



How to configure a tunnel
interface VPN (Route-Based
VPN)

**KNOWLEDGE
DATABASE**

How to configure a tunnel interface VPN (Route-Based VPN)

1. Go to **Manage | VPN | Base Settings** and click on **Add**.
2. The General tab of Tunnel Interface VPN named is shown with the **IPSec Gateway** equal to the other device's **X1 IP address**.

NOTE: The settings used on the Proposals tab are not shown, but these must be identical on the Tunnel Interface VPNs done on both appliances.

SONICWALL® Network Security Appliance

General Proposals Advanced

Security Policy

Policy Type: Tunnel Interface
 Authentication Method: IKE using Preshared Secret
 Name: ToSiteB
 IPsec Primary Gateway Name or Address:

IKE Authentication

Shared Secret: *****
 Confirm Shared Secret: ***** Mask Shared Secret
 Local IKE ID: IPv4 Address
 Peer IKE ID: IPv4 Address

3. Go to **Network | Routing** and click **Add**.
4. The **Route Policy** example shown below is one in which the source is **Any**, and the destination is the **siteb_subnet**, the service is **Any**, and the Interface is set to the name of the previously-created Tunnel Interface VPN, named **'to site b'**; note that the Gateway field is grayed out because SonicOS is smart enough to know that there is already a specific network interface tied to the tunnel interface VPN created above. The properties of the VPN network address object **siteb_subnet** are also shown: 192.168.10.0 / 255.255.255.0.

SONICWALL® Network Security Appliance

Name: Siteb_subnet
 Zone Assignment: VPN
 Type: Network
 Network: 192.168.10.0
 Netmask/Prefix Length: 255.255.255.0

Ready

General

Advanced

Route Policy Settings

Source: Any
 Destination: Siteb_subnet
 Service: Any
 Standard Route Multi-Path Route
 Interface: --Select an interface--
 Gateway: 0.0.0.0
 Metric:
 Comment:
 Disable route when the interface is disconnected
 Allow VPN path to take precedence
 WXA Group: None
 Probe: None
 Disable route when probe succeeds
 Probe default state is UP

• Now log into the SiteB SonicWall

1. Go to **VPN | Settings** and click on **Add**. The General tab of Tunnel Interface VPN is shown with the IPSec Gateway equal to the other device's **X1 IP address**.

General Proposals Advanced

Security Policy

Policy Type: Tunnel Interface

Authentication Method: IKE using Preshared Secret

Name: ToSiteA

IPsec Primary Gateway Name or Address:

IKE Authentication

Shared Secret: [masked]

Confirm Shared Secret: [masked] Mask Shared Secret

Local IKE ID: IPv4 Address

Peer IKE ID: IPv4 Address

Ready

OK CANCEL HELP

1. **NOTE:** The settings used on the Proposals tab are not shown, but these must be identical on the Tunnel Interface VPNs done on both appliances.

2. Go to **Network | Routing** and click **Add**.

3. The **Route Policy** example shown below is one in which the source is **Any**, and the destination is the **sitea_subnet**, the service is **Any**, and the Interface is set to the name of the previously-created Tunnel Interface VPN, named **'to site a'**; note that the Gateway field is grayed out because SonicOS is smart enough to know that there is already a specific network interface tied to the tunnel interface VPN created above. The properties of the VPN network address object **sitea_subnet** are also shown: 10.10.50.0 / 255.255.255.0.

General Advanced

Route Policy Settings

Source: Any

Destination: SiteA_subnet

Service: Any

Standard Route Multi-Path Route

Interface: --Select an interface--

Gateway: 0.0.0.0

Metric:

Comment:

Disable route when the interface is disconnected

Allow VPN path to take precedence

WXA Group: None

Probe: None

Disable route when probe succeeds

Probe default state is UP

Name: SiteA_subnet

Zone Assignment: VPN

Type: Network

Network: 10.10.50.0

Netmask/Prefix Length: 255.255.255.0

Ready