Implementing Hub and Spoke Site-to-Site VPN

KNOWLEDGE DATABASE

Implementing Hub and Spoke Site-to-Site VPN

It is possible to establish a site to site VPN between a hub SonicWall (such as a corporate headquarters) and multiple spoke SonicWalls (branch offices) where the branches are able to communicate using the hub as an intermediary. The purpose of this document is to outline all necessary steps to configure a VPN consisting of one hub and two spokes where all firewalls are running SonicOS Enhanced. An example is used throughout this document to clarify all concepts and instructions.

Example Hub and Spoke Network
Use of a simple example scenario will aid the creation of a hub and spoke VPN. It may be of further help to create a network diagram based on this information. The information from this example will be used throughout the rest of this document.

Example Hub and Spoke Specifications
Two branch offices (Networks A and C) will connect to a hub at the corporate headquarters (Network B). Networks A and C will be able to exchange traffic through the hub. Review the specifications in the following table:

Branch Office A	LAN A Subnet	10.0.1.0/24
	WAN A IP Address	192.168.1.1/24
Corporate Office (hub) B	LAN B Subnet	10.0.2.0/24
	WAN B IP Address	192.168.2.1/24
Branch Office C	LAN C Subnet	10.0.3.0./24
	WAN C IP Address	192.168.3.1./24

Create Address and Group Objects

A number of address objects are needed in the implementation of any site to site VPN. This need is greater in a hub and spoke configuration. Group objects will also be required. The address objects will specify local and destination networks, which will be grouped together to permit hub and spoke communication. Access the **Network | Address Objects** page in each firewall to configure the address and group objects as needed.

Create the Address Objects
Address objects must be configured as follows on all three firewalls to enable this VPN connection. Go to **Network | Address Objects** tab and Create the following address objects on Spoke A:

- Name: LAN B Subnet

Zone: VPN

Type: Network

IP Address: 10.0.2.0

Subnet Mask: 255.255.255.0

- Name: LAN C Subnet

Zone: VPN

Type: Network

IP Address: 10.0.3.0

Subnet Mask: 255.255.255.0

Create the following address objects on Hub B:

- Name: LAN A Subnet

Zone: VPN

Type: Network

IP Address: 10.0.1.0

Subnet Mask: 255.255.255.0

- Name: LAN C Subnet

Zone : VPN

Type: Network

IP Address: 10.0.3.0

Subnet Mask: 255.255.255.0

Create the following address objects on Spoke C:

Calle 146 #7-64. Bogotá D.C. Colombia
+57 1 466 0599 / +57 315 786 8258
sales@itclatam.com / tss@itclatam.com

- Name: LAN A Subnet

Zone: VPN

Type: Network

IP Address: 10.0.1.0

Subnet Mask: 255.255.255.0

- Name: LAN B Subnet

Zone: VPN

Type: Network

IP Address: 10.0.2.0

Subnet Mask: 255.255.255.0

Create the Group Objects

The need to specify multiple local and destination networks mandates the creation of address object groups, since only one such object may be selected in the VPN policy configuration screen. Create the groups as specified below on each firewall, then join the specified address objects to the groups.

Configure group on Spoke A:

- Group name: Destination B and C
  Members: LAN B Subnet, LAN C Subnet

Configure groups on Hub B:

- Group name: Local B and C
  Members: LAN Subnets, LAN C Subnet
- Group name: Local A and B
  Members: LAN Subnets, LAN A Subnet

Configure groups on Spoke C:

- Group name: Destination A and B
  Members: LAN A Subnet, LAN B Subnet

Making the Connections

Now that all address and group objects have been established, the security associations can be created to enable the hub and spoke VPN. Each spoke will need only one VPN policy pointing to the hub. The hub will require two VPN policies, one to each spoke. Each policy is created on the **VPN | Settings** page in the usual manner for any site to site tunnel, with the exception of the **Network tab** as shown below.

Spoke A VPN Policy

On the **Network tab** for this VPN policy, specify the **LAN Subnets** object as the local network and the Destination B and C group object as the destination network.

Hub B VPN Policy

There should be two policies defined on the hub SonicWall, one pointing to Spoke A and the other to Spoke B. Specify the **local and destination** objects on the **Network tab** for each policy as follows:

- Spoke A policy

Local Network: Local B and C

Destination Network: LAN A Subnet

- Spoke C policy

Local Network: Local A and B

Destination Network: LAN C Subnet

Spoke C VPN Policy

On the **Network tab** for this VPN policy, specify the **LAN Subnets** object as the local network and the Destination A and B object as the destination network.

Create the VPN to VPN Access Rule

Follow these steps to create the access rule on each SonicWall appliance (the hub and both spokes) allowing communication between VPN tunnels:

1. Click **Firewall | Access rules | select Matrix**.
2. Select the **edit icon** at the point of intersection for the **"VPN to VPN"** zone.
3. Add a new rule:
   Action: Allow
   Service: Any
   Source: Any
   Destination: Any
4. Click OK.

How to Test:

After following all of the above steps, a working VPN should be successfully established between one hub SonicWall and two spokes. Expansion of this basic model may enable VPN tunnels to hundreds of spokes through a hub given sufficient bandwidth. This example scenario may be simply tested by pinging the IP addresses of various computers on the LAN sides of each SonicWall. For example, from a computer behind the hub, ping computers behind the LANs of spokes A and C. Similarly, from each spoke, ping computers behind the hub and the opposite spoke.