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=12284
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>12 July 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 UTM-1 Edge R75.20 Administration Guide).
Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction to UTM-1 Edge Appliances</td>
<td>5</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Security and VPN Solutions for Different Sized Organizations</td>
<td>5</td>
</tr>
<tr>
<td>Solution for UTM-1 Edge Appliances</td>
<td>5</td>
</tr>
<tr>
<td>Finding the Right Check Point Management Solution</td>
<td>6</td>
</tr>
<tr>
<td>Typical Workflow</td>
<td>7</td>
</tr>
<tr>
<td>Advantages of UTM-1 Edge Appliances</td>
<td>8</td>
</tr>
<tr>
<td>UTM-1 Edge Device Functionality</td>
<td>8</td>
</tr>
<tr>
<td>Installation and Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Introduction to the Installation and Configuration Processes</td>
<td>10</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>10</td>
</tr>
<tr>
<td>Overview of Workflow with a Security Management Server</td>
<td>10</td>
</tr>
<tr>
<td>Overview of Workflow with Smart Provisioning</td>
<td>11</td>
</tr>
<tr>
<td>Configuration Operations</td>
<td>11</td>
</tr>
<tr>
<td>Installation &amp; Configuration Using a Security Management Server</td>
<td>11</td>
</tr>
<tr>
<td>Working with UTM-1 Edge Objects with a Security Management Server</td>
<td>11</td>
</tr>
<tr>
<td>Working with UTM-1 Edge objects for Smart Provisioning</td>
<td>13</td>
</tr>
<tr>
<td>SmartDashboard Content Inspection Configuration</td>
<td>14</td>
</tr>
<tr>
<td>Creating a Security Policy for UTM-1 Edge Appliance</td>
<td>15</td>
</tr>
<tr>
<td>Security Policy Operations</td>
<td>15</td>
</tr>
<tr>
<td>Managing UTM-1 Edge Devices with a Security Management Server</td>
<td>16</td>
</tr>
<tr>
<td>Remote Login to the Security Management server</td>
<td>17</td>
</tr>
<tr>
<td>Configuring VPN in Security Management</td>
<td>17</td>
</tr>
<tr>
<td>Viewing Logs in the SmartView Tracker</td>
<td>20</td>
</tr>
<tr>
<td>Downloading the Latest Firmware from Smart Update</td>
<td>21</td>
</tr>
<tr>
<td>Index</td>
<td>23</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction to UTM-1 Edge Appliances

In This Chapter

Introduction 5
Security and VPN Solutions for Different Sized Organizations 5
Solution for UTM-1 Edge Appliances 5

Introduction

Thank you for using Check Point UTM-1 Edge appliances, which provide secure connectivity and VPN solutions at affordable prices. Check Point UTM-1 Edge appliances are easy to install and user-friendly. With IPSO appliances and 3rd party appliances, such as NEC devices, they are seamlessly and securely integrated with different Security Management Server, Multi-Domain Security Management and SmartProvisioning management solutions.

This document describes how to deploy and manage UTM-1 Edge appliances using Check Point management solutions. In this document you will also learn about Check Point features that the UTM-1 Edge and other appliances support, and how to use these appliances for your network security solutions.

Security and VPN Solutions for Different Sized Organizations

All enterprises and organizations, large and small, require tailor-made security and VPN solutions for the management of their remote sites and branch offices. These solutions must take into consideration that remote sites or branch offices:

- Do not necessarily need enterprise-size solutions or costs for their moderate-sized employee-base.
- Do not require advanced Security Policy and VPN configurations but do require full security and connectivity.
- Do not necessarily employ a full-time security administrator and are not necessarily looking to manage the Security gateways themselves.

What these businesses require is a solution that offers connectivity and security at an affordable rate that is easy to integrate into existing infrastructure and is easy to use.

Solution for UTM-1 Edge Appliances

UTM-1 Edge is a series of appliances offered by Check Point that provides both Security and VPN solutions, that are affordable, easy to configure and simple to manage for securing enterprise remote sites and large-scale VPN deployments. UTM-1 Edge appliances support SMART management and can be used with any Security Gateway.

UTM-1 Edge appliances enable enterprises to quickly and easily create a seamless Check Point security infrastructure. These appliances can be centrally managed and easily incorporated into existing...
infrastructures. These appliances do not include moving parts, are easy to use, and do not compromise either connectivity or security.

**Finding the Right Check Point Management Solution**

UTM-1 Edge appliances can be managed using any one of the following Check Point management solutions: Security Management Server, Multi-Domain Security Management, or Smart Provisioning:

- A Security Management Server is considered the standard UTM-1 Edge management solution and is often used in conjunction with Smart Provisioning. A Security Management Server is useful for organizations with branch offices that are looking for affordable alternatives and basic security and VPN solutions for each branch office. UTM-1 Edge appliances are represented by an object called the UTM-1 Edge gateway, which is created and managed in SmartDashboard.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>UTM-1 Edge Appliance</td>
</tr>
<tr>
<td>3</td>
<td>SmartDashboard</td>
</tr>
<tr>
<td>4</td>
<td>Security Management Server</td>
</tr>
<tr>
<td>5</td>
<td>LAN</td>
</tr>
<tr>
<td>6</td>
<td>branch office</td>
</tr>
</tbody>
</table>
SmartProvisioning, is an extension of a Security Management Server, providing administrators with an effective means of provisioning and managing hundreds and thousands of SmartLSM Security Gateways. UTM-1 Edge Profiles and Profile policies are defined in SmartDashboard. SmartLSM Security Gateways are provisioned and managed using the SmartProvisioning GUI Client.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway (connecting VPN Pipes)</td>
</tr>
<tr>
<td>2</td>
<td>UTM-1 Edge Appliance</td>
</tr>
<tr>
<td>3</td>
<td>SmartDashboard</td>
</tr>
<tr>
<td>4</td>
<td>SmartProvisioning</td>
</tr>
<tr>
<td>5</td>
<td>LAN</td>
</tr>
<tr>
<td>6</td>
<td>UTM-1 Edge Profile 1</td>
</tr>
<tr>
<td>7</td>
<td>UTM-1 Edge Profile 2</td>
</tr>
</tbody>
</table>

Multi-Domain Security Management is used by large enterprises and by Managed Service Providers to centrally manage multiple, fully customized, Domains. UTM-1 Edge appliances integrate transparently with this solution. The management capabilities of Domain Management Servers are equivalent to those of the Security Management Server, including the SmartProvisioning extension. Global VPN Communities are currently not supported for UTM-1 Edge appliances.

**Typical Workflow**

1. Install your UTM-1 Edge appliance. For more information see your vendor documentation.
2. Create objects to represent these appliances in your Check Point management solution. This includes the creation of a UTM-1 Edge Profile and a Security gateway object, where the latter is the network object representing the UTM-1 Edge appliance.
3. Perform the initial configuration of the appliance and the connection to the Security Management Server using the Web GUI, called the UTM-1 Edge portal (http://my.firewall). It is imperative that trust is established between the Security Management Server and the device for them to communicate freely and securely. There must be a connection to the Security Management Server from the device so that management operations carried out by the Security Management Server can be applied. This establishment of trust is equivalent to the SIC (Secure Internal Communication) process that takes place between regular Security Gateways and the Security Management Server.
4. Perform management operations. All management operations - such as defining VPN relationships with other Security Gateways, fetching a policy, or updating the firmware (software version embedded in the appliance) - are performed by the Security Management Server using Check Point GUI management (SmartDashboard, SmartProvisioning or SmartDomain Manager), or the Command Line.

5. The Security Management Server uses a UDP-based protocol which is encrypted (called SWTP_SMS or SWTP_gateway) to communicate with the UTM-1 Edge appliance. This protocol is enforced in an implied rule in the Security Policy. For more about Security Management, see the R75.20 Security Management Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12277).

Advantages of UTM-1 Edge Appliances

There are several distinct advantages to working with UTM-1 Edge devices. The features that are supported depend on the device that you own:

- **Installation, Integration and Configuration** - The UTM-1 Edge appliance itself is easy to install and configure. Moreover, UTM-1 Edge appliances can be used immediately once the Security Management Server has been installed. The appliance is "diskless". It contains pre-configured software and can be used out-of-the-box.

- **VPN** - Check Point VPN solutions, which offer full encryption and authentication capabilities. These Appliances can participate as a peer gateway in the corporate VPN with just one click. The appliances can participate in a Site-to-Site Community (either Star or Meshed), or as a Remote Access client. For more information on building VPN Communities, see the R75.20 VPN Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12285).

- **Security** - A Security Policy can be enforced on UTM-1 Edge appliances. Some of the security highlights include: support for Check Point's patented Stateful Inspection, Anti-spoofing, DoS protection, and H.323 VoIP. Some of the networking highlights include DHCP, NAT support, and Access Control.

- **Logging and gleaning the status of appliances** - The status and traffic on UTM-1 Edge appliances can be monitored and logged using the Check Point SmartConsole clients: SmartView Tracker and SmartView Status. These tools can be used for troubleshooting purposes.

- **Centralized upgrading** - the UTM-1 Edge device firmware can be upgraded automatically using Check Point SmartUpdate support.

UTM-1 Edge Device Functionality

UTM-1 Edge gateways can participate in two types of VPN communities: Site-to-Site and Remote Access. These communities are explained in more detail in the R75.20 VPN Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12285).

Site-to-Site

UTM-1 Edge Device gateways are generally added to communities and participate in the VPN tunnel in the same manner as all Security Gateway objects; they are added, like regular participating Security Gateways into the VPN community (Star or Meshed). Consult the R75.20 VPN Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12285) for more information on building a VPN between gateways.

Note - On a Security Management server any UTM-1 Edge appliance that is connecting using Site-to-Site VPN is considered to be an additional managed site; therefore, you are required to obtain an additional license.

UTM-1 Edge as a Remote Access Client

You can configure the UTM-1 Edge appliance to act as a remote client by adding it to a Remote Access Community. In this case it is configured in an atypical VPN configuration where the UTM-1 Edge gateway is added as a User group to the VPN community. This user group is created by default and is called VPN-1 devices defined as Remote Access. All machines deployed behind the UTM-1 Edge gateway will also function as Remote Access Clients. This means that all traffic from these gateways will be tunneled as well.
**UTM-1 Edge Managed by an External Service Center**

UTM-1 Edge gateway objects can be managed by an external Management server. These objects can be used in VPN communities. Typically, externally managed Security Gateways are used in Extranet scenarios with partners, or with additional Management servers.

**UTM-1 Edge and Packet Filtering Firewall**

UTM-1 Edge appliances use Check Point's Stateful Inspection technology just like other Check Point Security gateways. Gateways receive their Security Policy from the Security Management Server. This policy enforces the manner in which connections are allowed (or not allowed) to pass to and from the UTM-1 Edge appliance.

Access Control is used to determine the resources and services that are authorized to be used. This access authorization sets the level of security. Rules are attributed to UTM-1 Edge gateways by installing the policy on a specific gateway. For more about Access Control, see the **R75.20 Firewall Administration Guide** (http://supportcontent.checkpoint.com/documentation_download?ID=12267).

UTM-1 Edge appliances can be used with the following actions in the Security Policy Rule Base: **Accept**, **Drop** and **Reject**.

**Logging in the SmartView Tracker**

UTM-1 Edge logs can be generated and sent to a logging server. This server consolidates all UTM-1 Edge logs in the SmartView Tracker. You can view regular logs and audit logs (for management operations) in the SmartView Tracker. You can use these logs to troubleshoot and confirm that connections are passing to and from the UTM-1 Edge appliance, according to what is specified in the Security Policy. SmartView Tracker includes a pre-defined query that can be used to focus on the logs generated from the appliance.

Since the UTM-Edge gateway sends logs at periodic intervals, you will notice that logs appear in the SmartView Tracker only after the periodic interval has passed.

**Viewing the Status of UTM-1 Edge Appliances and VPN Creation**

Use the SmartView Monitor in order to learn more about the status of the UTM-1 Edge appliances. SmartView Monitor is available to UTM-1 Edge customers. SmartProvisioning customers may view the status of their objects in SmartView Monitor, or in the SmartProvisioning GUI Client.

**Upgrading UTM-1 Edge Appliance Firmware using SmartUpdate**

The UTM-1 Edge gateway firmware represents the software that is running on the appliance. The UTM-1 Edge gateway firmware can be viewed and upgraded using SmartUpdate. This is a centralized management tool which is used to upgrade all Security Gateways in the system by downloading new versions from the Check Point Download Center. When installing new firmware, the firmware is prepared at the Security Management Server, downloaded and subsequently installed when the UTM-1 Edge gateway fetches for updates. Since the UTM-1 Edge gateway fetches at periodic intervals, you will notice the upgraded version on the gateway only after the periodic interval has passed.
Chapter 2

Installation and Configuration

In This Chapter

Introduction to the Installation and Configuration Processes 10
Before You Begin 10
Overview of Workflow with a Security Management Server 10
Overview of Workflow with SmartProvisioning 11
Configuration Operations 11

Introduction to the Installation and Configuration Processes

The installation and configuration process depends on a number of factors: the management solution that you are using (whether a Security Management Server, SmartProvisioning or Multi-Domain Security Management), the type of VPN community that you are configuring, and the type of device that you are using.

Before You Begin

Before you can work with the UTM-1 Edge appliance, you need to install and configure it via the UTM-1 Edge Portal. This is a Web GUI used expressly for the management of the appliance. In addition to the actual installation process, you need to perform a first time login to the UTM-1 Edge appliance via the portal. In this first time login, you set up initial administrator permissions and authorization permissions, as well as the management interface itself.

Overview of Workflow with a Security Management Server

This workflow assumes that you have installed a Security Management Server. For more information see the appropriate R75.20 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12269).

The following workflow represents the order in which you should work with UTM-1 Edge appliances. More details about each step in the workflow can be found in this document.

1. Install and configure your UTM-1 Edge appliance. If you are setting up the appliance on the network, make sure that it is successfully connected.
2. In SmartDashboard:
   - Create the UTM-1 Edge gateway objects. Make sure that you setup the UTM-1 Edge appliance's topology properly and add the gateway to a VPN Community.
   - Create rules for your objects and install the Security Policy. This step should be repeated whenever a UTM-1 Edge object is modified.
3. On the UTM-1 Edge portal, define your Security Management server as the UTM-1 Edge appliance's service center. This means that the Security Management server is now responsible for managing the
Overview of Workflow with SmartProvisioning

This workflow assumes that you have installed a Security Management Server.

The following workflow represents the order in which you should work with UTM-1 Edge appliances. More details about each step in the workflow can be found in this document.

1. Install and configure the UTM-1 Edge appliance. Refer to the R75.20 SmartProvisioning Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12280) for more information. If you are setting up the appliance on the network, make sure that it is successfully connected.

2. To enable SmartProvisioning, run the command **LSMenabler** on Security Management Server.

3. In SmartDashboard,
   - Create a Smart LSM UTM-1 Edge Profile. When creating the profile, specify the VPN community in which you would like the profile to participate. This step can also take place at a later stage.

   **Note** - In SmartProvisioning, the profile associated with the UTM-1 Edge Gateway can only participate in a Star community for Site-to-Site configuration.

   - Create one or more dynamic objects to be enforced on the SmartLSM Security gateway.
   - Create rules for your objects and install the Security Policy.
   - Close SmartDashboard.


5. Using the UTM-1 Edge portal, define your Security Management Server as the UTM-1 Edge appliance's service center. This means that the Security Management Server is now responsible for managing the appliance, including security policies, Access Control, Licensing and updates. The communication between the Security Management server and the UTM-1 Edge appliance is secure.

Configuration Operations

Installation & Configuration Using a Security Management Server

UTM-1 Edge support is enabled automatically during the installation of the Security Management server. There is no need to install any additional component.

**Note** - UTM-1 Edge cannot be managed from a Security Management server running on IPSO.

Working with UTM-1 Edge Objects with a Security Management Server

An object that represents a UTM-1 Edge appliance should be defined in SmartDashboard in order for the Security Management Server to manage the UTM-1 Edge appliance:
Create the UTM-1 Edge gateway that represents the UTM-1 Edge appliance and associate it with a UTM-1 Edge Profile. During this process you must assign the previously created profile to the UTM-1 Edge gateway that is being created.

**Creating a UTM-1 Edge Gateway**

A UTM-1 Edge gateway object is a network object that represents a UTM-1 Edge appliance. This gateway sits on the network and can be managed by the Security Management server or by an external service center.

1. In the **Network Objects** branch in the **Objects Tree** create a new UTM-1 Edge gateway.
2. In the **UTM-1 Edge Gateway - General** page:

   - Configure the general settings of the window, including its **Name** and **IP Address** (whether static or dynamic), the UTM-1 Edge Profile and version information (**Type**). It is very important to select the exact version of your appliance. It is also necessary to define a **Password** (also known as a **Registration Key**). This password is used for encryption and authentication purposes.

   - Configure the **Check Point Products** that will be active on the gateway. To allow the UTM-1 Edge gateway to become a member of a VPN community, select the **VPN** check box and select the VPN Community type (whether **Site to Site** or **Remote Access**). Select any other products that will be active on the gateway.

   - Configure the management settings, if this gateway is managed by an external server, check **Externally Managed Gateway**.

   - Enable the Web UI administration GUI within SmartDashboard by selecting **Configure Edge Using Web Interface**.

3. In the **UTM-1 Edge Gateway - Topology** page, the topology is set automatically because it represents the hard coded device.
The set topology includes the following three interfaces (two internal and one external):

- **DMZ** represents a logical second network behind the UTM-1 Edge appliance. You must connect DMZ computers to the LAN ports. DMZ is a dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, the DMZ can serve as a secondary WAN port.

- **LAN** represents the private network. LAN 1-4 Local Area Network switch: Four Ethernet ports (RJ-45) are used for connecting computers or other network devices.

- **WAN** represents the external interface to the router. A WAN interface card, is a network interface card (NIC) that allows devices to connect to a wide area network. Wide Area Network (WAN): An Ethernet port (RJ-45) used for connecting your cable or xDSL modem, or for connecting a hub when setting up more than one Internet connection.

Although these three interfaces automatically appear in the **Topology** window, they are not associated with an IP address and a Network Mask.

If you deselect the **Dynamic Address** option in the **General Properties** window and add a static IP address, the WAN automatically receives the specified static IP address and its Network Mask is 255.255.255.255.

The **Type** drop-down list in the **General Properties** window defines the hardware type and its associated topology. Currently all hardware types share the same topology. Every hardware type has one external interface and two internal interfaces. It is possible to add only one additional external interface.

Once you have defined the general settings as well as the topology definitions of the UTM-1 Edge gateway a certificate is automatically created.

**Note** - Pre-Shared Secrets work in conjunction with Static IP Addresses only.

For managed devices it is essential to specify the correct network. When managing multiple devices it is better to define the networks on the devices, so as to ensure that the networks do not overlap with one another.

For externally managed devices the networks specified depend upon both the NAT settings on the other side as well as the agreed configuration.

4. **On the UTM-1 Edge Gateway - IPSec VPN** page, associate the UTM-1 Edge gateway with the VPN community of your choice. This page can only be set by closing and reopening the UTM-1 Edge gateway object. At this point a certificate is created for the UTM-1 Edge gateway.

You can also add a Security Gateway to a selected VPN community by opening the VPN community directly from the **VPN Manager** view.

To enable High Availability configure a backup gateway. Refer to the **Configuring High Availability** section in the **UTM-1 Embedded NGX User Guide** (http://supportcontent.checkpoint.com/documentation_download?ID=11742).

**Note** - To perform a detailed configuration of the created UTM-1 Edge Gateway launch the gateway in a browser. To do this, right-click the specific UTM-1 Edge gateway and select Manage Devices...

5. **In the UTM-1 Edge Gateway - Advanced** page, enter the following information:

- **Product Key** enables you to remotely update the current UTM-1 Edge gateway license (18 hexadecimal characters in three groups separated by hyphens).

- **MAC Address** enables stronger validation of the UTM-1 Edge gateway when communicating with the Security Management server.

- **Configuration Script** enables you to enter a script for relevant commands and features. The written script will be downloaded automatically and executed to the UTM-1 Edge device.


**Working with UTM-1 Edge objects for SmartProvisioning**

The objects that are used with the SmartProvisioning management solution are partly created in SmartDashboard and partly in SmartProvisioning.

- **SmartLSM Security Gateway Security Management server object** - represents the UTM-1 Edge appliance. This object is created in SmartProvisioning.
• SmartProvisioning UTM-1 Edge Profile - represents an object that is associated with a SmartLSM Security Gateway and provides it with a basic Security Policy and VPN definition. This object is created in SmartDashboard.

• A dynamic object used by the SmartProvisioning UTM-1 Edge Profile in order to enforce the Security Policy. This object is created in SmartDashboard and is added to the SmartProvisioning UTM-1 Edge Profile in SmartProvisioning.

The order of the creation of the UTM-1 Edge objects is:
1. Create the SmartLSM Security Gateway in SmartDashboard.
2. Create a Dynamic Object in SmartDashboard.
3. Close SmartDashboard and open SmartProvisioning.
4. Create the SmartLSM Security Gateway that represents the UTM-1 Edge appliance in SmartProvisioning, and associate it with a profile. During this process you must assign a previously created profile to the new SmartLSM Security Gateway.

Creating a SmartProvisioning Security Gateway Profile

A security policy is defined for a UTM-1 Edge appliance, represented by a SmartLSM Security Gateway by associating it to a profile.

Defining SmartProvisioning Profiles

1. In SmartDashboard, right-click Network Objects and select New > SmartLSM profile > UTM-1 Gateway.
   
   Note - To see these options, the Security Management server must be SmartProvisioning enabled. (On the Security Management server, run: LSMenabler)

2. In the General page, enter the name and an optional comment.
3. On the IPS page, assign a profile.
4. On the Logging page, select your logging options.
5. On the IPSec VPN page, enter the type of community that you would like to associate with the said profile and save the profile by closing it.
6. In the Advanced page, enter the following information:
   - Configuration Script enables you to enter a script for relevant commands and features. The written script will be downloaded automatically and executed to the UTM-1 Edge device.

Creating a SmartLSM Security Gateway

A SmartLSM Security Gateway object is a network object that represents a UTM-1 Edge Appliance created and managed in SmartProvisioning. This Gateway sits on the network and can be managed by the Security Management server or by an external service center.

Defining SmartLSM Security Gateway

Before you can create the SmartLSM Security Gateway make sure that you have exited SmartDashboard, if it is in Read/Write mode.


SmartDashboard Content Inspection Configuration

To work on UTM-1 Edge gateways, Content Inspection must be configured in the Edge Anti-Virus section of the Anti-Virus & URL Filtering tab. The Edge Anti-Virus settings in the Anti-Virus & URL Filtering tab only work for Edge machines.
Creating a Security Policy for UTM-1 Edge Appliance


   When you are creating rules, be aware that the UTM-1 Edge gateway can be used in the Install On column even if there is a VPN Community specified in the VPN column.

   You may need a rule that allows designated services (such as, ftp, telnet and http) to be performed by the VPN community. In this rule, the Security Gateway should be your target.

   For example:

   Example: Rule allowing services for Site-to-Site and Remote Access communities respectively

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Mesh-comm</td>
<td>ftp</td>
<td>Accept</td>
<td>gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ftp</td>
<td>Accept</td>
<td>gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>telnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>http</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   Allowing connections from network to UTM-1 Edge Gateway

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge_Net</td>
<td>UTM-1 Edge</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Once the rules are complete install your Security Policy (Policy > Install Policy).

The UTM-1 Edge gateway periodically fetches the Security Policy from the Security Management server. When the policy installation is complete the Security Management server will attempt to update the UTM-1 Edge gateway with the new security policy. In order for the changes to take place immediately you can force a Policy update from the UTM-1 Edge Portal.

Security Policy Operations

Installing and Uninstalling the Security Policy

When the Security Policy is installed or uninstalled, the Security Policy is automatically downloaded to or uploaded from the Security Management server. When the UTM-1 Edge gateways check the Security Management server for updates, the activity (whether installation or uninstallation) is implemented.

- To install, select Policy > Install Policy.
- To uninstall, select Policy > Uninstall Policy.

Downloading a Security Policy

From the UTM-1 Edge Portal

1. Login from the UTM-1 Edge portal to http://my.firewall.
2. Click Services and Accounts and then click Refresh, or, click Services and Software Updates and then click Update Now.
3. When the UTM-1 Edge gateway looks for updates, it downloads the latest Security Policy.

Verifying that the Security Policy was downloaded

1. Login from the UTM-1 Edge portal to http://my.firewall.
2. Click Reports and then click Event Log.
3. Verify that the following message appears: Installed updated Security Policy (downloaded).
4. Click Setup > Tools > Diagnostics.
   The UTM-1 Edge object is displayed in the Policy field.

Managing UTM-1 Edge Devices with a Security Management Server

Before you can begin to work with the UTM-1 Edge Appliance, you need to log in to the UTM-1 Edge portal and define the Security Management Server as the active service center. This step allows the Security Management server to perform a number of management operations for the UTM-1 Edge such as VPN connections, updating the Security Policy and upgrading to later versions of firmware. Proceed as follows:

2. Enter your user name and password.
3. In the Account screen, connect to the Security Management server by clicking on Connect. A wizard is displayed in which you are required to configure the settings of the Security Management server.

During the Security Management Server setup, you are required to enter details about the UTM-1 Edge gateway object that you created. Note that the Gateway ID refers to the name of the said gateway and the Password refers to the Registration Key specified during the creation of the UTM-1 Edge gateway object.

Once this setup is successfully completed, the UTM-1 Edge appliance and the Security Management Server can communicate securely. For more information about this procedure, see the relevant vendor information.

Note - If your device is not installed locally, you will need to log in securely to the UTM-1 Edge Portal using HTTPS (https://<current IP Address>:981). For more information see the relevant vendor information.
Remote Login to the Security Management server

If your device is not installed locally, you will need to log in securely to the UTM-1 Edge Portal using HTTPS (https://<current IP Address>:981). For more information see the relevant vendor information.

Configuring VPN in Security Management

UTM-1 Edge Gateways can be added to Site-to-Site communities, as well as to Remote Access communities. The UTM-1 Edge Appliance can also be configured to act as a Remote Access client.

Gateway in Site-to-Site VPN Configuration

For VPN to be established the following must take place:

1. The UTM-1 Edge gateway must be defined and configured for Site-to-Site and a certificate created (if the VPN Community members are to use a certificate to authenticate).
   
   On the General page:
   
   • On the UTM-1 Edge gateway check VPN Enabled and select Site to Site in order to allow the UTM-1 Edge gateway to participate like any regular Security gateway in a star or meshed community. This means that any gateway can initiate a VPN tunnel to the UTM-1 Edge gateway and the UTM-1 Edge gateway can initiate a VPN tunnel to any other gateway.
   
   • In terms of IP addresses:
     
     • If the UTM-1 Edge gateway has a static IP Address, you can use a certificate or an IKE pre-shared secret to establish a VPN tunnel. In this case the password you enter is used for the IKE pre-shared secret.
     
     • If the UTM-1 Edge gateway has dynamic IP Address, (select Dynamic Address) only a certificate can be used in order to establish a VPN tunnel. In this case, make sure that you have selected Manually defined in the UTM-1 Edge gateway - Topology page (see Figure 2-2).
     
     • Make sure that the type that you select corresponds to the actual appliance that you have in your possession.
     
     • Add a Password that will be used later on the UTM Edge Portal and for the pre-shared secret (if you have a static IP Address).
     
   • On the Topology page:
     
     • All IP Addresses behind gateway based on Topology information is used for NAT implementation.
     
     • Manually Defined is used if the UTM Edge gateway is configured for dynamic IP Address or if NAT is not being implemented.

   On the VPN page generate the certificate and close the UTM-1 Edge gateway.

2. If you do not already have one, create a Star or Meshed community in the VPN Manager. For more about these communities and how to configure them, see the R75.20 VPN Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12285).

To create a Site-to-Site community

1. In the SmartDashboard navigation tree click the VPN Communities icon.

2. Select New > Site to Site > Meshed or Star.

In a Star Community

1. In the Central Gateways page click Add and select the desired UTM-1 Edge gateway. Click OK.

   Note - If you are creating a Star community, it is not recommended to include the UTM-1 Edge Gateway as a Central gateway.
2. In the **Satellite Gateways** page, click **Add** and select the desired UTM-1 Edge gateway. Click **OK**

![Satellite Gateways](image)

**In a Meshed Community**
- In the **Participating Gateways** page, click **Add** and select the desired UTM-1 Edge Gateway. Click **OK**.

**In Star and Meshed Communities**
1. In the **VPN Properties** page, specify the properties for the phases of IKE negotiation.
2. In the **Shared Secret** page, specify whether the VPN community member should be authenticated using a pre-shared secret or a certificate. If you would like to use a secret, make sure to select **Use only Shared Secret for all External members**. The secret used is the password defined when the UTM-1 Edge gateway object was created. If you would like to use certificates as a means of authentication, make sure that **Use only Shared Secret for all External members** is unchecked.
3. In the Rule Base, create the rules of your Security Policy.
4. Install the rule base on the Central gateways (for a Star community).
5. In the UTM-1 Edge Portal define the Security Management server as the active service center. In the **VPN** window of the UTM-1 Edge Portal, the Site-to-Site configuration is automatically loaded, including its topology and enterprise profile.

**Gateway in a Remote Access Client Configuration**
In order for the UTM-1 Edge gateway to function as a Remote Access Client, the gateway must be configured to participate in the Remote Access community. When the UTM-1 Edge gateway object is defined in the Check Point database, an additional User Group called **"All UTM-1 Edge Gateway Appliances"** is created. This User Group is used in the definition of the Remote Access community.

![Gateway in a Remote Access Client Configuration](image)

**Note** - The User Group **All UTM-1 Edge Gateway Appliances** is not a regular User Group and as such it does not appear in the **Users and Administrators** branch in the Objects Tree.

**Adding the UTM-1 Edge Gateway to a Remote Access Community**
There are two basic ways to add the UTM-1 Edge gateway to a community:
• In the UTM-1 Edge Gateway - VPN page, click on Add. Select the community to which you would like to associate the selected gateway.

• In the VPN Manager view, select the Remote Access community to which you would like to add the UTM-1 Edge gateway. Add the UTM-1 Edge gateway in the Participant User Group page by clicking on Add and selecting the default User Group called VPN-1 Embedded devices defined as Remote Access to which the UTM-1 Edge gateway is associated.

When UTM-1 Edge gateways are configured to work in client mode, it is important that the Security Management Server be deployed outside of the VPN domain of the Remote Access Client. If you are working with Remote Access Automatic login mode, the Security Management server may be within the VPN domain, however, in this case, you must create the VPN domain in the UTM-1 Edge gateway before connecting the UTM-1 Edge gateway to the Security Management Server.

For VPN to be established the following must take place:

1. Create a UTM-1 Edge gateway object. Make sure that you select VPN enabled and Remote Access on the General page. Remote Access means that the selected VPN Edge gateway can act as a Remote Access client to the corporate Security Gateway. No other Security Gateways will be able to initiate a VPN tunnel to this VPN Edge gateway. This UTM-1 Edge gateway can be enforced as part of a User Group in a Remote Access VPN community.

2. Create a Remittances community in the VPN Manager that includes the UTM-1 Edge gateway object.

3. In the Participating Gateways page click Add and select the Central gateway. Click OK.

4. In the Participant User Groups page, click Add and select VPN Embedded devices defined as Remote Access. Click OK.

5. Click OK to exit the Remote Access community window.


7. In the UTM-1 Edge Portal define the Security Management server as the active service center.

8. In the VPN window of the UTM-1 Edge Portal, the Remote Access configuration is automatically loaded. Create a new site to represent the Security gateway on the UTM-1 Edge appliance. On the VPN screen, click on New Site, run the wizard and perform the following steps:

9. Add the IP Address of the regular Security gateway.
10. Check **Download Configuration**.
11. Enter the name of the Site.
12. Under **VPN Login**, select **Automatic Login** and refer to the vendor documentation for more information.
13. In SmartDashboard, install the Security Policy.

**Management by an External Service Center**

You can configure a UTM-1 Edge appliance to be managed by an external Service Center. This means that it is not managed by the local Security Management Server or Multi-Domain Server. This scenario is typical for extranet or connection to partner sites. The configuration is in two locations.

This procedure is also applicable to locally managed Security Gateways.

1. On the UTM-1 Edge gateway object:
   - On the **General** page, check **Externally Managed Gateway**.
   - The setting defined in the **Topology** page, depends on the agreed configuration.
2. Modify the VPN Community to which you are adding the UTM-1 Edge. Make sure that you check **Use only Shared Secret for all External Members** on the **Advanced Settings > Shared Secret** page.
3. Modify the Security Policy, make sure that rule installed on the profile is disabled. Install the Security Policy.
   - On the UTM-1 Edge Portal on the **VPN** screen. Click on **New Site** and run the wizard and do the following steps:
     - Add the IP Address of the regular Security gateway.
     - Check **Download Configuration**.
     - Configure the routing destination and subnet mask of the external service center
     - Under **Authentication**, select **Use shared secret**.
     - Click on **Connect** in order to connect to the Security gateway.

**Configuring Security Gateways in Smart Provisioning**

SmartLSM Security Gateways can participate in meshed Site-to-Site communities. In Smart Provisioning, VPN is supported using IKE authentication with Check Point internal certificates:

1. In the UTM-1 Edge Portal, verify that a certificate has been installed on the UTM-1 Edge Device before establishing the VPN tunnel.
2. In Smart Provisioning:
   - Add a dynamic object to the SmartLSM Security Gateway. In order to implement VPN on SmartLSM Security Gateways, dynamic objects need to be added to the VPN domain of these objects. Make sure you check **Add to VPN domain**.
   - Update the Corporate Office (CO) Gateway.
3. In SmartDashboard, create a VPN Star community that includes the SmartLSM Security Gateway and the CO Gateway as follows:
   - In the **Central Gateway** page, click **Add**. Select the CO gateway from the displayed list and click **OK**.
   - In the **Satellite Gateways** page, click **Add**. Select the profile from the list and click **OK**.
   - In the **VPN Properties** page, specify the IKE phase properties.
   - In the **Shared Properties** page, uncheck the **Use only Shared secret for all External Members**. Make sure that shared secret is only used for external members and set the properties for the IKE negotiations.
   - A topology file and a certificate are downloaded to the SmartLSM Security Gateway. This topology file lists the members of the VPN community and specifies the encryption information.
4. On the UTM-1 Edge Portal, on the **VPN** screen specify the configuration type (whether Site-to-Site or Remote Access and check **Download Configuration**.

**Viewing Logs in the SmartView Tracker**

To view the logs, open the **Audit** view in the SmartView Tracker.
For your convenience add the Origin column to the Audit view (View > Query options > Query Properties, select Origin) and select the UTM-1 Edge appliance that you would like to track. This enables you to figure out from which UTM-1 Edge appliance the log was generated.

For security purposes, security logs are displayed in the Log view of the SmartView Tracker. Double-click the log in order to see more information.

**Downloading the Latest Firmware from SmartUpdate**

You can use SmartUpdate to get automatic updates of the latest firmware version. To download the latest firmware:

1. In the Product Repository pane, right-click a UTM-1 Edge gateway and select Add from Download Center.
2. In the displayed window, select the firmware that you would like to download and click Download.
3. In the Product Repository, right-click a UTM-1 Edge gateway and select Install Product.
4. Select the firmware and click OK.

The firmware is downloaded and sent to the Security Management Server that is responsible for downloading it to the UTM-1 Edge gateways when the latter is ready to receive it.