SOPHOS

# Proof of Concept Guide
# Sophos UTM

**Project / Customer:** ______________________________________

# Table of Content

# 1. Introduction

## 1.1. Purpose of the Document

This document offers a comprehensive overview of the most important aspects one has to take into consideration before and while realizing a *Proof of Concept* (PoC) with the Sophos UTM. It has been made for Sales Engineers within the Sophos organization and for technical people at Sophos partners, who want to set up a successful test installation for and with their prospects .

Please be aware that it is highly recommended to complete the Sophos certification program for UTM with both parts SCE and SCA (https://sophos.secure.force.com/partners/apex/TC2Training) before doing the first PoC.

## 1.2. Product information

All product related information within this document have been created based on the functionalities of Sophos UTM 9.x and Sophos UTM Manager (SUM) 4.x, but many parts are independent from the UTM version which will be used anyway.

# 2. Prerequisites

A lot of things have to be clarified before a PoC starts, especially if it is planned to integrate the UTM at the perimeter in a productive environment and not just into a lab or as a single homed device within a DMZ. It makes sense to discuss all technical and organizational aspects with the goal of getting as many questions as possible answered upfront.

## 2.1. Technical Aspects

### 2.1.1. Evaluation Content

Sophos UTM offers a lot of different functionalities. Please check what the prospect likes to see within the PoC, because not every customer will use each feature or buy each subscription. Knowing the objective of the test installation helps to focus on collecting the most important information. This PoC will include the following areas:

| | | |
|---|---|---|
| Firewall | YES | NO |
| VPN (Branch office/ Remote access) | YES | NO |
| Web Protection | YES | NO |
| Web Server Protection | YES | NO |
| Email Protection | YES | NO |
| Wireless Protection | YES | NO |

Endpoint Protection (via UTM) YES NO

High Availability (active-passive/active-active) YES NO

Special requirements: ______________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

Has the sizing of the PoC unit been made based on the UTM Sizing Guide? YES NO

### 2.1.2. Network Diagram

Having two network diagrams would be perfect: one with the current setup and a second one with the planned setup. A detailed network diagram of the current setup (without Sophos UTM) will help you to understand the environment of your prospect. Please ask them to add all existing active components to the diagram like:

- Routers, L3 switches, firewalls, internet uplinks, proxy servers, IPS, application control devices or similar transparent filter devices, WAN lines (PPPoE/PPPoA, leased lines, MPLS …), load balancers (internal or external/ISP balancers), wireless components, remote networks (via VPN or directly connected offices, partners, suppliers, etc.), RAS (direct dial-in) servers

- DNS servers, AD/LDAP servers, mail servers, proxy servers, NTP servers, DHCP servers, FTP servers, backup servers, network monitoring/SNMP systems, bandwidth shapers, VPN gateways, OTP/authentication servers, log servers, VoIP servers

Try to get the IP addresses, the net masks, the default gateways and eventually virtual IP addresses (in HSRP/VRRP or similar environments) of all components in the diagram.

Furthermore it might be interesting to know the bandwidths (upload/download) of the WAN links and how the services are getting balanced (if uplink balancing is already in place). Please do not forget to ask for routed networks, dynamic routing information and mail exchanger (MX).

The second network diagram with the planned setup (and Sophos UTM integrated) should at least show in a clear way the differences compared with the current topology and the IP addresses which can be used for the UTM.

## Current network topology:

### Planned network topology:

### 2.1.3. Network Information Checklist

It helps to get a proper overview of the collected basic network details by putting the information into the following list:

Do you have a firewall or UTM in your network today? YES NO

What brand/model? Please specify: ______________________________________________

Free IP addresses available for Sophos UTM:
LAN ______.______.______.______
WAN1 ______.______.______.______
WAN2 ______.______.______.______
DMZ ______.______.______.______
_______ ______.______.______.______
_______ ______.______.______.______

Router IP/ default gateway: ______.______.______.______

Mail server IP address: ______.______.______.______ MX ________________________

DNS server IP address: Local ______.______.______.______ ISP ______.______.______.______

AD/LDAP & domain controller: ______.______.______.______

Internal proxy server (uses by clients): ______.______.______.______

Upstream/parent proxy server: ______.______.______.______

PPPoE: Username ________________________
Password ________________________

Are you hosting your own server? YES NO

Server IP addresses (connected via NAT):
_______ ______.______.______.______
_______ ______.______.______.______
_______ ______.______.______.______

Web Server IP addresses (protected via WAF):
_______ ______.______.______.______
_______ ______.______.______.______
_______ ______.______.______.______

User authentication: YES NO
- AD/eDir/Apple SSO YES NO
- Radius YES NO
- Sophos Authentication Agent (SAA) YES NO
- Local user YES NO

### 2.1.4. Feature Related Questions to Ask

**Security:** What other security devices can influence the behaviour of the UTM? How about desktop AV, gateway AV, IPS or routers with ACLs in the environment?

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

**Email**: Which mail domains should be handled, what are the mail servers where incoming mails will be routed to, list of external mail servers (Pop3 mailboxes, ISP mail relay) where the prospect receives mails from?

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

**POP3**: List of external POP3 servers, users should be allowed to get POP3 mails from?

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

**Email Encryption (S/Mime, PGP):** List of users who should use email encryption, list of external communication partners?

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

**Active Directory**: Which AD groups should be used for Web Profiles, SSL-VPN access, etc.?

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

**Web Proxy:** Which are the networks from where the users connect, are there upstream/parent proxies, is there an internal CA (e.g. Microsoft CA used in the AD) which can be used for the HTTPS scanning (so roll-out of new trusted CA is not needed/easier)?

________________________________________________________________________________
________________________________________________________________________________
________________________________________________________________________________

**Web Policies**: Which filter mechanisms should be activated, what kind of policy should be defined for each user group?

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

**IPS:** Which operating systems and applications are used in the customer environment (to be able to tune the IPS), list of all web servers, DNS servers, SMTP servers, SQL-Servers (also for the IPS tuning)?

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

**Wireless:** What SSIDs are in use or needed, authentication schemes, how are the APs connected to the network, is meshing needed somewhere?

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

**VPN:** Parameter for establishing VPN connections to existing VPN gateways like encryption algorithms, remote IP addresses, PSKs, certificates?

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

**VPN (RED):** Is a static IP address needed for RED or is DHCP available in each RED location, local provisioning via USB stick or remote via RED provisioning server, which locations should be connected during the PoC?

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

**WAF**: Public FQDN hostname/domains of the web servers (for the virtual webserver), IP adresses of the real webservers – need to be in a different network than the WAN interface of the UTM (no bridge mode in WAF, eventually the real web servers must be reconfigured before starting the project/PoC)?

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

## 2.2. Organizational Aspects

### 2.2.1.Contact Details

A PoC is a part of the entire sales process and should be discussed and coordinated within the team of all responsible people. These are in this case:

**Customer/Prospect**
Technician/Admin: ___________________ @_______________________ ☎_______________
Decision maker: ___________________ @_______________________ ☎_______________

**Sophos Partner/Reseller/Distributor**
Sales Engineer: ___________________ @_______________________ ☎_______________
Sales: ___________________ @_______________________ ☎_______________

**Sophos**
Sales Engineer: ___________________ @_______________________ ☎_______________
Sales: ___________________ @_______________________ ☎_______________

**Other**
____________: ___________________ @_______________________ ☎_______________
____________: ___________________ @_______________________ ☎_______________

### 2.2.2. Timeline

It is important to schedule the PoC properly. The appliances have to be on-site in time, the prospect might have limited maintenance slots especially in productive environments, responsible people have to be available and at a certain point the PoC and the deal should be closed successfully.

Planned start of PoC: ________________________________________________

Expected end of PoC: ________________________________________________

Hardware shipment: ________________________________________________

Shipping delays due to customs regulation: ________________________________________________

Availability customer technician: ________________________________________________

Availability Partner/Reseller/Distributor SE: ________________________________________________

Availability Sophos SE: ________________________________________________

Maintenance slots: ________________________________________________

Other: ________________________________________________

### 2.2.3. Network Access and Credentials

In most cases a PoC requires the Sophos UTM to be integrated into an existing network. Please take care that you can get important information about the environment, when you are on-site:

- Do you know the free network ports on switches and patch fields? Who is responsible?

______________________________________________________________________________

- Has the network cabling been prepared/explained? Who is responsible?

______________________________________________________________________________

- Who is responsible for the existing setup and who knows the credentials and can make changes on the following components if necessary?
    - Active Directory (e.g. for credentials BIND user to access AD / “admin” user for enabling AD SSO with Sophos UTM)
    - Exchange
    - DHCP
    - Router/Switches
    - Other Servers

______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________

- Who decides, which passwords have to be used for new features (e.g. for webadmin, user portal, ssh, wireless SSIDs, etc.?

______________________________________________________________________________
______________________________________________________________________________

- Is there a naming convention in place for new network objects, which have to be created on the UTM?

______________________________________________________________________________
______________________________________________________________________________

### 2.2.4. Functionality Check

Detailed test criteria should have been defined before the PoC begins. The involved people should confirm to check out based on these criteria, whether the PoC was successful or not. The list has to be as detailed/granular as possible. It should be clear for each functionality what is needed to say finally “yes, approved”. The goal of the PoC is that all defined criteria are successfully implemented - but not more. Having such a list of criteria avoids that the customer wants additional things to get tested/demonstrated/implemented during a PoC, which were probably not in the original scope. The criteria can vary a lot from prospect to prospect. So please take the following *example* of a documented “PoC acceptance criteria catalogue” just as an idea how it could look like:

- *LACP / trunk is working between UTMs and Switch*
    - *Proof criteria 1: packet flow from internal to external through UTM is working*
    - *Proof criteria 2: cluster synchronization between UTMs is working*
    - *Proof criteria 3: connectivity is maintained even though a cable has been unplugged from the trunk*

- *Defined remote networks are reachable*
    - *Proof criteria 1: connection from "internal" system through UTMs to "external/remote" system is working*
    - *Proof criteria 2: connection from "external/remote" system "through UTMs to internal" system is working*
    - *Note 1: no dynamic routing protocol is configured on the UTM, routing information will be configured as static routes, as the target networks are located in a small amount of known and defined IP ranges*
    - *Note 2: hardware (clients & servers) for testing these criteria have to be provided by customer. Should have installed tools like iperf or netio, if customer wants to make throughput tests.*
    - *Note 3: for throughput test > 1 GBit/sec the testing hardware provided by the customer must be capable of these throughput numbers too*

- *Web filtering is working*
    - *Proof criteria 1: access of a website blocked by category is blocked*
    - *Proof criteria 2: access of a website blocked by category but allowed by whitelist is allowed*
    - *Proof criteria 3: access of a website blocked by blacklist is blocked*
    - *Proof criteria 4: download of a file via browser with an extension which is forbidden is blocked*
    - *Proof criteria 5: EICAR test virus pattern is being detected and blocked*
    - *Note 1: implementing/testing user authentication for surf users is not part of the project and not of the PoC*
    - *Note 2: HTTPS content scanning can not be implemented, if accessing users have not imported the UTMs proxy CA into their "trusted certificate issuer" store*

- *High Availability is working*
    - *Proof criteria 1: turning off all UTMs but the master UTM will not lead to a malfunction/system down , functionality is still there (with lower performance)*
    - *Proof criteria 2: turning off the master UTM will not result in a malfunction/system down, functionality is still provided*
    - *Note 1: to avoid file system harm, "turning off" will be simulated by either powering down the machines or unplugging all network cables from the UTM*
    - *Note 2: if Master gets turned off, a takeover time of 1-5 seconds is normal and acceptable*
    - *Note 3: to allow takeover, surrounding switches have to accept "gratitious arp broadcasts". Some switches with enabled security features do not allow this - in this case these features have to be turned off by customer.*

- *Note 4: currently running downloads and connections over the proxy of one UTM will always be interrupted and cancelled, if the UTM is unplugged/powered off. This will lead to error messages like "download stopped" or "connection reset by peer" at the client side. The download/connection must be re-established by the client again. Downloads running via the other machines will continue to work. This is by design and not an error/malfunction.*

*If all above mentioned test scenario criteria are successfully demonstrated/tested, the PoC is considered as being successful.*

# 3. Integration

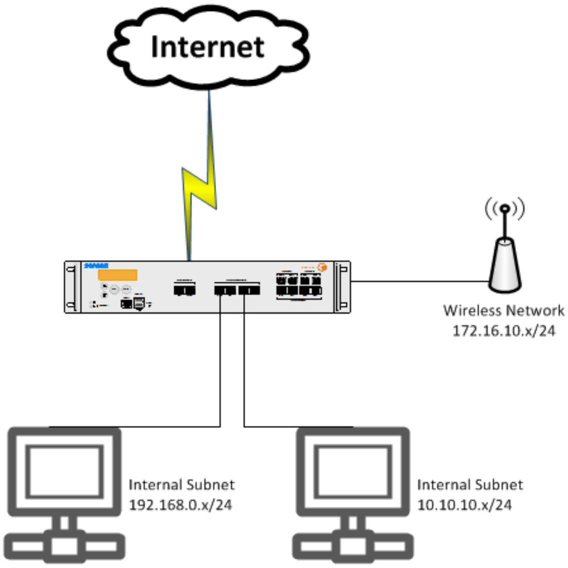
If all prerequisites and the schedule for the PoC have been arranged in a proper way, the PoC can be started. This chapter offers some best practice ideas for the UTM setup and several links to detailed technical explanations in the Sophos UTM knowledgebase.

http://www.sophos.com/en-us/support/knowledgebase/b/2450.aspx

## 3.1. Installation of Hardware

### 3.1.1. UTM Routed Mode

The Sophos UTM by default uses 'routed mode' where at least an internal and an external interface are configured in different subnets. The External (WAN) interface should be configured with a default Gateway IP address which will be used to route traffic out to the internet. An initial wizard is offered when first logging into the UTM which configures both the internal and WAN interfaces and sets up basic routing and security features such as a masquerade rule, suggested firewall rules, IPS, and a basic Web Protection settings. Note that if the wizard is not used you must configure these items manually in order to pass traffic.



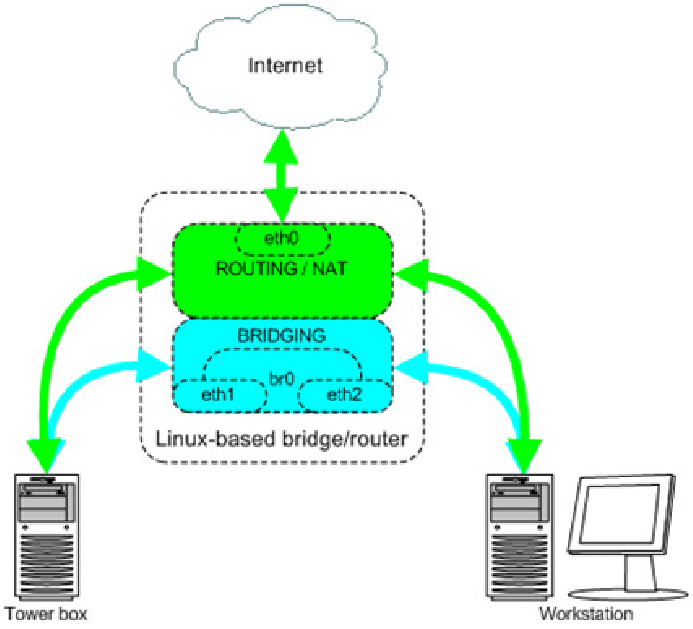
http://www.sophos.com/en-us/support/knowledgebase/2450/6500/6650/118899.aspx

### 3.1.2. UTM Bridge Mode

Sophos UTM interfaces can also be configured to use 'bridge mode'. Bridge mode allows you to configure all or some interfaces to emulate a layer 2 switch. The most common use for bridge mode is placing the UTM 'inline' in the network so that you do not have to remove existing firewalls for demonstration purposes or for passive monitoring. While using bridge mode most UTM functionality is still available and you can selectively test certain features, or passively gather information to show customers what's going on in their network.

Bridging is a packet forwarding technique primarily used in Ethernet networks. Unlike routing, bridging makes no assumptions about where in a network a particular address is located. Instead, it depends on broadcasting to locate unknown devices.

Through bridging, several Ethernet networks or segments can be connected to each other. The data packets are forwarded through bridging tables, which assign the MAC addresses to a bridge port. The resulting bridge will transparently pass traffic across the bridge interfaces.



http://www.sophos.com/en-us/support/knowledgebase/119360.aspx

### 3.1.3.RED Installation

Sophos RED devices provide plug and play remote office secure connectivity. No local configuration is needed and therefore no technical knowledge is necessary at the remote site. Simply plug the RED device into an internet connection and it will use a cloud broker service to find its UTM controller where all configuration is set.

http://www.sophos.com/en-us/support/knowledgebase/116573.aspx

### 3.1.4. Wireless Access Point Installation

Wireless APs use a discovery protocol to 'find' the UTM controller once plugged into the network or a RED device. Once connected the AP's register, and then advertise any configured wireless networks.

http://www.sophos.com/en-us/medialibrary/PDFs/documentation/sophosaccesspointsqsg.pdf

## 3.2. Best Practice Configuration Options

For detailed and complete information on all UTM, RED and wireless features see the UTM Administration Guide. The information below is provided to help you with common configuration options, and to highlight important items which if not addressed could lead to longer configuration time or support issues. Our goal in providing this information is to guide you in proper configuration to reduce deployment time and increase customer satisfaction.

The UTM manual is available on the UTM itself via menu Support/Documentation or on our website:

http://www.sophos.com/en-us/medialibrary/PDFs/documentation/utm9106_manual_eng.pdf

The Sophos UTM provides initial installation wizards to help set common UTM features and to easily connect RED and wireless access points. It is recommended that these wizards are used on new installations as they often configure overlooked items such as masquerade rules which can prevent traffic from passing. The sections below include suggestions to help ensure a successful deployment, and to avoid common issues and misconfiguration.

### 3.2.1.Management

#### 3.2.1.1. System Settings>Hostname

It is suggested that a Fully Qualified Domain Name (FQDN) be used in this section, and if the UTM will be joined to a backend authentication service such as Active Directory (AD) this is a requirement. This hostname does not have to be a publicly resolvable name and if joining to an AD domain this hostname should match a configured DNS 'A' record in the internal Active Directory domain.

Best practice is to always enter a publically resolvable FQDN into the UTM host settings during the basic system setup. It ensures that all the CAs (VPN CA, WebAdmin CA) will include publically resolvable hostnames. The mail proxy will correctly answer requests, the Quarantine Manager and the SSL VPN  downloader hostname are also set up correctly and do not need to be changed manually afterwards. When the basic setup is done, it makes sense to change the system hostname to an internally resolvable FQDN – the one the UTM will have in the internal ActiveDirectory / DNS settings.

#### 3.2.1.2. System Settings>Time and Date

It is suggested that the local time and date settings are used to ensure that log files reflect the proper time settings to aid with administration and troubleshooting. If the UTM will be joined to a backend authentication service such as AD then the time/date settings on the UTM must match those used in the local domain.

#### 3.2.1.3. System Settings>Shell Access

Shell access is not needed for daily administration tasks but may be necessary or preferable for more advanced support. It is suggested that once enabled the default ‘Any’ network definition be changed to limit access to known networks. **Warning:** Any modifications done as the ‘root’ account will void your support.

#### 3.2.1.4. Licensing

All UTMs come with a 30 day evaluation license which unlocks all features. Once this license has expired only ‘Essential Firewall’ functionality will remain active, and access to the GUI will be denied until a valid license has been uploaded.

#### 3.2.1.5. Backup/Restore

UTM backup configuration files are automatically created on the UTM and available in the *Management>Backup/Restore* section of the WebAdmin GUI, are sent out to the default ‘admin’ email address, and can be stored on a SUM system. Backup files contain all UTM configuration details and can be used to easily restore settings to a new or re-imaged UTM. These backup files can be restored via the WebAdmin GUI, or via a standard USB key during the boot process.

The UTM also offers the option to create a backup that removes host specific information. This allows you the ability to create backup files containing basic configuration which can then be applied to multiple UTMs using the methods described above. Once applied these backup file types will display the initial setup wizard upon login which provides the opportunity to set site specific information such as hostname, WAN connection type, and local administrative information and passwords. This option may be useful if you need to pre-configure UTMs with certain settings for quick deployment on a customer site. For example: configure firewall rules, web filter policy, connection to SUM server, etc.

Sophos also offers a useful tool called a ‘Smart Installer’. This special USB stick emulates a USB CD-ROM drive and allows for easy installation of the UTM ISO image. A pre-installed software utility connects to the Sophos FTP site where updated images are stored and available for download. A second partition on the Smart Installer provides space to store a UTM configuration file which can then be used to re-apply all settings with a simple reboot.

http://www.sophos.com/en-us/support/knowledgebase/115187.aspx
http://www.sophos.com/en-us/support/utm-downloads/utm-smart-installer.aspx

#### 3.2.1.6. User Portal

The UTM user portal is used to provide email and remote VPN self-service options to end users.

http://www.sophos.com/en-us/support/knowledgebase/115157.aspx

#### 3.2.1.7. Notifications

UTM notifications can be sent via email and/or SNMP. Alerts can be used to notify administrators and/or partners about events, problems, or to create cases or log activity in many RMM and CRM systems.

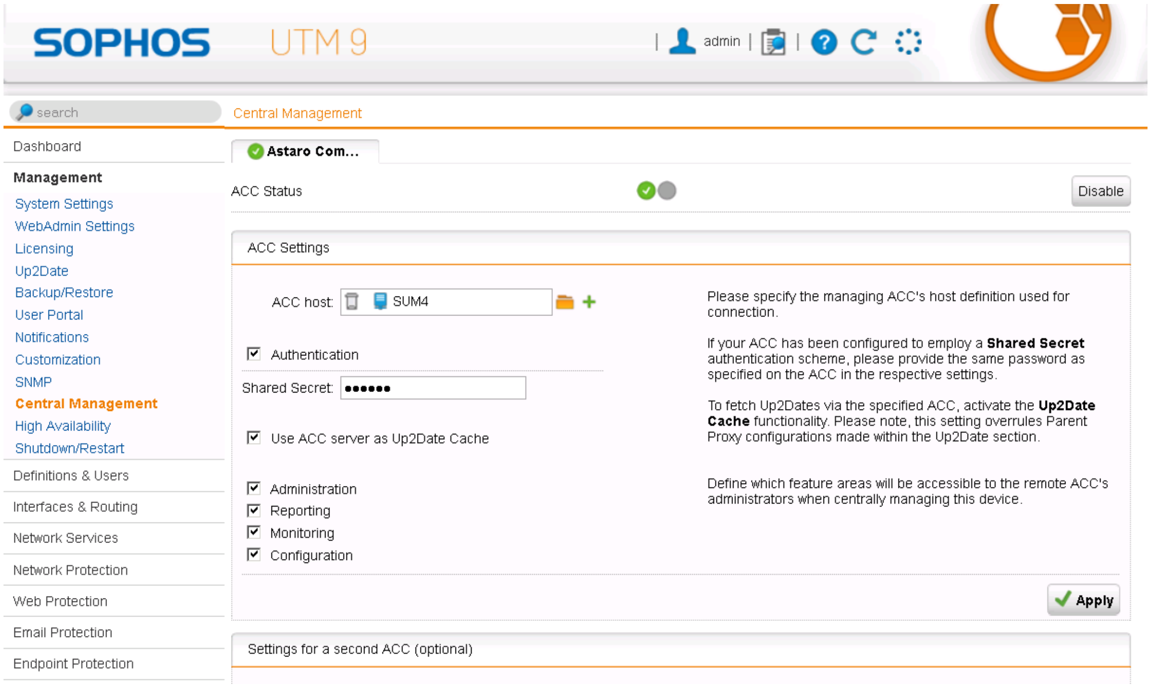
http://www.sophos.com/en-us/support/knowledgebase/119371.aspx

### 3.2.1.8. Central Management

All UTMs can be configured to connect to one or two SUM servers. Setup is simple and only a few pieces of information are needed such as the hostname or IP address of the SUM server, and a shared secret. Once connected the UTM will maintain contact with SUM and send updates on health and security events. The SUM server can also be used to 'push' policies to managed UTMs to simplify administration of multiple devices, and SUM also provides high level reporting information which is 'pulled' from connected devices.

Connections between a customer's UTM and a SUM server require a few configuration settings on each side. A customer's UTM simply needs to know where they are connecting to and the shared secret to use when registering with SUM. The SUM server must be configured to allow all connections, or connections only from specific networks. The SUM server must also have a matching shared secret which is shared across all connected UTMs. UTM details can be pre-configured as part of a UTM backup file so that once connected to the Internet they'll create a connection and register with the appropriate SUM server.

1. On UTM go to Management>Central Management and click 'Enable'
2. Create SUM network object (Host or DNS host) by clicking on the green + icon. This new object should be the public IP address used to connect to SUM, or the publicly resolvable hostname.
3. Click on the 'Authentication' checkbox and enter a shared secret which will be used to connect to the SUM server (this same shared secret will be entered on the SUM server.)
4. Choose which options are needed. Note that choosing the 'Use ACC server as Up2Date Cache' may result in increased bandwidth at the site hosting the SUM server.
5. Click 'Apply' to save.



Central Management

Astaro Com...

ACC Status ● ● Disable

ACC Settings

ACC host: SUM4

Please specify the managing ACC's host definition used for connection.

☑ Authentication

Shared Secret: ••••••

If your ACC has been configured to employ a **Shared Secret** authentication scheme, please provide the same password as specified on the ACC in the respective settings.

☑ Use ACC server as Up2Date Cache

To fetch Up2Dates via the specified ACC, activate the **Up2Date Cache** functionality. Please note, this setting overrules Parent Proxy configurations made within the Up2Date section.

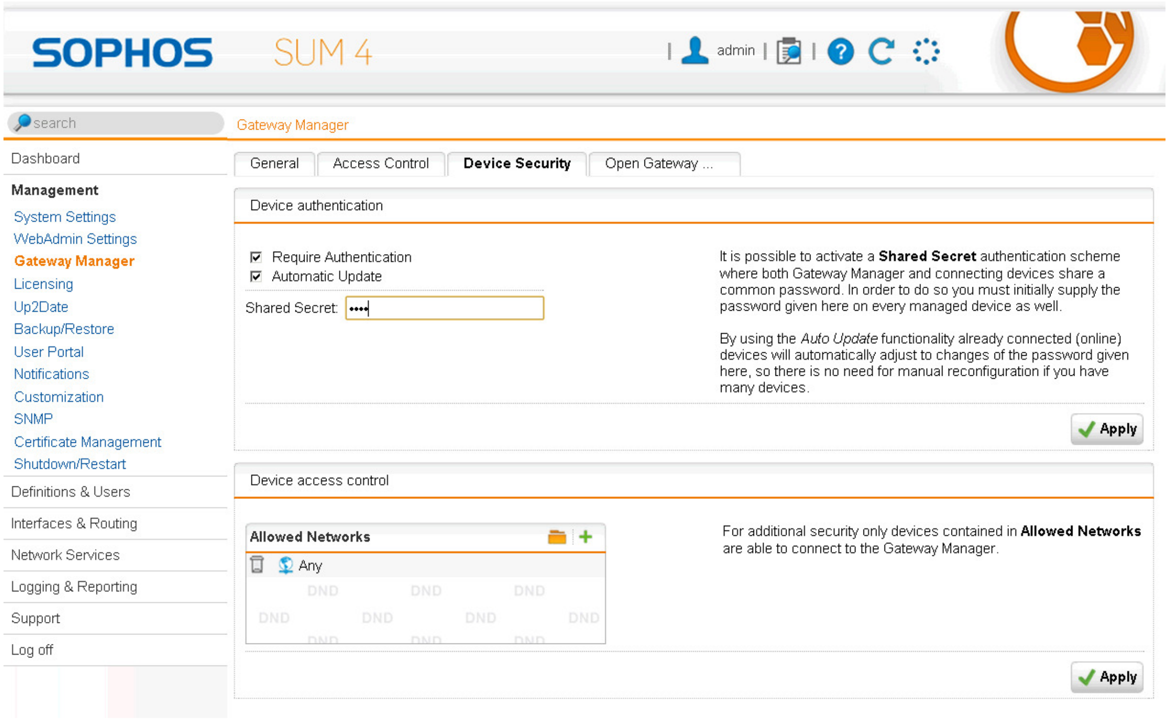
☑ Administration
☑ Reporting
☑ Monitoring
☑ Configuration

Define which feature areas will be accessible to the remote ACC's administrators when centrally managing this device.

✓ Apply

Settings for a second ACC (optional)

6. On the SUM server login to the WebAdmin GUI using port ‘4444’ and go to Management>Gateway Manager>Access Control section.
7. Configure the Allowed Administrators and Users that will manage the UTMs connected to SUM. Note that defining ‘Allowed Users’ provides more granular administrative permissions.
8. Configure the networks allowed to connect to the SUM server (the ‘Any’ network definition is often used here to allow Administration via the Internet).
9. Go to Management>Gateway Manager>Device Security section.
10. Click on the checkboxes for ‘Require Authentication’ and ‘Automatic Update’ and enter the shared secret configured on the UTM(s).
11. Add all networks UTMs will connect from in the ‘Allowed Networks’ section. Note that often the ‘Any’ network definition is used since UTMs may be connecting from Dynamic public IP’s.



Device authentication

☑ Require Authentication
☑ Automatic Update

Shared Secret: ••••

It is possible to activate a **Shared Secret** authentication scheme where both Gateway Manager and connecting devices share a common password. In order to do so you must initially supply the password given here on every managed device as well.

By using the *Auto Update* functionality already connected (online) devices will automatically adjust to changes of the password given here, so there is no need for manual reconfiguration if you have many devices.

Device access control

**Allowed Networks**

Any

For additional security only devices contained in **Allowed Networks** are able to connect to the Gateway Manager.

http://www.sophos.com/en-us/support/knowledgebase/2450/6700/6800/118580.aspx

### 3.2.1.9. High Availability

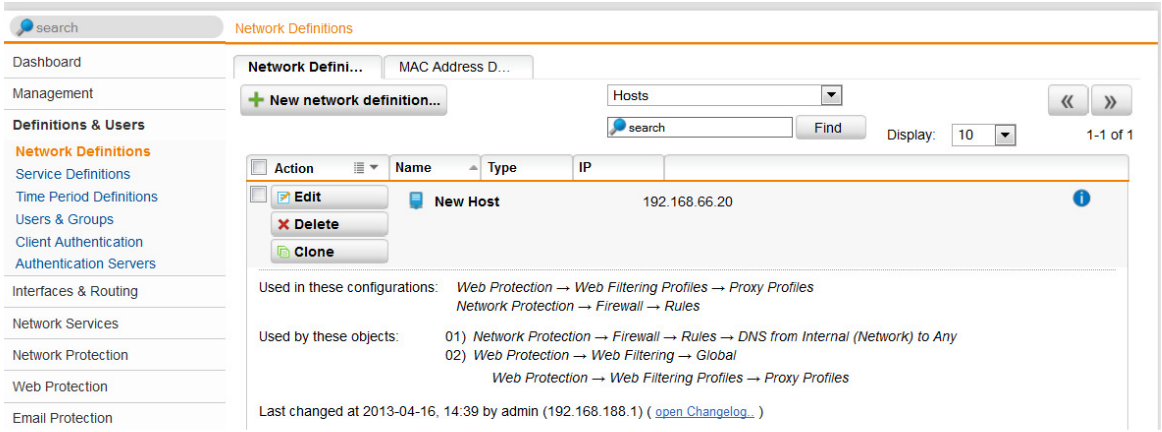
All Sophos UTMs offer both Active/Passive and Active/Active High availability (HA) options to help guard against a single point of failure. All nodes in an HA group must be either the same hardware appliance type (*UTM 220/UTM 220*) or use the same level of software/virtual license (*50 Protected IP's/50 Protected IP's*). UTM hardware appliances come pre-configured for Active/Passive failover with Eth3 configured as the dedicated HA port. Setup is as simple as configuring one UTM, and then connecting another UTM of the same model via the dedicated HA port (Eth3 on hardware UTMs).

The already configured UTM will sense the new unit, setup the HA connection and databases, and then configure the new unit to act as a mirrored device. The units will then use that dedicated connection to synchronize configuration settings, reports, and logs, and will use heartbeats to monitor connectivity. To change to Active/Active mode and add additional units you simply need to update your license to the reflect Active/Active cluster option, apply it to your primary UTM, and then change the HA mode in the High Availability>Configuration section. See the link below for detailed information on the HA feature set.

http://www.sophos.com/en-us/medialibrary/PDFs/documentation/asg_8_HA_deployment_geng.pdf

## 3.2.2. Definition & Users

The UTM uses a shared object database to ease administration and provide change tracking and control. Objects can be created on the UTM while configuring various items such as firewall rules, web policies, or VPN profiles, and once created can be used again in other policy settings. Changes to objects can be done from anywhere in the configuration that the object is used, or in the 'Definition & Users' section. Changes only need be made in once place and all changes are recorded for later review by clicking on the info Icon contained in a blue circle and located to the right of the object.



| ☐ Action | Name | Type | IP |
|---|---|---|---|
| ☐ | New Host | | 192.168.66.20 |

Used in these configurations: *Web Protection → Web Filtering Profiles → Proxy Profiles*
*Network Protection → Firewall → Rules*

Used by these objects: 01) *Network Protection → Firewall → Rules → DNS from Internal (Network) to Any*
02) *Web Protection → Web Filtering → Global*
*Web Protection → Web Filtering Profiles → Proxy Profiles*

Last changed at 2013-04-16, 14:39 by admin (192.168.188.1) ( open Changelog.. )

As of version 9.1 the Sophos UTM also allows administrators the ability to create 'Unified Host Objects' which combine DNS, DHCP, and MAC address information in a single object.

http://www.sophos.com/en-us/support/knowledgebase/119097.aspx

#### 3.2.2.1. Users & Groups

The UTM is set up with a single pre-configured user account (called 'admin') but allows you to create additional local or backend synced user objects for use in policies and/or administration. Note that the email address information is used to create a unique X.509 certificate and so each user object must use a unique email address. Check your 'admin' account object to ensure it is not using the same email address as another account you may want to use later.

#### 3.2.2.2. Client Authentication

The Sophos UTM provides an Authentication Agent (SAA) for both Windows and Mac OS X which allows users to authenticate directly with the UTM, and which allows the UTM to associate the user IP address with the username. This allows for rule creation by username, and also whenever possible replaces user IP addresses with the usernames in reports.

#### 3.2.2.3. Authentication Servers>Global

The 'Global' tab allows for the creation of user objects automatically when using a configured backend such as RADIUS or Active Directory. This is useful and necessary when providing VPN access to backend groups as each user needs a local user object on the UTM before they will be able to login to the User Portal.

#### 3.2.2.4. Authentication Servers>Servers

When configuring connections to backend servers such as Active Directory (AD) you can use the 'Test' buttons to confirm server credential settings, and to test backend user group membership. When configuring the 'BIND DN' section for use with AD you normally need to enter the full path to container that the 'Administrator' object is stored in. If using Windows 2008 R2 you can simplify this by using the syntax 'username@domain.com'. If not using Win2008 you can use a Windows tool called 'ADSIEDIT' to identify and then cut and paste the proper information needed. The information should look as follows: *CN=administrator,CN=Users,DC=example,DC=com*

Active Directory Troubleshooting KB Article
http://www.sophos.com/en-us/support/knowledgebase/115725.aspx

RADIUS configuration options KB Article
http://www.sophos.com/en-us/support/knowledgebase/115050.aspx

#### 3.2.2.5. Authentication Servers>Single Sign On

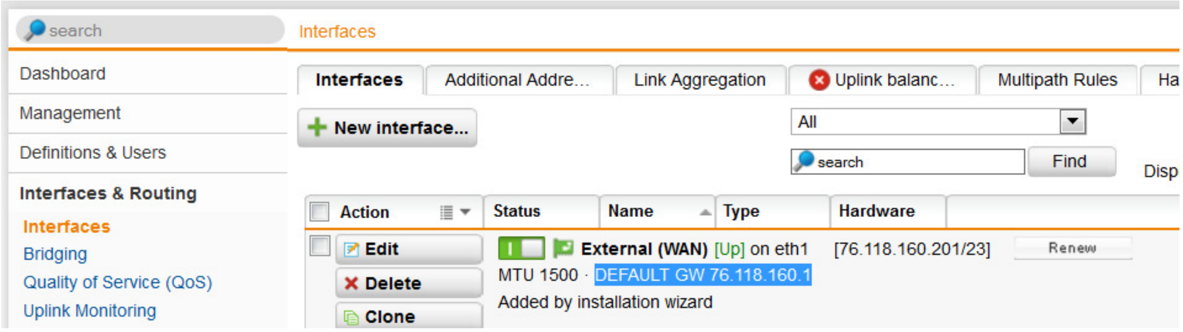
Single sign-on functionality is available for both Active Directory and eDirectory. With this functionality users logged into a domain workstation will have their credentials used to transparently authenticate them for Web access when used with the HTTP/S proxies.

http://www.sophos.com/en-us/support/knowledgebase/115659.aspx

### 3.2.3. Interface & Routing

The Sophos UTM offers support for commonly used Interface types including DLS, cable modem, VLAN, and offers support for both static and dynamic Ethernet connections. The 'Interface' section is also where the UTM default route is set which is defined on the 'WAN' interface as the 'Default GW'.

Once your interfaces are configured and a Default GW is assigned to your WAN, the UTM will know how to route to any directly connected networks, and to the Internet (via the Default GW). To route to any other networks such as internal subnets which are not directly connected to the UTM, additional routes must be configured using either static or dynamic routing.



External (WAN) [Up] on eth1 [76.118.160.201/23]
MTU 1500 · DEFAULT GW 76.118.160.1
Added by installation wizard

http://www.sophos.com/en-us/support/knowledgebase/118899.aspx

The uplink balancing functionality allows you to configure up to 32 interfaces of any type with their own default gateways. Normally only one default gateway is allowed on a UTM but once uplink balancing is enabled you can configure as many as you need, and the UTM will create routing tables for each interface. This allows you to group your interfaces together for failover and load balancing of outbound traffic. Grouped interfaced are represented by a dynamic interface object called 'Uplink Interfaces'. This object can be used in firewall rules, or to provide inbound traffic a single connection point to avoid issues when a single WAN is unavailable. This is done by configuring a dynamic DNS hostname on the UTM which is then linked to the Uplink Interfaces. See the Network>DNS section for information on configuring this feature, and the article link below for a detailed description of uplink balancing.

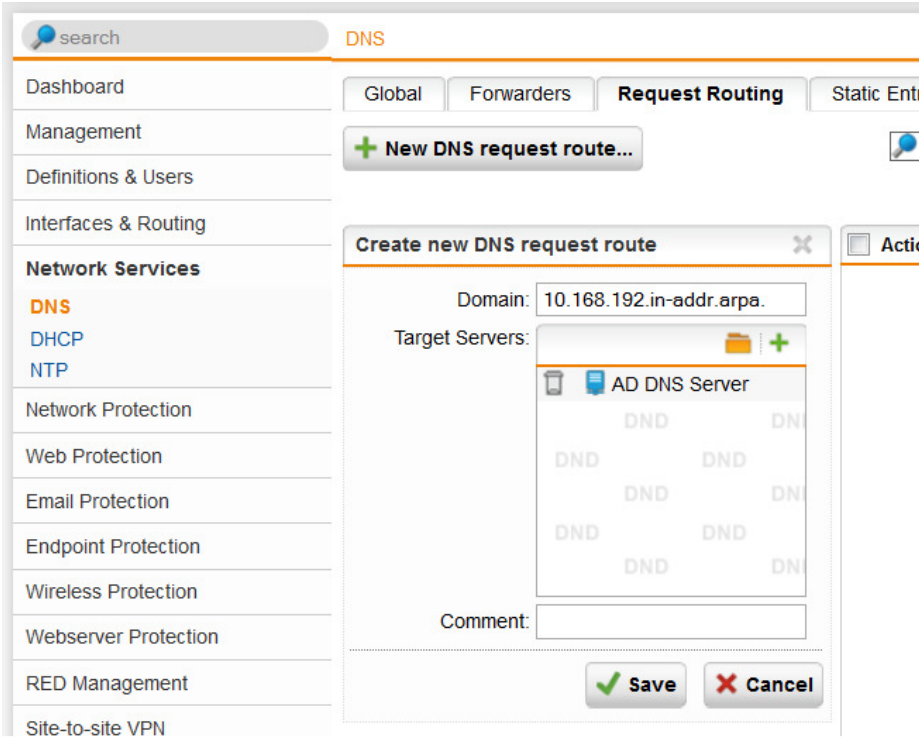
http://www.sophos.com/en-us/support/knowledgebase/118457.aspx

## 3.2.4. Network Services

### 3.2.4.1. DNS

To enhance reporting details a RDNS request route can be configured when the UTM is connected to a backend domain such as AD. The below example would provide reverse lookups for the 192.168.10.0 network. This would allow the UTM to display machine names in reports and dashboards which can be more useful than IP addresses.

DNS static entries can be used to ensure that internal devices with both public and private hostname are reachable by internal users using the UTM Web proxy. Simply configure a static entry which points to the Internal IP address of the device. Usage examples include web servers which are not resolving when using the Web Protection HTTP/S proxy features.



Create new DNS request route

Domain: 10.168.192.in-addr.arpa

Target Servers: AD DNS Server

Comment:

DynDNS hostnames are very useful for ensuring inbound connections such as VPN's do not need to be changed if a WAN address or interface changes. DynDNS hostnames can be configured to work with one or more WAN interfaces and the built-in client will allow the UTM to update dynamic DNS records when it registers a change of some type (e.g., IP address change, or failover from one WAN to another). See the article link below for information on configuring DNS static entries and dynamic DNS hostnames.

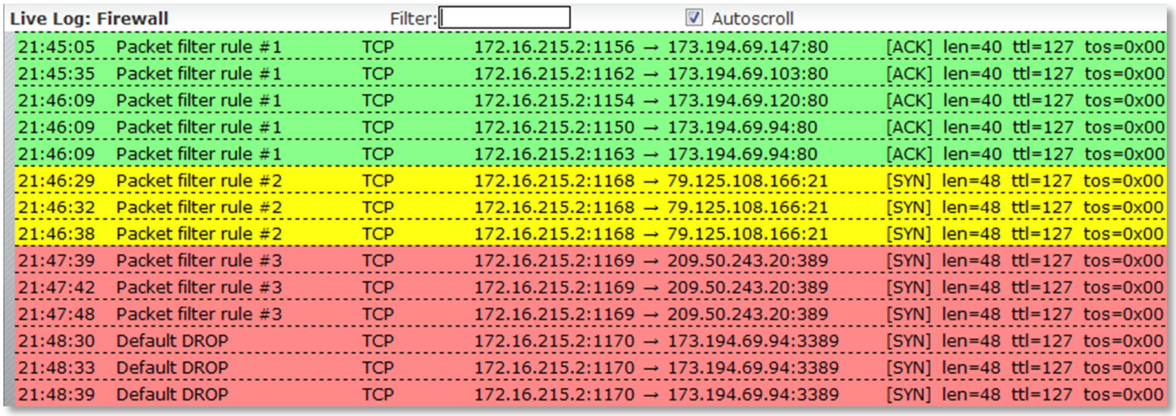
http://www.sophos.com/en-us/support/knowledgebase/115146.aspx

## 3.2.5. Network Protection

### 3.2.5.1. Firewall

The Network Protection section provides firewall, IPS (intrusion prevention system), server load balancing, VoIP and additional (advanced) proxy options. Global ICMP options are also controlled in this section and depending on the options chosen during the initial setup wizard, these settings may interfere with ICMP traffic often used for testing connectivity. Global ICMP settings override any specific rules created in the firewall section, and these settings do not log. To create specific ICMP rules or to turn off these settings simply uncheck the options on this tab and then create ICMP rules in the Firewall section.

The Firewall 'Live Log' is a very useful tool which can be used to troubleshoot connections and which can be used when creating firewall rules. This live log is color coded and provides a filter so that you can easily see dropped traffic.



Live Log: Firewall Filter: ☑ Autoscroll

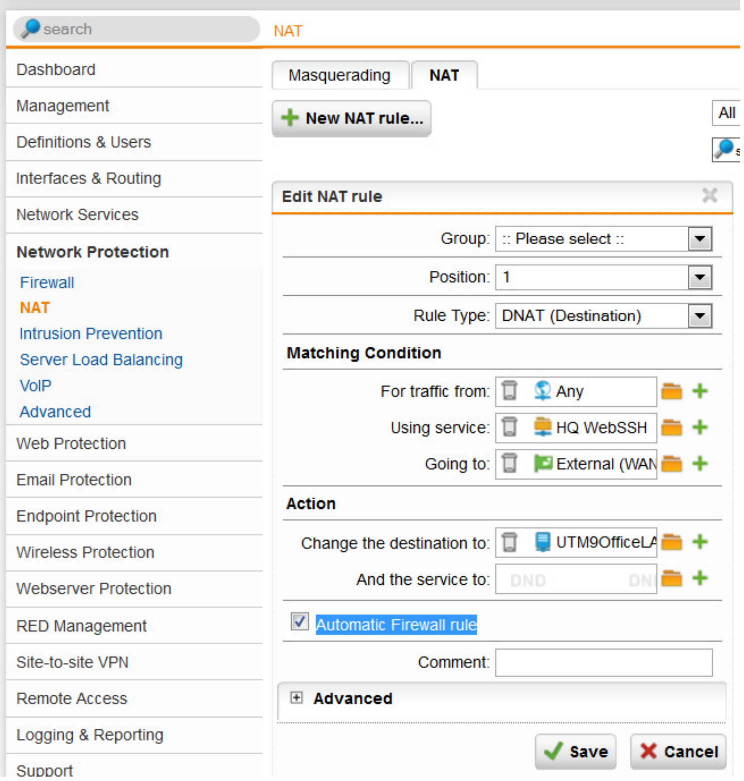
```
21:45:05  Packet filter rule #1  TCP  172.16.215.2:1156 → 173.194.69.147:80   [ACK] len=40 ttl=127 tos=0x00
21:45:35  Packet filter rule #1  TCP  172.16.215.2:1162 → 173.194.69.103:80   [ACK] len=40 ttl=127 tos=0x00
21:46:09  Packet filter rule #1  TCP  172.16.215.2:1154 → 173.194.69.120:80   [ACK] len=40 ttl=127 tos=0x00
21:46:09  Packet filter rule #1  TCP  172.16.215.2:1150 → 173.194.69.94:80    [ACK] len=40 ttl=127 tos=0x00
21:46:09  Packet filter rule #1  TCP  172.16.215.2:1163 → 173.194.69.94:80    [ACK] len=40 ttl=127 tos=0x00
21:46:29  Packet filter rule #2  TCP  172.16.215.2:1168 → 79.125.108.166:21   [SYN] len=48 ttl=127 tos=0x00
21:46:32  Packet filter rule #2  TCP  172.16.215.2:1168 → 79.125.108.166:21   [SYN] len=48 ttl=127 tos=0x00
21:46:38  Packet filter rule #2  TCP  172.16.215.2:1168 → 79.125.108.166:21   [SYN] len=48 ttl=127 tos=0x00
21:47:39  Packet filter rule #3  TCP  172.16.215.2:1169 → 209.50.243.20:389   [SYN] len=48 ttl=127 tos=0x00
21:47:42  Packet filter rule #3  TCP  172.16.215.2:1169 → 209.50.243.20:389   [SYN] len=48 ttl=127 tos=0x00
21:47:48  Packet filter rule #3  TCP  172.16.215.2:1169 → 209.50.243.20:389   [SYN] len=48 ttl=127 tos=0x00
21:48:30  Default DROP           TCP  172.16.215.2:1170 → 173.194.69.94:3389  [SYN] len=48 ttl=127 tos=0x00
21:48:33  Default DROP           TCP  172.16.215.2:1170 → 173.194.69.94:3389  [SYN] len=48 ttl=127 tos=0x00
21:48:39  Default DROP           TCP  172.16.215.2:1170 → 173.194.69.94:3389  [SYN] len=48 ttl=127 tos=0x00
```

http://www.sophos.com/en-us/support/knowledgebase/2450/2750/4350/115155.aspx

### 3.2.5.2. NAT

The Sophos UTM offers more than one type of NAT, but one of the most commonly used beside Masquerading is DNAT which is also referred to as 'port forwarding'. DNAT translates the destination of inbound traffic and is useful when setting up access to internal resources from untrusted networks and the Internet. The below article discusses how to setup DNAT, and one thing to note is that DNAT takes place before firewall rules are applied. Therefore it is always suggested that the 'Automatic Firewall Rule' option be used.

http://www.sophos.com/en-us/support/knowledgebase/115145.aspx



Edit NAT rule

Group: :: Please select ::

Position: 1

Rule Type: DNAT (Destination)

Matching Condition

For traffic from: Any

Using service: HQ WebSSH

Going to: External (WAN

Action

Change the destination to: UTM9OfficeLA

And the service to: DND

☑ Automatic Firewall rule

Comment:

⊞ Advanced

Masquerading rules are used to ‘hide’ networks behind a UTM Interface IP and are required so that internal network traffic can be routed to the public Internet. This type of NAT is used to ‘hide’ private networks behind the UTM public IP assigned to the WAN interface, but it can also be useful when using Remote VPN options. Remote VPN users that connect using one of the available clients will receive an IP address from a pre-defined VPN DHCP pool. These addresses will not be recognized and routed properly on networks that are not directly connected to the UTM. To avoid having to create new routes a masquerade rule can be used to ‘hide’ the VPN pool network behind the UTM Internal Interface.

See the below link for more useful articles on both firewall and NAT functionality.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/2750/4350.aspx

#### 3.2.5.3. IPS

The UTM IPS is an essential tool for protecting your networks, but in some cases it may block legitimate traffic. The IPS has a live log which can be used to troubleshoot issues and the below links discuss initial setup of the IPS, and the TCP flood detection feature. IPS can influence the throughput of the UTM – please use the optimization options in the IPS menu under Advanced/Performance Tuning and think about changing the rule age for IPS patterns to a smaller value (menu Attack Patterns).

http://www.sophos.com/en-us/support/knowledgebase/b/2450/2750/4400.aspx

### 3.2.6. Web Protection

This subscription offers many features useful to organizations that are looking to control and report on web usage, while protecting users against common web based threats. Web Filtering profiles provide different levels of access to certain users, groups, or networks and can be combined with backend authentication servers such as AD to offer Single Sign-on functionality. This allows for greater flexibility when creating web usage rules, and when using authentication reports will show usernames instead of just IP addresses. If using AD SSO or another type of backend authentication, it’s often useful to also have a ‘Transparent Mode’ web surfing profile configured as a fallback profile. This will ensure that all traffic is scanned even if authentication is not used and can be used for guest access and/or BYOD (bring your own device) which may not use authentication. The link below contains a number of useful articles on configuring features of the UTM Web Protection subscription.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/2800.aspx

### 3.2.7. Email Protection

See the below link which discuss setting up SMTP Profiles, configuring POP3 Transparent scanning, the UTM encryption capabilities.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/2850.aspx

### 3.2.8. Endpoint Protection

The Sophos Endpoint Protection agent protects Windows-based machines both on and off the network to ensure that policies are enforced for AV and web usage, and to ensure that data is controlled through device control settings. See the below link which discuss setting up features related to the UTM Endpoint Protection subscription.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/2900.aspx

### 3.2.9. Wireless Protection

This subscription connects the plug and play Access Points (APs) to the UTM so that wireless networks and users can be protected with the same policies in place for wired networks. As multiple SSIDs are supported it is suggested that separate networks be configured for staff versus guest users. Staff networks may take advantage of backend authentication via RADIUS which means that already configured user policies can be used without additional configuration. Guest traffic can be isolated on its own network, and conditions can be put in place to control these users and ensure compliance with usage policies. See the below links which discuss setting up wireless networks, configuring Hotspots, and for authenticating wireless users against Active Directory via RADIUS.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/2950.aspx
http://www.sophos.com/en-us/support/knowledgebase/116144.aspx

### 3.2.10. Web Server Protection

Web-facing servers such as web servers or Outlook Web Access (OWA) servers are often overlooked when designing perimeter security. Attackers know this and often look for these servers when trying to gain access to an organizations network. This subscription is designed to easily protect these vulnerable servers and their applications using a combination of tools such as inbound scanning, SSL offloading, and reputation checking. The link below contains useful articles on configuring and using these features.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/3000.aspx

### 3.2.11. RED Management

Sophos RED is the easiest and most cost effective branch office connectivity solution available. RED devices require no direct configuration and instead simply download their settings from the Sophos Cloud based provisioning service. This is done using TCP/UDP ports 3400 and 3410, and though this port is normally allowed through most security devices it may occasionally be blocked. The below link is to the RED technical guide which discusses how to troubleshoot connectivity issues and provides links to a testing application.

http://www.sophos.com/en-us/support/knowledgebase/116573.aspx

The link below contains a number of useful RED articles including explanation of blink codes, and using a UTM Wireless Access Point behind a RED device.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/3050/5200.aspx

### 3.2.12.Site-to-site VPN

The Sophos UTM offers site-to-site VPN connectivity options including IPsec. IPsec tunnels can be easily created using pre-configured policies and best practice settings, and then connected to any other IPsec compatible device.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/3100/5250.aspx

### 3.2.13.Remote Access

The six remote access VPN options included provide support for different types of devices and are designed to ease administration by empowering users. The link below discusses options such as the clientless HTML5 VPN portal, and address issues and questions related to the SSL, PPTP, L2TP, and IPsec options.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/3100/5300.aspx

### 3.2.14.Logging & Reporting

The UTM 'Logging & Reporting' section contains both daily as well as historical reporting information which can be used by administrators to gain a better understanding of their network and associated traffic. Detailed logs can be used for troubleshooting and to aid administration while graphical reports can be used to provide visibility into the health of the network, and to identify traffic and usage patterns.

http://www.sophos.com/en-us/support/knowledgebase/2450/6000/115804.aspx

### 3.2.15.Support Section

The 'Support' section contains useful information such as the full Administrator Guide, an option to generate a printable configuration, tools to help with network troubleshooting such as ping, traceroute, and DNS lookup, and an 'Advanced' area where you can view shell level information such as the UTM process list and routes table. See the link below for articles related to this section.

http://www.sophos.com/en-us/support/knowledgebase/b/2450/3200.aspx

# 4. Legal Notices

Please send your suggestions for document improvements to lutz.linzenmeier@sophos.com.