.
First Time Configuration Wizard – Secondary Firewall

1. Repeat the process for the secondary system, choosing "secondary" instead of "primary" in step 8 above.
2. Additionally, between steps 9 and 10 above, you will be prompted for the SIC communications activation key:

   Write down or remember the activation key used above, you will require it again in a subsequent step.
Configuring the Cluster in SmartDashboard

1. Log in to SmartDashboard, approve the First Time Fingerprint Verification. The UTM-1 Cluster Wizard will run, presenting an introductory page. Click Next.
2. Provide a name for the cluster object, then click Next.
3. Provide the information requested about the secondary cluster member - this includes the Activation Key recorded when installing the secondary cluster member. Click Next.
4. The Wizard will pull topology information and present the topology property page. Provide the IP address of the cluster interface, and click **Next**:

![Wizard screenshot showing topology properties](image)

5. Repeat step 4 for all clustered interfaces.

6. The Wizard Completion page appears. If desired, mark the checkbox to edit the cluster in Advanced Mode to bring up the cluster object properties for further configuration, such as setting the cluster mode from HA to Load Sharing, enabling / disabling additional blades, etc.

7. Click **Finish**.

### Completing the Procedure

At the end of the procedure, you are left in SmartDashboard, with the configured cluster that you just created in front of you.

### Verifying

- Double-check that you made no typos when you entered the data.