Application Note
GRE forwarding for external PPtP Clients

External PPtP Clients are using an internal Windows server behind a Trust-Gate and therefore needs forwarding of the GRE protocol for authentication.

This document illustrates with a few screenshots the necessary NAT and Firewall rules.

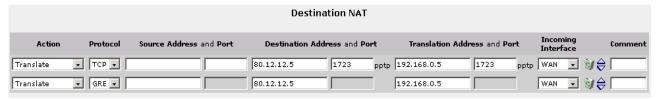**Version: 1.0, 2011**

secomea

Table of Contents

secomea
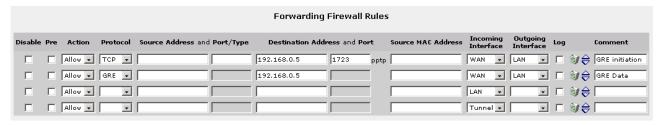
1. TrustGate Setup

Server Address = 192.168.0.5

Public Address = 80.12.12.5

PPtP is using the GRE protocol for data and TCP destination port 1723 for authentication.

You will only have to configure the following Destination NAT and Forwarding firewall Rules:

Destination NAT							
Action	Protocol	Source Address and Port	Destination Address and Port	Translation Address and Port	Incoming Interface	Comment
Translate	TCP			80.12.12.5	1723	pptp	192.168.0.5	1723	pptp	WAN		
Translate	GRE			80.12.12.5			192.168.0.5			WAN		

Add the following rule as the first firewall rule:

Disable	Pre	Action	Protocol	Source Address and Port/Type	Destination Address and Port	Source MAC Address	Incoming Interface	Outgoing Interface	Log	Comment
☐	☐	Allow	TCP			192.168.0.5	1723	pptp		WAN	LAN	☐	GRE initiation
☐	☐	Allow	GRE			192.168.0.5				WAN	LAN	☐	GRE Data
☐	☐	Allow								LAN		☐	
☐	☐	Allow								Tunnel		☐	

NOTE: Firmware: 4072 or later is required.

secòmea

2. Notices

Publication and copyright

Trademarks

TrustGate™ is a trademark of Secomea A/S. Other trademarks are the property of their respective owners.

Disclaimer

secomea