ScreenOS Site-to-Site IPSEC VPN Connections

Product: ScreenOS

Version: 6.0 and up

Network Topology:

Two sites that have internet connections and a firewall that supports IPSEC VPN. This procedure creates the Virtual Private Network across the internet between the sites.

Description:

The screenOS platform offers two basic types of VPN for site-to-site tunnels, route based and policy based. The policy based option is what all standard VPN capable firewalls offer for connectivity. These create a simple point-to-point connection over the internet between the two sites and permit the traffic. Route based options add a layer of flexibility to the connection. These permit the use of standard routing features like BGP or OSPF across the tunnel and allow deny policies and more ganular traffic control on the connection.

Proxy-id

Proxy-id is the method of identification of which ip ranges are connecting on a VPN on both sides. When tunnels are created each ip address on site A needs a matching proxy-id pair on Site B. When the tunnels are created each pair of connections creates a Security Association (SA) for that tunnel. Vendors all have slightly different ways to wrap the creation of these SA into their interface. But all of the pairs must be present on both sites A & B. for all of the traffic to pass. Some vendors will not create any of the SA unless ALL of the SA are present. Other vendors will create all the SA that they can match and just log errors for the pairs they cannot match.

When there is more than one SA pair on a policy VPN you must have all proxy-id pairs created. In ScreenOS these are automatically created by the creation of the tunnel action policy for policy VPN. Here you leave the proxy-id section blank.

With route based VPN we also leave the proxy-id blank on both sides as this by default allows any ip traffic we send down the tunnel interface only subject to the polices created.

ScreenOS Site-to-Site IPSEC VPN Connections

When connecting route based VPN to a policy VPN on the remote side we must submit matching proxy-id pairs to the policy based engine. If there is more than one proxy-id pair you will need to use ScreenOS version 6.3 or higher.

Policy VPN

http://kb.juniper.net/InfoCenter/index?page=content&id=KB8534

These are a good choice for simple connections with a wide variety of 3rd party solutions. They connect the two sites and automatically create the necessary static routing along with the permit traffic policies in a few steps. These also operate exactly as a policy VPN standard that allows easy interoperability.

Route VPN

http://kb.juniper.net/InfoCenter/index?page=content&id=KB8533

Here the VPN is bound to an virtual interface on the firewall. This interface allows the creation of routing policies using any routing protocol supported on the firewall. This also then allows the use of routing preferences to automatically send traffic to alternate paths when this particular VPN interface goes down. The VPN tunnel interface can be unnumbered and associated with any physical interface on the firewall. Or the tunnel interface can be assigned an ip address and zone independent of other interfaces and zones on the firewall.

Policy is also more flexible. The policies that allow either the sending or receiving of traffic on the VPN tunnel interface can be narrow in ip scope and/or ports permitted. In addition, the deny policy can be applied to the tunnel interface for the specific ports and addresses desired.

You can create route based VPN on the ScreenOS side and connect to a standard policy VPN on the remote side of the connection.

Zones and Policies

Another feature of route based VPN is great flexibility in controlling traffic on VPN tunnels. ScreenOS provides the option to place VPN tunnel interfaces into any existing zone including custom zones created for this purpose. Thus you can bind VPN tunnels to trust zones which would automatically allow trust to trust traffic between sites and not require the creation of any permit traffic policies on the one side or place them into the untrust fully restricted zone or create and control a custom zone for these connections.

Verification:

SA status

Once the VPN is created the SA should be seen in the firewall.

ScreenOS Site-to-Site IPSEC VPN Connections

CLI

get sa

HEX ID Gateway Port Algorithm SPI Life:sec kb Sta PID vsys

00000026< 1.1.1.1 500 esp:3des/sha1 08af61f7 2524 unlim A/U -1 0

The column “Sta” is status and the first letter is an A for active and up and I for inactive, tunnels should be active when working and passing traffic.

Web

VPNs – Monitor Status

The SA should show as “Active”

If the SA does not come up or the SA is up but traffic cannot pass, then follow the troubleshooting steps listed in these kb articles.

Flow Chart Troubleshooting Guide

http://kb.juniper.net/kb/documents/public/resolution_path/J_visio_kb9221.htm

Question and Answer troubleshooting guide

http://kb.juniper.net/InfoCenter/index?page=content&id=KB9221

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

Knowledge Base Articles on VPN

Top level solution guide to creating and troubleshooting VPN for both Site-to-Site and Dialup

http://kb.juniper.net/kb/documents/public/resolution_path/J_FW_VPN_Config_or_Trblsh.htm

Solutions for Site-to-Site Route Based VPN

http://kb.juniper.net/InfoCenter/index?page=content&id=KB8533

ScreenOS Site-to-Site IPSEC VPN Connections

Solutions for Site-to-Site Policy Based VPN

http://kb.juniper.net/InfoCenter/index?page=content&id=KB8534

Solutions for 3rd Party Compatibility VPN

http://kb.juniper.net/InfoCenter/index?page=content&id=KB8554

Troubleshooting VPN Issues

Flow Chart Troubleshooting Guide

http://kb.juniper.net/kb/documents/public/resolution_path/J_visio_kb9221.htm

Question and Answer troubleshooting guide

http://kb.juniper.net/InfoCenter/index?page=content&id=KB9221