

# Application Note: 2 Peers to one Dual-Wan TrustGate



This document guides you through the set up of two PEER/Tunnels between two TrustGate appliances. The only prerequisite is that one of the TrustGate appliances has 2 WAN interfaces (Dual-Wan), and with two Public IP addresses.

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

**Version: 1.0, Jan 2011**



## Table of Contents

<b>1. Introduction</b>	<b>3</b>
<b>2. How to set up TrustGate with 2 PEERs/Tunnels to the same TrustGate.</b>	<b>3</b>
2.1. TrustGate160 configuration (Single WAN site)	4
2.2. TrustGate260 – DualWAN Appliance	7
2.3. Result	10
<b>3. Pending tasks</b>	<b>10</b>
<b>4. Notices</b>	<b>11</b>

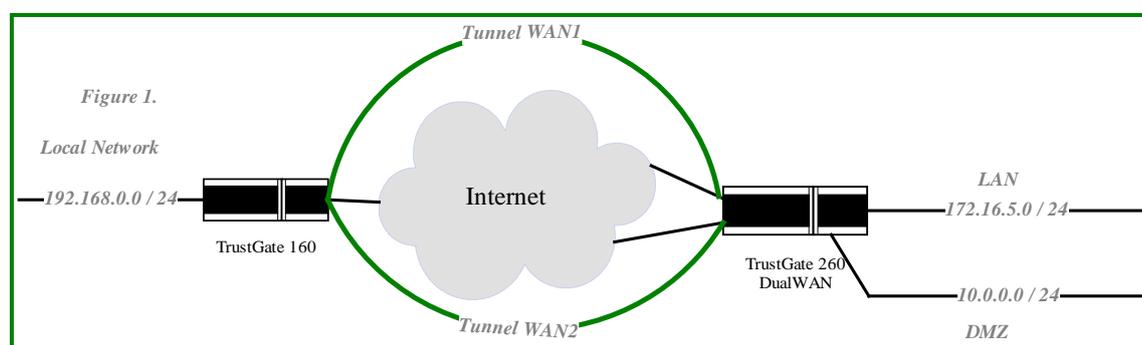
## 1. Introduction

In this example a TrustGate160 (TG160) will be set up to have 2 tunnels to the same remote TrustGate (TG260). Tunnel WAN1 will terminate on WAN1 on the TG260 and Tunnel WAN2 will terminate on WAN2 in the TG260.

**Why so:** In some cases it is necessary to allocate ex. WAN2 only for VoIP traffic to an internal voice server (PBX) and not affecting the WAN1 connection.

**The technique:** To be able to have 2 tunnels between the 2 TrustGates it is necessary for the TG260 to differentiate between the two tunnels that are actually coming from the same remote appliance (TG160). This is where we will be using different ID Types for each tunnel; domain Name for the first tunnel and IP address for the second tunnel.

**Tunnel and PEERS:** Tunnel is not just a tunnel. In this document a Tunnel consist of a PEER and a tunnel. A PEER can have multiple tunnels. This part of the technique is not handled in this document. In our case a Tunnel is represented by one PEER and one tunnel.



### Settings:

TrustGate160

> WAN1 = 140.1.1.11

TrustGate260

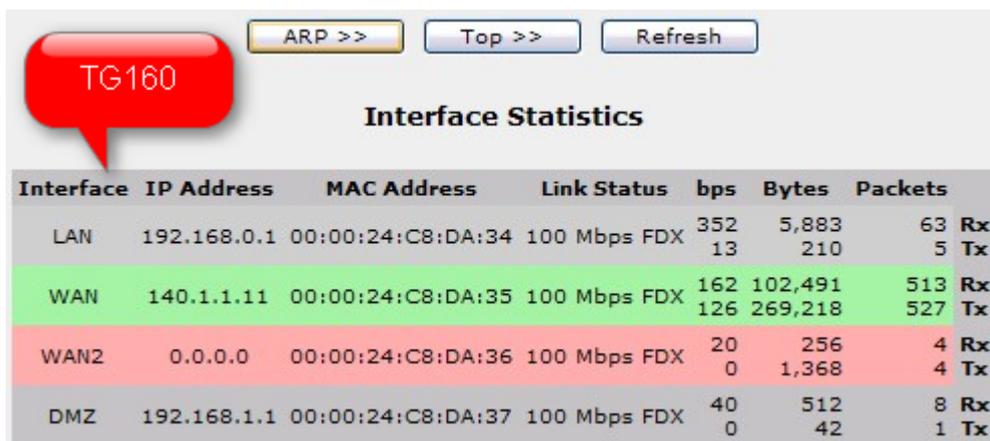
> WAN = 140.2.1.20

> WAN2 = 141.2.1.2

## 2. How to set up TrustGate with 2 PEERs/Tunnels to the same TrustGate.

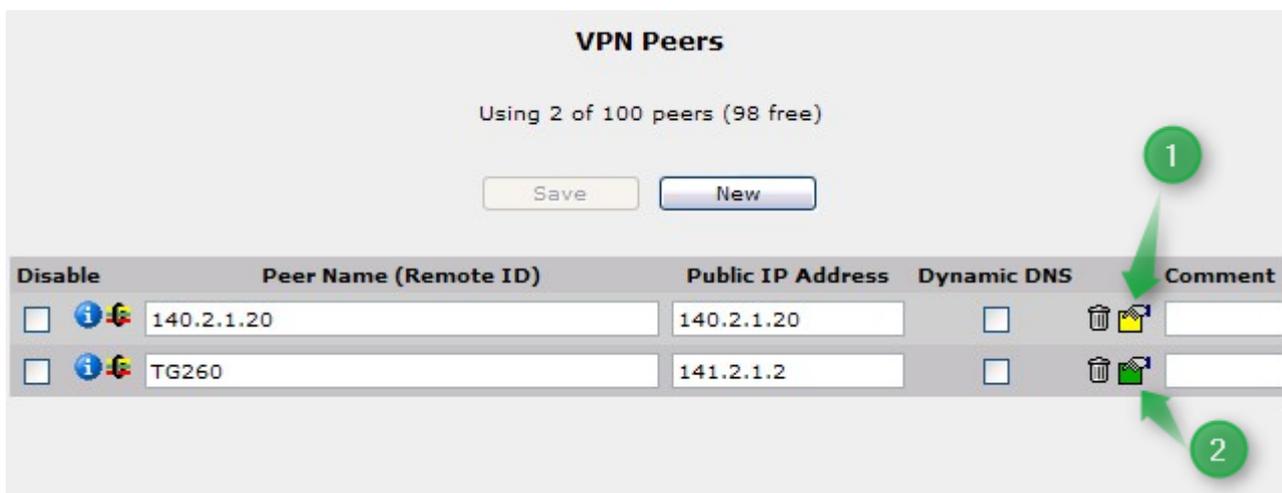
In the following we will show how to set up 2 PEERs to the same remote site. The first PEER will use ID Type = Domain Name and the other will be using ID Type = IP Address.

## 2.1. TrustGate160 configuration (Single WAN site)



Interface	IP Address	MAC Address	Link Status	bps	Bytes	Packets	
LAN	192.168.0.1	00:00:24:C8:DA:34	100 Mbps FDX	352 13	5,883 210	63 5	Rx Tx
WAN	140.1.1.11	00:00:24:C8:DA:35	100 Mbps FDX	162 126	102,491 269,218	513 527	Rx Tx
WAN2	0.0.0.0	00:00:24:C8:DA:36	100 Mbps FDX	20 0	256 1,368	4 4	Rx Tx
DMZ	192.168.1.1	00:00:24:C8:DA:37	100 Mbps FDX	40 0	512 42	8 1	Rx Tx

WAN on the TrustGate160.



Using 2 of 100 peers (98 free)

Save New

Disable	Peer Name (Remote ID)	Public IP Address	Dynamic DNS	Comment
<input type="checkbox"/>	140.2.1.20	140.2.1.20	<input type="checkbox"/>	
<input type="checkbox"/>	TG260	141.2.1.2	<input type="checkbox"/>	

First PEER is using IP address as ID and also Pre-Shared key.

> 140.2.1.20 = WAN1 on TG260

Second PEER is using Domain Name as ID and Pre-Loaded Certificate.

> 141.2.1.2 = WAN2 on TG260

**1**

### Advanced Properties for 140.2.1.20

Using Pre-Shared Key

Pre-Shared Key:

Hex 12345678

IPSec Parameters:

ID Type: IP Address

Encryption Algorithm: Use General Setting

Hash Algorithm: Use General Setting

Diffie-Hellman Group: Use General Setting

Perfect Forward Secrecy: Use General Setting

Miscellaneous:

Backup IP Address or DNS Name: 141.2.1.2

Peer Is Always Initiator: No

Bind To Interface: Any

Save Cancel

PEER1 on TG160 [1] (IP address)

Configure a Pre-Shared key.

Configure ID Type = IP address

Backup IP address or DNS Name = WAN2 IP address on TG260. (Specifying the second WAN interface on the TG260 here, will make the tunnel fail-over to use WAN2 of this tunnel if WAN1 goes down.)

**2** **Advanced Properties for TG260**

Using Pre-Loaded Certificate

IPSec Parameters:

ID Type:

Encryption Algorithm:

Hash Algorithm:

Diffie-Hellman Group:

Perfect Forward Secrecy:

Miscellaneous:

Backup IP Address or DNS Name:

Peer Is Always Initiator:

Bind To Interface:

PEER2 on TG160 [2] (Domain Name)

Configure ID Type = Domain Name

Paste in the certificate from [TG260](#) using the icon.

**NOTE:** The certificate is the Local Certificate from the TG260. Go to the TG260 WEB GUI and select the menu: Certificate > Local > Copy

Backup IP address or DNS Name = WAN1 IP address on TG260. (Specifying the first WAN interface on the TG260 here will make the tunnel failover to use WAN1 of this tunnel if WAN2 goes down.)

Tunnel Configuration:

**VPN Tunnels**

Using 2 of 2000 tunnels (1998 free)

Disable	Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress	Comment
<input type="checkbox"/>	140.2.1.20	192.168.0.0	255.255.255.0	172.16.5.0	255.255.255.0	<input type="checkbox"/>	
<input type="checkbox"/>	TG260	192.168.0.0	255.255.255.0	10.0.0.0	255.255.255.0	<input type="checkbox"/>	

Create corresponding tunnels for each PEER. In this case the (2) Tunnel is destination DMZ interface on the TG260 appliance.

## 2.2. TrustGate260 – DualWAN Appliance

ARP >>    Top >>    Refresh

**TG260**

### Interface Statistics

Interface	IP Address	MAC Address	Link Status	bps	Bytes	Packets	Rx	Tx
LAN	172.16.5.1	00:00:24:CB:5F:A4	100 Mbps FDX	0	9,280	145	1	
WAN	140.2.1.20	00:00:24:CB:5F:A5	100 Mbps FDX	1,281 3,443	342,987 300,251	4,958 2,488		
WAN2	141.2.1.2	00:00:24:CB:5F:A6	100 Mbps FDX	57 40	85,372 55,246	1,393 1,251		
DMZ	10.0.0.1	00:00:24:CB:5F:A7	100 Mbps FDX	0	49,116	517		

### VPN Peers

Using 2 peers and 3 EasyTunnels of 600 peers (595 free)

Save    New

Disable	Peer Name (Remote ID)	Public IP Address	Dynamic DNS	Comment
<input type="checkbox"/>	140.1.1.11	140.1.1.11	<input type="checkbox"/>	
<input type="checkbox"/>	TG160	140.1.1.11	<input type="checkbox"/>	

First PEER is using IP address as ID and also Pre-Shared key.

Second PEER is using Domain Name ID and Pre-Loaded Certificate.

**3**

### Advanced Properties for 140.1.1.11

Using Pre-Shared Key

Pre-Shared Key:

Hex 12345678

IPSec Parameters:

ID Type: IP Address

Encryption Algorithm: Use General Setting

Hash Algorithm: Use General Setting

Diffie-Hellman Group: Use General Setting

Perfect Forward Secrecy: Use General Setting

Miscellaneous:

Backup IP Address or DNS Name:

Peer Is Always Initiator: No

Bind To Interface: WAN

Save Cancel

PEER1 on TG260 [3] (IP address)

Configure a Pre-Shared key.

Configure ID Type = IP address

Bind To Interface = WAN (to make sure that TG260 will use WAN(1) in case it is the TG260 appliance that starts the tunnel).

### Advanced Properties for TG160

Using Pre-Loaded Certificate

4

IPSec Parameters:

ID Type:

Encryption Algorithm:

Hash Algorithm:

Diffie-Hellman Group:

Perfect Forward Secrecy:

Miscellaneous:

Backup IP Address or DNS Name:

Peer Is Always Initiator:

Bind To Interface:

PEER2 on TG260 [4] (Domain Name)

Configure ID Type = Domain Name

Paste in the certificate from [TG160](#) using the  icon.

**NOTE:** The certificate is the Local Certificate from the TG160. Go to the TG160 WEB GUI and select the menu: Certificate > Local > Copy

Bind To Interface = WAN2 (to make sure that TG260 will use WAN2 in case it is the TG260 appliance that starts the tunnel).

### VPN Tunnels

Using 2 of 10000 tunnels (9998 free)

Disable	Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress	Comment
<input type="checkbox"/>	140.1.1.11 	172.16.5.0	255.255.255.0	192.168.0.0	255.255.255.0	<input type="checkbox"/>	 
<input type="checkbox"/>	TG160 	10.0.0.0	255.255.255.0	192.168.0.0	255.255.255.0	<input type="checkbox"/>	 

Configure the 2 tunnels for each peer according to your set up

## 2.3. Result

TG160		Standard Tunnels											
Peer	Interface	Status	Local Network	Remote Network	Algo.	Age	Idle	Local LB	Remote LB	Comp.	Bytes	Packets	
<a href="#">140.2.1.20</a>	WAN	Up	192.168.0.0/24	172.16.5.0/24	AES	00:02:09	00:00:18 00:00:18			off	304 480	4 4	Rx Tx
<a href="#">TG260</a> <a href="#">141.2.1.2</a>	WAN	Up	192.168.0.0/24	10.0.0.0/24	AES	00:02:27	00:00:00 00:00:00			off	3,674,471 399,192	6,183 3,403	Rx Tx

### TrustGate160

TG260		Standard Tunnels											
Peer	Interface	Status	Local Network	Remote Network	Algo.	Age	Idle	Local LB	Remote LB	Comp.	Bytes	Packets	
<a href="#">140.1.1.11</a>	WAN	Up	172.16.5.0/24	192.168.0.0/24	AES	00:05:14	00:00:22 00:00:22			off	760 1,200	10 10	Rx Tx
<a href="#">TG160</a> <a href="#">140.1.1.11</a>	WAN2	Up	10.0.0.0/24	192.168.0.0/24	AES	00:03:21	00:00:00 00:00:00			off	2,349,318 49,025,240	37,567 75,703	Rx Tx

### TrustGate260 ( DualWAN)

## 3. Pending tasks

To make Tunnels fallback to the primary interface you must set the rekey time to e.g. 30 minutes. Do not set the value lower than 10 minutes or the tunnel might go down before a new soft-state is ready.

**VPN General**

EasyTunnel Mode:

SoftClient Deployment Port:

Custom SoftClient (x86) CAB URL:

Custom SoftClient (x64) CAB URL:

Default ID Type:

Specific ID (IP Address):

Default Encryption Algorithm:

Default Hash Algorithm:

Default Diffie-Hellman Group:

Default Perfect Forward Secrecy:

ISAKMP SA Lifetime:  minutes [1-1440]

IPSec SA Lifetime:  minutes [1-1440]

Keying Tries:

Virtual Address Assignment:

Manual Address:

VPN Router:

NAT-Traversal:

NAT-T Keep Alive:

NAT-T Keep Alive Interval:  seconds [1-300]

NAT-T Port Floating:

Tunnel MTU Mode:

Tunnel MTU:  bytes

ECN Usage:

DiffServ Domain Model:

---

## 4. 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™ is a 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](mailto:sales@secomea.com)  
[www.secomea.com](http://www.secomea.com)