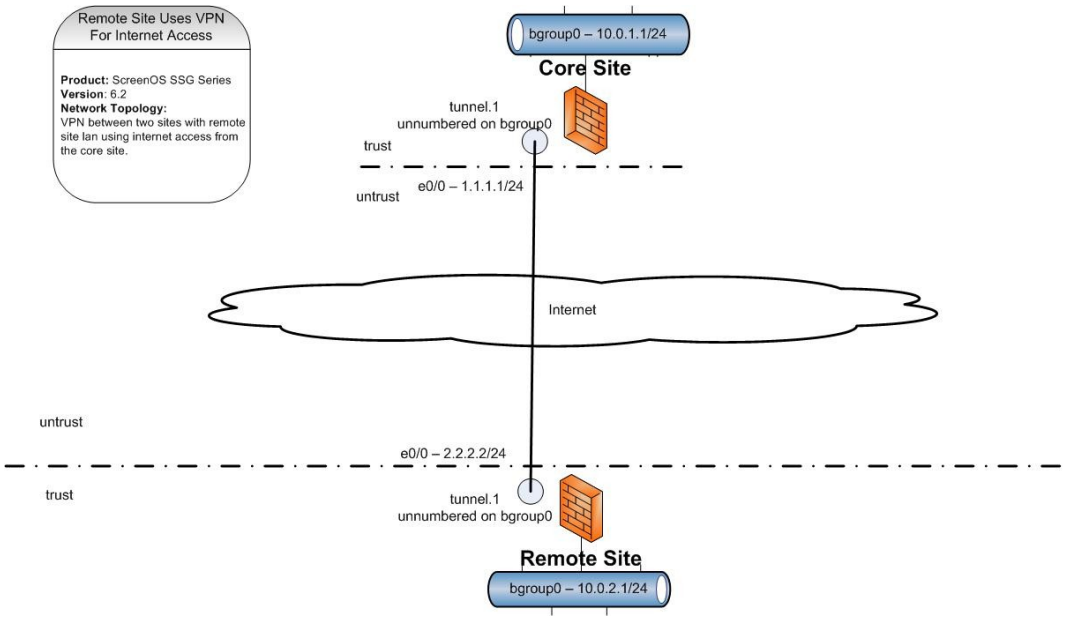
ScreenOS - Remote Site Uses VPN to Core Site for Internet Access

Product: ScreenOS SSG Series
Version: 6.2

Network Topology:



Two sites connect via IPEC VPN across the internet. The internet requests from the remote site are forwarded down the VPN tunnel to the core site and uses the core site internet access connection.

Description:

Each site has internet access to establish the VPN connection. But all browsing from client machines on the remote site are directed to the core site. The process uses source based routing to force all requests from the remote LAN down the VPN to the core site gateway. On arrival at the core site the source address needs to be translated to a local core site LAN ip and then forwarded for internet access.

The process utilizes IPSEC VPN in route mode, source based routing and address translation.

1. Create an IPSEC VPN between sites
2. Configure source routing on the remote site
3. Configure the address translation for the remote LAN on the core site

Zone Layout

untrust interface is ethernet0/0

trust interface is bgroup0

ScreenOS - Remote Site Uses VPN to Core Site for Internet Access

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 core and remote 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.

1. Create IPSEC VPN Between Sites

Create the tunnel.1 interface on each site as unnumbered and associated with bgroup0. This is the same on both sites.

CLI

set interface tunnel.1 zone Trust

set interface tunnel.1 ip unnumbered interface bgroup0

Set routes to these tunnel interfaces for each site

CLI

Core site

set route 10.0.2.0/24 interface tunnel.1 gateway 10.0.2.1

Remote Site

set route 10.0.1.0/24 interface tunnel.1 gateway 10.0.1.1

WEB

Core site

Network – Routing – Destination

New button

10.0.2.0/24

interface tunnel.1

gateway 10.0.2.1

Remote Site

Network-Routing – Destination

New button

10.0.1.0/24

interface tunnel.1

Gateway 10.0.1.1

WEB

Network – Interfaces – List

New tunnel interface in the upper right

ScreenOS - Remote Site Uses VPN to Core Site for Internet Access

Trust zone

Unnumbered with the bgroup0 interface

Create the VPN gateways

CLI

Core Site

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

Remote Site

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

WEB

Core Site

VPNs – AutoKey Advanced – Gateway

Create new gateway

Name Remote-GW

IP: 2.2.2.2

Advanced button

Preshared key: juniper

Outgoing interface ethernet0/0

Remote Site

VPNs – AutoKey Advanced – Gateway

Create new gateway

Name Core-GW

IP: .1.1.1.1

Advanced button

Preshared key: juniper

Outgoing interface ethernet0/0

Create AutoKey IKE Objects

Core Site

CLI

set vpn Remote gateway Remote-GW sec-level standard

set vpn Remote bind interface tunnel.1

WEB

ScreenOS - Remote Site Uses VPN to Core Site for Internet Access

VPNs – AutoKey IKE

Create New

Name Remote

Associated gateway Server-GW

Advanced button

Tunnel interface tunnel.1

Remote Site

CLI

set vpn Core gateway Core-GW sec-level standard

set vpn Core bind interface tunnel.1

WEB

VPNs – AutoKey IKE

Create New

Name Core

Associated gateway Core-GW

Advanced button

Tunnel interface tunnel.1

2. Configure Source Routing on Remote Site

Enable source routing on the trust virtual router

CLI

set source-routing enable

WEB

Network – Routing – Virtual Routers (edit trust-vr)

Check box - Enable Source Based Routing

Create a rule to forward all LAN traffic down the VPN tunnel

CLI

set route source 10.0.2.0/24 interface tunnel.1 gateway 10.0.1.1

WEB

Network – Routing – Source (new button upper right)

Network: 10.0.2.0/24

Interface: tunnel.1

Gateway: 10.0.1.1

ScreenOS - Remote Site Uses VPN to Core Site for Internet Access

3. Configure the address translation for the remote LAN on the core site

Create a standard web access policy from trust to untrust using policy based source nat.

CLI

set policy from Trust to Untrust Any Any ANY nat src permit log

WEB

Policy – Policies

Select trust to untrust (new button upper right or edit the existing general policy)

Source: any

Destination: any

Action: permit

Logging: checked

Advanced button

Source translation: checked for egress interface

Verification:

Confirm internet access on remote site and observe translations in the policy log on the core site.

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

Source Based Routing

Volume 7 Routing

Chapter 2 – Source Based Routing Table

Network Address Translation

Concepts & Examples Guide

Volume 8 Address Translation

ScreenOS - Remote Site Uses VPN to Core Site for Internet Access

Chapter 2