

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	3
2. Configuring Firewall rules	4
3. Configuring Destination NAT rules	5
4. Ensure access to the TrustGate WEB GUI	7
Notices	8

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)

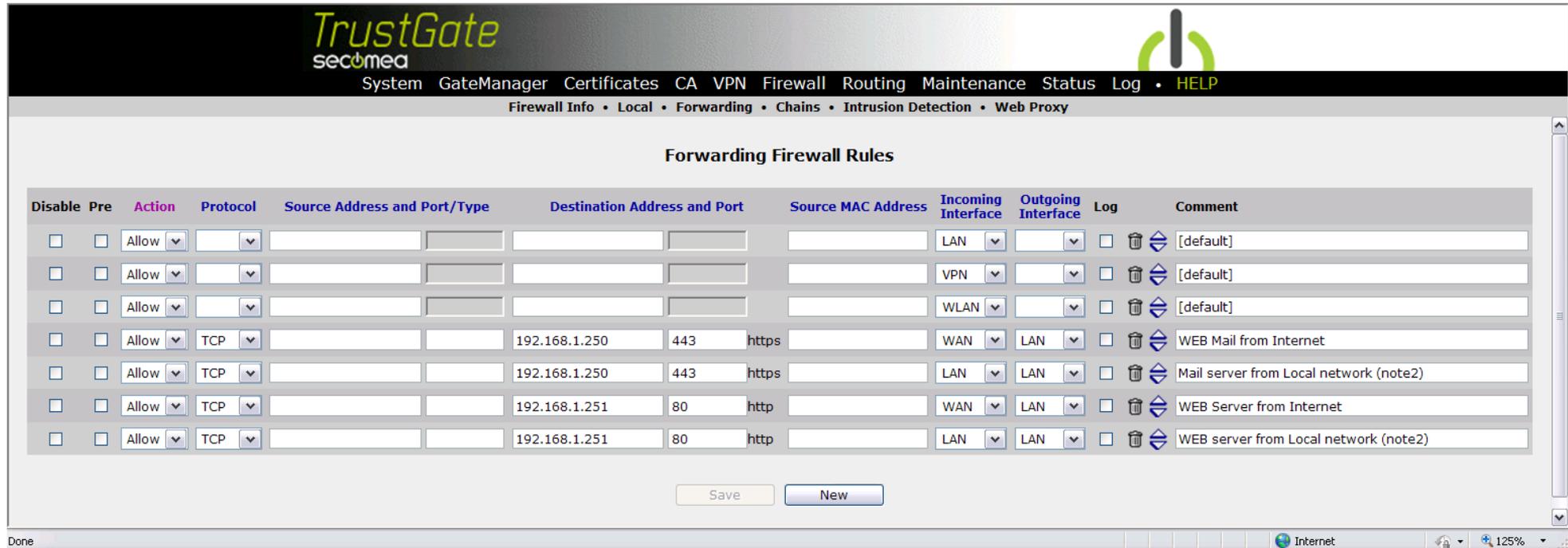
TrustGate LAN = 192.168.1.1

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 addresses on port 443 and 80 for both WAN and LAN.



The screenshot shows the TrustGate Firewall configuration interface. The top navigation bar includes: System, GateManager, Certificates, CA, VPN, Firewall, Routing, Maintenance, Status, Log, and HELP. The breadcrumb trail is: Firewall Info • Local • Forwarding • Chains • Intrusion Detection • Web Proxy. The main title is "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
<input type="checkbox"/>	<input type="checkbox"/>	Allow					LAN		<input type="checkbox"/>	[default]
<input type="checkbox"/>	<input type="checkbox"/>	Allow					VPN		<input type="checkbox"/>	[default]
<input type="checkbox"/>	<input type="checkbox"/>	Allow					WLAN		<input type="checkbox"/>	[default]
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.250 443 https		WAN	LAN	<input type="checkbox"/>	WEB Mail from Internet
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.250 443 https		LAN	LAN	<input type="checkbox"/>	Mail server from Local network (note2)
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.251 80 http		WAN	LAN	<input type="checkbox"/>	WEB Server from Internet
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		192.168.1.251 80 http		LAN	LAN	<input type="checkbox"/>	WEB server from Local network (note2)

Buttons: Save, New

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

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface	Translation Address and Port	Comment
<input type="checkbox"/>	Translate	TCP		80.212.1.8 444 snpp	WAN	192.168.1.1 443 https	TG WEB Access
<input type="checkbox"/>	Translate	TCP		80.212.1.8 443 https	WAN	192.168.1.250 443 https	WEB Mail Server from Internet
<input type="checkbox"/>	Translate	TCP		80.212.1.8 80 http	WAN	192.168.1.251 80 http	WEB server from Internet
<input type="checkbox"/>	Translate	TCP		80.212.1.8 443 https	LAN	192.168.1.250 443 https	WEB Mail Server from Local network
<input type="checkbox"/>	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 fourth 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

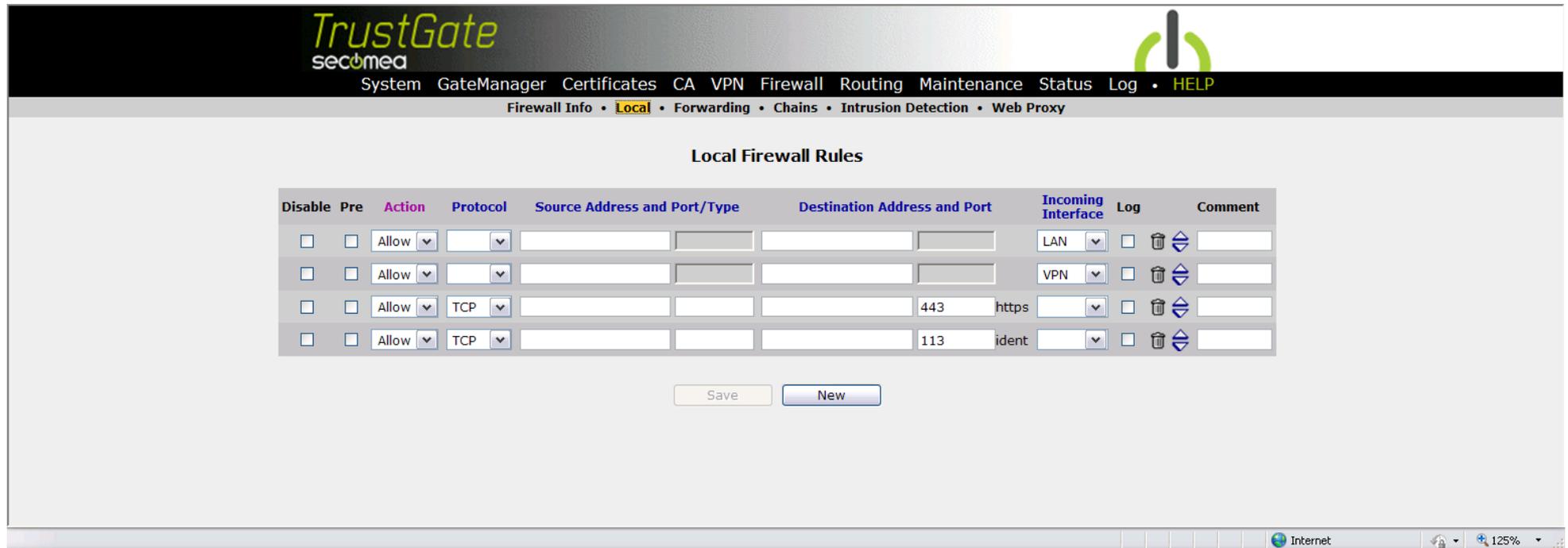
Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Outgoing Interface	Translation Address and Port	Comment
<input type="checkbox"/>	Translate				WAN*		
<input type="checkbox"/>	Translate	TCP		192.168.1.250 443 https	LAN		Access to WEB server from local network.
<input type="checkbox"/>	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)



The screenshot displays the TrustGate WEB GUI interface. At the top, the TrustGate logo and 'sec0mea' branding are visible. A navigation menu includes System, GateManager, Certificates, CA, VPN, Firewall, Routing, Maintenance, Status, Log, and HELP. Below this, a breadcrumb trail shows Firewall Info > Local > Forwarding > Chains > Intrusion Detection > Web Proxy. The main content area is titled 'Local Firewall Rules' and contains a table with the following columns: Disable, Pre, Action, Protocol, Source Address and Port/Type, Destination Address and Port, Incoming Interface, Log, and Comment. The table lists four rules, with the third rule being the one of interest: it is an 'Allow' rule for 'TCP' protocol, with destination port '443' and 'https' protocol, and 'Internet' as the incoming interface. Below the table are 'Save' and 'New' buttons. The browser's status bar at the bottom shows 'Internet' and a zoom level of '125%'.

Disable	Pre	Action	Protocol	Source Address and Port/Type	Destination Address and Port	Incoming Interface	Log	Comment
<input type="checkbox"/>	<input type="checkbox"/>	Allow				LAN	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	Allow				VPN	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		443 https		<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	Allow	TCP		113 ident		<input type="checkbox"/>	

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

© **Copyright Secomea A/S 2011**. All rights reserved. You may download and print a copy for your own use. As a high-level administrator, you may use whatever you like from contents of this document to create your own instructions for deploying our products. Otherwise, no part of this document may be copied or reproduced in any way, without the written consent of Secomea A/S. We would appreciate getting a copy of the material you produce in order to make our own material better and – if you give us permission – to inspire other users.

Trademarks

TrustGate™ and GateManager™ are trademarks of Secomea A/S. Other trademarks are the property of their respective owners.

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