

Application Note: Split Public Addresses between WAN and DMZ



This document is intended for the person in charge of configuring and/or installing the Secomea TrustGate, and needs instructions for a specific technical challenge.

This document consists of standard instructions that may not fit your particular solution. Please visit our support website for latest information and revisions of documentation and firmware: <http://www.secomea.com>

Version: 1.1, Jan 2014



Table of Contents

1.	About	3
2.	Related documents	3
3.	In short	3
4.	Setting up connection from Internet to Server	3
4.1.	Configure your TrustGate	3
4.1.1.	Routes:	3
4.1.2.	WAN interface:	4
4.1.3.	NAT rules:	4
4.1.4.	Firewall rules:	4
4.2.	Configure the server	4
5.	Access Local WAN network from Server	5
6.	Notices	6

1. About

The topic of this application note covers the rare scenario when a client on the LAN network needs a public IP address. This application note is based on the firmware v12154. If you haven't already done so, please upgrade your TrustGate.

The description in the following is based on the following sample values:

ISP gateway = 80.16.15.1/24

TrustGate WAN IP = 80.16.15.2/24

TrustGate DMZ IP = 172.222.15.1/24

Server IP = 80.16.15.3/24

2. Related documents

TrustGate Installation and Getting Started Guides (see Secomea website -> Office -> Guides and Documentation.)

If you have not already read these documents, you should start reading them. They will cover the basics about how to install and configure your TrustGate.

3. In short

You take one of your public IP addresses and reserve that for your server on the DMZ interface. Then you tell the TrustGate that this IP address is no longer on the WAN interface by creating a Static Route. At the same time you enable Proxy Arp the WAN interface this will enable the WAN network/ISP router to broadcast for the server IP even though it is no longer in the broadcast network.

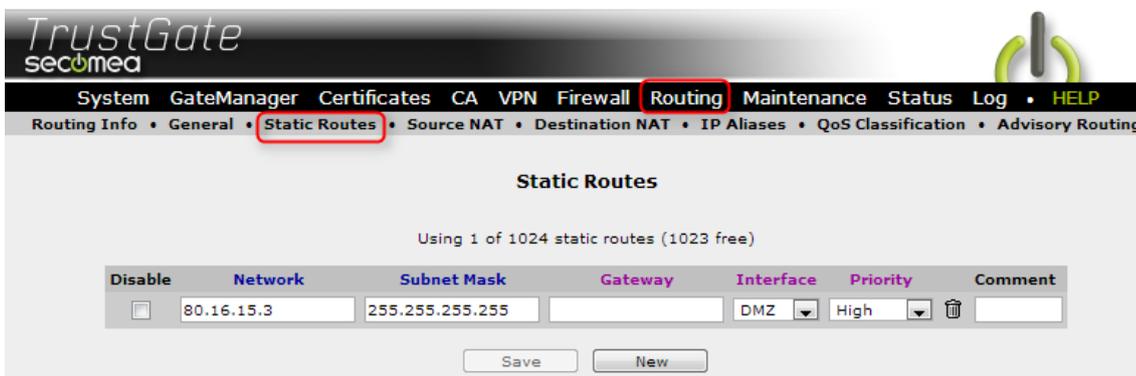
If you previously have configured the IP address as a IP Alias on the TrustGate – then you must delete this.

4. Setting up connection from Internet to Server

4.1. Configure your TrustGate

4.1.1. Routes:

Create a static route with high priority on the DMZ interface. The network IP should be the Server IP, and subnet mask 255.255.255.255. Go to Routing → Static Routes



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 • Advisory Routing

Static Routes

Using 1 of 1024 static routes (1023 free)

Disable	Network	Subnet Mask	Gateway	Interface	Priority	Comment
<input type="checkbox"/>	80.16.15.3	255.255.255.255		DMZ	High	

Save New

4.1.2. WAN interface:

Afterwards, proxy ARP should be enabled on the WAN interface. Go to System → WAN and select "Enabled" from the drop-down menu at proxy ARP.

TrustGate
secu^omeda

System GateManager Certificates CA VPN Firewall Routing Maintenance Status Log • HELP

System Info • General Time • LAN • DMZ • WLAN • WAN • WAN2 • WAN3

WAN

WAN (default) is up.

Mode: Static

IP Address: 80.16.15.2

Subnet Mask: 255.255.255.0

Default Gateway: 80.16.15.1

Ethernet Settings: Autonegotiation

Proxy ARP: Enabled

MAC Address:

MTU Mode: Auto

MTU: 1500 bytes [68-1500]

Respond To Ping: Yes

4.1.3. NAT rules:

Configure a Source NAT rule so the server IP address is shown public - select **Routing > Source NAT** and create the **Don't Translate** role as shown in RED. Make sure that this role is listed above the default role shown in GREEN.

TrustGate
secu^omeda

System GateManager Certificates CA VPN Firewall Routing Maintenance Status Log • HELP

Routing Info • General • Static Routes • Source NAT • Destination NAT • IP Aliases • QoS Classification • Advisory Routing

Source NAT

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Outgoing Interface and VLAN	Translation Address and Port	Comment
<input type="checkbox"/>	Don't Translate		80.16.15.3		WAN*		
<input type="checkbox"/>	Translate				WAN*		

4.1.4. Firewall rules:

As minimum firewall rules you must have rule (1) for access to the internet and rule (2) for access from Internet to the Server:

TrustGate
secu^omeda

System GateManager Certificates CA VPN Firewall Routing Maintenance Status Log • HELP

Firewall Info • Local • Forwarding • Chains • Intrusion Detection • Web Proxy

Forwarding Firewall Rules

Disable	Status	Pre	Action	Protocol	Source Address and Port/Type	Destination Address and Port	Source MAC Address	Incoming Interface and VLAN	Outgoing Interface and VLAN	Log
<input type="checkbox"/>	1	<input type="checkbox"/>	Allow		80.16.15.3			DMZ	WAN*	<input type="checkbox"/>
<input type="checkbox"/>	2	<input type="checkbox"/>	Allow			80.16.15.3		WAN*	DMZ	<input type="checkbox"/>

4.2. Configure the server

The Server's default gateway should be the TrustGate's WAN IP address in this case the 80.16.15.2

If the server is using the TrustGate as DNS proxy/WINS server you must use the DMZ IP address – in this case 172.222.15.1

5. Access Local WAN network from Server

If you need the server to communicate with other units on the WAN network, then proxy ARP should also be enabled on the DMZ interface. Select System → DMZ and select Enabled from the drop-down menu at Proxy ARP.

6. Notices

Publication and copyright

© **Copyright Secomea A/S 2014**. 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™ is trademark 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