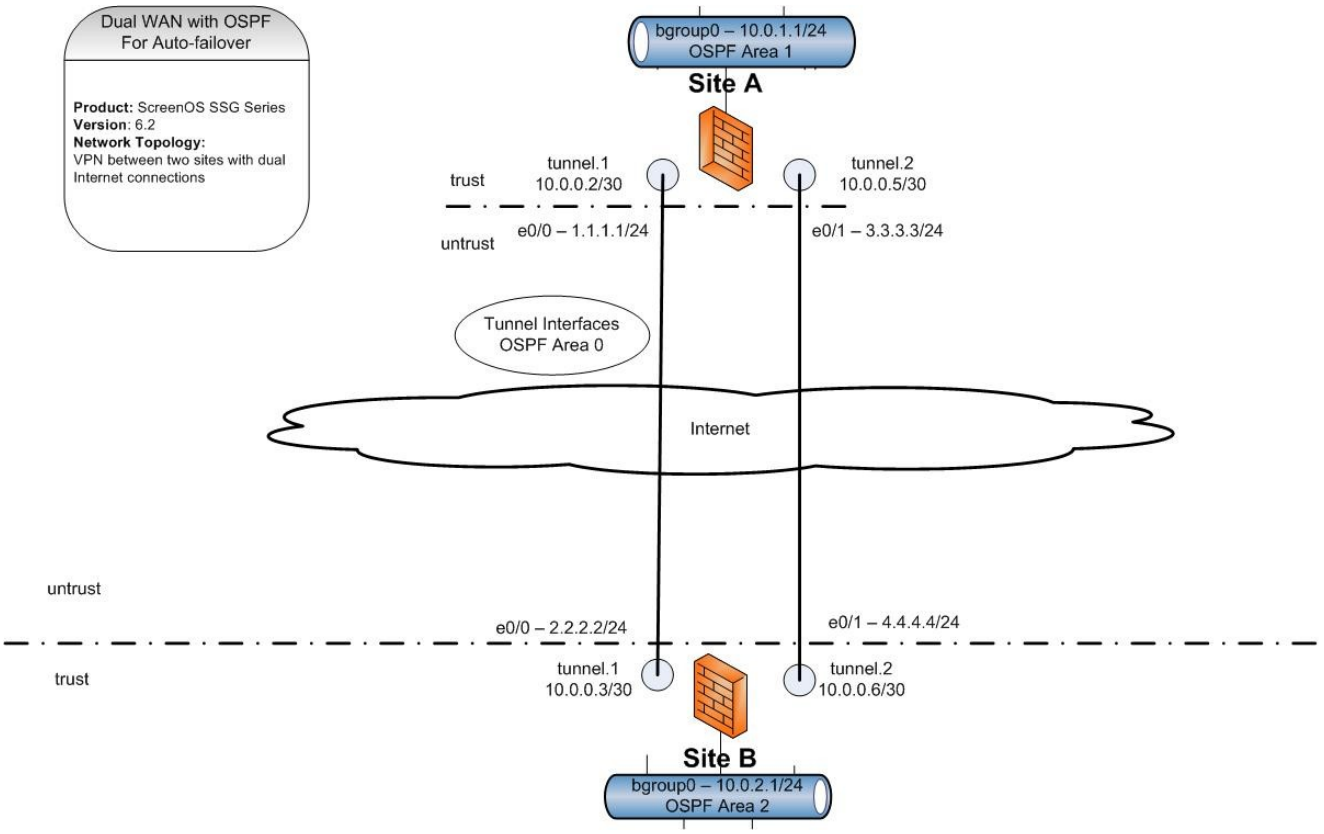
ScreenOS – Dual WAN with OSPF on Two Sites

Product: ScreenOS

Version: 6.0 or better

Network Topology



Two sites that each have redundant internet connections. This establishes two VPN tunnels and uses OSPF to set routing priorities over the tunnels to use the primary line.

Description:

Each site has two internet connections and interfaces that allow route based VPNs to exist at the same time. Using OSPF route priorities the primary line is in use unless this fails. When the first tunnel fails the second will automatically take over. On restoration of the first line route priorities automatically revert to the primary line.

The process utilizes IPSEC VPN in route mode and OSPF.

1. Create OSPF settings on the trust virtual router
2. Assign the interfaces to the OSPF settings needed
3. Create the IPSEC VPN gateway and connection

ScreenOS – Dual WAN with OSPF on Two Sites

Zone Layout

untrust interface is ethernet0/0 and etherent0/1

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. Create OSPF Settings

CLI

Set vr trust router-id 10.0.1.1 **Change to match LAN ip address on site B

set vr trust protocol ospf

set vr trust protocol ospf enable

set vr trust protocol ospf area 1 (** Change to area 2 on Site B)

Web

Network – Virtual Routers – Trust-vr (select edit)

Set router id and hit apply

Click on “Create OSPF instance”

Check enable OSPF on bottom (not distribute default route) and apply

Hit the Area Menu

Create Area 1 on site A and Area 2 on Site B

2. Assign OSPF settings to interfaces

Setup the bgroup0 LAN interface

CLI

set interface bgroup0 protocol ospf area 1 (**Change area 2 on site B)

set interface bgroup0 protocol ospf enable

WEB

ScreenOS – Dual WAN with OSPF on Two Sites

Network – Interfaces – List

Select bgroup0 edit button

Select OSPF tab

Check Bind to Area 1 (**Change area 2 on site B)

Select Enable button

Remove reduce flooding default

Apply

Create and setup the tunnel interfaces for the VPN

CLI

set interface tunnel.1 zone Trust

set interface tunnel.1 ip 10.0.0.2/30 (** change ip address to 10.0.0.3 for site B)

set interface tunnel.1 protocol ospf area 0.0.0.0

set interface tunnel.1 protocol ospf enable

set interface tunnel.2 zone Trust

set interface tunnel.2 ip 10.0.0.5/30 (**change ip address to 10.0.0.6 for site B)

set interface tunnel.2 protocol ospf area 0.0.0.0

set interface tunnel.2 protocol ospf enable

set interface tunnel.2 protocol ospf cost 20

WEB

Create tunnel.1 and tunnel.2 with these parameters

Network – Interfaces – List

New Tunnel IF in upper right

Trust zone

Unnumbered

bgroup0 interface

OSPF tab

Check Bind to Area 0

Check enable

Remove demand circuit and reduce flooding

Set as Point-to-point

On tunnel.2 raise the cost to 20

3. Create IPSEC VPN Gateways and connection

Gateways to remote site. Create two on each firewall and be sure to change the outgoing interface to the correct one for the primary and backup connections.

CLI

Firewall Site A

set ike gateway SiteB1-GW address 2.2.2.2 Main outgoing-interface ethernet0/0 preshare juniper sec-level standard

set ike gateway SiteB2-GW address 4.4.4.4 Main outgoing-interface ethernet0/1 preshare juniper sec-level standard

Firewall Site B

set ike gateway SiteA1-GW address 1.1.1.1 Main outgoing-interface ethernet0/0 preshare juniper sec-level standard

set ike gateway SiteA2-GW address 3.3.3.3 Main outgoing-interface ethernet0/1 preshare juniper sec-level standard

WEB

Firewall Site A

VPNs – AutoKey Advanced – Gateway

Create new gateway

Name SiteB1-GW (**Change to SiteB2-GW for secondary)

IP: 2.2.2.2 (**change to 4.4.4.4 for SiteB2-GW)

Advanced button

Preshared key: juniper

Outgoing interface ethernet0/0 (Change to ethernet 0/1 for SiteB2-GW)

Firewall Site B

VPNs – AutoKey Advanced – Gateway

Create new gateway

Name SiteA1-GW (**Change to SiteA2-GW for secondary)

IP: .1.1.1.1 (**change to 2.2.2.2 for SiteA2-GW)

Advanced button

Preshared key: juniper

ScreenOS – Dual WAN with OSPF on Two Sites

Outgoing interface ethernet0/0 (Change to ethernet 0/1 for SiteA2-GW)

Create AutoKey IKE Objects

Firewall Site A

CLI

set vpn SiteB1 gateway SiteB1-GW sec-level standard

set vpn SiteB1 bind interface tunnel.1

set vpn SiteB2 gateway SiteB2-GW sec-level standard

set vpn SiteB2 bind interface tunnel.2

WEB

VPNs – AutoKey IKE

Create New

Name SiteB1 (**change to SiteB2 for Secondary)

Associated gateway SiteB1-GW (**change to SiteB2-GW for Secondary)

Advanced button

Tunnel interface tunnel.1 (**change to tunnel.2 for secondary)

Firewall Site B

CLI

set vpn SiteA1 gateway SiteA1-GW sec-level standard

set vpn SiteA1 bind interface tunnel.1

set vpn SiteA2 gateway SiteA2-GW sec-level standard

set vpn SiteA2 bind interface tunnel.2

WEB

VPNs – AutoKey IKE

Create New

Name SiteA1 (**change to SiteA2 for Secondary)

Associated gateway SiteA1-GW (**change to SiteA2-GW for Secondary)

Advanced button

Tunnel interface tunnel.1 (**change to tunnel.2 for secondary)

ScreenOS – Dual WAN with OSPF on Two Sites

Verification:

From Site B checking routes to Site A

Testing from Site B

Using primary Connection

Check OSPF connection status

Verify that both connections show the neighbor status

get vr trust protocol ospf neighbor

VR: trust-vr RouterId: 10.0.2.1

Neighbor(s) on interface tunnel.2 (Area 0.0.0.0)

IpAddr/IfIndex RouterId Pri State Opt Up StateChg

10.0.0.5 10.0.1.1 1 Full E 00:09:47 (+6 -0)

Neighbor(s) on interface tunnel.1 (Area 0.0.0.0)

IpAddr/IfIndex RouterId Pri State Opt Up StateChg

10.0.0.2 10.0.1.1 1 Full E 00:01:33 (+6 -0)

Neighbor(s) on interface bgroup0 (Area 0.0.0.2)

get route protocol ospf

IPv4 Dest-Routes for <trust-vr> (15 entries)

ID IP-Prefix Interface Gateway P Pref Mtr Vsys

---

* 41 10.0.1.0/24 tun.1 10.0.0.2 O 60 11 Root

Total number of ospf routes: 1

During failover

get route protocol ospf

```
------------------------------------------------------------------------------
       ID        IP-Prefix      Interface       Gateway   P Pref    Mtr     Vsys
------------------------------------------------------------------------------
*      39        10.0.1.0/24        tun.2       10.0.0.5  O  60     21      Root
```

Total number of ospf routes: 1

WEB

Network – Routing - Destination

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

OSPF

Concepts & Examples Guide

Volume 7 Routing

Chapter 3