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

secomea

Table of Contents

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.

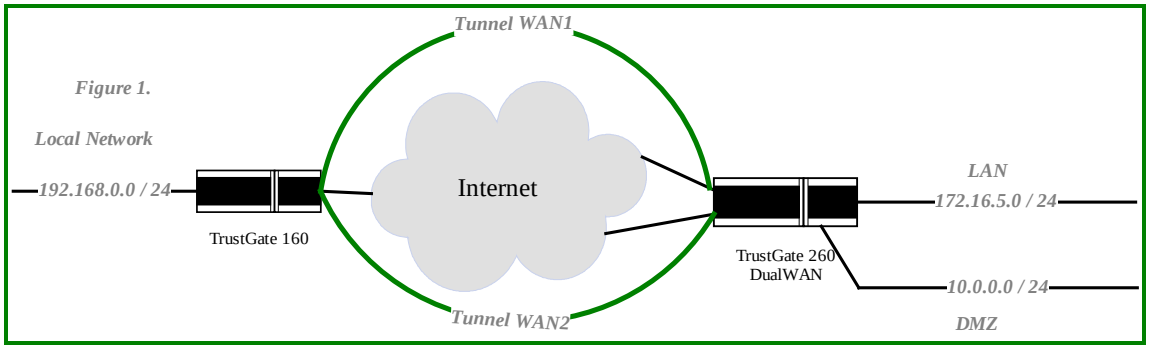


Figure 1.

Settings:

TrustGate160

> WAN1 = 140.1.1.11

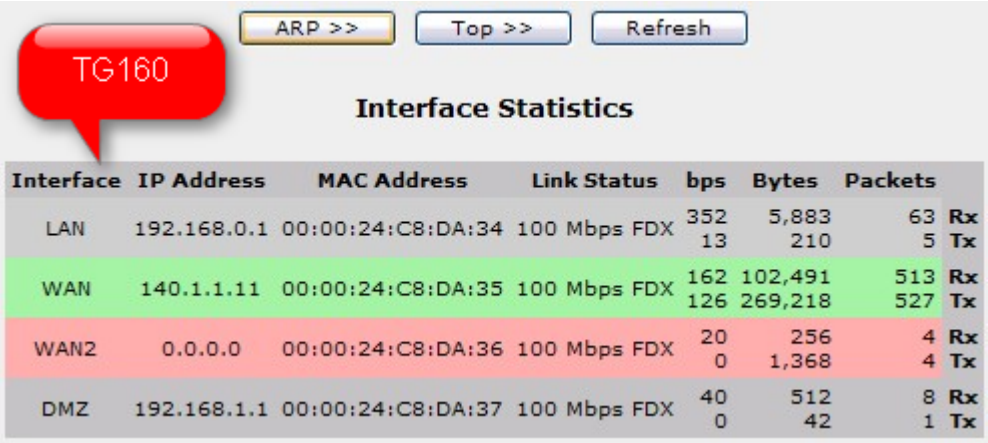
TrustGate260

- WAN = 140.2.1.20
- WAN2 = 141.2.1.2

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

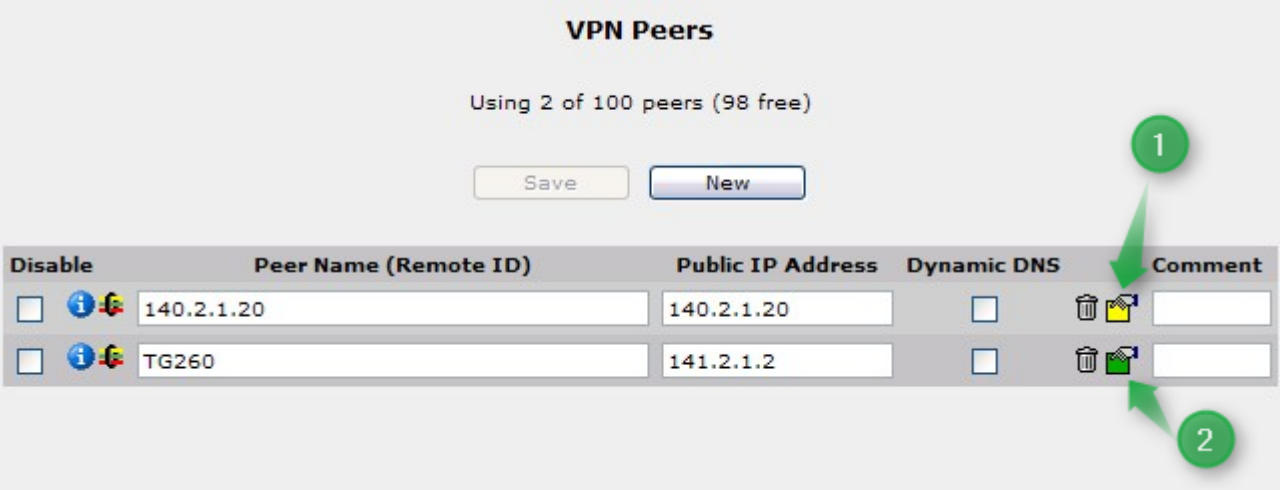
In the following we will show who to set up 2 PEERs to the same remote site. The first PEER will use ID Type = Domain Name and the other will be using ID Type = IP Address.

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.

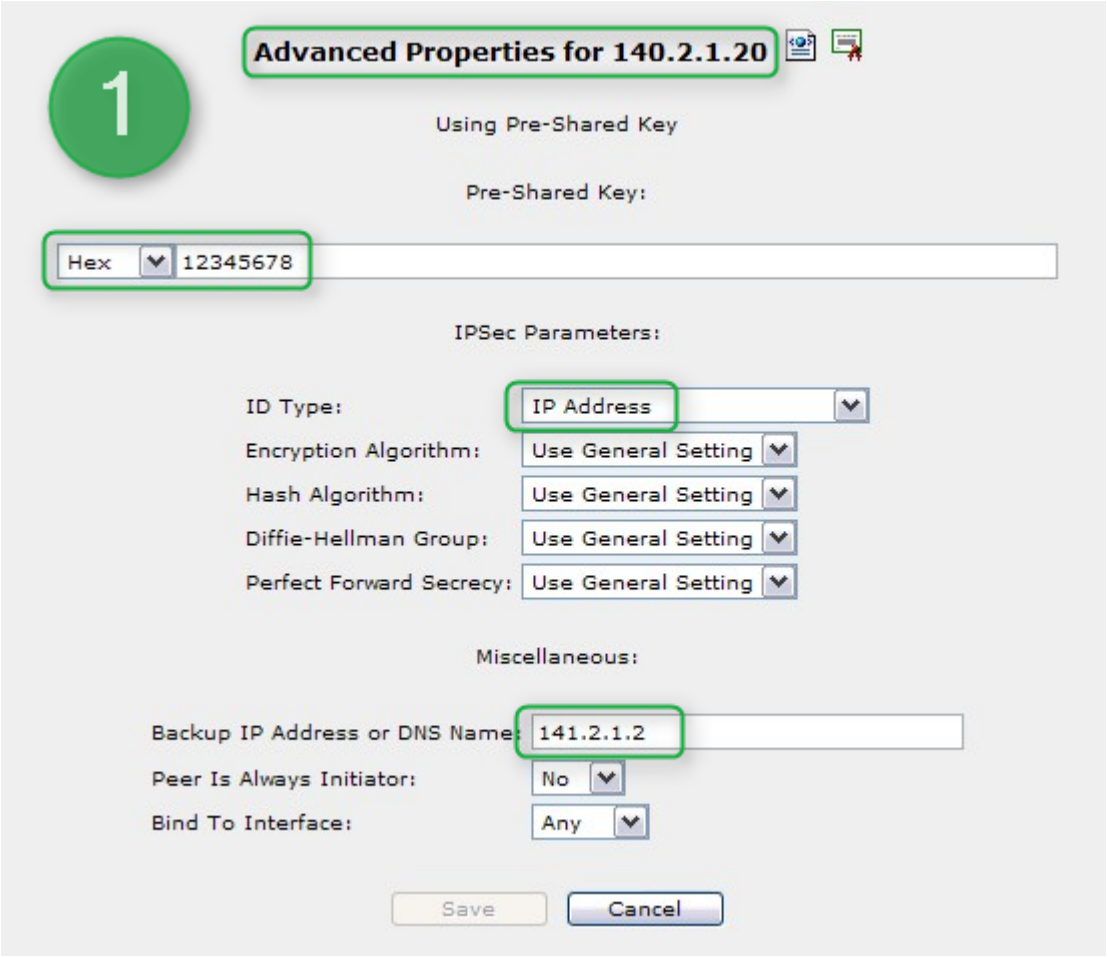


First PEER is using IP address as ID and also Pre-Shared key.

> 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

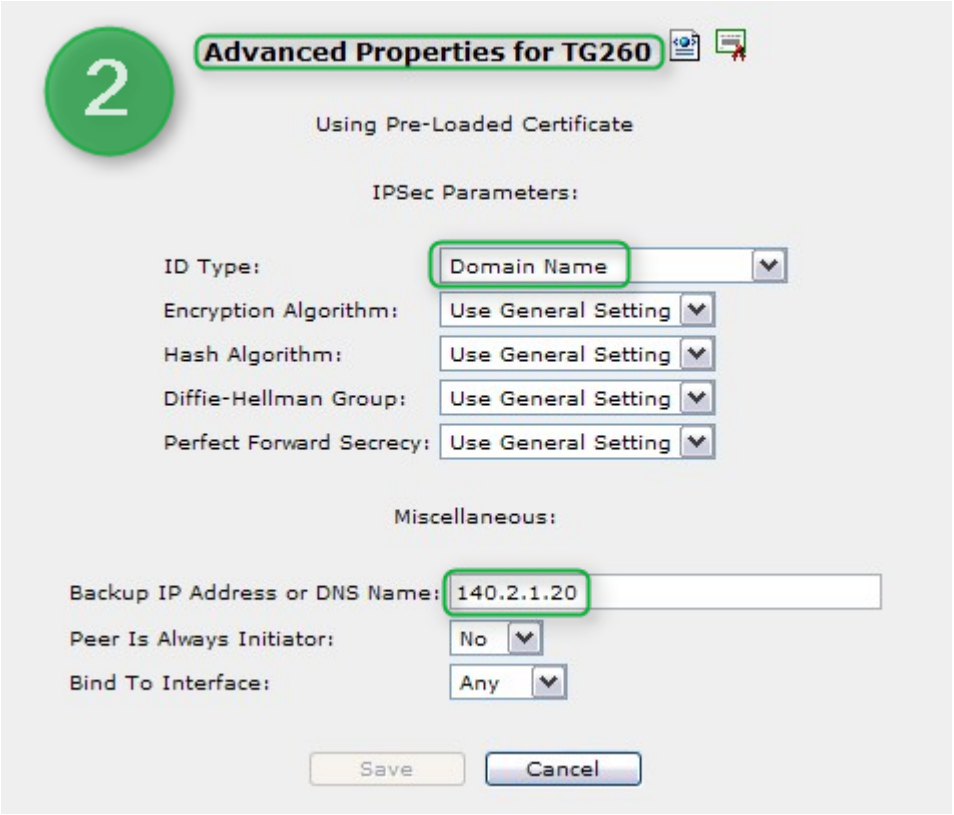


PEER1 on TG160 [1] (IP address)

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 failover to use WAN2 of this tunnel if WAN1 goes down.)



PEER2 on TG160 [2] (Domain Name)

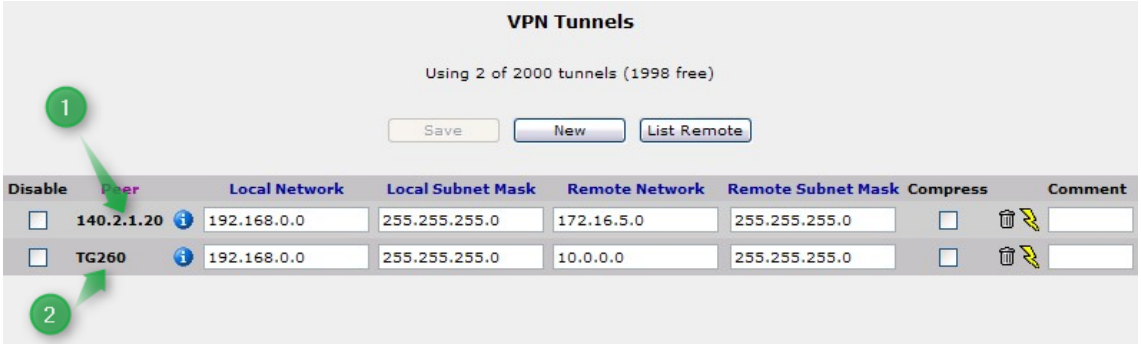
Configure ID Type = Domain Name

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

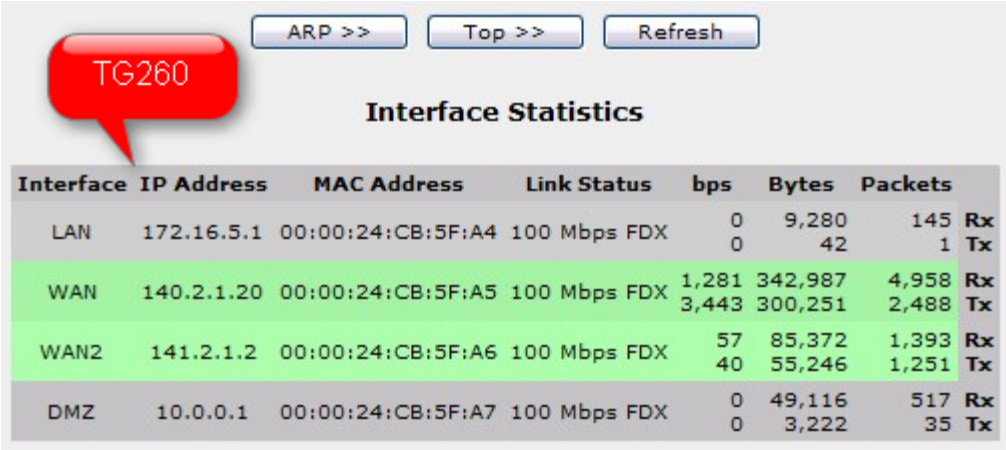
Backup IP address or DNS Name = WAN1 IP address on TG260. (Specifying the first WAN interface on the TG260 here will make the tunnel failover to use WAN1 of this tunnel if WAN2 goes down.)

Tunnel Configuration:

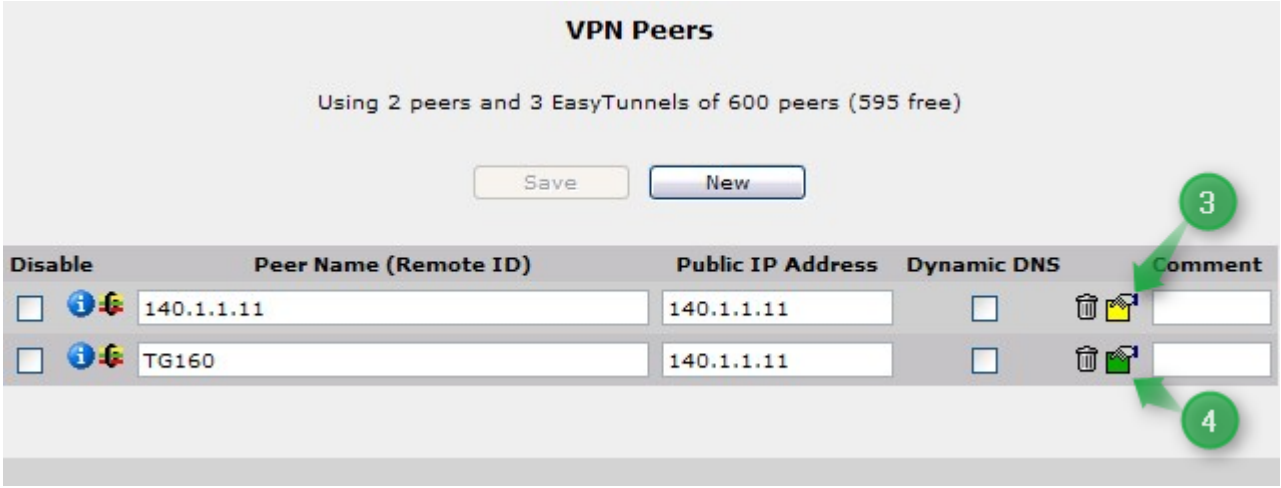


Create corresponding tunnels for each PEER. In this case the (2) Tunnel is destination DMZ interface on the TG260 appliance.

2.2. TrustGate260 – DualWAN Appliance

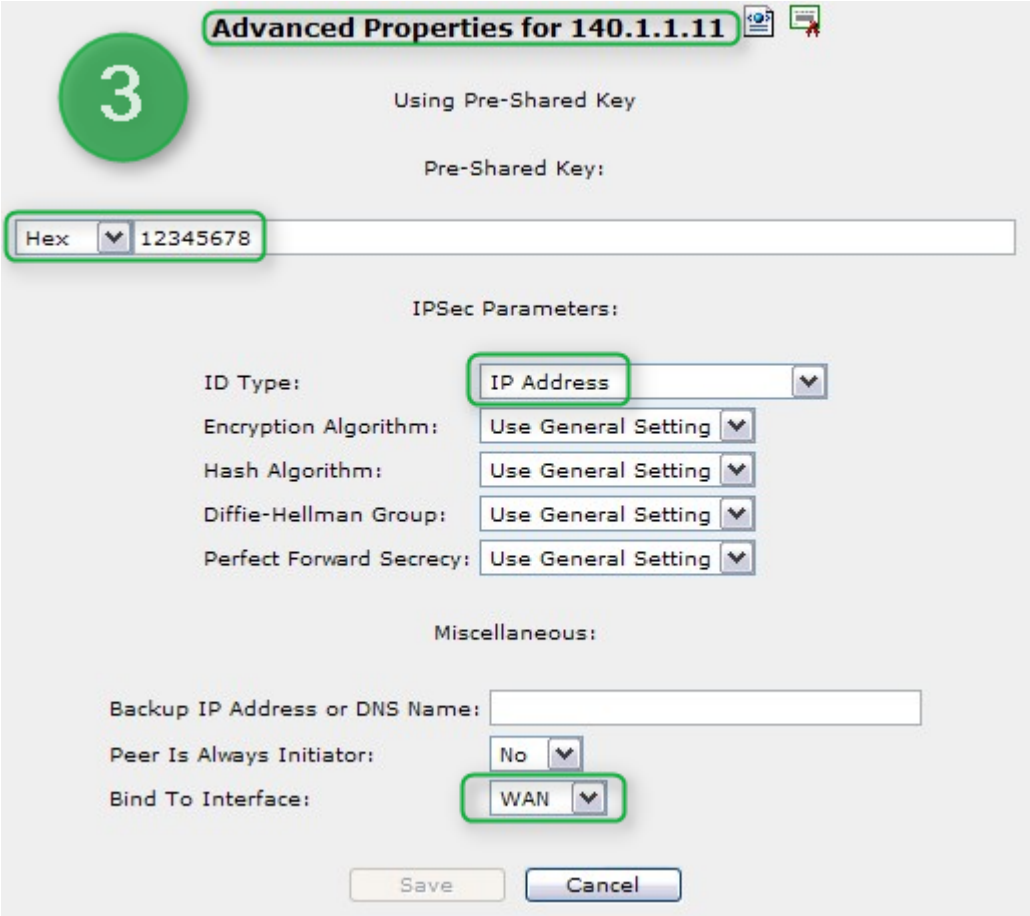


Interface	IP Address	MAC Address	Link Status	bps	Bytes	Packets	
LAN	172.16.5.1	00:00:24:CB:5F:A4	100 Mbps FDX	0	9,280	145	Rx
				0	42	1	Tx
WAN	140.2.1.20	00:00:24:CB:5F:A5	100 Mbps FDX	1,281	342,987	4,958	Rx
				3,443	300,251	2,488	Tx
WAN2	141.2.1.2	00:00:24:CB:5F:A6	100 Mbps FDX	57	85,372	1,393	Rx
				40	55,246	1,251	Tx
DMZ	10.0.0.1	00:00:24:CB:5F:A7	100 Mbps FDX	0	49,116	517	Rx
				0	3,222	35	Tx



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

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

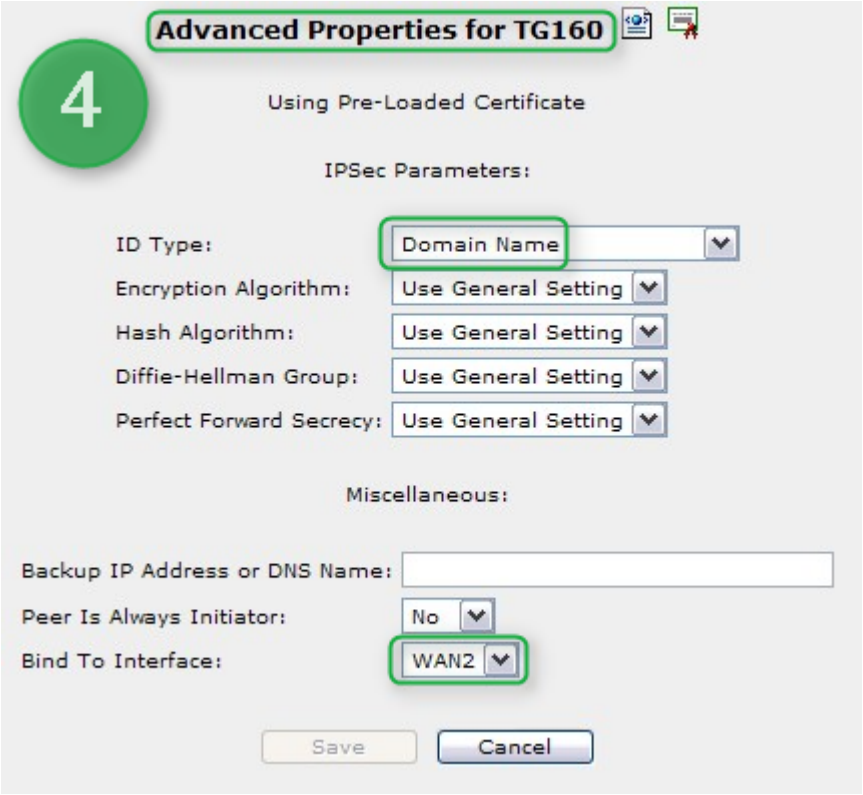


PEER1 on TG260 [3] (IP address)

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).



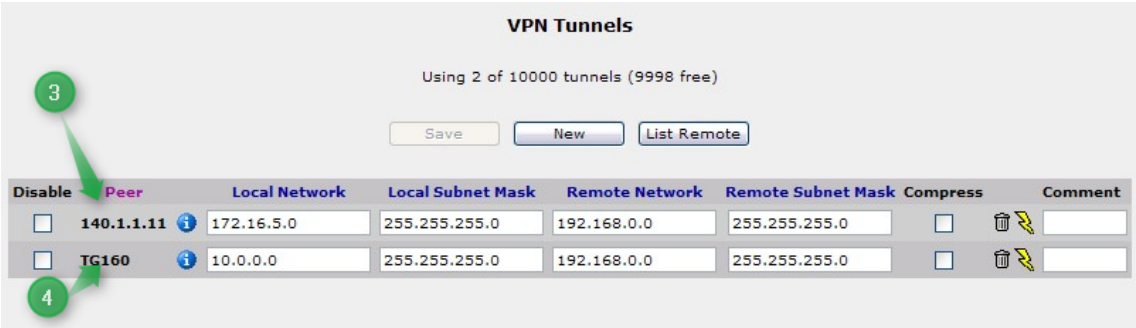
PEER2 on TG260 [4] (Domain Name)

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).



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	
140.2.1.20	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
TG260 141.2.1.2	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	
140.1.1.11	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
TG160 140.1.1.11	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 then 10 minutes or the tunnel might go down before a new soft-state is ready.

VPN General

EasyTunnel Mode:	Disabled
SoftClient Deployment Port:	
Custom SoftClient (x86) CAB URL:	
Custom SoftClient (x64) CAB URL:	
Default ID Type:	Domain Name
Specific ID (IP Address):	0.0.0.0
Default Encryption Algorithm:	Any
Default Hash Algorithm:	Any
Default Diffie-Hellman Group:	Any
Default Perfect Forward Secrecy:	On
ISAKMP SA Lifetime:	30 minutes [1-1440]
IPSec SA Lifetime:	30 minutes [1-1440]
Keying Tries:	Infinite
Virtual Address Assignment:	Use LAN Address
Manual Address:	192.168.0.1
VPN Router:	0.0.0.0
NAT-Traversal:	Enabled
NAT-T Keep Alive:	Auto
NAT-T Keep Alive Interval:	20 seconds [1-300]
NAT-T Port Floating:	Enabled
Tunnel MTU Mode:	Auto
Tunnel MTU:	1422 bytes
ECN Usage:	Forbid
DiffServ Domain Model:	Uniform

4. Notices

Publication and copyright

Trademarks

Disclaimer

Secomea A/S
Denmark

CVR No. DK 31 36 60 38

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