Unified Threat Manager

Quick Installation Guide

allo.com

Copy Right

Proprietary Rights

The information in this document is Confidential to Allo and is legally privileged. The information and this document are intended solely for the addressee. Use of this document by anyone else for any other purpose is unauthorized. If you are not the intended recipient, any disclosure, copying, or distribution of this information is prohibited and unlawful.

Disclaimer

Information in this document is subject to change without notice and should not be construed as a commitment on the part of **allo.com.** And does not assume any responsibility or make any warranty against errors. It may appear in this document and disclaims any implied warranty of merchantability or fitness for a particular purpose.

About this manual

This manual describes the allo product application and explains how to work and use it major features. It serves as a means to describe the configuration and how to use it to accomplish common tasks. This manual also describes the underlying assumptions and users make the underlying data model.

Document Conventions

In this manual, certain words are represented in different fonts, typefaces, sizes, and weights. This highlighting is systematic; different words are represented in the same style to indicate their inclusion in a specific category. Additionally, this document has different strategies to draw User attention to certain pieces of information. In order of how critical the information is to your system, these items are marked as a note, tip, important, caution, or warning.

Icon	Purpose
📝	**Note**
💡	**Tip/Best Practice**
★	**Important**
✋	**Caution**
⚠	**Warning**

- **Bold** indicates the name of the menu items, options, dialog boxes, windows and functions.
- The color blue with underline is used to indicate cross-references and hyperlinks.
- Numbered Paragraphs - Numbered paragraphs are used to indicate tasks that need to be carried out. Text in paragraphs without numbering represents ordinary information.
- The Courier font indicates a command sequence, file type, URL, Folder/File name e.g. http://www.allo.com

Support Information

Every effort has been made to ensure the accuracy of the document. If you have comments, questions, or ideas regarding the document contact online support: **http://support.allo.com/**

Table of Contents

1. Unified Threat Manager

Congratulations on your purchase of the Shield UTM appliance to protect your networks and hosts. This Quick Start Guide describes the steps involved in setting up the Shield UTM Appliance.

2. Package Contents

- Take the UTM device and all accessories out of the box
- Check that you have all the items listed below.

1 UTM Appliance

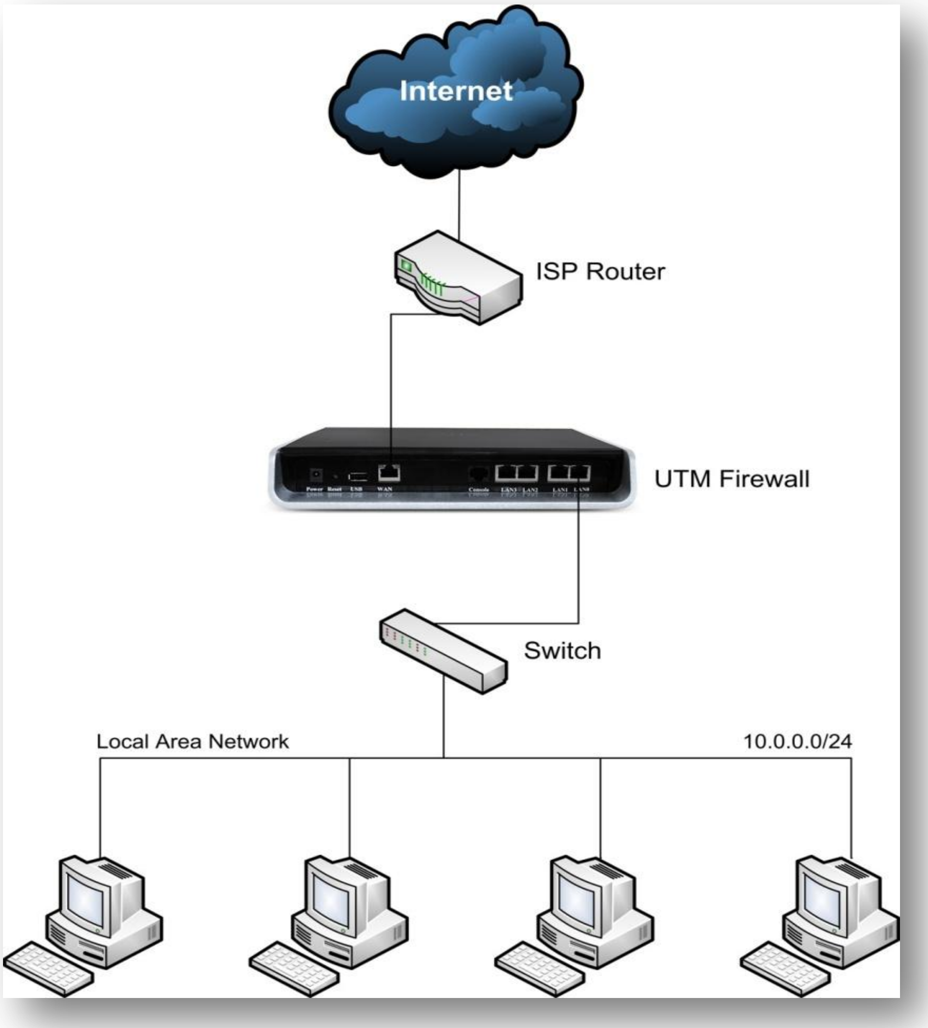
1 Power Adapter

2 Power chords

1 Console Cable

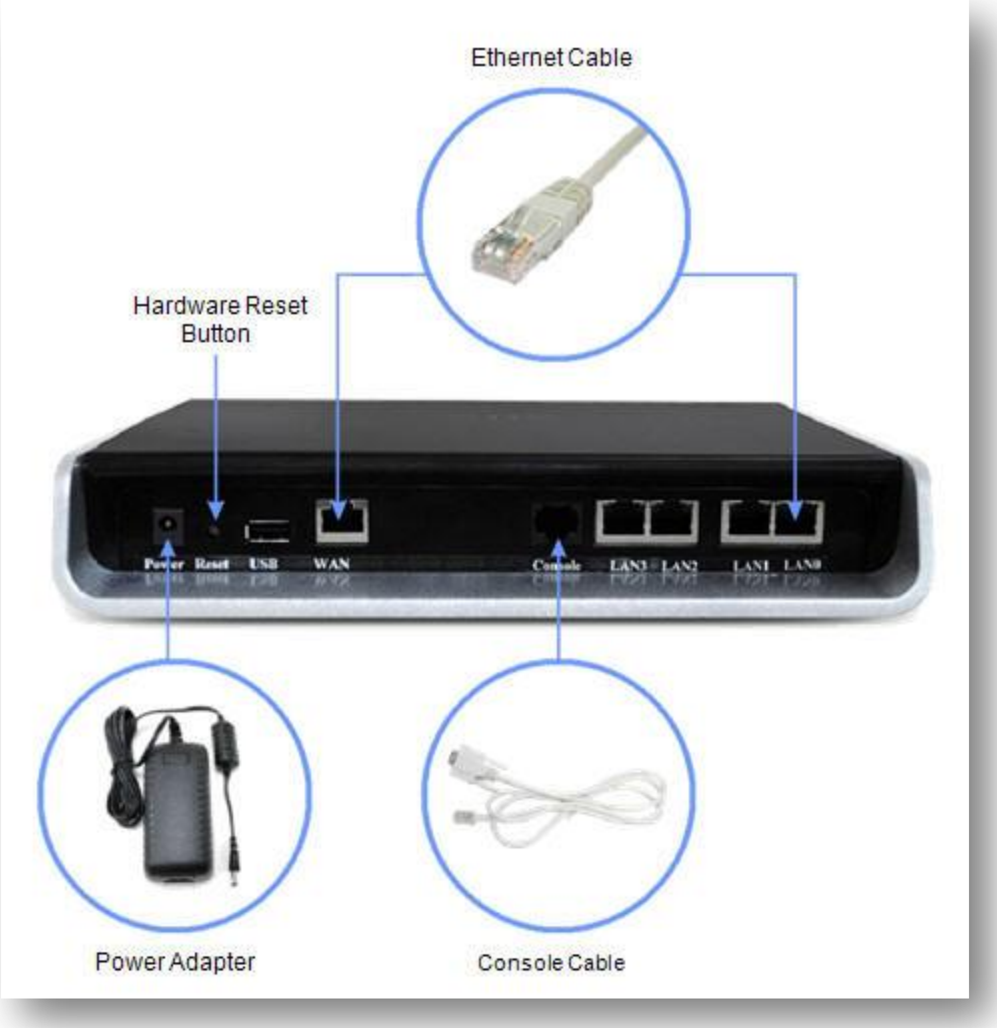
2 Ethernet Cable

3. Network Deployment



Network Deployment

4. Connecting the Hardware



Connecting the Hardware

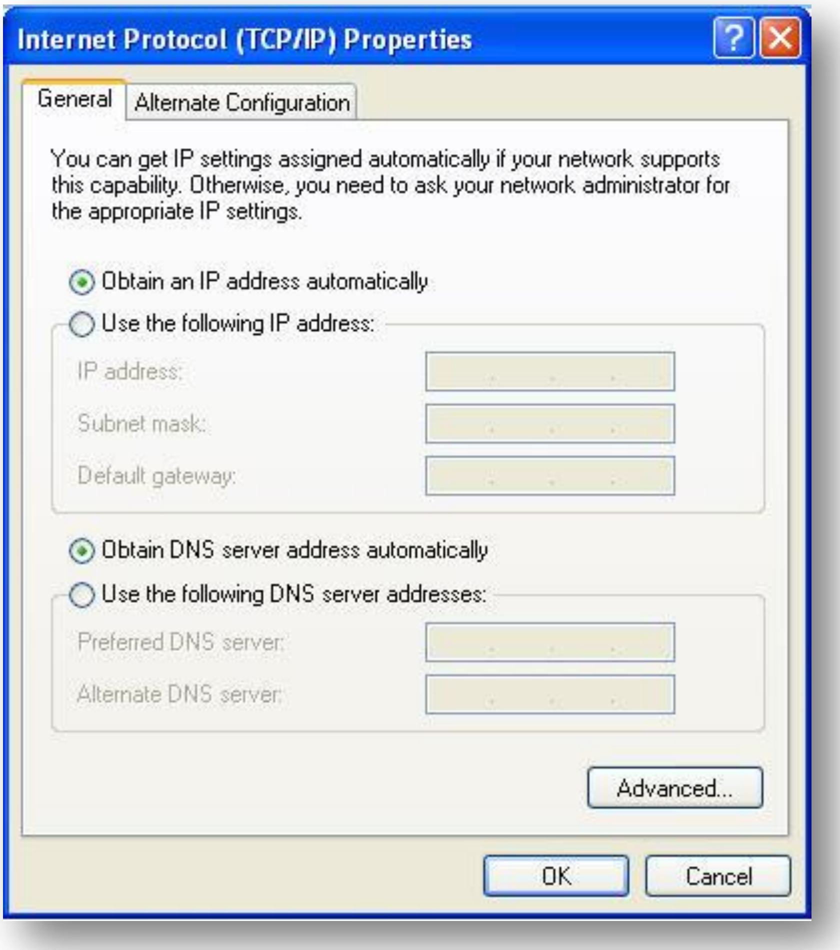
5. Default configuration

Ethernet Port	IP Address
LAN 0-3 > eth1	10.0.0.1/255.255.255.0
WAN > eth0	10.1.0.1/255.255.255.0
Management VLAN(Accessible via LAN Ports)	192.168.1.1/255.255.255.0
Default Firewall Mode	Router

Management Service	Default Credentials
Web UI	admin/admin
SSHCLI	admin/admin123

6. Network Configuration on Client Side

- UTM Firewall will have default Network Configuration it is necessary to configure your Personal Computer accordingly.
- Launch the network adapter configuration dialog of your Windows operating system and modify the TCP/IP configuration to obtain an IP Address automatically.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

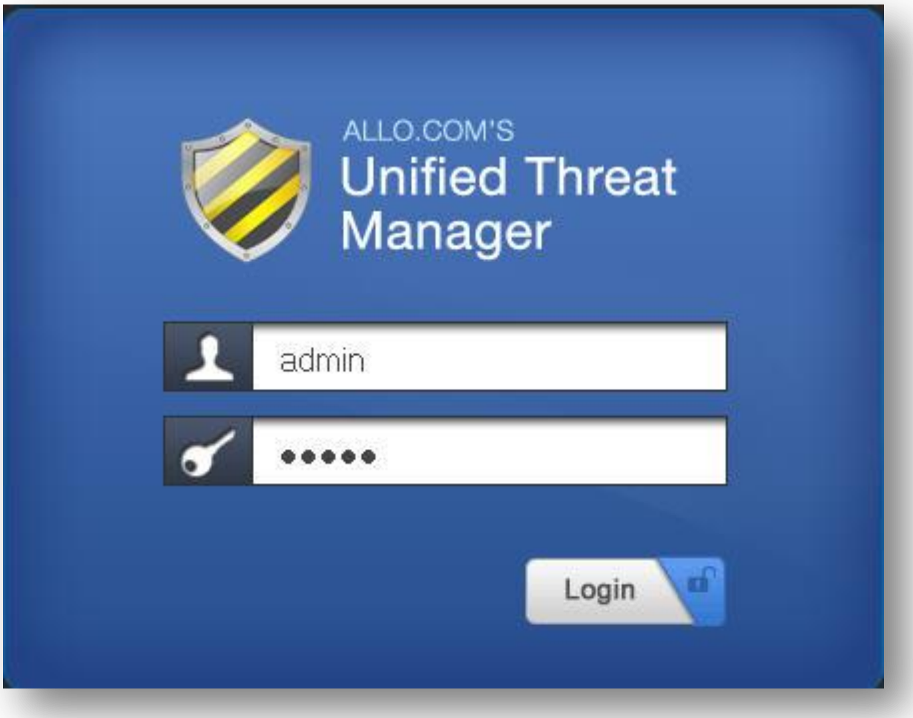
Network Configuration

7. Connect UTM Firewall

- Connect the appliance to the power socket using the power cable.
- Connect the PC to one of the LAN ports of the Appliance.
- Your PC will get an IP address from 10.0.0.0/24 subnet.
- You can access the Configuration management WebUI from the browser on the PC with the URL http://10.0.0.1/ or http://192.168.1.1

In case you won't start out any IP address for LAN, and so you have to configure manually.

- The recommended browsers for accessing UTM 1.0 WebUI is Mozilla Firefox / Internet Explorer 8 and above.
- Accept the Self signed SSL Certificate and Login to the UTM appliance using default Web UI credentials.



admin

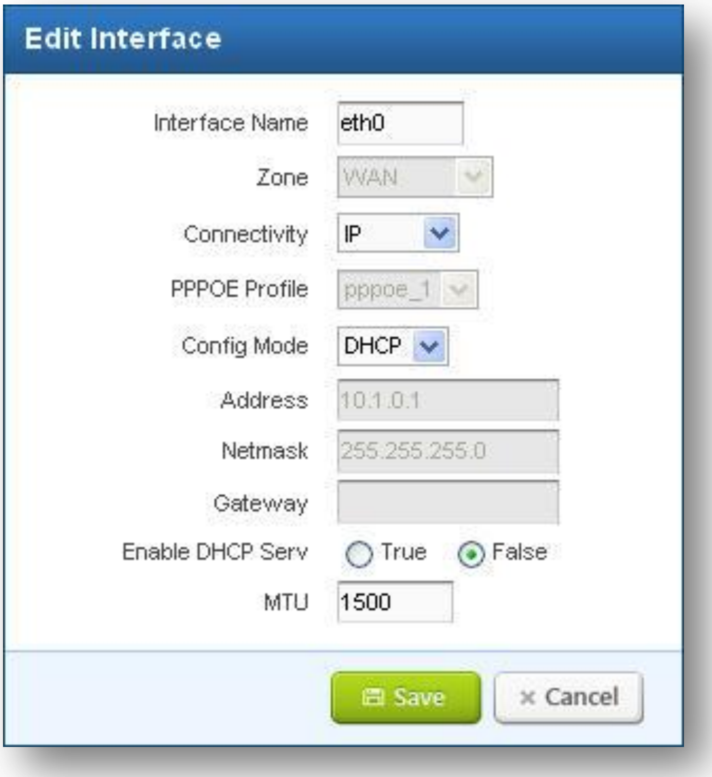
●●●●●

UTM Login Page

- WebUI is running on the secure http server. Accessing http://10.0.0.1 or http://192.168.1.1 will redirect to https://10.0.0.1/ or https://192.168.1.1/

8. Connect Internet Service Provider

- The WAN interface (eth0) is configured with static IP address by default in UTM1.0 Appliance
- If you're ISP provides a Static IP address for the WAN need to configure Static IP for eth0 port.
- If your ISP assigns the WAN IP address through the DHCP protocol, need to configure eth0 to DHCP Config mode.
- Enable the available WAN connection types and configure it according to the settings provided by your Internet Service Provider.
- Navigate to: Network > Interfaces > eth0 > Edit > Config Mode > Static/DHCP.



Edit Interface

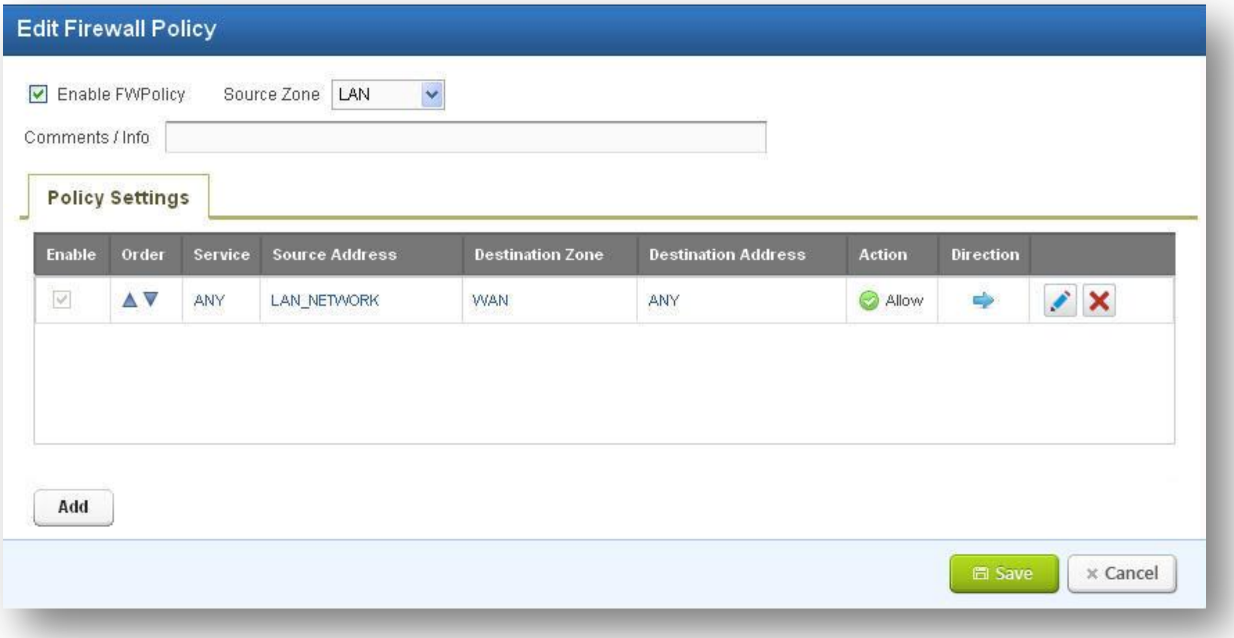
Interface Name	eth0
Zone	WAN
Connectivity	IP
PPPOE Profile	pppoe_1
Config Mode	DHCP
Address	10.1.0.1
Netmask	255.255.255.0
Gateway	
Enable DHCP Serv	○ True ● False
MTU	1500

WEB Interface

- To apply the current changes navigate to: Apply Changes >
- Configuration Setting > Yes > (You can view results of applied configuration in same dialog Box). You can close the dialog by clicking the 'Close' button.
- To check if the WAN IP address assignment was successful, navigate to: Status Info > Interfaces > eth0 > UP.

9. Firewall Policies

- The default policy configuration of the UTM Firewall allows all connections from LAN to WAN.
- To check /Modify Navigate to: Policies > Firewall Policies > LAN > Edit > Policy Setting > (You can see here Destination Zone 'WAN' Action 'Allow' Direction 'OUTBOUND')



Edit Firewall Policy

☑ Enable FWPolicy   Source Zone: LAN

Comments / Info:

Policy Settings

Enable	Order	Service	Source Address	Destination Zone	Destination Address	Action	Direction	
☑	▲▼	ANY	LAN_NETWORK	WAN	ANY	✓ Allow	➡	✎ ✖

Firewall Policies

For sales please contact

Canada
Toll Free: +1 877 339 2556
Direct: +1 778 892 2877
Email: andre@allo.com
Skype: allovoiphardware

For more information please contact

Engineering Facility
Adarsh Eco Place
#176, Ground Floor,
EPIP Industrial Area, Kundalahalli
KR Puram Hobali, Whitefield
Bangalore - 66, India

Phone: +91 80 67080808
Fax: +91 80 67080810

Manufacturing Plant
143 - A1, Bommasandra Industrial Area
Anekal Taluk, Hosur Road
Bangalore - 99, India

Website: WWW.ALLO.COM   WWW.SHIELD.COM