SOPHOS

Cybersecurity made simple.

Sophos UTM

Administration Guide

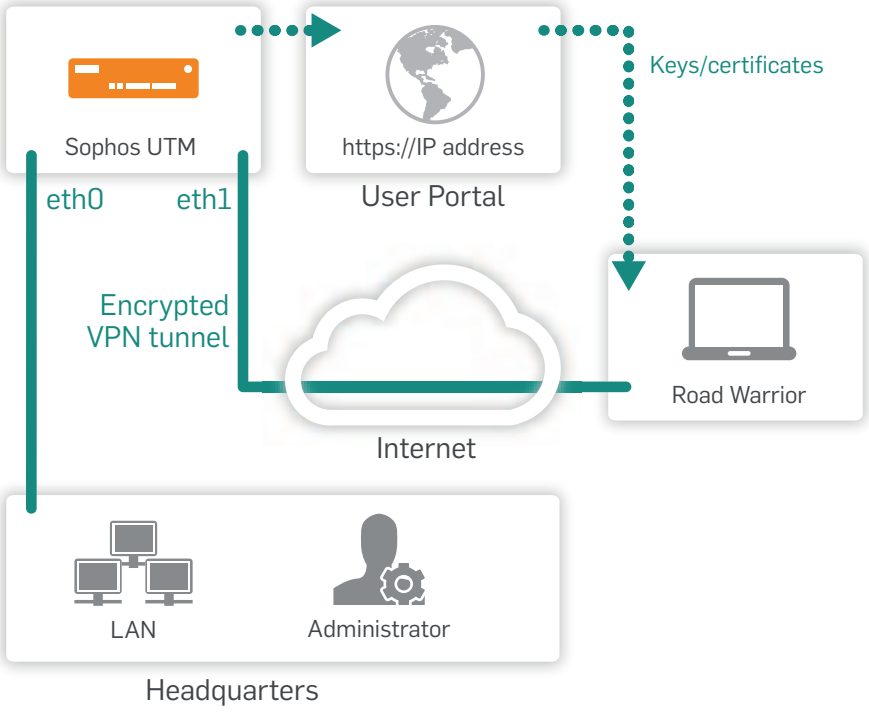
Product version: 9.600

Document date: Monday, December 10, 2018

Contents

1 Introduction

This guide describes step by step the configuration of a remote access to the UTM by using L2TP over IPsec. L2TP over IPsec is a combination of the Layer 2 Tunneling Protocol and of the IPsec standard protocol. L2TP over IPsec allows you, while providing the same functions as PPTP, to give individual hosts access to your network through an encrypted IPsec tunnel. The structure is described in the following chart. On Microsoft Windows systems, L2TP over IPsec is easy to set-up, and requires no special client software.



First, the system administrator configures the Sophos UTM to allow remote access. Additionally he enables the User Portal of the Sophos UTM for the remote access users.

The User Portal offers the necessary keys and a configuration guide to the remote access user. Login data for the User Portal should be provided by the system administrator.

Additional information

This guide contains complementary information on the Administration Guide and the Online Help. If you are not sure whether you have the current version of this guide, you can download it from the following Internet address:

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

If you have questions or find errors in the guide, please, contact us under the following e-mail address:

nsg-docu@sophos.com

For further help use our support forum under ...

http://www.astaro.org

... or our knowledgebase under ...

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

... or use the Sophos support offers:

http://www.sophos.com/en-us/support/contact-support/utm-support.aspx

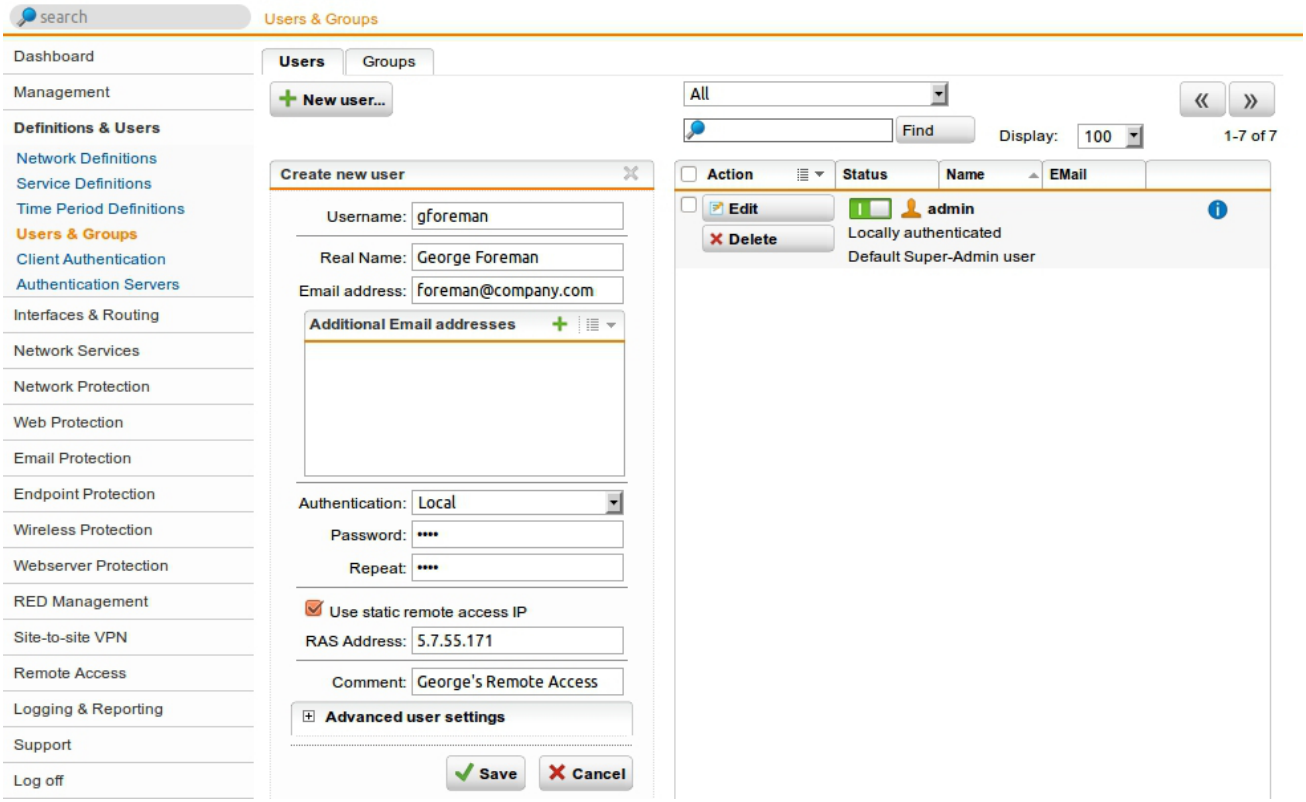
2 Configuring UTM

The UTM is configured via the web-based WebAdmin configuration tool from the administration PC. Opening and using this configuration tool is extensively described in the UTM administration guide.

2.1 Defining a User Account

First, you need to create a user account which is necessary for accessing the User Portal and for actually using the VPN connection.

1. **Open the *Definitions & Users* > *Users & Groups* > *Users* tab.**
2. **Click the *New User* button.**
   The *Create New User* dialog box opens.



3. **Make the following settings:**
   Username: Enter a specific username (e.g., `gforeman`). In doing so remember that the remote user will need this username later to log in to the User Portal.

   Real name: Enter the full name of the remote user (e.g., `George Foreman`).

Email address: Enter the e-mail address of the user. When you specify an e-mail address, an X.509 certificate for this user will be generated automatically while creating the user account, using the e-mail address as the certificate's VPN ID. The cer-

tificate will be displayed on the *Remote Access* > *Certificate Management* > *Certificates* tab.

Authentication: For the remote access via L2TP over IPsec the *Local* and *RADIUS* authentication methods are supported. With the *Local* authentication method the following two fields will be displayed for the definition of the password.

- **Password:** Enter the password for the user. In doing so remember that the remote user will need this password later to log in to the User Portal.
- **Repeat:** Confirm the password.

Use static remote access IP (optional): Each remote access user can be assigned to a specific IP address. The assigned IP address must not originate from the *IP address pool* used in the remote access settings (see below). During the dial-up the address is automatically assigned to the host. Enter the static IP address in the *RAS address* box.

Comment (optional): Enter a description or additional information on the user.

4. **Click *Save*.**
   Your settings will be saved.

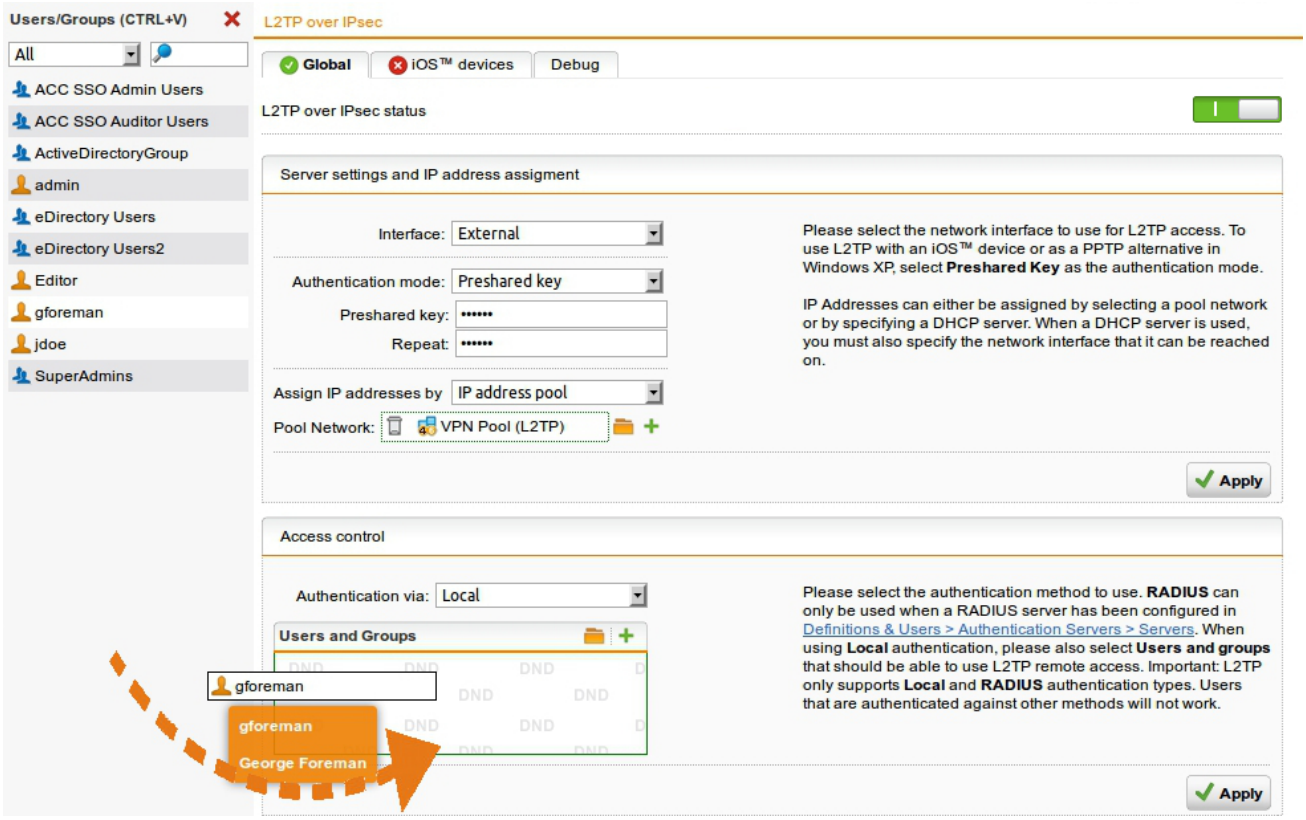
Cross Reference – More detailed information on the configuration of a user account and detailed explanations of the individual settings can be found in the UTM administration guide in chapter *Definitions & Users*.

2.2 Configuring L2TP Settings

This chapter describes how to enable L2TP, configuring basic settings and access control.

1. **Open the *Remote Access* > *L2TP over IPsec* > *Global* tab.**
2. **Enable L2TP over IPsec.**
   Enable L2TP over IPsec remote access by clicking the *Enable* button.

   The toggle switch turns amber and the page becomes editable.



2.2.1 Server Settings and IP Address Management

1. **In the *Server Settings and IP Address Management* section, make the following settings:**
   Interface: Select the network interface to use for L2TP access.

   Note – If you use uplink balancing, only the primary interface that is up will be used for L2TP traffic.

   Authentication mode: L2TP over IPsec remote access supports authentication based on *Preshared keys* or *X.509 CA check*:

   - **Preshared key**

     With this method you can use *L2TP over IPsec* as an easy PPTP alternative in Windows XP.

     Preshared key: Enter the shared secret. This shared secret is a secure phrase or password that is used to set up a secure tunnel.

     Repeat: Confirm the shared secret.

     Security Note – Use a secure password! Your name spelled backwards is, for example, not a secure password–while something like xfT35!4z would be. Ensure that this password does not fall into the hands of unauthorized third

parties. With this password, an attacker can build a connection to the internal network. We recommend changing this password at regular intervals.

- **X.509 CA check**

  Certificate: Select the local X.509 certificate to authenticate the server.

Assign IP addresses by: The IP addresses can either be assigned from a predefined IP address pool during the dial-up or can be automatically requested from a DHCP server.

- **IP address pool**

  Pool network: The default settings assign addresses from the private IP space 10.242.3.x/24. This network is called the *VPN Pool (L2TP)*. If you wish to use a different network, simply change the definition of the *VPN Pool (L2TP)* on the *Definitions & Users* > *Network Definitions* page. Alternatively, you can create another IP address pool by clicking the Plus icon.

  Note – If you wish the L2TP-connected users to be allowed to access the Internet, you additionally need to define appropriate Masquerading or NAT rules.

- **DHCP server**

  DHCP server: Select the DHCP server here. Please note that the local DHCP server is not supported. The DHCP server to be specified here must be running on a physically different system. Clicking the Folder icon opens a list that displays all networks and hosts that had been defined on the *Definitions & Users* > *Network Definitions* page.

  Via interface: Define the network card through which the DHCP server is connected. Note that the DHCP does not have to be directly connected to the interface–it can also be accessed through a router.

2. **Click *Apply* to save your settings.**
   The toggle switch turns green. L2TP over IPsec is active now.

2.2.2 Access Control

L2TP remote access supports *Local* and *RADIUS* authentication. For users using other authentication methods remote access will not work. For local users, UTM supports the authentication protocols MS-CHAPv2 and PAP (local authentication). By default, a MS Windows client negotiates MS-CHAPv2.

You can use RADIUS authentication, if you have defined a RADIUS server on the *Definitions & Users* > *Authentication Servers* > *Servers* tab. In conjunction with RADIUS authentication, UTM supports the authentication protocols MS-CHAPv2, MS-CHAP, CHAP, and PAP. The authentication requests are forwarded to the RADIUS server. The

L2TP module sends the following string as NAS-ID to the RADIUS server: `l2tp`. The authentication algorithm gets automatically negotiated between client and server.

Cross Reference – The configuration of the Microsoft IAS RADIUS server and the configuration of RADIUS within WebAdmin is described in the UTM administration guide in chapter *Definitions & Users*.

1. **In the *Access Control* section, select an authentication method.**
   Authentication via: Select the authentication method.

   Users and groups: When using *Local* authentication, please also select the users and groups that should be able to use L2TP remote access.
2. **Click *Apply* to save your settings.**

Cross Reference – More detailed information on the configuration of a remote access and detailed explanations of the individual settings can be found in the UTM administration guide in chapter *Remote Access*.

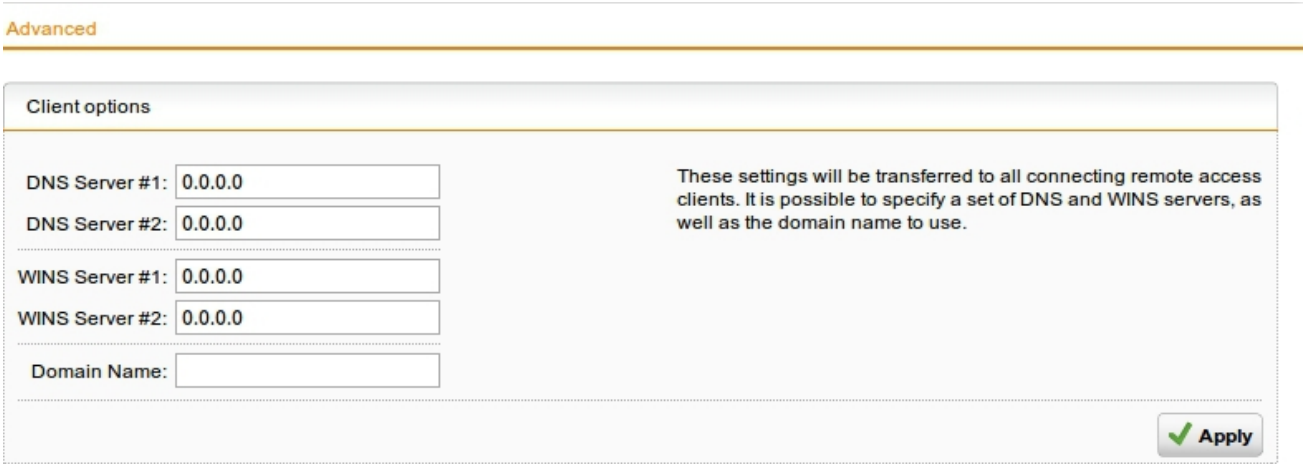
2.3 Configuring Advanced L2TP Settings

1. **Open the *Remote Access* > *L2TP over IPsec* > *Debug* tab.**
   The options on this page control how much debug output is generated in the log file. Select relevant options if you encounter connection problems and need detailed information about the negotiation of client parameters.

   In the *IKE Debugging* section, there are the following options available:

   - **Control Flow:** Displays control messages of IKE state
   - **Outbound Packets:** Displays content of outgoing IKE messages
   - **Inbound Packets:** Displays content of incoming IKE messages
   - **Kernel Messaging:** Displays communication messages with the Kernel
   - **High Availability:** Displays communication with other HA nodes

   In the *L2TP Debugging* section, if you select *Enable debug mode*, the IPsec VPN log file contains extended information about L2TP or PPP connection negotiation.
2. **Click *Apply* to save your settings.**
3. **Open the *Remote Access* > *Advanced* page.**
   This page allows you to define name servers (DNS and WINS) and the name service domain, which should be assigned to hosts during the connection establishment.

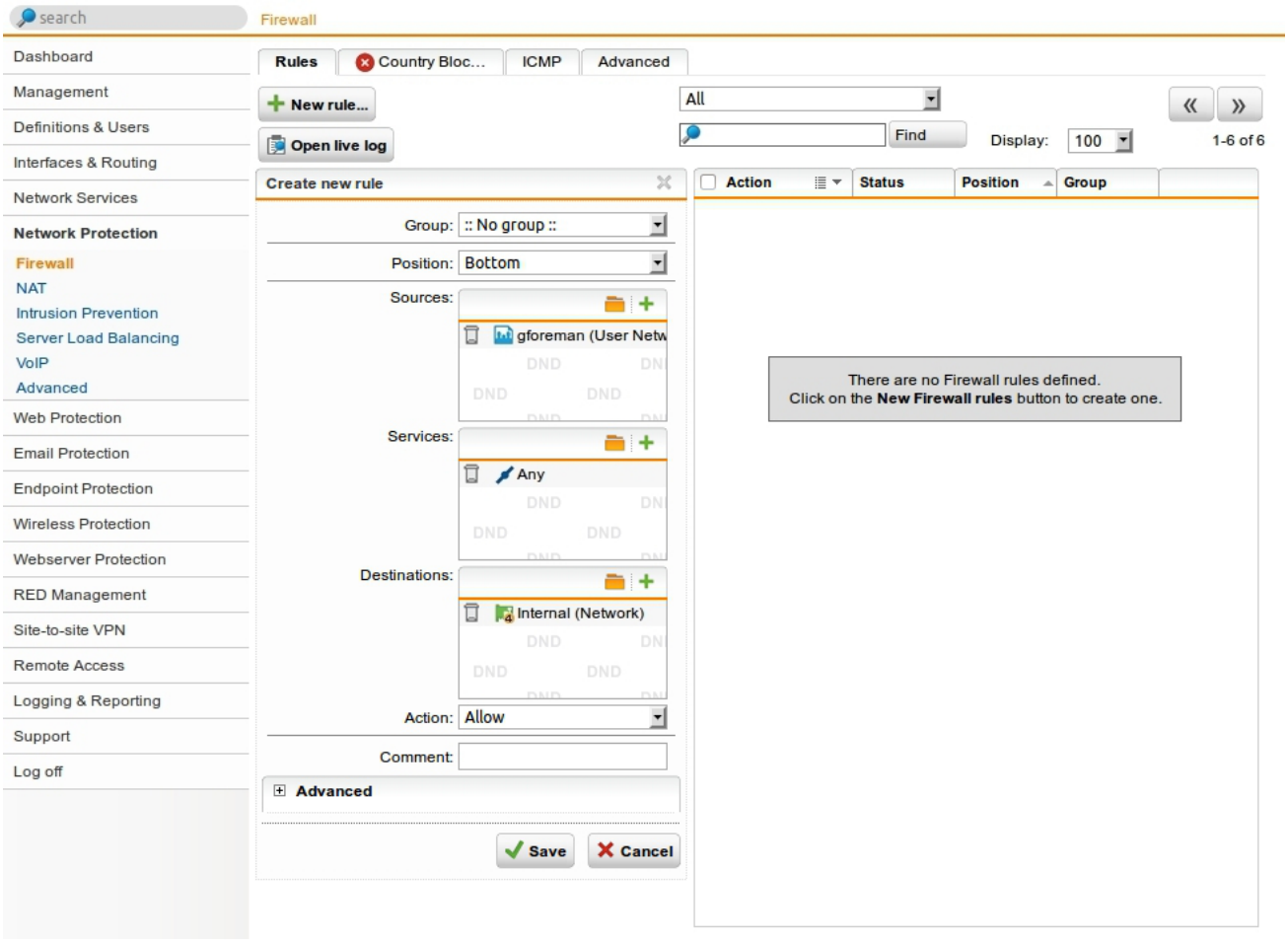


4. Click *Apply* to save your settings.

2.4 Creating Firewall and Masquerading Rules

2.4.1 Defining a Firewall Rule

1. Open the *Network Protection* > *Firewall* > *Rules* tab.
2. Click the *New Rule* button.
   The dialog box *Create New Rule* opens.



3. **Make the following settings:**
   Sources: Add the remote host or user (in this example: *gforeman*).

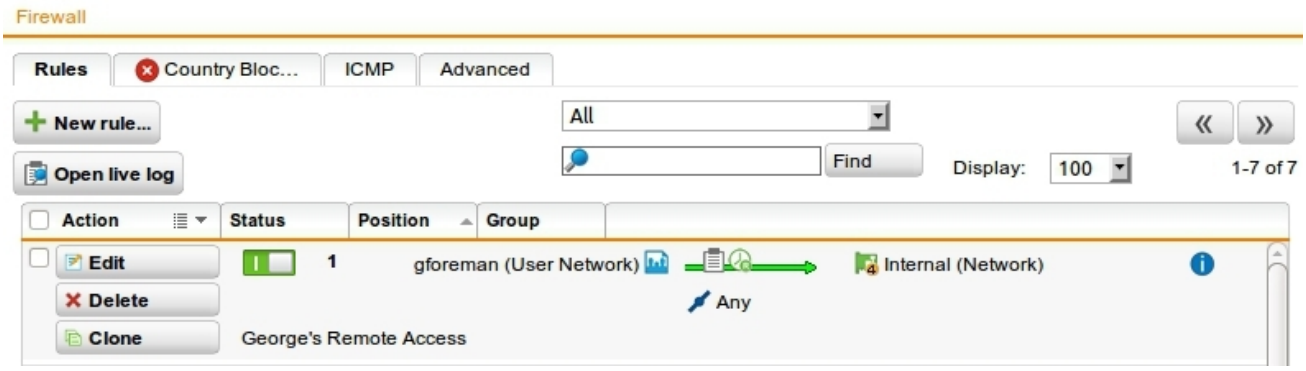
   Services: Add the allowed services.

   Destinations: Add the allowed networks (in this example: *Internal (Network)*). For the remote user to be able to access Internet you should e.g. select the *Internet* or *Any* network definition.

   Action: Select *Allow*.

4. **Click *Save*.**
   The new firewall rule is added to the list and remains disabled (toggle switch shows gray).

5. **Enable the rule by clicking the toggle switch.**
   The toggle switch turns green.



Security Note – Active rules are processed in the order of the numbers (next to the toggle switch) until the first matching rule. Then the following rules will be ignored! The sequence of the rules is thus very important. Therefore never place a rule such as *Any – Any – Any – Allow* at the beginning of the rules since all traffic will be allowed through and the following rules ignored.

Cross Reference – More detailed information on the definition of Firewall rules and detailed explanations of the individual settings can be found in the UTM administration guide in chapter *Network Protection*.

2.4.2 Defining a Masquerading Rule

Note – This is an optional step depending on your environment.

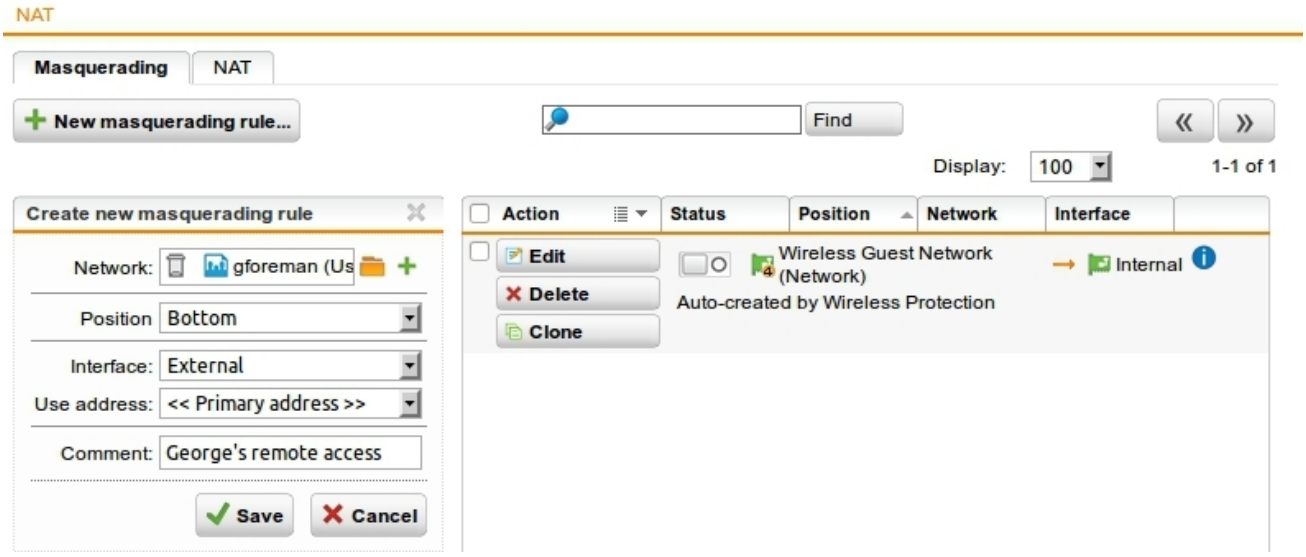
Masquerading is used to mask the IP addresses of one network (in this example: *gforeman*) with the IP address of a second network (e.g. *External*). Thus remote users who have only private IP addresses can e.g. surf on the Internet with an official IP address. Depending on your system configuration masquerading can also be necessary for other connection types.

1. **Open the *Network Protection* > *NAT* > *Masquerading* tab.**
2. **Click the *New Masquerading Rule* button.**
3. **Make the following settings:**
   Network: Select the network of the remote endpoint (in this example: *gforeman*).

   Interface: Select the interface that should be used to mask the clients (in this example: *External*).

   Use address: If the interface you selected has more than one IP address assigned, you can define here which IP address is to be used for masquerading.
4. **Click *Save*.**
   Your settings will be saved.

The new masquerading rule is added at the end of the list and remains disabled (toggle switch shows gray).



5. **Enable the rule by clicking the toggle switch.**
   The toggle switch turns green.

Cross Reference – More detailed information on the definition of masquerading rules and detailed explanations of the individual settings can be found in the UTM administration guide in chapter *Network Services*.

6. **Optionally, activate the proxies:**
   If the remote employees should access URL services via the remote access you may configure the required proxies on the UTM – this would be the DNS and HTTP proxy for example.

   Cross Reference – More detailed information on the configuration of proxies and detailed explanations of the individual settings can be found in the UTM administration guide.

7. **Open the *Management* > *User Portal* > *Global* tab.**
   The User Portal needs to be activated for the remote access user.

   If the toggle switch is gray, click the *Enable* button to enable the User Portal.

8. **Select the networks that are allowed to access the User Portal.**
   To the *Allowed networks* box, add the networks that should be allowed to access the User Portal (in this example: *Any* or the respective *VPN Pool*, or just *gforeman*).

   Cross Reference – More detailed information on the configuration of the User Portal and detailed explanations of the individual settings can be found in the UTM administration guide in chapter *Management*.

After configuring the VPN server (headquarter) you need to configure the road warrior. Depending on the security policy of your organization and the requirements of your network, you might have to make additional settings.

3 Configuring the Remote Client

To be able to access the UTM via L2TP over IPsec VPN, you need to configure your remote computer. To do so, access the UTM User Portal with a browser on the remote client. There, the necessary installation instructions and the preshared key or the certificate are available for download. Then you configure the VPN connection on Windows.

3.1 Getting a Preshared Key or Certificate

The UTM User Portal is available to all remote access users. From this portal, you can download guides and tools for the configuration of your client. You should get the following user credentials for the User Portal from your system administrator: IP address, username, and password.

Especially for the L2TP remote access with authentication based on *Preshared key*, the User Portal offers the shared secret. For authentication with *X.509 certificate*, the User Portal offers the necessary certificate.

1. **Start your browser and open the User Portal.**
   Start your browser and enter the management address of the User Portal as follows: `https://IP address` (example: `https://218.93.117.220`).

   A security note will be displayed.

   Accept the security note. Depending on the browser, click *I Understand the Risks* > *Add Exception* > *Confirm Security Exception* (Mozilla Firefox), or *Proceed Anyway* (Google Chrome), or *Continue to this website* (Microsoft Internet Explorer).

2. **Log in to the User Portal.**
   Enter your credentials:

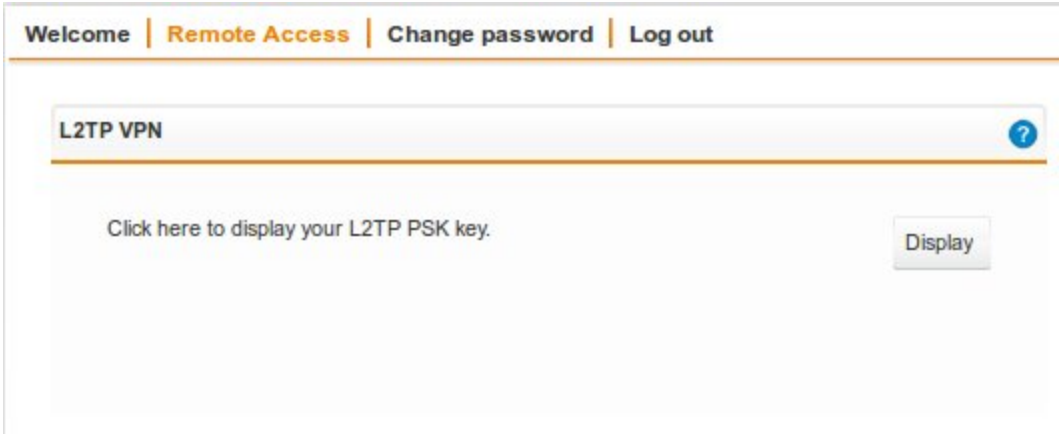
   Username: Your username, which you received from the administrator.

   Password: Your password, which you received from the administrator. Please note that passwords are case-sensitive.

   Click *Login*.

3. **On the *Remote Access* page, download the tools and/or configuration guide for setting up your remote access connection.**
   This page can contain up to five sections, depending on the remote access connection types (IPsec, SSL, L2TP, PPTP, iOS devices) your administrator enabled for you.

   At the top of most of the sections you find a help icon which opens the respective remote access guide.



The available data depends on the authentication mode configured by the administrator. With preshared key, click the *Display* button to see the preshared key. Otherwise, a certificate is available. In the *Export password* field, enter a password to secure the PKCS#12 container before downloading the certificate. Note that you will need the security password of the certificate later on.

4. **Close the User Portal session by clicking *Log out*.**

The rest of the configuration takes place on the remote user client. This step will require the IP address or hostname of the server, which should be supplied by the system administrator.

3.2 Using a Preshared Key

This chapter describes the configuration of Microsoft Windows XP/Vista/7 for using a preshared key as L2TP over IPsec authentication.

3.2.1 Configuring Windows Vista or 7

1. **Click *Start* and then *Control Panel*.**
2. **In the Control Panel, click *Network and Internet*, then *Network and Sharing Center*.**
3. **Click *Set up a new connection or network*.**
   The *Set up a Connection or Network* wizard opens.
4. **Click *Connect to a workplace* and *Next*.**
5. **Define the dial-up Internet connection.**
   If you have a permanent connection to the Internet, select the *Use my Internet connection (VPN)* option. Otherwise, click *Dial directly*, and then select your dial-up Internet connection from the list.
6. **Click *Next*.**
7. **Enter the hostname or the IP address of the gateway.**
   Enter the hostname or the IP address of the gateway that you want to connect to, and enter a descriptive name for the connection. Consider the following options:

Allow other people to use this connection: Select this option if you want the connection to be available to anyone who logs on to the client.

Don't connect now; just set it up so I can connect later: Select this option.

8. **Click *Next*.**
9. **Enter the user credentials.**
   Enter the *User name* and *Password* (*Remote User Account*).
10. **Click *Create*.**
    The wizard closes.
11. **In the *Network and Sharing Center*, click *Connect to a network*.**
    A list with the available network connection opens.
12. **Right-click the new connection and select *Properties*.**
    The *Connection Properties* dialog box opens.
13. **Only for Windows Vista, do the following:**
    1. **Select the *Networking* tab.**
    2. **In the *Type of VPN* section, select *L2TP IPsec VPN*.**
    3. **Click the *IPsec Settings* button.**
       Select *Use preshared key for authentication*, enter the *Preshared Key*, and click *OK*.
    4. **Select the *Security* tab.**
    5. **Select the *Advanced (custom settings)* option and click the *Settings* button.**
    6. **Set the *Data encryption* option to *Optional encryption (connect even if no encryption)*.**
    7. **Click *OK*.**
14. **Only for Windows 7, do the following:**
    1. **Select the *Security* tab.**
    2. **In the *Type of VPN* section select *Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)*.**
    3. **Click the *Advanced settings* button.**
       Select *Use preshared key for authentication*, enter the *Preshared Key*, and click *OK*.
    4. **Set the *Data encryption* option to *Optional encryption (connect even if no encryption)*.**
15. **To close the dialog box, click *OK*.**
    Now you can directly establish the connection with your username and password in the login window.

    How to establish the connection if the login window is not open is described in chapter Connecting to the VPN.

3.2.2 Configuring Windows XP

1. **Click *Start* > *Settings*, and then click *Control Panel*.**
2. **In the Control Panel, double-click *Network Connections*.**
   The *Network Connections* window opens.
3. **Click *Create a new connection*.**
   The *New Connection Wizard* window opens.
4. **Click *Next*.**
5. **Click *Connect to the network at my workplace* and then *Next*.**
6. **Define how to connect to your network.**
   Select *Virtual Private Network connection* if you use a VPN connection over Internet.
7. **Click *Next*.**
8. **Enter the name of the company or a descriptive name for the connection.**
9. **Click *Next*.**
10. **Define the dial-up Internet connection.**
    If you have a permanent connection to the Internet, select the *Do not dial the initial connection* option. Otherwise, click *Automatically dial this initial connection*, and then select your dial-up Internet connection from the list.
11. **Click *Next*.**
12. **Enter the hostname or the IP address of the gateway that you want to connect to.**
13. **Click *Next*.**
14. **Select who should be able to use this connection.**
    Click *Anyone's use* if you want the connection to be available to anyone who logs on to the client. Otherwise, click *My use only*, to make the connection only available for your account.
15. **Click *Next*.**
16. **If you want to create a shortcut on the desktop, click *Add a shortcut to this connection to my desktop*.**
17. **Click *Finish*.**
    The login window opens.
18. **In the login window, click *Properties*.**
    The *Properties* dialog box opens.
19. **Open the *Security* tab.**
20. **Disable the *Require data encryption (disconnect if none)* option.**
21. **Click *IPsec Settings*.**
22. **Select *Use pre-shared Key for authentication* and enter the preshared key.**

23. Click *OK*.
24. Open the *Networking* tab.
25. In the *Type of VPN* section, select *L2TP IPsec VPN*.
26. To close the dialog box, click *OK*.
    Now you can directly establish the connection with your username and password in the login window.

    How to establish the connection if the login window is not open is described in chapter Connecting to the VPN.

3.3 Using a Certificate

This chapter describes the configuration of Microsoft Windows XP/Vista/7 for using X.509 certificates as IPsec authentication. The configuration is generated in two steps:

3.3.1 Importing a Certificate into Microsoft Windows XP, Vista, or 7

1. Start the management console.
   - In Windows Vista or 7, click *Start*, then, in the *Search* field, enter *mmc*.
     The program *mmc* is displayed in the *Programs* list.

     Click the *mmc* entry.

     Depending on your settings, you need to confirm with *Yes* or *Continue*. The management console opens.
   - In Windows XP, click *Start* > *Run*. Enter `mmc` and click *OK*.
2. From the menu, select *File* > *Add/Remove Snap-in*.
3. Click *Add*.
4. Select *Certificates*, then click *Add*.
5. Select *Computer account*, then click *Next*.
6. Select *Local computer (the computer this console is running on)*.
7. Click *Finish*, then *Close*, and then *OK*.
8. In the tree view on the left side, in the category *Certificates (Local Computer)*, right-click *Personal*.
9. From the context menu select *All Tasks* > *Import*.
   The *Certificate Import Wizard* opens.
10. Click *Next*.
11. Select *Browse* and select the *PKCS#12 container file* to import.
    You might have to select the correct file extension .p12 in the drop-down list to be displayed the PKCS#12 container files.
12. Click *Next*.

13. **Enter the security password.**
    Enter the security password of the certificate that you used while downloading the certificate from the User Portal.
14. **Click *Next*.**
15. **Select *Automatically select the certificate store based on the type of certificate*.**
16. **Click *Next* and then *Finish*.**
17. **Select *Action* > *Refresh*.**
    Now, the newly imported certificate should be visible.
18. **Close the management console.**
    If asked whether you want to save anything, you don't need to.
19. **Move the CA certificate to the root CA folder, if necessary.**

3.3.2 Configuring Windows Vista or 7

1. **Click *Start* and then *Control Panel*.**
2. **In the Control Panel, click *Network and Internet*, then *Network and Sharing Center*.**
3. **Click *Set up a new connection or network*.**
   The *Set up a Connection or Network* wizard opens.
4. **Click *Connect to a workplace* and *Next*.**
5. **Define the dial-up Internet connection.**
   If you have a permanent connection to the Internet, select the *Use my Internet connection (VPN)* option. Otherwise, click *Dial directly*, and then select your dial-up Internet connection from the list.
6. **Click *Next*.**
7. **Enter the hostname or the IP address of the gateway.**
   Enter the hostname or the IP address of the gateway that you want to connect to, and enter a descriptive name for the connection. Consider the following options:

   Allow other people to use this connection: Select this option if you want the connection to be available to anyone who logs on to the client.

   Don't connect now; just set it up so I can connect later: Select this option.
8. **Click *Next*.**
9. **Enter the user credentials.**
   Enter the *User name* and *Password* (*Remote User Account*).
10. **Click *Create*.**
    The wizard closes.
11. **In the *Network and Sharing Center*, click *Connect to a network*.**
    A list with the available network connection opens.

12. **Right-click the new connection and select *Properties*.**
    The *Connection Properties* dialog box opens.
13. **Only for Windows Vista, do the following:**
    1. **Select the *Networking* tab.**
    2. **In the *Type of VPN* section, select *L2TP IPsec VPN*.**
    3. **Select the *Security* tab.**
    4. **Select the *Advanced (custom settings)* option and click the *Settings* button.**
    5. **Set the *Data encryption* option to *Optional encryption (connect even if no encryption)*.**
    6. **Click *OK*.**
14. **Only for Windows 7, do the following:**
    1. **Select the *Security* tab.**
    2. **In the *Type of VPN* section select *Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)*.**
    3. **Set the *Data encryption* option to *Optional encryption (connect even if no encryption)*.**
15. **To close the dialog box, click *OK*.**
    Now you can directly establish the connection with your username and password in the login window.

    How to establish the connection if the login window is not open is described in chapter Connecting to the VPN.

3.3.3 Configuring Windows XP

1. **Click *Start* > *Settings*, and then click *Control Panel*.**
2. **In the Control Panel, double-click *Network Connections*.**
   The *Network Connections* window opens.
3. **Click *Create a new connection*.**
   The *New Connection Wizard* window opens.
4. **Click *Next*.**
5. **Click *Connect to the network at my workplace* and then *Next*.**
6. **Define how to connect to your network.**
   Select *Virtual Private Network connection* if you use a VPN connection over Internet.
7. **Click *Next*.**
8. **Enter the name of the company or a descriptive name for the connection.**
9. **Click *Next*.**
10. **Define the dial-up Internet connection.**

If you have a permanent connection to the Internet, select the *Do not dial the initial connection* option. Otherwise, click *Automatically dial this initial connection*, and then select your dial-up Internet connection from the list.

11. Click *Next*.
12. Enter the hostname or the IP address of the gateway that you want to connect to.
13. Click *Next*.
14. Select who should be able to use this connection.
    Click *Anyone's use* if you want the connection to be available to anyone who logs on to the client. Otherwise, click *My use only*, to make the connection only available for your account.
15. Click *Next*.
16. If you want to create a shortcut on the desktop, click *Add a shortcut to this connection to my desktop*.
17. Click *Finish*.
    The login window opens.
18. In the login window, click *Properties*.
    The *Properties* dialog box opens.
13. Open the *Security* tab.
14. Disable the *Require data encryption (disconnect if none)* option.
15. Open the *Networking* tab.
16. In the *Type of VPN* section select *L2TP IPsec VPN*.
17. To close the dialog box, click *OK*.
    Now you can directly establish the connection with your username and password in the login window.

    How to establish the connection if the login window is not open is described in chapter Connecting to the VPN.

4 Connecting to the VPN

When the connection is configured and the login window is closed, you can establish the connection as follows:

1. **Open the connections list.**
   In Windows Vista or 7, in the *Network and Sharing Center*, click *Connect to a network*. A list of available network connections opens.

   Alternatively, in Windows Vista, click *Start* > *Connect To*. Or, if you added a connection shortcut to the desktop, just double-click the shortcut on the desktop.

   Alternatively, in Windows 7, click the Network Connection icon on the right of the task bar.

   In Windows XP, the *Network Connections* window shows a list of available VPN connections.

2. **Initiate the connection.**
   In Windows Vista or 7, in the network connections list, click the appropriate connection. In Windows XP, right-click the connection and select *Connect*.

   If you are not currently connected to the Internet, MS Windows offers to connect to the Internet. After your computer connects to the Internet, the VPN server prompts you for your username and password.

3. **Type your username and password, and then click *Connect*.**
   Your network resources should be available to you just like they are when you connect directly to the network.

To disconnect from the VPN, right-click the Network Connection icon on the right of the task bar, then click *Disconnect from* and select the connection.

Further information is usually available from the network administrator.

Glossary

A

AES
Advanced Encryption Standard

C

CA
Certificate Authority

Certificate Authority
Entity or organization that issues digital certificates for use by other parties.

CHAP
Challenge-Handshake Authentication Protocol

CRL
Certificate Revocation List

D

DN
Distinguished Name

DNS
Domain Name Service

F

FTP
File Transfer Protocol

H

HTTP/S
Hypertext Transfer Protocol Secure

HTTPS
Hypertext Transfer Protocol Secure

Hypertext Transfer Protocol
Protocol for the transfer of information on the Internet.

Hypertext Transfer Protocol over Secure Socket Layer
Protocol to allow more secure HTTP communication.

I

Internet Protocol
Data-oriented protocol used for communicating data across a packet-switched network.

IP
Internet Protocol

IP Address
Unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard.

IPsec
Internet Protocol Security

L

L2TP
Layer Two (2) Tunneling Protocol

LDAP
Lightweight Directory Access Protocol

M

Masquerading
Technology based on NAT that allows an entire LAN to use one public IP address to communicate with the rest of the Internet.

MD5
Message-Digest algorithm 5

Message-Digest algorithm 5
Cryptographic hash function with a 128-bit hash value.

MSCHAPv2
Microsoft Challenge Handshake Authentication Protocol Version 2

N

NAS
Network Access Server

NAT
Network Address Translation

Network Address Translation
System for reusing IP addresses.

P

PAP
Password Authentication Protocol

PKCS
Public Key Cryptography Standards

Port
Virtual data connection that can be used by programs to exchange data directly. More specifically, a port is an additional identifier—in the cases of TCP and UDP, a number between 0 and 65535 – that allows a computer to distinguish between multiple concurrent connections between the same two computers.

PPTP
Point to Point Tunneling Protocol

Protocol
Well-defined and standardized set of rules that controls or enables the connection, communication, and data transfer between two computing endpoints.

Proxy
Computer that offers a computer network service to allow clients to make indirect network connections to other network services.

PSK
Preshared Key

R

RADIUS
Remote Authentication Dial In User Service

RAS
Remote Access Server

S

Secure Sockets Layer
Cryptographic protocol that provides secure communications on the Internet, predecessor of the Transport LayerSecurity (TLS).

Shared Secret
Password or passphrase shared between two entities for secure communication.

SSH
Secure Shell

T

TCP
Transmission Control Protocol

Transmission Control Protocol
Protocol of the Internet protocol suite allowing applications on networked computers to create connections to one another. The protocol guarantees reliable and in-order delivery of data from sender to receiver.

U

URL
Uniform Resource Locator

UTM
Unified Threat Management

V

Virtual Private Network
Private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol such as PPTP or IPsec.

VPN
Virtual Private Network

W

WebAdmin
Web-based graphical user interface of Sophos/Astaro products such as UTM, SUM, ACC, ASG, AWG, and AMG.

Windows Internet Naming Service
Microsoft's implementation of NetBIOS Name Server (NBNS) on Windows, a name server and service for NetBIOS computer names.

WINS
Windows Internet Naming Service

X

X.509
Specification for digital certificates published by the ITU-T (International Telecommunications Union – Telecommunication). It specifies information and attributes required for the identification of a person or a computer system.

Copyright Notice

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to nsg-docu@sophos.com.