

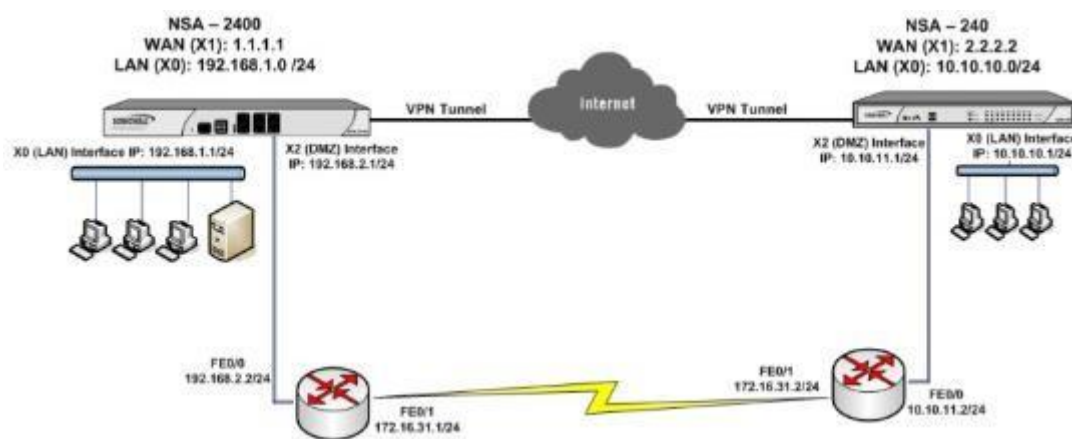


**Configuring VPN Failover using
Static Routes and Network
Monitor Probes**

**KNOWLEDGE
DATABASE**

Configuring VPN Failover using Static Routes and Network Monitor Probes

This article illustrates a scenario wherein two sites with SonicWall UTM devices are connected to each other over a direct connection or an MPLS connection. A site to site VPN connection is defined concurrently between the two sites. The primary connection between the two sites is the direct or the MPLS connection and when it fails, traffic would automatically be routed through a site to site VPN (policy based).



For this article, we'll be using the following IP addresses as examples. You can substitute your IP addresses for the examples shown here:

NSA 2600 (Site A)

WAN (X1): 1.1.1.1

LAN (X0): 192.168.1.1/24

MPLS Router fe0/0 IP: 192.168.2.2/24

MPLS Router fe0/1 IP: 172.16.31.1/24

TZ300 (Site B)

WAN (X1): 2.2.2.2

LAN (X0): 10.10.10.1/24

MPLS Router fe0/0 IP: 10.10.11.2/24

MPLS Router fe0/1 IP: 172.16.31.2/24

NOTE: This article does not describe the method to create a site to site VPN or an MPLS connection. Before defining the methods to configure the failover, the following factors are assumed to be in place:

1. That a site to site VPN has been configured correctly and tunnel is up.
2. That a direct or MPLS connection exists between Site A and Site B.
3. That although a direct connection exists between Site A and Site B, traffic is passing to the other side over the VPN tunnel.

The procedure to configure a failover is the following:

Create a probe-dependent static route to route all traffic destined to the remote MPLS network. This route would take precedence over the VPN route. The probe target should be the IP address of the MPLS router

on the other side. The probe target is defined by creating a **Network Monitor Policy** under **Network | Network Monitor**.

A separate route should be created defining the path to take to reach the probe target. Network Monitor Policy would probe the target regularly. Failure of the MPLS connection would also result in the failure of the probe target. When the probe fails, SonicWall would disable the static route thus allowing the VPN kernel routes (hidden) to take precedence.

When the probe target is reachable again, the static route would be re-enabled, forcing traffic over the MPLS connection.

1. Create the following address objects under

- **Network | Address Objects** and group them.

TZ300

#	Name	Details	Type	IP Version	Zone	Class
1	IphPolicyDstAuto_0		Group			Custom
2	Local Site		Group			Custom
3	NSA2600		Group			Custom
	NSA2600 DMZ	192.168.2.0/255.255.255.0	Network	IPv4	DMZ	Custom
	NSA2600 LAN	192.168.1.0/255.255.255.0	Network	IPv4	DMZ	Custom
4	Remote Site		Group			Custom

NSA 2600

#	Name	Details	Type	IP Version	Zone	Class
5	TZ300		Group			Custom
	TZ300 LAN	10.10.11.0/255.255.255.0	Network	IPv4	DMZ	Custom
	TZ300 DMZ	10.10.10.0/255.255.255.0	Network	IPv4	DMZ	Custom

- Create the following additional address objects

NSA 2600

SONICWALL™ Network Security Appliance

Name:

Zone Assignment:

Type:

IP Address:

TZ300

SONICWALL™ Network Security Appliance

Name:

Zone Assignment:

Type:

IP Address:

SONICWALL™ Network Security Appliance

Name:

Zone Assignment:

Type:

IP Address:

SONICWALL™ Network Security Appliance

Name:

Zone Assignment:

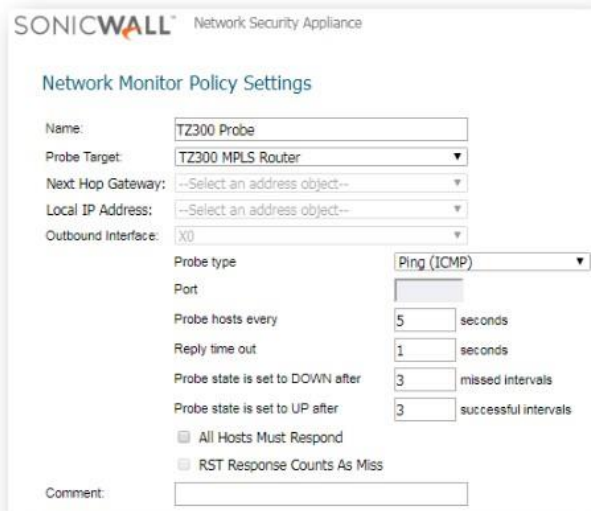
Type:

IP Address:

2. Create a Network Monitor Policy

- The probe target is defined by creating a **Network Monitor Policy** under **Network | Network Monitor**

NSA 2600



SONICWALL® Network Security Appliance

Network Monitor Policy Settings

Name: TZ300 Probe

Probe Target: TZ300 MPLS Router

Next Hop Gateway: --Select an address object--

Local IP Address: --Select an address object--

Outbound Interface: X0

Probe type: Ping (ICMP)

Port: []

Probe hosts every: 5 seconds

Reply time out: 1 seconds

Probe state is set to DOWN after: 3 missed intervals

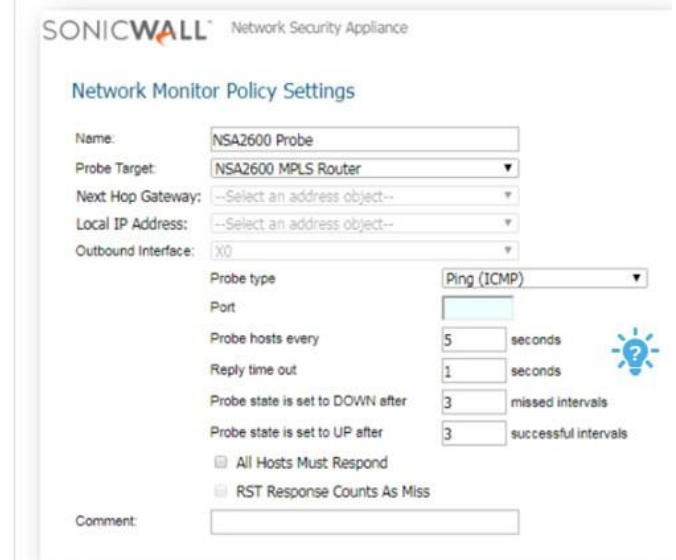
Probe state is set to UP after: 3 successful intervals

All Hosts Must Respond

RST Response Counts As Miss

Comment: []

TZ300



SONICWALL® Network Security Appliance

Network Monitor Policy Settings

Name: NSA2600 Probe

Probe Target: NSA2600 MPLS Router

Next Hop Gateway: --Select an address object--

Local IP Address: --Select an address object--

Outbound Interface: X0

Probe type: Ping (ICMP)

Port: []

Probe hosts every: 5 seconds

Reply time out: 1 seconds

Probe state is set to DOWN after: 3 missed intervals

Probe state is set to UP after: 3 successful intervals

All Hosts Must Respond

RST Response Counts As Miss

Comment: []

Create a static route to route traffic to the probe target

- Go to **Network | Routing | Add**

NSA 2600



SONICWALL® Network Security Appliance

General Advanced

Route Policy Settings

Source: Any

Destination: TZ300 MPLS Router

Service: Any

Standard Route Multi-Path Route

Interface: X1

Gateway: NSA2600 DMZ Gateway

Metric: 1

Comment: []

Disable route when the interface is disconnected

Allow VPN path to take precedence

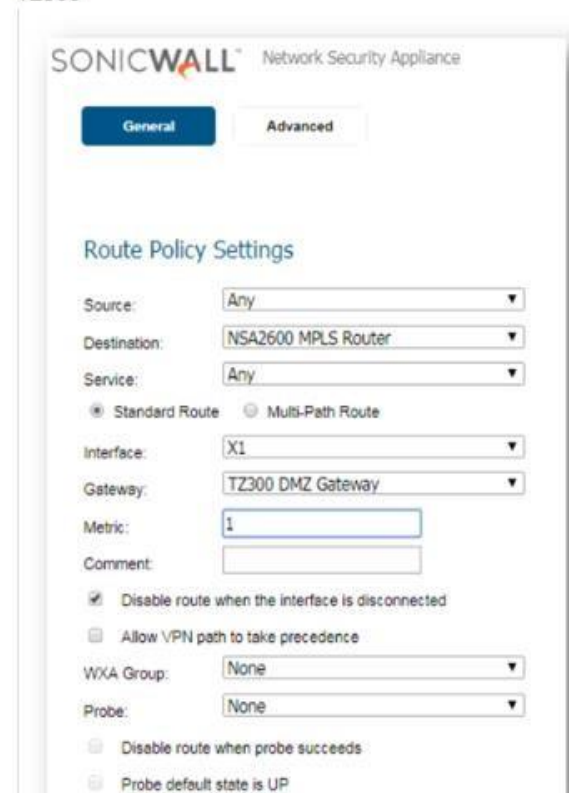
WXA Group: None

Probe: None

Disable route when probe succeeds

Probe default state is UP

TZ300



SONICWALL® Network Security Appliance

General Advanced

Route Policy Settings

Source: Any

Destination: NSA2600 MPLS Router

Service: Any

Standard Route Multi-Path Route

Interface: X1

Gateway: TZ300 DMZ Gateway

Metric: 1

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

- Create a static route to pass all traffic over the direct connection with probing enabled.

NSA 2600

SONICWALL Network Security Appliance

General Advanced

Route Policy Settings

Source: Any

Destination: TZ300

Service: Any

Standard Route Multi-Path Route

Interface: X1

Gateway: NSA2600 DMZ Gateway

Metric: 1

Comment:

Disable route when the interface is disconnected

Allow VPN path to take precedence

WXA Group: None

Probe: TZ300 Probe

Disable route when probe succeeds

Probe default state is UP

TZ300

SONICWALL Network Security Appliance

General Advanced

Route Policy Settings

Source: Any

Destination: NSA2600

Service: Any

Standard Route Multi-Path Route

Interface: X1

Gateway: TZ300 DMZ Gateway

Metric: 1

Comment:

Disable route when the interface is disconnected

Allow VPN path to take precedence

WXA Group: None

Probe: NSA2600 Probe

Disable route when probe succeeds

Probe default state is UP

This concludes the configuration portion of this article.

How to Test:

On creating the routes traffic would be forwarded through the direct or MPLS connection. The site to site VPN policy would still show as up with a green light. To test whether failover and fallback is functioning as intended, perform the following:

1. Disconnect, either physically or logically, the MPLS connection.
2. The Network Monitor policy will become inactive as the probing defined in the policy to the probe target will fail.
3. Consequent to the probe failure, the static route created to route traffic to the other side will be disabled.
4. When the static route is disabled, the VPN kernel routes will be re-enabled and traffic will be forwarded over the VPN tunnel.
5. Re-connect the MPLS connection.
6. The Network Monitor policy will become active again as the probing defined in the policy is successful.
7. When the probe succeeds the static route will be re-enabled automatically.
8. As static route takes precedence over VPN routes, traffic will again be routed through the direct or MPLS connection.

RESOLUTION FOR SONICOS 6.5 AND LATER

SonicOS 6.5 was released September 2017. This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 and later firmware.

The procedure to configure a failover is the following:

Create a probe-dependent static route to route all traffic destined to the remote MPLS network. This route would take precedence over the VPN route. The probe target should be the IP address of the MPLS router on the other side. The probe target is defined by creating a **Network Monitor Policy** under **Network | Network Monitor**.

A separate route should be created defining the path to take to reach the probe target. Network Monitor Policy would probe the target regularly. Failure of the MPLS connection would also result in the failure of the probe target. When the probe fails, SonicWall would disable the static route thus allowing the VPN kernel routes (hidden) to take precedence.

When the probe target is reachable again, the static route would be re-enabled, forcing traffic over the MPLS connection.

1. Create the following address objects under
 - **Manage** tab
 - **Objects | Address Objects** and group them.

TZ300

#	Name	Details	Type	IP Version	Zone	Class
1	IphPolicyDstAuto_0		Group			Custom
2	Local Site		Group			Custom
3	NSA2600		Group			Custom
	NSA2600 DMZ	192.168.2.0/255.255.255.0	Network	IPv4	DMZ	Custom
	NSA2600 LAN	192.168.1.0/255.255.255.0	Network	IPv4	DMZ	Custom
4	Remote Site		Group			Custom

NSA 2600

5	TZ300		Group			Custom
	TZ300 LAN	10.10.11.0/255.255.255.0	Network	IPv4	DMZ	Custom
	TZ300 DMZ	10.10.10.0/255.255.255.0	Network	IPv4	DMZ	Custom

- Create the following additional address objects

NSA 2600

SONICWALL™ Network Security Appliance

Name: TZ300 MPLS Router
 Zone Assignment: DMZ
 Type: Host
 IP Address: 172.16.31.2

TZ300

SONICWALL™ Network Security Appliance

Name: NSA2600 MPLS Router
 Zone Assignment: DMZ
 Type: Host
 IP Address: 172.16.31.1

SONICWALL™ Network Security Appliance

Name: NSA2600 DMZ Gateway
 Zone Assignment: DMZ
 Type: Host
 IP Address: 192.168.2.2

SONICWALL™ Network Security Appliance

Name: TZ300 DMZ Gateway
 Zone Assignment: DMZ
 Type: Host
 IP Address: 10.10.11.2

2. Create a Network Monitor Policy

- The probe target is defined by creating a **Network Monitor Policy** under the **Investigate** tab | **Network Probes**

NSA 2600

SONICWALL™ Network Security Appliance

Network Monitor Policy Settings

Name: TZ300 Probe
 Probe Target: TZ300 MPLS Router
 Next Hop Gateway: --Select an address object--
 Local IP Address: --Select an address object--
 Outbound Interface: X0
 Probe type: Ping (ICMP)
 Port:
 Probe hosts every: 5 seconds
 Reply time out: 1 seconds
 Probe state is set to DOWN after: 3 missed intervals
 Probe state is set to UP after: 3 successful intervals
 All Hosts Must Respond
 RST Response Counts As Miss
 Comment:

TZ300

SONICWALL™ Network Security Appliance

Network Monitor Policy Settings

Name: NSA2600 Probe
 Probe Target: NSA2600 MPLS Router
 Next Hop Gateway: --Select an address object--
 Local IP Address: --Select an address object--
 Outbound Interface: X0
 Probe type: Ping (ICMP)
 Port:
 Probe hosts every: 5 seconds
 Reply time out: 1 seconds
 Probe state is set to DOWN after: 3 missed intervals
 Probe state is set to UP after: 3 successful intervals
 All Hosts Must Respond
 RST Response Counts As Miss
 Comment:

Create a static route to route traffic to the probe target

- Go to the **Manage** tab
- Click **Network | Routing**

NSA 2600



SONICWALL Network Security Appliance

General Advanced

Route Policy Settings

Source: Any

Destination: TZ300 MPLS Router

Service: Any

Standard Route Multi-Path Route

Interface: X1

Gateway: NSA2600 DMZ Gateway

Metric: 1

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

TZ300



SONICWALL Network Security Appliance

General Advanced

Route Policy Settings

Source: Any

Destination: NSA2600 MPLS Router

Service: Any

Standard Route Multi-Path Route

Interface: X1

Gateway: TZ300 DMZ Gateway

Metric: 1

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

Create a static route to pass all traffic over the direct connection with probing enabled.

NSA 2600



SONICWALL Network Security Appliance

General Advanced

Route Policy Settings

Source: Any

Destination: TZ300

Service: Any

Standard Route Multi-Path Route

Interface: X1

Gateway: NSA2600 DMZ Gateway

Metric: 1

Comment:

Disable route when the interface is disconnected

Allow VPN path to take precedence

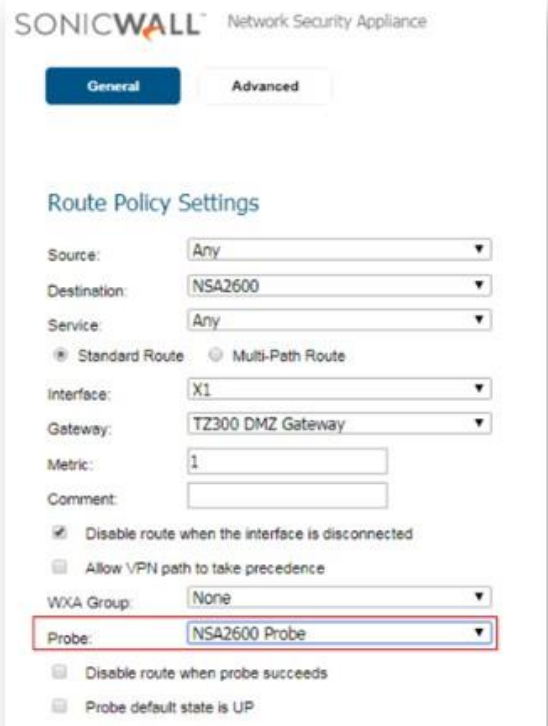
WXA Group: None

Probe: TZ300 Probe

Disable route when probe succeeds

Probe default state is UP

TZ300



SONICWALL Network Security Appliance

General Advanced

Route Policy Settings

Source: Any

Destination: NSA2600

Service: Any

Standard Route Multi-Path Route

Interface: X1

Gateway: TZ300 DMZ Gateway

Metric: 1

Comment:

Disable route when the interface is disconnected

Allow VPN path to take precedence

WXA Group: None

Probe: NSA2600 Probe

Disable route when probe succeeds

Probe default state is UP

This concludes the configuration portion of this article.

How to Test:

On creating the routes traffic would be forwarded through the direct or MPLS connection. The site to site VPN policy would still show as up with a green light. To test whether failover and fallback is functioning as intended, perform the following:

1. Disconnect, either physically or logically, the MPLS connection.
2. The Network Monitor policy will become inactive as the probing defined in the policy to the probe target will fail.
3. Consequent to the probe failure, the static route created to route traffic to the other side will be disabled.
4. When the static route is disabled, the VPN kernel routes will be re-enabled and traffic will be forwarded over the VPN tunnel.
5. Re-connect the MPLS connection.
6. The Network Monitor policy will become active again as the probing defined in the policy is successful.
7. When the probe succeeds the static route will be re-enabled automatically.
8. As static route takes precedence over VPN routes, traffic will again be routed through the direct or MPLS connection.