

10 Minute Configuration of Juniper Netscreen Firewalls

Modern Firewalls:

It is a fact that the modern day firewalls don't fit into any category since all of them out there are 'hybrid' in nature and does break the categorization and is difficult to fit into any kinds. Most important features are 'Packet Filtering' with 'Proxy feature' and 'Application Layer Gateways'

There are plenty out there and one of the hottest & comparable firewall series are from Juniper's Netscreen Firewall series. The product portfolio falls into different categories to fit in any market ranging from home user to Enterprise Networks. The buzzword of 'Intrusion Prevention' is integrated as well.

Models to Play with:

| | |
|-----------------------|---|
| Low End Targets | NS-5gt, NS-5gt-adsl, NS-5gt-wireless and NS-5xt |
| Small Office Segments | NS-25, NS-50, NS-204, NS-208, SSG-520, SSG-550 |
| Medium Segments | ISG-1000, ISG-2000 |
| Enterprise Segments | NS-500, NS-5200, NS-5400 |

A detailed datasheet/feature set division can be found at Juniper site, at this link;

<http://www.juniper.net/products/integrated/>

Basic configuration :

| | |
|--|--|
| Configure Hostname. | Set hostname <Hostname> |
| Configure the Clock on the firewall. | set clock { <i>date</i> [<i>time</i>] dst-off ntp timezone <i>number</i> } |
| Configure Interfaces. | Set interface Trust ip x.x.x.x/x Set interface Untrust ip y.y.y.y/x |
| Configure the default gateway pointing to ISP. | Set route 0.0.0.0/0 int untrust gateway y.y.y.z |
| Configure a Policy to allow traffic flow from trust side to untrust. | Set policy id 1 from trust to untrust any any any permit log |

That's it! The firewall is ready to be plugged into the network and traffic flow from internal network to external network will be on without any problem.

Analyze what we did:

1. Create a hostname for the router

2. Set the ip addresses for internal and external interfaces. In Netscreen terms;

Trust is the Internal Network and Untrust is the External network as the name explains.

3. Configure the Default Gateway pointing to the ISP network so that all the traffic can exit to internet

4. Create a policy to allow all traffic going from internal network to external (with source ip=any, destination ip=any, service=any and log the traffic)

How about natting/patting the traffic while it goes to internet ? By default, the trust interface will be in Nat mode and Untrust interface will be in Route mode. The significance is that any traffic coming onto the trust interface and exit out of untrust interface will be 'patted' using the untrust interface ip address.

Advanced Configuration:

| | |
|--|---|
| Set administration station ip in the firewall (Only that machine will be able to logon to the firewall). | Set admin manager-ip <ip-address> <mask> |
| Create a user with admin privileges. | Set admin user "Username" password "Password" privilege "ALL" |

| | |
|--|---|
| | |
| Set DNS server address on the firewall. | <pre>Set dns host dns1 <DNS Server IP1> Set dns host dns2 <DNS Server IP2></pre> |
| Set NTP server for time synchronization. | <pre>set ntp server "nist.gov.in" set ntp server src-interface "untrust"</pre> |
| Static address translation (1-1 translation) | <pre>Set interface untrust mip <PublicIP> <Netmask> <PrivateIP> <Netmask> vrouter trust-vr</pre> <p>Then bind the traffic policy to allow the traffic using the following policy;</p> <pre>Set policy id <id> from untrust to trust any mip(<PublicIP> <Service> permit log</pre> |
| Port forwarding using a single ip address (Host multiple services using a single ip) | <pre>Set vip multi-port Set interface untrust vip <Public-ip> <port> <Internal-ip> <port></pre> <p>Then bind the traffic policy to allow the traffic using the following policy;</p> |

| | |
|--|---|
| | Set policy id <id> from untrust to trust any vip(Public-ip) <service> permit log |
|--|---|

Example for MIP (Mapped IP):

So for a web server, the static translation can be configured as;

Public IP -> 1.1.1.1

Private IP -> 10.1.1.1

Set interface untrust mip 1.1.1.1 255.255.255.255 10.1.1.1 255.255.255.255 vrouter trust-vr

Set policy id 1 from untrust to trust any mip(1.1.1.1) http permit log

Example for VIP (Virtual IP):

So for a web server and email server, the VIP can be configured as;

Private IP for web -> 10.1.1.1

Private IP for mail- -> 10.1.1.5

Static untrust Interface IP -> 1.1.1.1

Set interface untrust vip 1.1.1.1 80 10.1.1.1 80

Set interface untrust vip 1.1.1.1 25 10.1.1.5 25

Set policy id 1 from untrust to trust any vip(1.1.1.1) http permit log

Set policy id 1 from untrust to trust any vip(1.1.1.1) smtp permit log

Features Offered in a Glance:

The Netscreen firewall is one of the very flexible hardware firewall which gives in more than just packet filtering . In short if we were to take a glance on the features offered, they are;

- Basic Firewall
- Advanced Routing (RIP, OSPF, BGP)
- DI (Deep Inspection of Packets Traversed)
- Anti-Spam
- Webfiltering & Webtrends

- VPN Capabilities (Site to Site, Client to Firewall, IPSEC, PPTP and L2TP)
- PPPoE, PPPoA configuration feature sets
- Application Layer Gateway
- High Availability (NSRP)
- Traffic-Shaping
- Virtual Firewalls
- SNMP and much more....

Conclusion:

This isn't an exclusive guide for configuration options available for Netscreen Firewalls but is meant to be used as a guide to setup the firewall and bring up the network protection in 10 minutes, with basic configuration set. A much elaborate feature configuration guide can be found at www.juniper.net

Author Biography:

Rajesh T Sivanandan holds a Bachelors Degree in Electrical and Electronics Engineering. He is currently working with Juniper Networks India Pvt. Ltd., Bangalore, India. He is having 6+ years of experience in Networking and held certifications like MCSE, CCNA, CCNP, CSS-1, CCIE (Theory).