Route Based Virtual Private Network

Document Scope

This solutions document provides details about Route Based Virtual Private Network (VPN) Technology, its advantages, and procedures to configure a Static Route Based VPN.

This document contains the following sections:

- "Overview" section on page 1
- "Using Route Based VPN" section on page 2

Overview

This section provides an introduction to Route Based VPN. This section contains the following subsections:

- "What is a Route Based VPN?" section on page 1
- "Benefits" section on page 2
- "Platforms" section on page 2

What is a Route Based VPN?

In general, a Virtual Private Network (VPN) is a way for companies to have the same security as if all the distributed networks were together, with only one access to the private network, or intranet. Each location has a firewall, configured specially so that it recognizes all the other firewall locations. When the firewall sees a packet headed outward to another protected location, the packet is encrypted. After it travels across the Internet, the receiving firewall then decrypts the packet.

A policy-based approach forces the VPN policy configuration to include the network topology configuration. This makes it difficult for the network administrator to configure and maintain the VPN policy with a constantly changing network topology.

With the Route Based VPN approach, network topology configuration is removed from the VPN policy configuration. The VPN policy configuration creates a Tunnel Interface between two end points. Static routes can then be added tothe Tunnel Interface. The Route Based VPN approach moves network configuration from the VPN policy configuration to Static Route configuration. This requires changes only to the Static Route when network topology changes.

Benefits

Not only does Route Based VPN make configuring and maintaining the VPN policy easier, a major advantage of the Route Based VPN feature is that it provides flexibility on how traffic is routed. With this feature, users can now define multiple paths for overlapping networks over a clear or redundant VPN.

Platforms

The Route Based VPN feature is supported on SonicOS 5.5 Enhanced and higher.

Using Route Based VPN

Route based VPN configuration is a two step process. The first step involves creating a Tunnel Interface. The crypto suites used to secure the traffic between two end-points are defined in the Tunnel Interface. The second step involves creating a static route using Tunnel Interface.

This section contains the following subsections:

- "Configuration Overview" section on page 2
- "Adding a Tunnel Interface" section on page 3
- "Creating a Static Route for Tunnel Interface" section on page 4
- "Route Entries for Different Network Segments" section on page 5
- "Redundant Static Routes for a Network" section on page 5

Configuration Overview

The Tunnel Interface is created when a Policy of type "Tunnel Interface" is added for the remote gateway. The Tunnel Interface must be bound to a physical interface and the IP address of that physical interface is used as the source address of the tunneled packet.

A Static Route ties the traffic (source, destination, and service) to the Tunnel Interface. Any number of overlapping static routes can be added for the tunneled traffic. When networks are added or removed from the topology, the static routes only need to be updated accordingly; the tunnel interface configuration does not need to be updated.

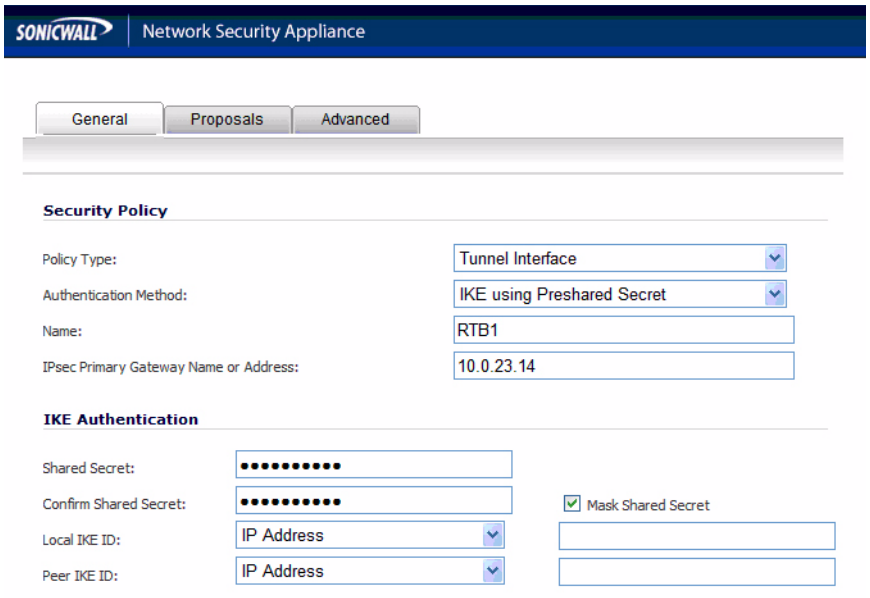
For more details about a general tunnel interface configuration, please refer to the SonicOS Enhanced 5.4 Administrator's Guide: http://www.sonicwall.com/

Adding a Tunnel Interface

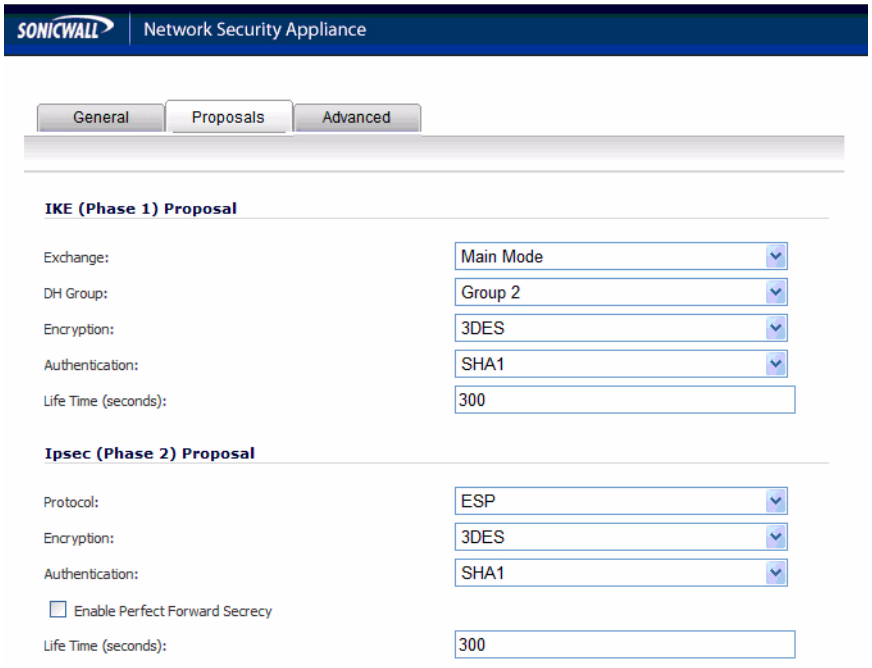
The following procedures explain how to add a Tunnel Interface:

Step 1 Navigate to **VPN>Settings>VPN Policies**. Click the **Add...** button. This will open the VPN Policy Configuration dialog box.

Step 2 On the **General** tab, select the policy type as "Tunnel Interface."

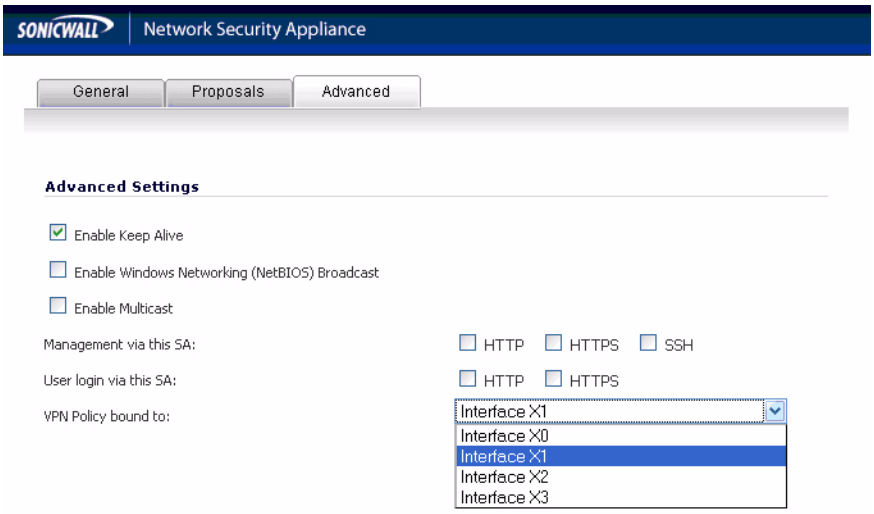


Step 3 Next, navigate to the **Proposal** tab and configure the IKE and IPSec proposals for the tunnel negotiation.



Step 4 Navigate to the **Advanced** tab to configure the advanced properties for the Tunnel Interface. By default, "Enable Keep Alive" is enabled. This is to establish the tunnel with remote gateway proactively.

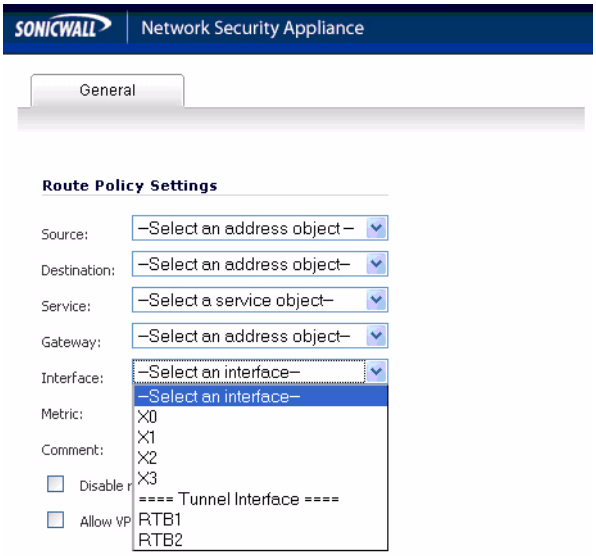
Also, the default tunnel interface is bound to the X1 interface, but can be bound to any of the available interfaces.



Creating a Static Route for Tunnel Interface

After you have successfully added a Tunnel Interface, you may then create a Static Route. Follow the procedures to create a Static Route for a Tunnel Interface.

Step 1 Navigate to **Network>Routing>Route Policies**. Click the **Add...** button. A dialogue window appears for adding Static Route. Note that the "Interface" dropdown menu lists all available tunnel interfaces.

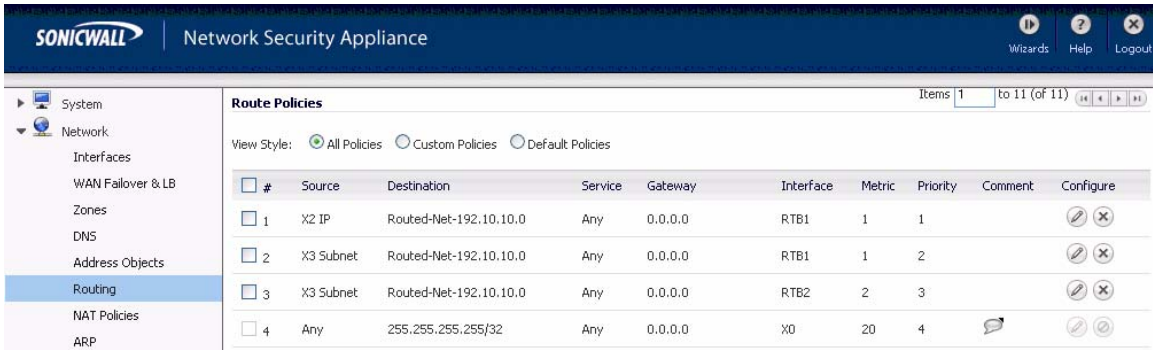


Note If the "Auto-add Access Rule" option is selected, firewall rules are automatically added and traffic is allowed between the configured networks using tunnel interface.

Route Entries for Different Network Segments

After a tunnel interface is created, multiple route entries can be configured to use the same tunnel interface for different networks. This provides a mechanism to modify the network topology without making any changes to the tunnel interface.

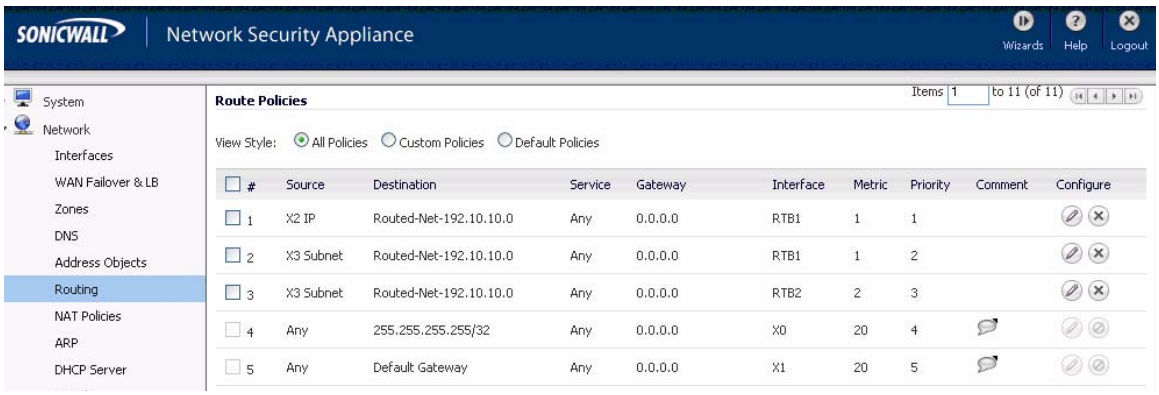
The image below shows an example of same tunnel interface for different networks:



Redundant Static Routes for a Network

Also after more than one tunnel interface is configured, you can add multiple overlapping static routes; each static route uses a different tunnel interface to route the traffic. This provides routing redundancy for the traffic to reach the destination.

The image below illustrates redundant static routes for a network:

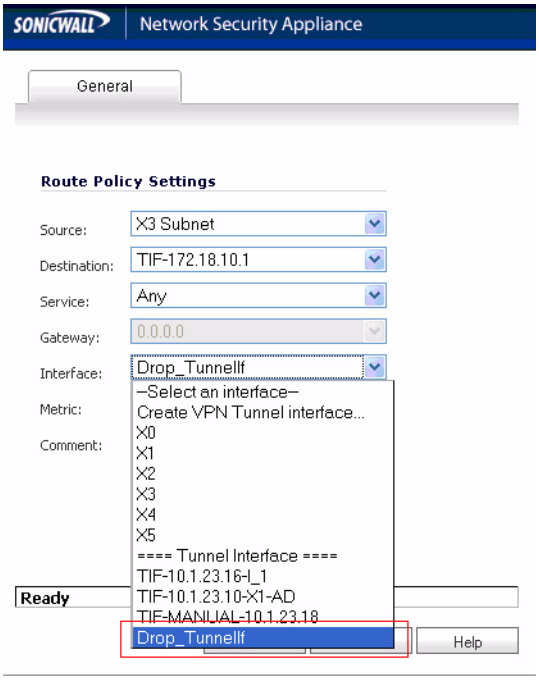


Drop Tunnel Interface

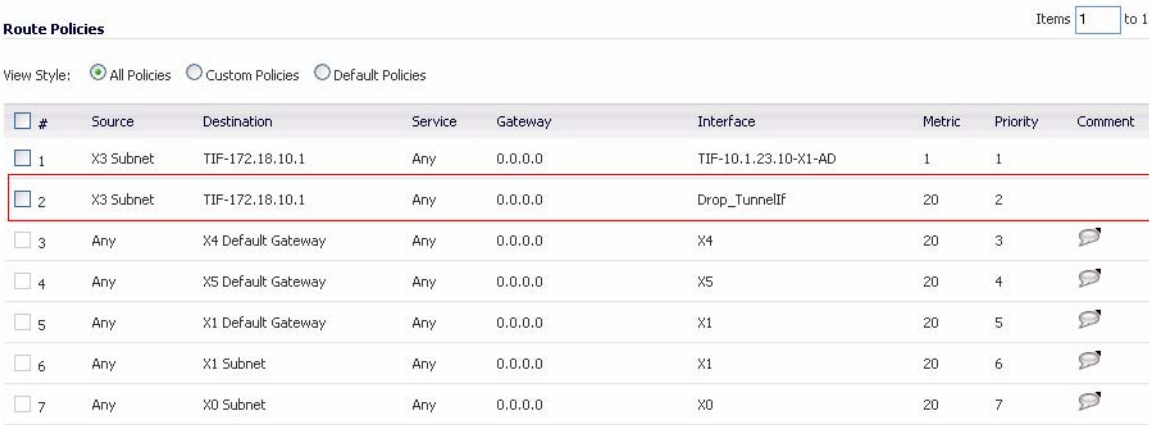
The Drop Tunnel Interface is a pre-configured tunnel interface. This interface provides added security for traffic. An example of this would be if a static route bind interface is deemed the drop tunnel interface, then all the traffic for that route is dropped and not forwarded in clear. If a static route bind to tunnel interface is defined for traffic (source/destination/service), and it is desired that traffic should not be forwarded in the clear if the tunnel interface is down, it is recommended to configure a static route bind to drop tunnel interface for the same network traffic. As a result, if the tunnel interface is down, traffic will be dropped due to the drop tunnel interface static route.

Creating a Static Route for Drop Tunnel Interface

To add a static route for drop tunnel interface, navigate to **Network>Routing>Routing Policies**. Click the **Add...** button. Similar to configuring a State route for a Tunnel Interface, configure the values for Source, Destination, and Service Objects. Under Interface, select "Drop_tunnelIf."



Once added, the route is enabled and displayed in the Route Policies.



Solution Document Version History

Version Number	Date	Notes
1	6/24/2009	This document was created by Angela Mendoza.
2	7/20/2009	Incorporated feedback from Naveen Kulshreshtha.
3	7/20/2009	Incorporated feedback from Patrick Lydon.
4	7/27/2009	Incorporated feedback from Naveen Kulshreshtha.