Configuring route-resiliency in SimSafe via Dynamic Routing and Multiple Agents

Contents

Intended Audience

Network Professionals and IT Administrators deploying a SimSafe routed-mode network. We recommend that readers of this document have at least a basic knowledge of IP Routing.

Introduction

This is a guide detailing how to configuring route-resiliency in SimSafe via **Dynamic Routing** and Multiple VPN Agents. Two types of network examples:

- **Proxied Mode** network

- **Routed Mode** network. The majority of SimSafe networks run like this, this guide concentrates on this mode.

"Automatic load balancing" in **Proxied Mode** means that if we have e.g. two agents in the network they will take equal number of connections. First device will connect to first agent, second device to second agent, third device to first agent and so on. When one of the agents goes down all connections will be automatically redirected to second available agent.

Load Balancing on **Routed Mode** network works more less the same way but instead of Load Balancing on IP packages we have to look into entire connection for each host (called tunnel).

SimSafe fully supports dynamic routing via RIPv2. By deploying multiple VPN Agents and configuring RRAS/RIPv2 on VPN Agent host servers and on your core router(s), it is possible to achieve full route resiliency on your SimSafe network. Note that this is applicable to **Routed Mode** networks only.

This guide below explains how to configure route-resiliency in SimSafe via **Dynamic Routing** and Multiple VPN Agents.

A typical SimSafe deployment involves setting up one or more Windows Servers running VPN Agents that act as gateways to a “stub network” of remote clients (e.g. an estate of cellular modems). It is desirable to provide route resiliency from the core to the client stub network, so that if one of these gateways goes down (either by losing connectivity to SimSafe, or for example by losing the Agent host server itself), an alternative route to the client network is automatically found.

This can be achieved by deploying multiple VPN Agents on Windows Servers running the Routing and Remote Access Service (RRAS) and configuring dynamic routing using RIP (Routing Information Protocol).

This guide shows how to configure RIP on your VPN Agent host servers to provide route resiliency. Note that this is applicable to **Routed Mode** networks only.

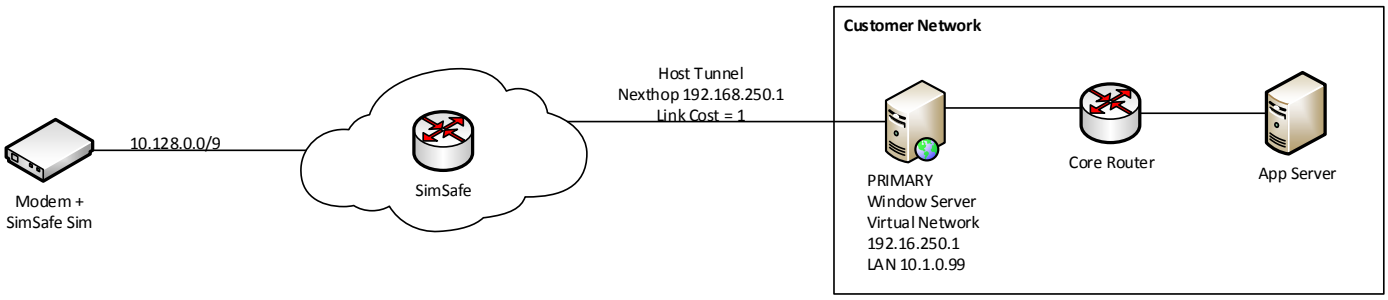
Prerequisites

1) Routed-Mode SimSafe network
2) "Stub" Network topology – i.e. a VPN Agent host is an IP Gateway to a remote subnet [e.g. of (say) cellular modems]
3) Internal network has a RIP-capable core router
4) VPN Agents run on Windows Server 2003 or newer.
5) 2 or more VPN Agent licenses

Example Network

In this guide we'll describe how to add route-resiliency to the typical SimSafe network described below:

1) Client Stub network on 10.128.0.0/9.
2) SimSafe routed-mode network with a single VPN Agent Host Tunnel (Nexthop = 192.168.250.1, Link Cost = 1, Routing Enabled)
3) Internal core router configured to route 10.128.0.0/9 via the VPN Agent host – the Windows Server "Primary". Thus "Primary" acts as an IP Gateway for the stub network 10.128.0.0/9.

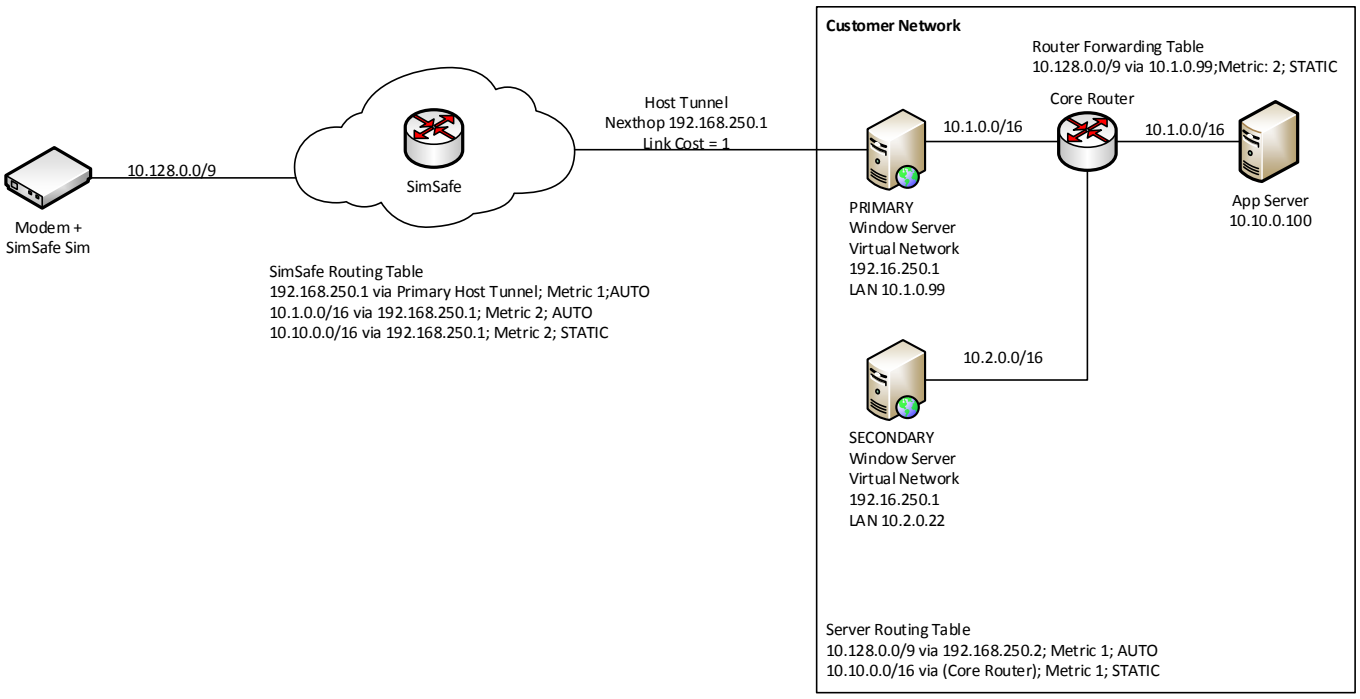


Desired Goal

To add resiliency to the link between the Core Router and SimSafe. Failure of this link could occur if (for example) the server "Primary" goes down for any reason, or the Internet connection for the "Primary" is lost.

Choose “Secondary” VPN Agent Host

The first step is to identify (or add) a suitable server on which to install the secondary VPN Agent. A suitable host is one running Windows 2003 Server or newer. It should not be on the same physical hardware as the primary agent host, and ideally should have an alternate routing path to the Internet (i.e. use a different ISP).
For the purposes of this example, I have assumed that there is a second Windows Server on another network segment. This is illustrated in the diagram below, together with a sample corporate network configuration and the relevant routing table entries for the network:



[Note that in the representational routing table entries in the diagram above, “AUTO” refers to routes that are automatically configured by SimSafe, “STATIC” refers to routes that have been statically configured by the network admin, and “DYNAMIC” refers to dynamic routes that have “learnt” via RIP.]

While it is possible to setup a secondary Agent on the same network segment as the primary agent, but obviously there are more shared points of failure in this scenario. The main requirements on the Secondary server are that it be on separate physical hardware (e.g. not on the same VM host), and that it have a separate route to the Internet (e.g. use separate ISP). The first requirement gives redundancy in the case that the server itself fails, while the second deals with ISP outages.

Add second VPN Agent

First we need to install a VPN Agent in the secondary server. Depending on your subscription plan, you may need to purchase additional VPN Agent licenses. From the Secondary server, login to your SimSafe administration.

To add a VPN Agent:
1. Select **Network** -> **Agents** -> **Choose An Action…** -> **Add Agent**

2. Choose a name for the new Agent (say "Secondary"), and click **Add Agent**

3. Download and Install the new Agent, and click **Done** once complete.

Add Host Tunnel

We now need to create a host tunnel to on the new VPN Agent. This host tunnel will provide an alternate route between SimSafe and the corporate network
To add a Host Tunnel:
1. Select **Network** -> **Static Addressing** -> **Tunnels**

2. Click **Add** Tunnel, select **Add Host Tunnel** and click **Continue.**

3. Select the Agent we just created from the dropdown menu, and choose a name for the tunnel (say "Secondary")

4. Choose a **Next Hop** address that does not conflict with your existing network (say 192.168.251.1).

5. If you wish to load balance traffic across your tunnels, set the **Link Cost** to 1. If you want to favour the other tunnel, set this to a value > 1.

6. Set **Enable Routing** to "yes" and click **Add.**

7. Click **Restart Now** to force a restart of the VPN Agent.

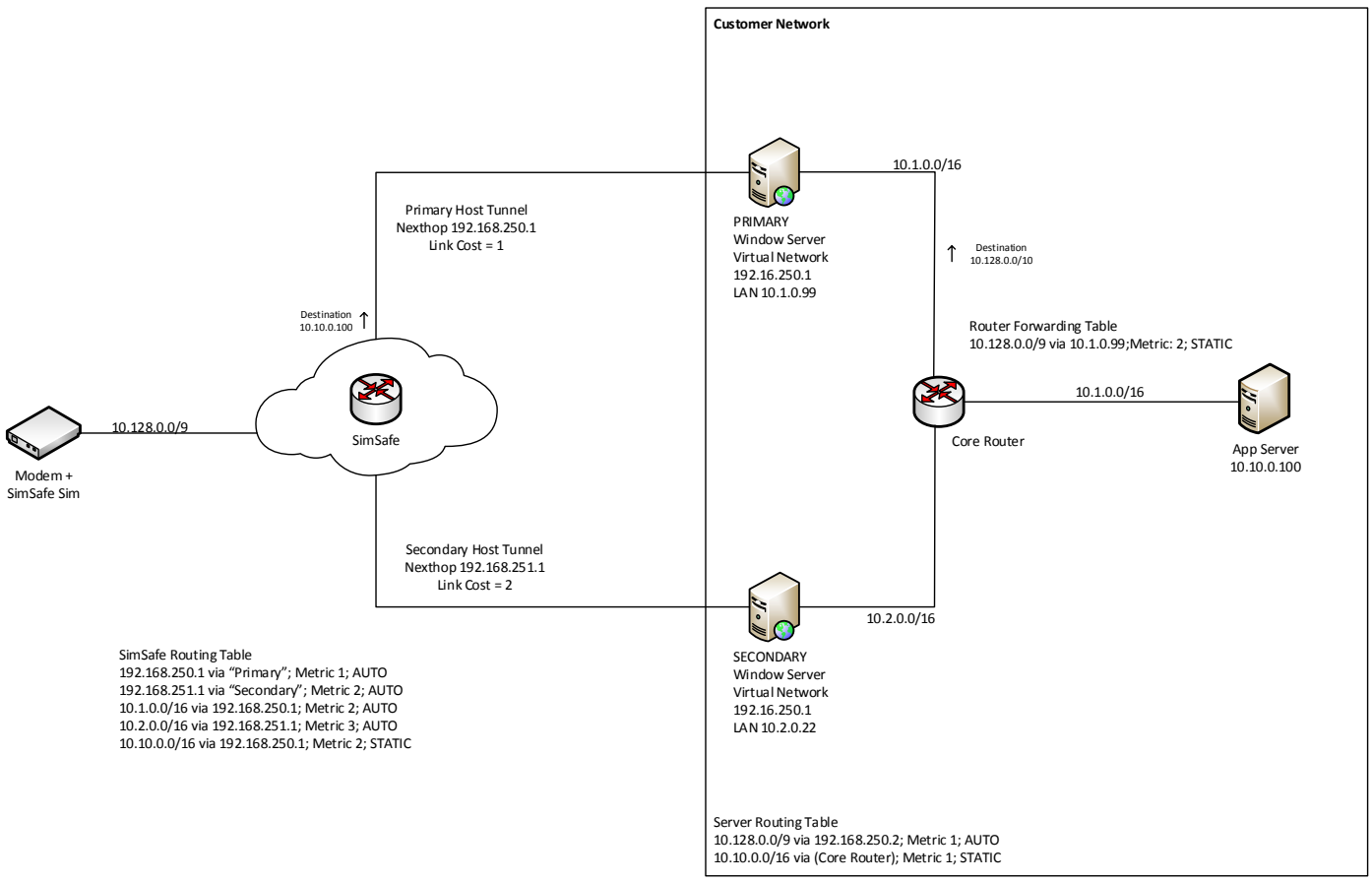
Install the Virtual Adapter

Once the VPN Agent restarts it will pick up the updated tunnel configuration and prompt us to install the Virtual Network Adapter on the secondary Agent host.

To Install the Virtual Adapter

1. Open the VPN Agent Manager on the secondary host.
2. Click **Install Network Adapter** and follow the instructions.
3. After a minute or 2, the tunnel should show as **Connected.**

At this stage, you should be able to verify network connectivity from both “Primary” and “Secondary” to clients on the stub network. This is illustrated in the diagram below:



Note in particular the statically configured routes on (a) SimSafe and (b) the Core Router. SimSafe automatically configures as many routes as it can, but in the single-agent scenario, we had to configure these static routes to ensure that (a) SimSafe could route traffic from the client stub network to the 10.10.0.0/16 network, and that (b) the Core Router knew to route traffic for the client stub 10.128.0.0/9 via the Primary Agent host 10.1.0.99. If we do not make further changes, these static routes mean that packets to and from the App Server ALWAYS traverse the network via the Primary agent, and never actually use the Secondary. We could add further static routes via the Secondary, but these will not provide automatic failover. To achieve this, we now turn to Dynamic Routing.

Introducing RIP and RRAS

RIP (Routing Information Protocol) is an Interior Gateway Protocol (IGP) used to share routes between routers in the same IP Routing Domain. Most routers support RIP and SimSafe can listen to RIP route announcements. On Windows, RIP is provided by the Routing and Remote Access Service (RRAS). To enable Dynamic Routing on our network, we first need to enable and configure RRAS on each Agent Host Server. For the purposes of this document, I am assuming that the Agent hosts are all running Windows Server 2008.

Enable RRAS

RRAS is not enabled by default. Also, RRAS has many features, but we will restrict ourselves to discussing LAN routing and RIP here. RRAS must be enabled on both the Primary and the Secondary servers.

Follow the instructions here: http://technet.microsoft.com/en-us/library/dd469845.aspx

Configure RRAS for LAN Routing

If this is the first time RRAS has been installed, you may need to run-through the RRAS Setup Wizard. We will configure RRAS for LAN Routing only.
NB: This step should not be performed until AFTER the VPN Agent and Virtual Adapter is fully installed on each server.

To configure RRAS for LAN Routing:
1. Open the RRAS MMC Snap-In (**Programs** -> **Administrative Tools** -> **Routing and Remote Access**)
2. Right-click on the server name. If the option to "**Configure and Enable Routing and Remote Access**" not greyed out, then click it (otherwise it is already configured!)
3. The RRAS Setup Wizard starts. Under "Configuration", choose "**Custom Configuration**" and click "Next".
4. Then choose "**LAN Routing**" and click "Next".
5. Then click "Finish", and the service should start.

Enable and Configure RIP

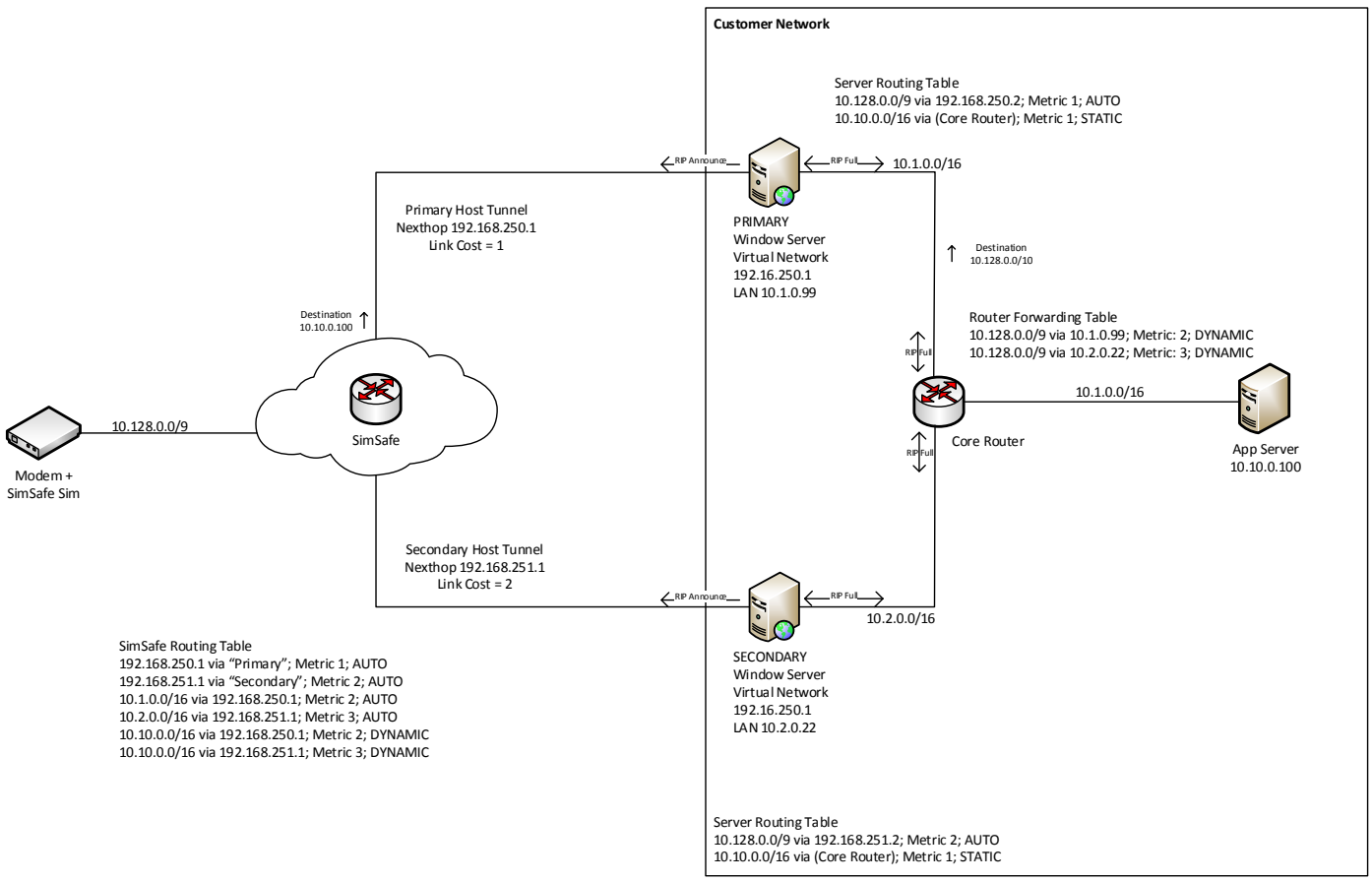
By default, RIP is not enabled on a RRAS server. Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure. We will configure RIP on both the Virtual Adapter (Host Tunnel) Interface, and the LAN Interface on all VPN Agent Hosts.
While RIP on the LAN Interfaces can usually left at the defaults, on the Virtual Adapter (Tunnel) interfaces, we need to specify RIPv2 Multicast, and ignore incoming routes (SimSafe does not announce routes in any case). Finally it is also a good idea not to re-announce the route to the stub network (10.128.0.0/9 in this case).
Follow these steps on both the Primary and the Secondary server,

To enable and configure RIP

1. In the RRAS MMC snap-in, expand **IPv4**, right-click **General**, and then click **New Routing Protocol**.
2. Select **RIP Version 2 for Internet Protocol**, and then click **OK**. **RIP** now appears in the navigation pane under **IPv4**.
3. Right-click **RIP**, and then click **New Interface**.
4. Select the LAN interface and click **OK**.
5. It is usually OK to leave RIP on the LAN Interfaces configured with default settings. If these are satisfactory, click **OK** to save your changes. For information about configuring the RIP options for this interface, see here.
6. Repeat steps 1 – 4 for the Virtual Adapter (Host Tunnel) Interface. We need to change the default settings for this interface.
7. On the **General** tab, under **Incoming Packet Protocol,** select "**Ignore Incoming Packets**".
8. On the **General** tab, under **Outgoing Packet Protocol,** select "**RIP version 2 multicast**".
9. On the **Security** tab, under **Action**, select "**for outgoing routes**", and select "**Do not announce all routes in the ranges listed**"
10. Under "**From**" enter "10.128.0.0". Under "**To**", enter "10.255.255.255", and click **Add**.
11. To accept these changes, click **OK**.

Now both Agent host servers should be announcing their routes to both SimSafe and the Core Router, (and receiving routes from the core router). No explicit RIP configuration is required in SimSafe – it always listens for route announcements from Agent Hosts.
You will need to ensure that RIP on the core router is correctly configured for RIP. The final step is to remove the static route on the core router to 10.128.0.0/9 via the primary host. How to do this on your particular core router is outside the scope of this document.

Updated network diagram



Assuming this is done correctly, we see the following behaviour:

a. SimSafe dynamically "learns" that there are 2 routes to the 10.10.0.0/16 network (1 via each tunnel), as the static routes configured on the Agent host servers will be "ripped" out to SimSafe (Note that this allows us to remove the static route via the Primary tunnel we had to add in the pre-RIP setup.)

b. The Core Router "learns" that there are 2 routes to the 10.128.0.0/9 stub network (1 via each server), as RRAS "rips" out the route that is automatically configured by SimSafe on the LAN Interface for each server.

c. SimSafe and the core router use usual "best-route" analysis to determine how to route traffic – in the scenario depicted here, where both agents are "up", the route via the "Primary" will be chosen as it has a lower metric.

d. If the primary goes down (or its link to the Internet), RIP will ensure that both SimSafe and the core router are informed (via the dynamic routes via the Primary expiring or being actively removed). In any case, the routing tables will be automatically updated and traffic will route via the alternate Agent host.

Summary

SimSafe fully supports dynamic routing via RIPv2. By deploying multiple VPN Agents and configuring RRAS/RIPv2 on your VPN Agent host servers, and on your core router(s), it is possible to achieve full route resiliency on your SimSafe network.