Application Note
Accessing WEB and WEB MAIL servers on LAN

This document guides you through the set up a TrustGate to allow access from the Internet to WEB and WEB MAIL servers located on the LAN.

The document consists of standard instructions that may not fit your particular solution. Please visit our support web site for information on the latest revisions of documentation and firmware.

Version: 1.1, September 2011

Table of Contents

1. Introduction

In order to allow access from the Internet to WEB and WEB MAIL servers on the LAN side of the TrustGate, you must configure proper forwarding rules for incoming traffic on the WAN interface port 80 (Web server) and port 443 (Web mail), to the address of the server(s) in the LAN.

We will take into consideration that you may still want to be able to access the WEB interface of the TrustGate from the Internet. This will be solved by changing the TrustGate WEB GUI port from TCP:443 to TCP:444.

We will also ensure that you can access WEB MAIL and/or the WEB server from a PC in the LAN, without having to make any special rules on the PC. This will be solved by a Source NAT rule.

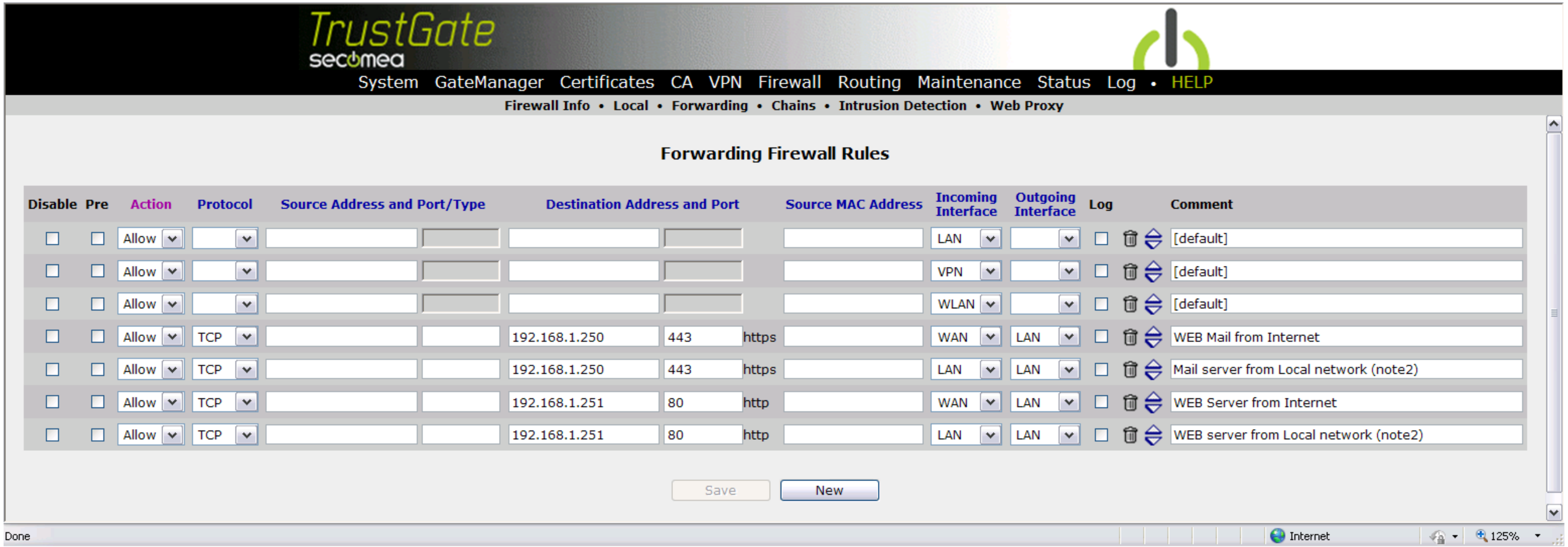
In the following example these addresses are used

WEB MAIL server	= 192.168.1.250 (port 443)
WEB server	= 192.168.1.251 (port 80)
TrustGate LAN	= 192.168.1.1
TrustGate WAN	= 80.212.2.8

Note: If configuring the TrustGate from the WAN side, it is a good idea to create proper firewall rules first.

2. Configuring Firewall rules

Create a forwarding firewall rules that allow access to the WEB and WEB MAIL server IP addresse on port 443 and 80 for both WAN and LAN.


TrustGate
secomea
System GateManager Certificates CA VPN Firewall Routing Maintenance Status Log • HELP
Firewall Info • Local • Forwarding • Chains • Intrusion Detection • Web Proxy
Save
New
Done
Internet
125%

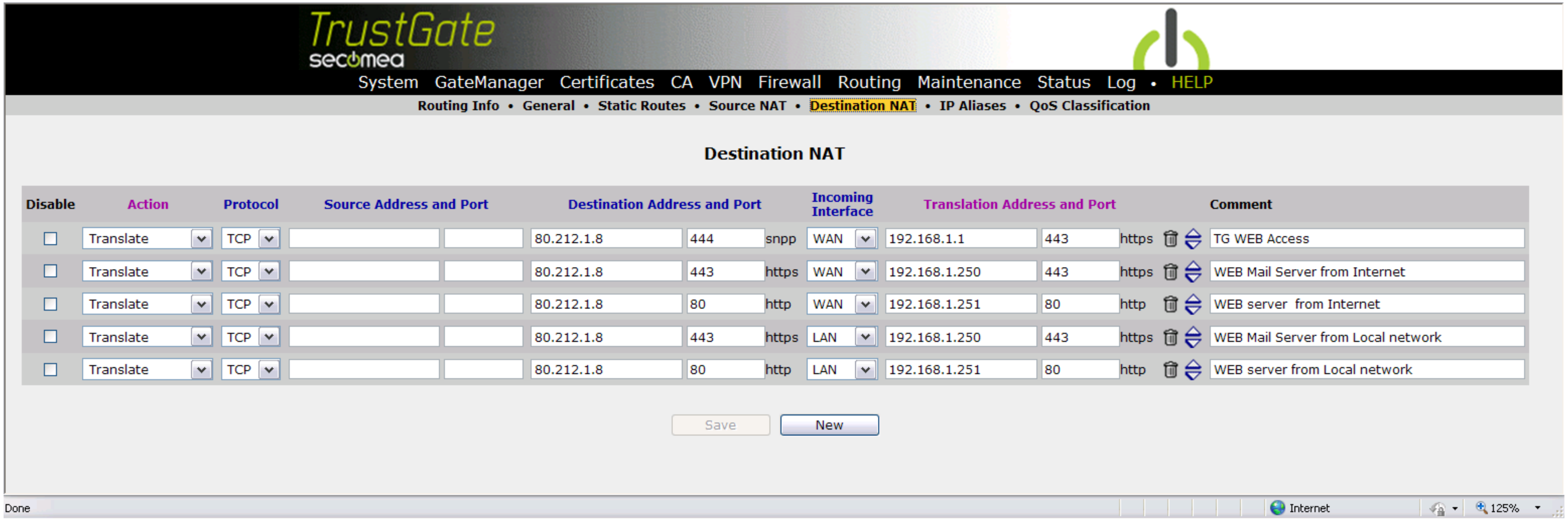
Forwarding Firewall Rules

Disable	Pre	Action	Protocol	Source Address and Port/Type		Destination Address and Port			Source MAC Address	Incoming Interface	Outgoing Interface	Log	Comment
□	□	Allow								LAN		□	[default]
□	□	Allow								VPN		□	[default]
□	□	Allow								WLAN		□	[default]
□	□	Allow	TCP			192.168.1.250	443	https		WAN	LAN	□	WEB Mail from Internet
□	□	Allow	TCP			192.168.1.250	443	https		LAN	LAN	□	Mail server from Local network (note2)
□	□	Allow	TCP			192.168.1.251	80	http		WAN	LAN	□	WEB Server from Internet
□	□	Allow	TCP			192.168.1.251	80	http		LAN	LAN	□	WEB server from Local network (note2)

Note2: The two rules for incoming LAN are not needed as it is allowed by the first default rule. But it is still a good idea, should you ever consider constraining the security level for LAN access.

3. Configuring Destination NAT rules

Create Destination NAT rules that translates access to the WAN IP (Public IP address) to the different destinations

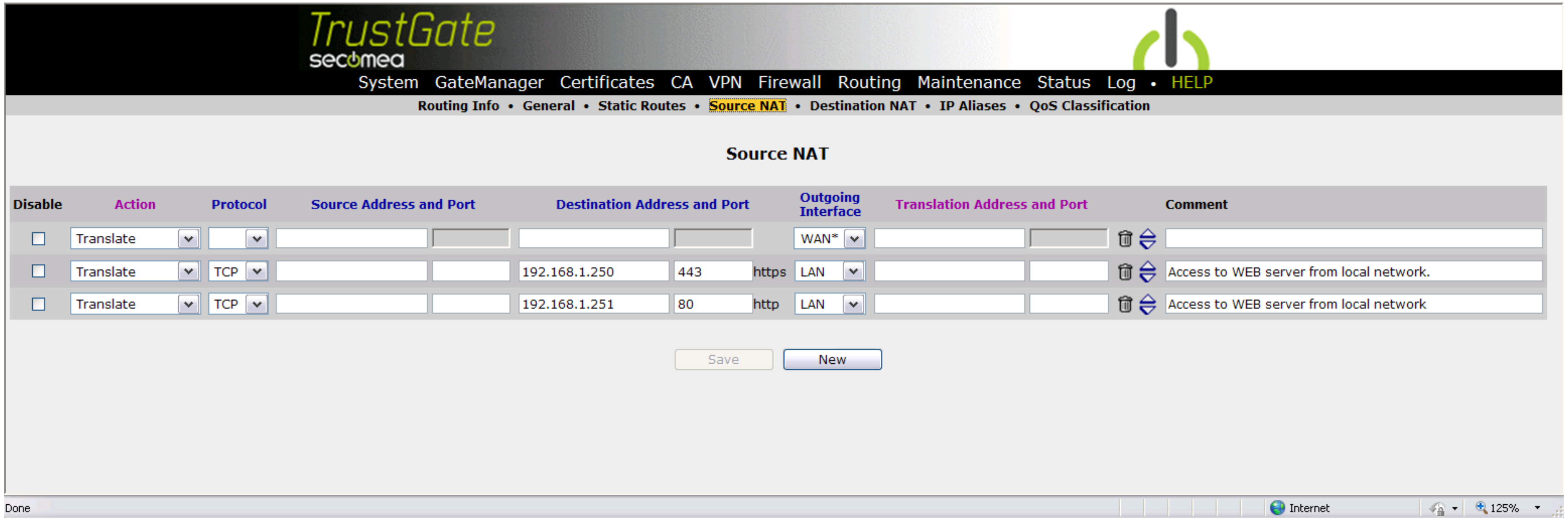

TrustGate
secomea
System GateManager Certificates CA VPN Firewall Routing Maintenance Status Log • HELP
Routing Info • General • Static Routes • Source NAT • Destination NAT • IP Aliases • QoS Classification
Save
New
Done
Internet
125%

Destination NAT

Disable	Action	Protocol	Source Address and Port		Destination Address and Port			Incoming Interface	Translation Address and Port			Comment
☐	Translate	TCP			80.212.1.8	444	snpp	WAN	192.168.1.1	443	https	TG WEB Access
☐	Translate	TCP			80.212.1.8	443	https	WAN	192.168.1.250	443	https	WEB Mail Server from Internet
☐	Translate	TCP			80.212.1.8	80	http	WAN	192.168.1.251	80	http	WEB server from Internet
☐	Translate	TCP			80.212.1.8	443	https	LAN	192.168.1.250	443	https	WEB Mail Server from Local network
☐	Translate	TCP			80.212.1.8	80	http	LAN	192.168.1.251	80	http	WEB server from Local network

1. The first rule ensures that if you enter the address http://80.222.1.8:444 in a browser, you can reach the WEB GUI of the TrustGate itself from the Internet.
2. The second rule ensures that if you enter https://80.222.1.8 in a browser, you can reach the WEB MAIL server from the Internet
3. The third rule ensures that if you enter http://80.222.1.8 in a browser, you can reach the WEB server from the Internet.
4. The forth rule ensures that if you enter https://80.222.1.8 in a browser, you can reach the WEB MAIL server from a PC in the LAN behind the TrustGate (Must be combined with the Source NAT rules show in the following page)
5. The fifth rule ensures that if you enter http://80.222.1.8 in a browser, you can reach the WEB server from a PC in the LAN behind the TrustGate (Must be combined with the Source NAT rules show in the following page)

Create Source NAT rules that translates access to the WAN IP (Public IP address) to the different destinations


TrustGate
secomea
System GateManager Certificates CA VPN Firewall Routing Maintenance Status Log • HELP
Routing Info • General • Static Routes • Source NAT • Destination NAT • IP Aliases • QoS Classification
Save
New
Done
Internet
125%

Source NAT

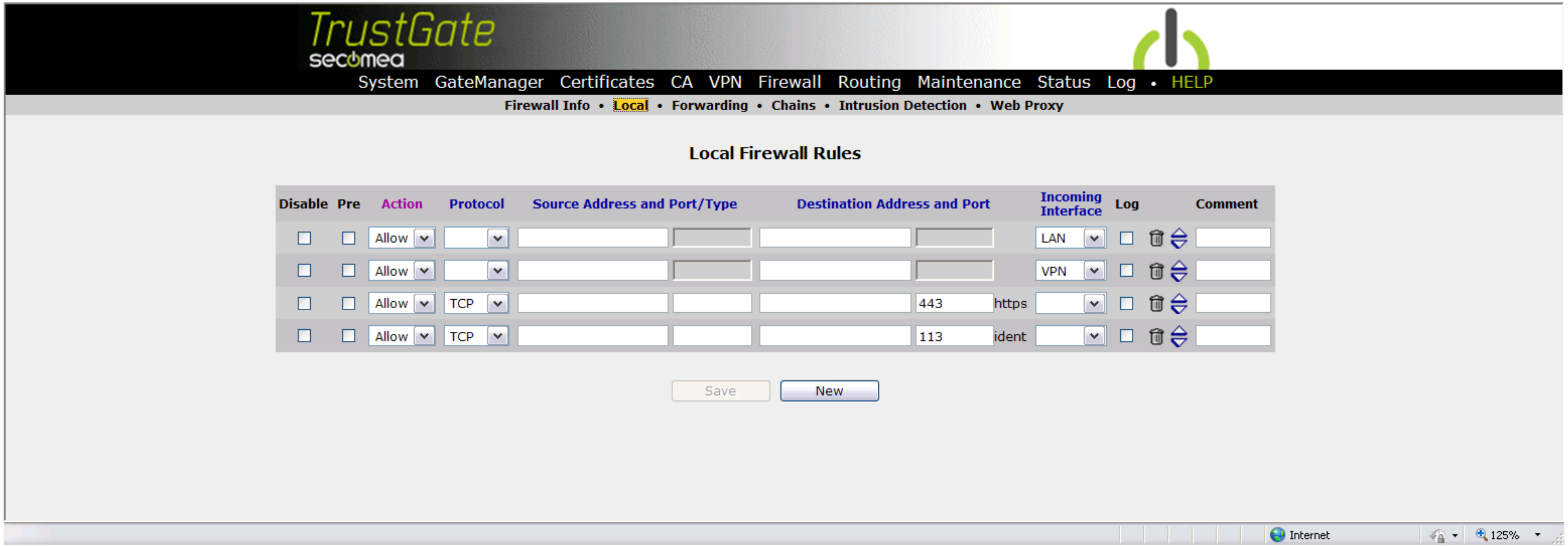
Disable	Action	Protocol	Source Address and Port		Destination Address and Port		Outgoing Interface	Translation Address and Port		Comment
□	Translate						WAN*			
□	Translate	TCP			192.168.1.250	443 https	LAN			Access to WEB server from local network.
□	Translate	TCP			192.168.1.251	80 http	LAN			Access to WEB server from local network

1. The first rule is default included in the TrustGate, and ensure that LAN devices can reach the Internet.
2. The second rule ensures that you can reach the WEB MAIL server from a PC in the LAN behind the TrustGate.
3. The third rule ensures that you can reach the WEB server from a PC in the LAN behind the TrustGate.

4. Ensure access to the TrustGate WEB GUI

You should check that access is allowed from the Internet to port 443 on the TrustGate itself. This is provided by the third rule in this list (This is the factory default configuration of the Local Firewall Rules).

Note that this should be the translated port (443), and not the port used for destination NAT (444)



Local Firewall Rules

Disable	Pre	Action	Protocol	Source Address and Port/Type		Destination Address and Port			Incoming Interface	Log		Comment
□	□	Allow							LAN	□		
□	□	Allow							VPN	□		
□	□	Allow	TCP				443	https		□		
□	□	Allow	TCP				113	ident		□		

Note: from the LAN side you can of course still access the TrustGate WEB GUI on the LAN address of the TrustGate on port 443. Also Go To Appliance from the GateManager is not affected by this.

Notices

Publication and copyright

Trademarks

Disclaimer

Secomea A/S reserves the right to make changes to this publication and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S. Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we cannot guarantee that there are none.

The following paragraph does not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

SECOMEA A/S SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGE ALLEGED IN CONNECTION WITH THE FURNISHING OR USE OF THIS INFORMATION.

Secomea A/S
Denmark

CVR No. DK 31 36 60 38

E-mail: sales@secomea.com
www.secomea.com