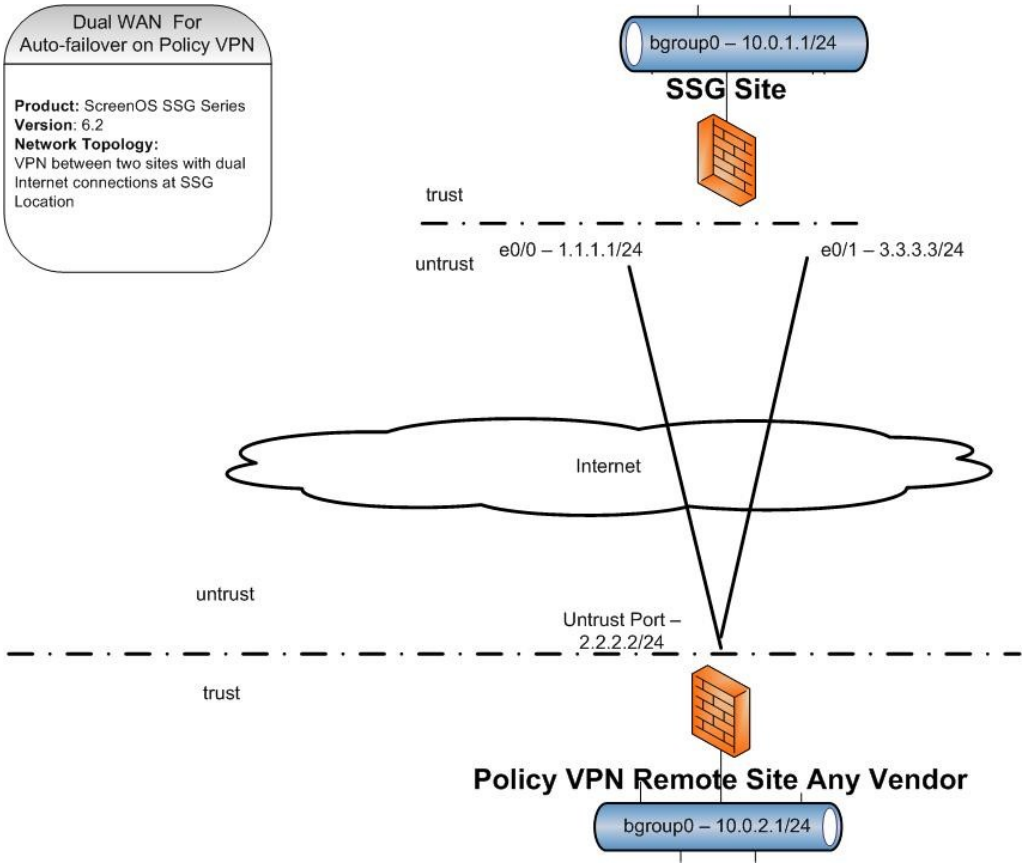
ScreenOS – Redundant Internet Connections on a Policy VPN

Product: ScreenOS

Version: 6.0 or up

Network Topology



Two sites connected by VPN with one site having two internet access connections. They connect using policy based VPN.

Description:

This configuration has a redundant internet link on one side of a policy based vpn connection. The creation of two gateways and a group allows for failover between the two links and setting one as the priority link.

1. Create a VPN Group
2. Configure two gateways, one for each outbound interface
3. Configure an AutoKey IKE for each of the gateways and select the VPN group designating the primary connection with the higher priority number.

4. Configure the Policy using the VPN tunnel option and associate this with the VPN group

Configuration

1. Create VPN Group:

This allows the two circuits connections to be treated as a single device to the VPN tunnel policy.

CLI

set vpn-group id 1

Web

VPNs – AutoKey Advanced – VPN Groups

New

2. Configure two Gateways

Create a gateway for each of the two outbound interfaces

CLI

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

set ike gateway Backup-GW address 2.2.2.2 Main outgoing-interface "ethernet0/1" preshare Juniper== sec-level standard

Web

VPNs – AutoKey Advanced – Gateway

New and select the correct interface for each on the advanced page

3. Configure AutoKey IKE

Create IPSEC object on each gateway and place into group

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

set vpn-group id 1 vpn RemotePrimary weight 10

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

set vpn-group id 1 vpn RemoteSecondary weight 1

Web

VPNs – AutoKey IKE

New select the correct gateway on the opening page

select the group on the advanced tab and set priority (higher is Primary)

4. Configure Policy Tunnel

The tunnel will associate with the group and can use either circuit connection but will prefer the higher priority one first.

CLI

set address Trust LocalLAN 10.0.1.0 255.255.255.0

set address Untrust RemoteLAN 10.0.2.0 255.255.255.0

set policy name RemoteVPN from Untrust to Trust LocalLAN ClinicLAN ANY tunnel vpn-group 1

set policy name RemoteVPN from Trust to Untrust LocalLAN RemoteLAN ANY tunnel vpn-group 1

Web

Policies – Policy Objects – Addresses – List

Create Remote LAN address in Untrust zone

Create Local LAN address in trust zone

Policies – Policy

Create trust to untrust policy and check the box to create a matching policy

Select tunnel and select the VPN group

Verification:

Confirm SA is up

CLI

get sa

Web

VPNs – Monitor Status

Disconnect the primary ethernet cable and confirm the failover occurs

ScreenOS – Redundant Internet Connections on a Policy VPN

References:

ScreenOS Concepts & Examples Guides

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

Volume 5 Virtual Private Networks

Chapter 3 VPN Guidelines

Chapter 4 VPN: Sit-to-site VPN Configurations