

Application Note

Remote subnet is all the same



This application note describes 3 different scenarios when the remote subnet is the same, and the NAT issue related to these situations.

The document consists of standard instructions that may not fit your particular solution. Please visit our support website for more information and latest revisions of document and firmware:

<http://www.secomea.com/Service-and-Support-85.aspx>

Version 1.07, 2010



Table of Contents

1. Scope	3
2. Background	3
3. Scenarios	3
3.2. Scenario 1	4
3.3. Scenario 1 solved	4
3.4. Scenario 2	6
3.5. Scenario 2 solved	6
3.6. Scenario 3	8
3.7. Scenario 3 solved	8
4. Notices	10

1. Scope

This document describes a solution for VPN tunnels to multiple appliances that has the same Local Subnet or in another way has a remote network conflict.

The guide only deals with the NAT issue related to this problem, and not on how to configure a tunnel between two appliances. For information about creating VPN Tunnels see documentation like VPN Quick guide or the online help.

2. Background

To understand this document you need to be familiar with TrustGate appliances, especially the Routing (not least NAT) and how to create manual VPN Tunnels.

3. Scenarios

As a requirement or you can say a limitation of a VPN tunnel you can not have the same subnet on both your local network and on the remote network.

Following 3 cases are covered here:

- Two remote networks are using the same subnet.
- Local subnet is the same as the remote subnet.
- Your ISP (Internet Service Provider) provides you with a subnet that is the same as the remote subnet.

3.1.1. VIRTUAL NETWORK:

The solution for these cases is to insert a virtual network - a network that virtually represents the remote network. A virtual network must always have the same subnet size as the network that it represents. If the remote network is a class C (subnet = 255.255.255.0 or mask = /24) then the virtual network must also be class C.

A server with the physical address 192.168.1.52 on the remote network will be represented with the virtual IP address like 172.16.1.52 on the local network.

3.2. Scenario 1

From the Local network point of view it is necessary to see the remote networks as distinct networks. In this case it will not be possible to access Remote network01 because Remote network02 has the same subnet.

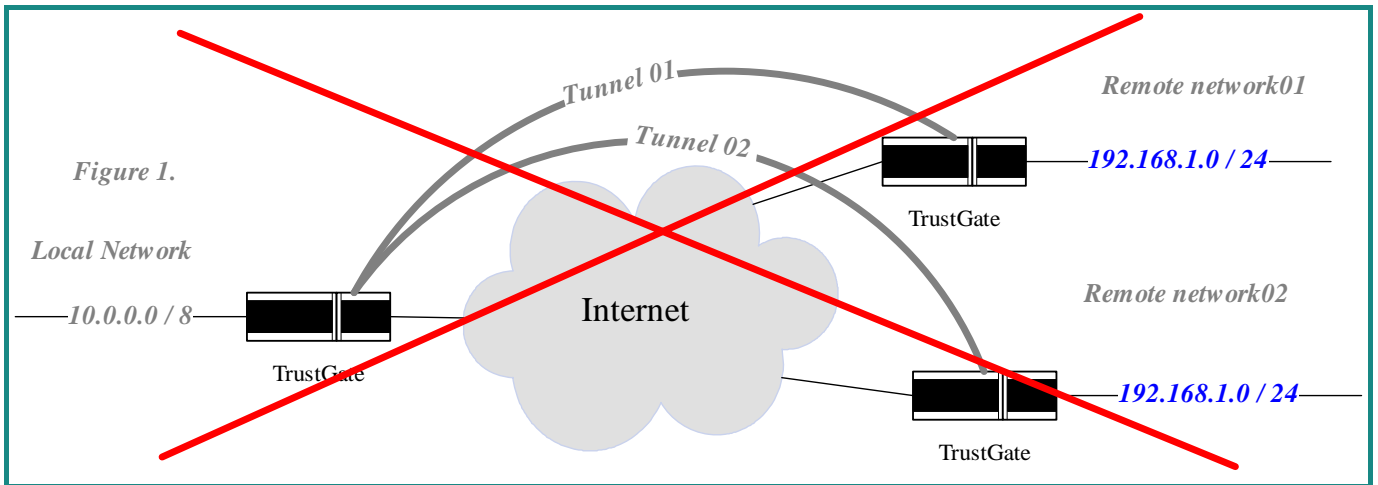


Figure 1 – both remote networks are within the same IP subnet

3.3. Scenario 1 solved

To solve the problem we introduce a Virtual Subnet for one of the Remote networks.

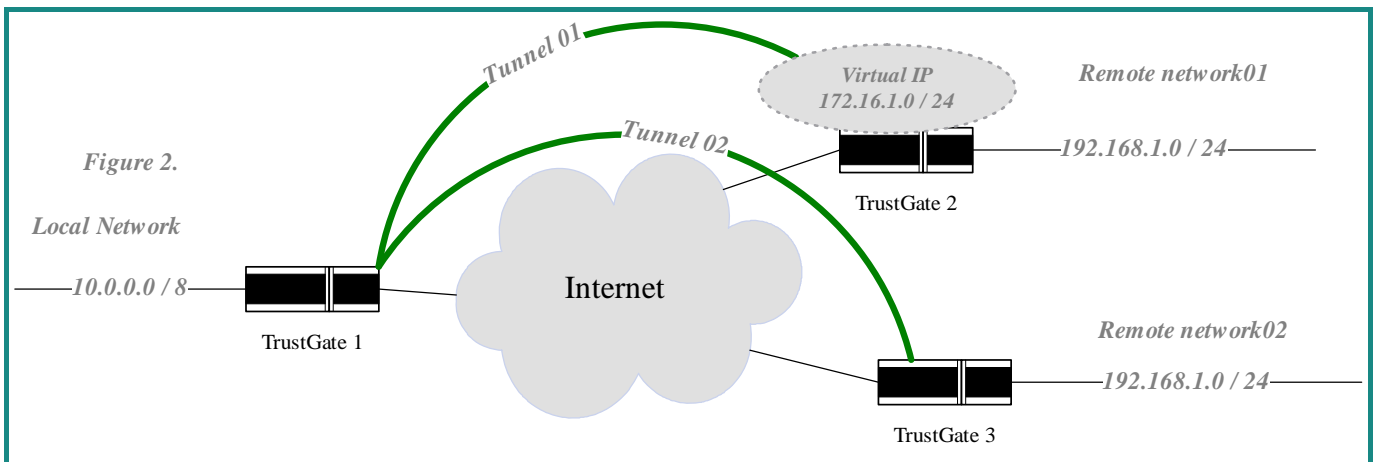


Figure 2 – one of the remote networks is replaced by a virtual network

3.3.1. Tunnel configuration on TrustGate 1

Disable	Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress	
<input type="checkbox"/>	TrustGate2	10.0.0.0	255.0.0.0	172.16.1.0	255.255.255.0	<input type="checkbox"/>	
<input type="checkbox"/>	TrustGate3	10.0.0.0	255.0.0.0	192.168.1.0	255.255.255.0	<input type="checkbox"/>	

3.3.2. Tunnel configuration on TrustGate 2

Disable	Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress	
<input type="checkbox"/>	TrustGate1	172.16.1.0	255.255.255.0	10.0.0.0	255.0.0.0	<input type="checkbox"/>	

3.3.3. Tunnel configuration on TrustGate 3

Disable	Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress	
<input type="checkbox"/>	TrustGate1	192.168.1.0	255.255.255.0	10.0.0.0	255.0.0.0	<input type="checkbox"/>	

3.3.4. Required Destination NAT rule on TrustGate 2

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface and VLAN	Translation Address and Port	
<input type="checkbox"/>	Translate		10.0.0.0/8	172.16.1.0/24	VPN	192.168.1.0/24	

3.3.5. Required Source NAT rule on TrustGate 2

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Outgoing Interface and VLAN	Translation Address and Port	
<input type="checkbox"/>	Translate		192.168.1.0/24	10.0.0.0/24	VPN	172.16.1.0/24	

Note: No NAT rules are required for TrustGate 1 or TrustGate 3.

3.4. Scenario 2

In the next scenario both Local and Remote network are the same.

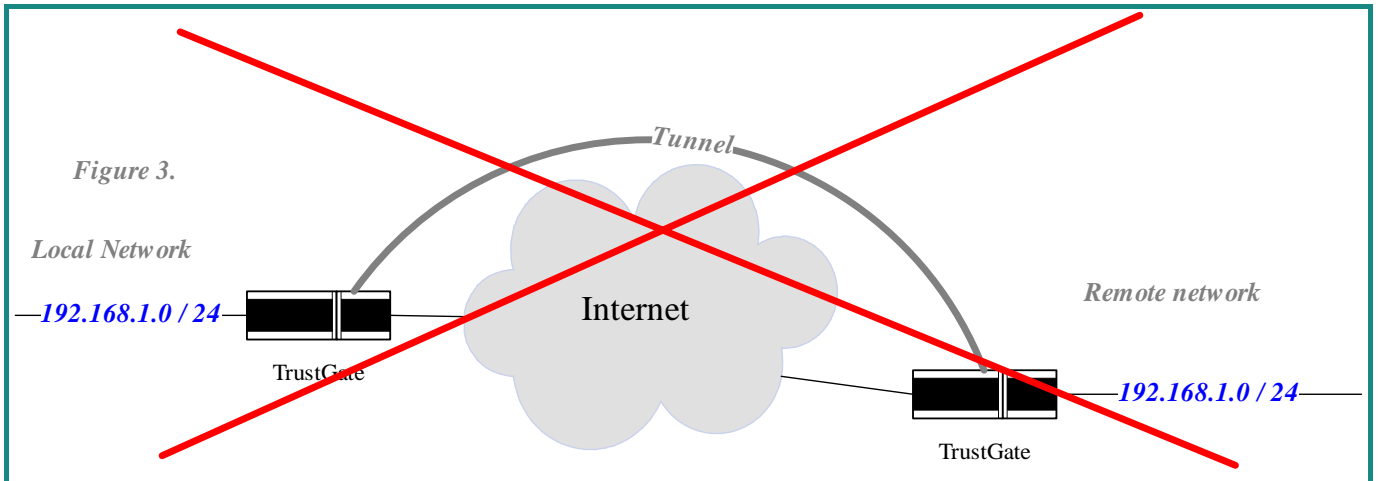


Figure 3 – both local and remote networks are the same

3.5. Scenario 2 solved

Just like scenario 1 we will solve this case by introducing virtual networks. In this case we will need to use 2 virtual networks.

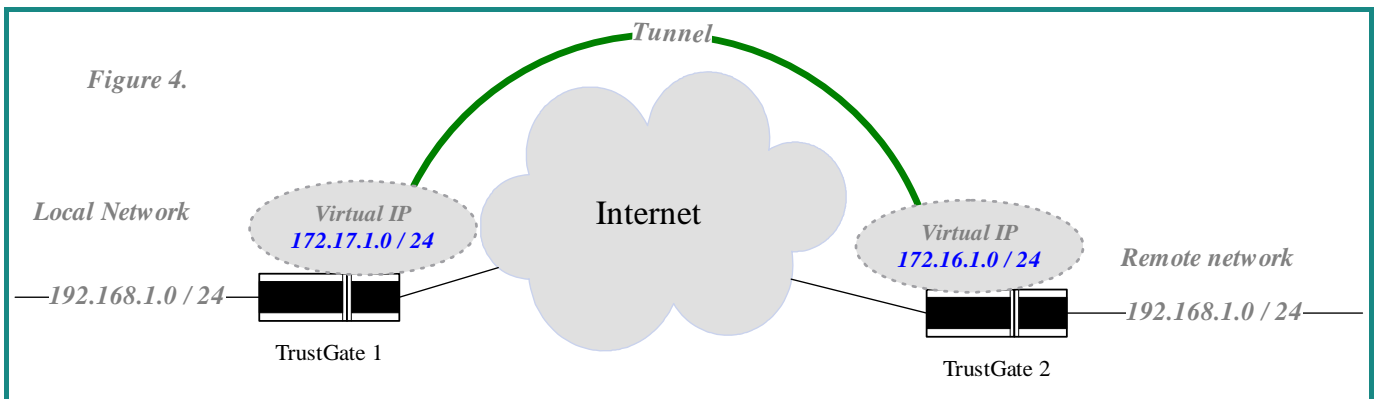


Figure 4 – two virtual networks are required to solve this case

3.5.1. Tunnel configuration on TrustGate 1

Disable	Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress
<input type="checkbox"/>	TrustGate 1	172.17.1.0	255.255.255.0	172.16.1.0	255.255.255.0	<input type="checkbox"/>

3.5.2. Required Destination NAT rule on TrustGate 1

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface and VLAN	Translation Address and Port
<input type="checkbox"/>	Translate		172.16.1.0/24	172.17.1.0/24	VPN	192.168.1.0/24

3.5.3. Required Source NAT rule on TrustGate 1

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Outgoing Interface and VLAN	Translation Address and Port
<input type="checkbox"/>	Translate		192.168.1.0/24	172.16.1.0/24	VPN	172.17.1.0/24

3.5.4. Tunnel configuration on TrustGate 2

Disable	Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress
<input type="checkbox"/>	TrustGate 2	172.16.1.0	255.255.255.0	172.17.1.0	255.255.255.0	<input type="checkbox"/>

3.5.5. Required Destination NAT rule on TrustGate 2

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface and VLAN	Translation Address and Port
<input type="checkbox"/>	Translate		172.17.1.0/24	172.16.1.0/24	VPN	192.168.1.0/24

3.5.6. Required Source NAT rule on TrustGate 2

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Outgoing Interface and VLAN	Translation Address and Port
<input type="checkbox"/>	Translate		192.168.1.0/24	172.17.1.0/24	VPN	172.16.1.0/24

3.6. Scenario 3

In this case the ISP router between the TrustGate and the Internet provides an IP subnet that is the same as the remote network.

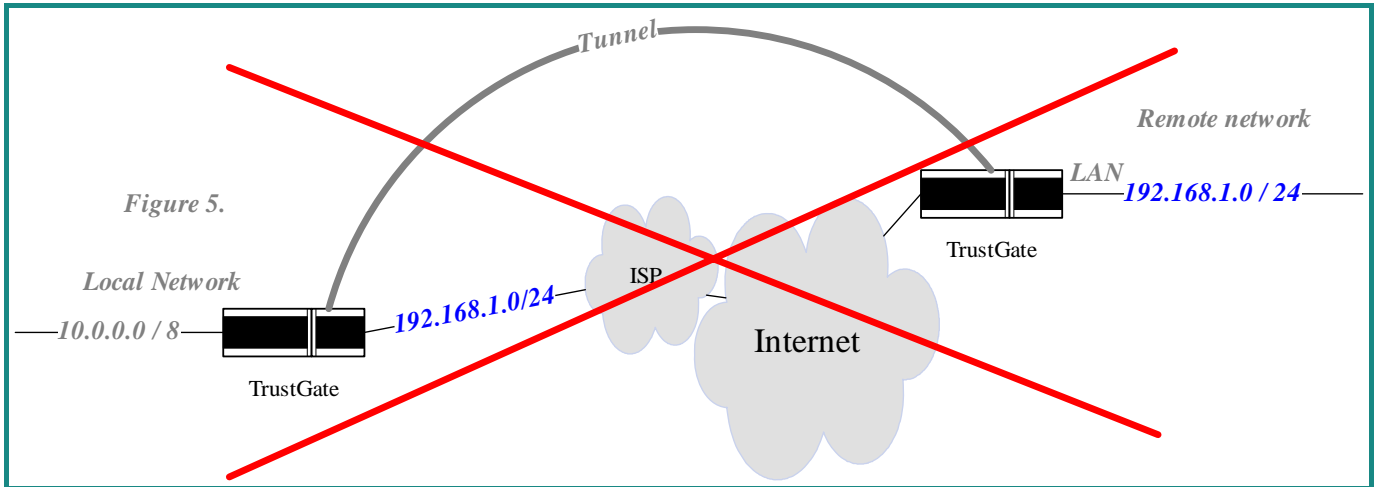


Figure 5 – network in between is the same as remote network

3.7. Scenario 3 solved

Again we introduce a virtual network and this time it is necessary that the virtual network is configured on the Remote network.

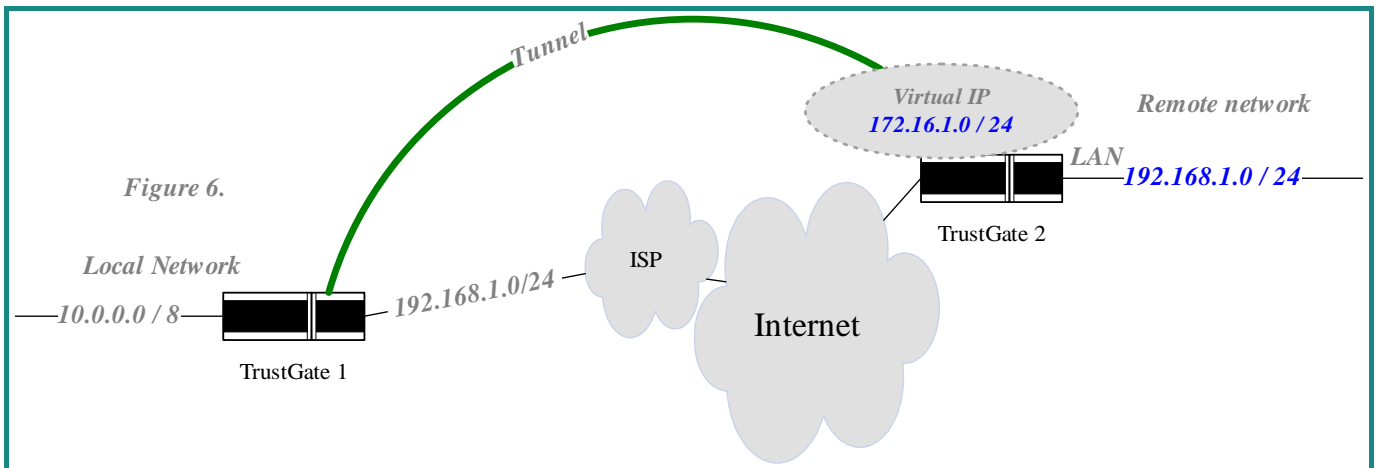


Figure 6 – Virtual network on remote site solve the in between network

3.7.1. Tunnel configuration on TrustGate 1

Disable	Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress
<input type="checkbox"/>	TrustGate2	10.0.0.0	255.0.0.0	172.16.1.0	255.255.255.0	<input type="checkbox"/>

3.7.2. Required Destination NAT rule on TrustGate 1

No destination NAT needed.

3.7.3. Required Source NAT rule on TrustGate 1

No source NAT needed.

3.7.4. Tunnel configuration on TrustGate 2

Disable	Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress
<input type="checkbox"/>	TrustGate1	172.16.1.0	255.255.255.0	10.0.0.0	255.0.0.0	<input type="checkbox"/>

3.7.5. Required Destination NAT rule on TrustGate 2

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface and VLAN	Translation Address and Port
<input type="checkbox"/>	Translate		10.0.0.0/8	172.16.1.0/24	VPN	192.168.1.0/24

3.7.6. Required Source NAT rule on TrustGate 2

Disable	Action	Protocol	Source Address and Port	Destination Address and Port	Outgoing Interface and VLAN	Translation Address and Port
<input type="checkbox"/>	Translate		192.168.1.0/24	10.0.0.0/8	VPN	172.16.1.0/24

4. Notices

Publication and copyright

Application Note - Remote subnet is all the same, version 1.07, 2010

© **Copyright Secomea A/S 2008-2010**. 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

GateManager™ and TrustGate™ 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 can not 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