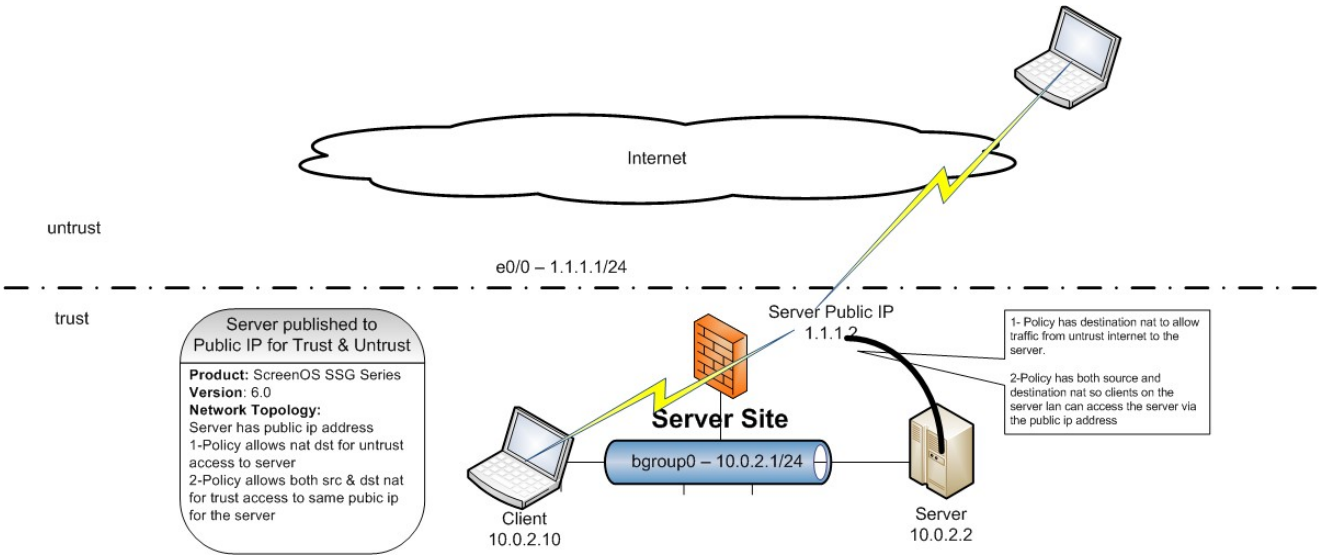
ScreenOS – Server published to Public IP for both Trust & Untrust Connections

Product: ScreenOS

Version: 6.0 or up

Network topology



The local trust zone server has a public ip address assigned for accessing services. This has two policies created. One allows destination nat for the untrust internet traffic to access the services. The second allows local trust lan computers to access the same public ip address for these same services. This policy requires both source and destination nat.

Description

The server publishes services to a public ip address on the firewall. The public ip address is placed int the trust zone and policy based nat is used to make the necessary address translations.

The untrust to trust access also requires that proxy arp be enabled for the published address. Note that the method for proxy arp changes with version 6.3 of ScreenOS.

The trust to trust access requires that the direct lan connection between the two computers at layer two be prevented from kicking in. This is accomplished by translating the requesting computer source address to the firewall interface ip address. This forces the reply from the server local ip address to come to the firewall and not returned directly to the requesting computer. Thus the session setup for the public ip address by the local computer is maintained and the connection can be managed.

The process requires two separate policies

1. Untrust to Trust for the internet access to the server with destination nat

ScreenOS – Server published to Public IP for both Trust & Untrust Connections

2. Trust to Trust for the local LAN access via the public ip address with both source and destination nat.

Zone Layout

untrust interface is ethernet0/0

trust interface is bgroup0

The public ip address is placed into the trust zone

Configuration

Proxy ARP

CLI

6.2 or earlier

set arp nat-dst

6.3

set interface ethernet0/0 proxy-arp-entry 1.1.1.2 1.1.1.2

WEB (6.3 only. 6.2 only available in CLI)

Network – Interfaces

edit interface ethernet0/0

Proxy-arp menu

add 1.1.1.2

Address Object for public ip address into Trust Zone

CLI

set address Trust ServerPublic 1.1.1.2 255.255.255.255

set address Trust LAN 10.0.2.0 255.255.255.0

WEB

Policy—Policy Elements—Addresses—List

New

trust zone

ServerPublic

1.1.1.2/32

ScreenOS – Server published to Public IP for both Trust & Untrust Connections

New

trust zone

LAN

10.0.2.0/24

1. Untrust to Trust for the internet access to the server with destination nat

CLI

set policy name ServerUntrust from Untrust to Trust any ServerPublic HTTP dst ip 10.0.2.2 permit log

WEB

Policy—Policies

Untrust to Trust

New

From Any to ServerPublic

Select services from list

Permit

Check log button

Advanced button

Destination translation and enter the server ip address 10.0.2.2

2. Trust to Trust for the local LAN access via the public ip address with both source and destination nat.

CLI

set policy name ServerInternal from Trust to Trust LAN ServerPublic HTTP nat src dst ip 10.0.2.2 permit log

Change or add services that are needed in place of PING

WEB

Policies – Policy – set trust to trust – Create New

Name: ServerInternal

Source: Any

Destination: ServerPublic

select the required server services

permit

check log button

Advanced button

Check destination translation and enter the server ip address 10.0.2.2

Check source translation and leave on the default egress interface

Verification:

Attempt server access from internal computer using public address and open the policy log. Verify that both the source and destination translation are occurring as expected.

Attempt the server access from the untrust zone to the public address and verify connection in log.

References:

ScreenOS Concepts & Examples Guides

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

Network Address Translation

Concepts & Examples Guide

Volume 8 Address Translation

Chapter 3 – Nat-src and Nat-dst in the same policy

KB12631

http://kb.juniper.net/InfoCenter/index?page=content&id=KB12631