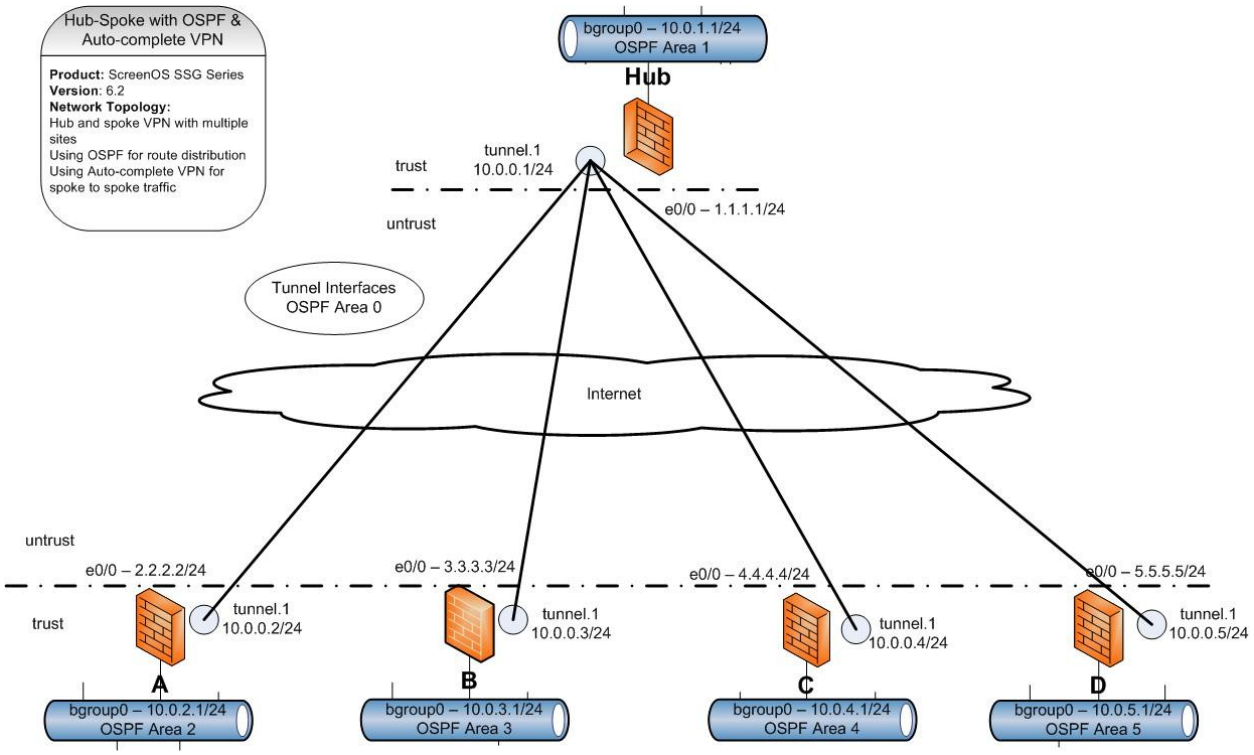
ScreenOS – Hub and Spoke AutoComplete VPN with OSPF

Product: ScreenOS SSG Series

Version: 6.2

Network Topology:



Hub and spoke VPN with multiple sites using point to multipoint

Using OSPF for route distribution

Using Auto-complete VPN for spoke to spoke traffic

Description:

The combines two of the convenience vpn features on the ScreenOS platform, dynamic routing protocol vpn and the on demand auto-complete vpn between spokes on a hub and spoke network. This allows a relatively standard spoke configuration process where only a few parameters are changed in the creation of a new spoke. But when the new site is added to the network full routing is established and efficient direct tunnels are created as needed.

The process relies on these basic technologies:

- IPSEC VPN in route mode

ScreenOS – Hub and Spoke AutoComplete VPN with OSPF

- Point to multipoint tunnel interface
- OSPF dynamic protocol configuration to distribute routes
- AutoComplete-VPN to create the on demand tunnels to avoid looping all traffic through the hub

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
    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.

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

Create AC-VPN gateway profile

set ike gateway ac-spoke-gw acvpn-profile sec-level standard

Create AC-VPN profile

set vpn ac-vpn acvpn-profile ac-spoke-gw no-replay tunnel idletime 0 sec-level standard

ScreenOS – Hub and Spoke AutoComplete VPN with OSPF

Enable & Configure NHRP for VPN usage

set vrouter trust-vr

set protocol nhrp

set protocol nhrp acvpn-profile ac-vpn

exit

set interface tunnel.1 protocol nhrp enable

Enable & Configure OSPF

set vr trust protocol ospf

set vr trust protocol ospf enable

set vr trust protocol ospf area 1

set interface bgroup0 protocol ospf area 1

set interface bgroup0 protocol ospf enable

set interface tunnel.1 protocol ospf area 0

set interface tunnel.1 protocol ospf link-type p2mp

set interface tunnel.1 protocol ospf enable

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

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

set vpn SpokeA bind interface tunnel.1

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

set vpn SpokeB bind interface tunnel.1

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

set vpn SpokeC bind interface tunnel.1

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

set vpn SpokeD bind interface tunnel.1

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.

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

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 AC-VPN Dynamic gateway

set ike gateway ac-hub-gw acvpn-dynamic

Create ACVPN Dynamic VPN

set vpn ac-hub-vpn acvpn-dynamic ac-hub-gw hub

Enable & Configure NHRP on router

set vrouter trust-vr

set protocol nhrp

set protocol nhrp nhs 10.0.0.1

set protocol nhrp cache 10.0.2.0/24

**Change the ip address to match the bgroup0 LAN on spoke

exit

set interface tunnel.1 protocol nhrp enable

ScreenOS – Hub and Spoke AutoComplete VPN with OSPF

Enable & Configure OSPF

set vr trust protocol ospf

set vr trust protocol ospf enable

set vr trust protocol ospf area 2

**Change area to match Spoke LAN assignment

set interface bgroup0 protocol ospf area 2

**Change area to match Spoke LAN assignment

set interface bgroup0 protocol ospf enable

set interface tunnel.1 protocol ospf area 0

set interface tunnel.1 protocol ospf enable

Verification:

routing table checks

Running "get route protocol ospf" on a spoke should show the routes to all other spokes and the hub as learned from OSPF the capital "O" label below. This should contain all the connected spokes and the hub if routes are fully distributed properly.

This output is from spoke C

get route protocol ospf

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
*	10	10.0.0.1/32	tun.1	10.0.0.1	O	60	10	Root

*	13	10.0.1.0/24	tun.1	10.0.0.1	O	60	21	Root
*	12	10.0.2.0/24	tun.1	10.0.0.1	O	60	11	Root
*	11	10.0.3.0/24	tun.1	10.0.0.1	O	60	21	Root
*	14	10.0.5.0/24	tun.1	10.0.0.1	O	60	21	Root

Total number of ospf routes: 5

On the hub verify NHRP full connectivity

get route protocol nhrp

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> (19 entries)

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	19	10.0.0.2/32	tun.1	10.0.0.2	N	35	0	Root
*	16	10.0.0.3/32	tun.1	10.0.0.3	N	35	0	Root
*	17	10.0.0.4/32	tun.1	10.0.0.3	N	35	0	Root
*	17	10.0.0.5/32	tun.1	10.0.0.3	N	35	0	Root
*	19	10.0.2.0/24	tun.1	10.0.0.3	N	35	0	Root
*	21	10.0.3.0/24	tun.1	10.0.0.4	N	35	0	Root
*	20	10.0.4.0/24	tun.1	10.0.0.2	N	35	0	Root
*	23	10.0.5.0/24	tun.1	10.0.0.5	N	35	0	Root

Total number of nhrp routes: 8

get vrouter trust protocol nhrp cache

---

flags: R-registered, C-cached, L-replied, P-pushed, S-static, I-imported,

F-in FIB, D-being deleted.

Prefix	nhop-public-IP	nhop-private-IP	Pref	Flags	Expire(in sec)
10.0.0.4/32	4.4.4.4	10.0.0.4	128	C	257
10.0.3.0/24	3.3.3.3	10.0.0.3	128	RF	283
10.0.0.2/32	2.2.2.2	10.0.0.2	128	CF	283
10.0.0.2/32	5.5.5.5	10.0.0.5	128	CF	283
10.0.0.3/32	3.3.3.3	10.0.0.3	128	CF	283
10.0.2.0/24	2.2.2.2	10.0.0.2	128	RF	283
10.0.5.0/24	5.5.5.5	10.0.0.2	128	RF	283
10.0.4.0/24	4.4.4.4	10.0.0.4	128	RF	257

Confirm setup of ac-vpn

On spoke look for the sa configuration for the AC-VPN

get sa

sa: 2

HEX ID	Gateway	Port	Algorithm	SPI	Life:sec	kb	Sta	PID	vsys
00000006<	1.1.1.1	500	esp:3des/sha1	677cddab	1987	unlim	A/-	-1	0
00000006>	1.1.1.1	500	esp:3des/sha1	8e6fb985	1987	unlim	A/-	-1	0
00000007<	0.0.0.0	500	esp:3des/sha1	00000000	expir	unlim	I/I	-1	0
00000007>	0.0.0.0	500	esp:3des/sha1	00000000	expir	unlim	I/I	-1	0

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

ScreenOS – Hub and Spoke AutoComplete VPN with OSPF

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: Multple Tunnels per Tunnel Interface

OSPF

Concepts & Examples Guide

Volume 7 Routing

Chapter 3

AutoConnect-VPN

Concepts & Examples Guide

Volume 5 Virtual Private Networks

Chapter 8