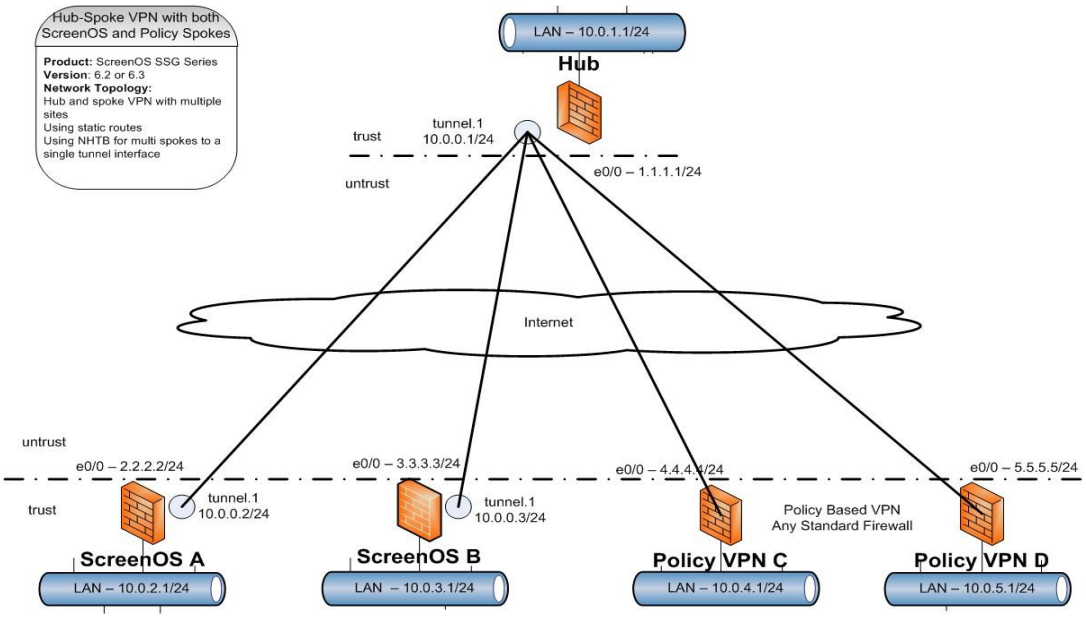
ScreenOS - Hub-Spoke VPN with mix of Policy and Route spoke sites

Product: ScreenOS SSG Series

Version: 6.2

Network Topology:



Hub and spoke VPN with multiple sites using point to multipoint

Two sites routing VPN with SSG

Two sites Policy VPN with any standards based firewall

Description:

This hub and spoke setup allows multiple sites on either route or policy based VPN to connect to a common tunnel interface. This uses static routes and NHTB (Next hop Tunnel Binding) to direct traffic in the network. These allow the mixing of SSG and non-SSG policy based VPN on the same hub and spoke network.

The configuration requires a base setup on the hub location where primary services are connected. Each spoke then has a configuration set to connect and provide these services to the hub. While the hub adds a section for each new spoke that is created in the system.

1. Configure base services on the hub location. This occurs only once and remains the same no matter how many spokes are added to the system.
2. For each spoke there are two sets of configuration
   A) Hub configuration for VPN access to the spoke

ScreenOS - Hub-Spoke VPN with mix of Policy and Route spoke sites

B) Spoke configuration settting up basic services and the VPN to the hub

Zone Layout

untrust interface is ethernet0/0

trust interface is bgroup0

tunnel.1 interface is in trust zone

This zone layout puts all sites and tunnels into the same security zone. No policies need to be created on any device for full communications across the entire hub and spoke network. This is assuming that intra zone blocking is NOT enabled on any of the firewalls for the trust zone. This is the default behavior for the trust zone. You can change the zone of the tunnel interface to untrust and create policies as needed to allow traffic.

Configuration

1. Hub location base configuration:
This sets up and configures all needed services on the hub shared by all tunnels

Create VPN tunnel interface

set interface tunnel.1 zone Trust

set interface tunnel.1 ip 10.0.0.1/24

2. A. Hub location per spoke configuration:
Repeat only these commands for additional spoke sites

Create VPN Gateway to spoke

set ike gateway SpokeA-GW address 2.2.2.2 Main outgoing-interface "ethernet0/0" preshare Juniper== sec-level standard

set ike gateway SpokeB-GW address 3.3.3.3 Main outgoing-interface "ethernet0/0" preshare Juniper== sec-level standard

set ike gateway SpokeC-GW address 4.4.4.4 Main outgoing-interface "ethernet0/0" preshare Juniper== sec-level standard

set ike gateway SpokeD-GW address 5.5.5.5 Main outgoing-interface "ethernet0/0" preshare Juniper== sec-level standard

Create VPN tunnel bound to tunnel interface

SSG tunnels use the remote tunnel interface as the NHTB gateway

set vpn SpokeA gateway SpokeA-GW no-replay tunnel idletime 0 sec-level standard

set vpn SpokeA bind interface tunnel.1

ScreenOS - Hub-Spoke VPN with mix of Policy and Route spoke sites

set interface tunnel.1 nhtb 10.0.0.2 vpn SpokeA

set vpn SpokeB gateway SpokeB-GW no-replay tunnel idletime 0 sec-level standard

set vpn SpokeB bind interface tunnel.1

set interface tunnel.1 nhtb 10.0.0.3 vpn SpokeA

Policy Based Tunnels add the Proxy-id for the connection and the remote router ip for the NHTB gateway

set vpn SpokeC gateway SpokeC-GW no-replay tunnel idletime 0 sec-level standard

set vpn SpokeC bind interface tunnel.1

set interface tunnel.1 nhtb 10.0.4.1 vpn SpokeC

set vpn SpokeC proxy-id local-ip 10.0.1.0/24 remote-ip 10.0.4.0/24 "ANY"

set vpn SpokeD gateway SpokeD-GW no-replay tunnel idletime 0 sec-level standard

set vpn SpokeD bind interface tunnel.1

set interface tunnel.1 nhtb 10.0.5.1 vpn SpokeD

set vpn SpokeD proxy-id local-ip 10.0.1.0/24 remote-ip 10.0.5.0/24 "ANY"

Create Static Routes to spoke sites

set route 10.0.2.0/24 interface tunnel.1 gateway 10.0.0.2

set route 10.0.3.0/24 interface tunnel.1 gateway 10.0.0.3

SSG use the tunnel interface as the gateway

set route 10.0.4.0/24 interface tunnel.1 gateway 10.0.4.1

set route 10.0.5.0/24 interface tunnel.1 gateway 10.0.5.1

Policy based VPN use the remote LAN router interface as the gateway

2. B. Spoke location:

All steps on spokes are identical with exceptions noted below. Change the indicated parameters to match the spoke location on the network as each new spoke is added.

These only apply the SSG route based VPN sites. The policy sites are configured by the normal standard on the remote equipment.

Create VPN tunnel interface

set interface tunnel.1 zone Trust

set interface tunnel.1 ip 10.0.0.2/24

**Change the ip address to match the spoke location

Create VPN Gateway to hub

ScreenOS - Hub-Spoke VPN with mix of Policy and Route spoke sites

set ike gateway Hub-gw address 1.1.1.1 Main outgoing-interface ethernet0/0 preshare juniper== sec-level standard

Create VPN tunnel bound to tunnel interface

set vpn Hub gateway Hub-GW no-replay tunnel idletime 0 sec-level standard

set vpn Hub bind interface tunnel.1

Create Static route to hub

set route 10.0.1.0/24 interface tunnel.1 gateway 10.0.0.1

NHTB is only needed on the hub as each spoke has only one tunnel

Verification:

routing table checks

Running "get route protocol static" on a spoke should show the routes to the hub with a capital S label. The hub site will show all of the sites with their static routes.

get route protocol static

IPv4 Dest-Routes for <untrust-vr> (0 entries)

H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
N: NHRP
iB: IBGP eB: EBGP O: OSPF E1: OSPF external type 1
E2: OSPF external type 2 trailing B: backup route

IPv4 Dest-Routes for <trust-vr> (14 entries)

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	13	10.0.2.0/24	tun.1	10.0.0.2	S	20	1	Root
*	12	10.0.3.0/24	tun.1	10.0.0.3	S	20	1	Root
*	11	10.0.4.0/24	tun.1	10.0.4.1	S	20	1	Root
*	14	10.0.5.0/24	tun.1	10.0.5.1	S	20	1	Root

From the hub site confirm ping to all remote router ip addresses

ping 10.0.2.1 from bgroup0
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 192.168.141.1, timeout is 1 seconds from bgroup0

ScreenOS - Hub-Spoke VPN with mix of Policy and Route spoke sites

!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=62/62/63 ms

References:

ScreenOS Concepts & Examples Guides

http://www.juniper.net/techpubs/software/screenos/screenos6.2.0/index.html

Route based VPN tunnels

Concepts & Examples Guide

Volume 5 Virtual Private Networks

Chapter 3 VPN Guidelines

Chapter 4 VPN: Sit-to-site VPN Configurations

Point to multi-point tunnels to share tunnel interfaces

Concepts & Examples Guide

Volume 5 Virtual Private Networks

Chapter 7 Advanced VPN Features: Multiple Tunnels per Tunnel Interface