

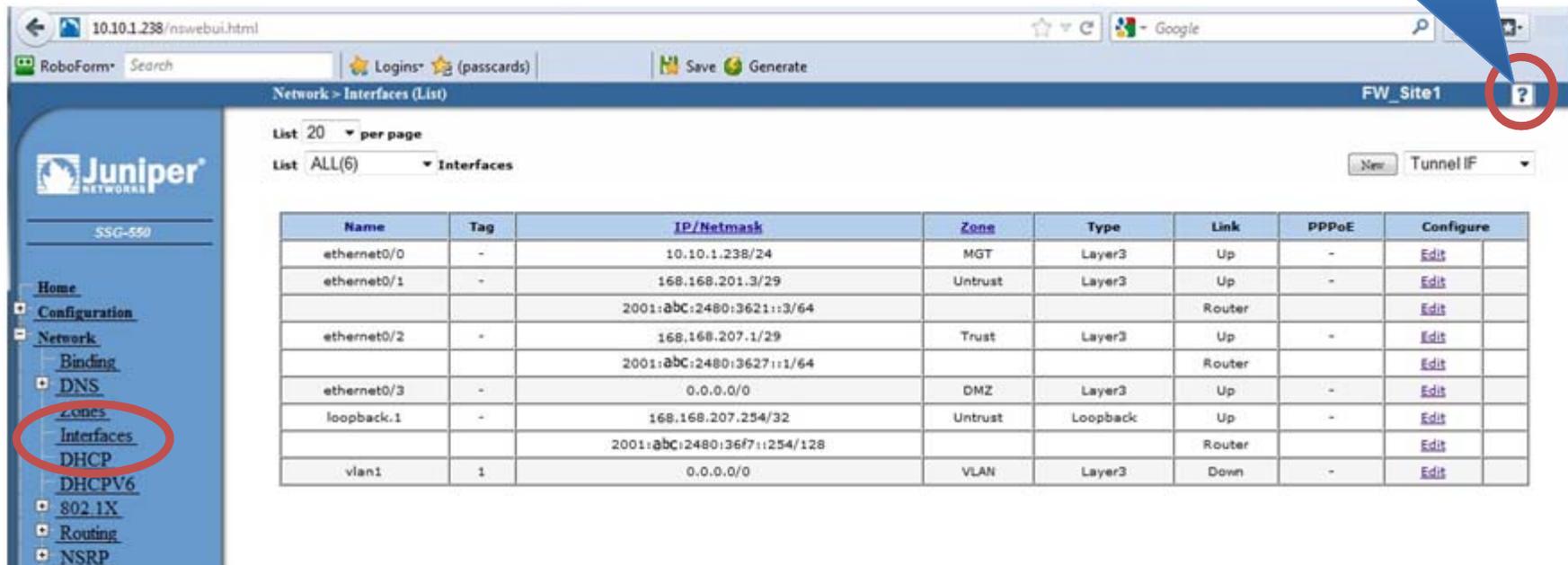
Juniper Netscreen Security Device



Netscreen Firewall - Interfaces

- Below is a screen shot for a Netscreen Firewall interface. All interfaces have an IPv6 address except ethernet0/0. We will step through configuring this interface.

Remember...The Help Menu is your friend!



Network > Interfaces (List) FW_Site1

List 20 per page
List ALL(6) Interfaces

Name	Tag	IP/Netmask	Zone	Type	Link	PPPoE	Configure
ethernet0/0	-	10.10.1.238/24	MGT	Layer3	Up	-	Edit
ethernet0/1	-	168.168.201.3/29	Untrust	Layer3	Up	-	Edit
		2001:abC:2480:3621::3/64		Router			Edit
ethernet0/2	-	168.168.207.1/29	Trust	Layer3	Up	-	Edit
		2001:abC:2480:3627::1/64		Router			Edit
ethernet0/3	-	0.0.0.0/0	DMZ	Layer3	Up	-	Edit
loopback.1	-	168.168.207.254/32	Untrust	Loopback	Up	-	Edit
		2001:abC:2480:36f7::254/128		Router			Edit
vlan1	1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

Netscreen Firewall – IPv6

- To configure, enable IPv6, determine mode and enter IPv6 address with prefix.
- Use Host Mode to accept RA messages.
- User Router Mode to send RA messages.

Interface: ethernet0/0

Properties: [Basic](#) [IPv6](#)

Interface Name ethernet0/0 0023.9c82.2100

Enable IPv6

Mode None Host Router

Interface ID(64-bit HEX)

Link Local Address

Unicast Address 1 / Prefix /

Unicast Address 2 / Prefix /

Unicast Address 3 / Prefix /

Path MTU(IPv6)

Netscreen – Configure IPV6

- After configuring the IPv6 addresses and clicking apply, the Neighbor Discovery (ND) and Router Advertisement (RA) settings are now available for configuration.

Interface: ethernet0/0 [Back To Interface List](#)

Properties: [Basic](#) **IPv6**

Interface Name ethernet0/0 0023.9c82.2100

Enable IPv6

Mode None Host Router

Interface ID(64-bit HEX)

Link Local Address fe80::223:9cff:fe82:2100

Unicast Address 1 / Prefix /

Unicast Address 2 / Prefix /

Unicast Address 3 / Prefix /

Path MTU(IPv6)

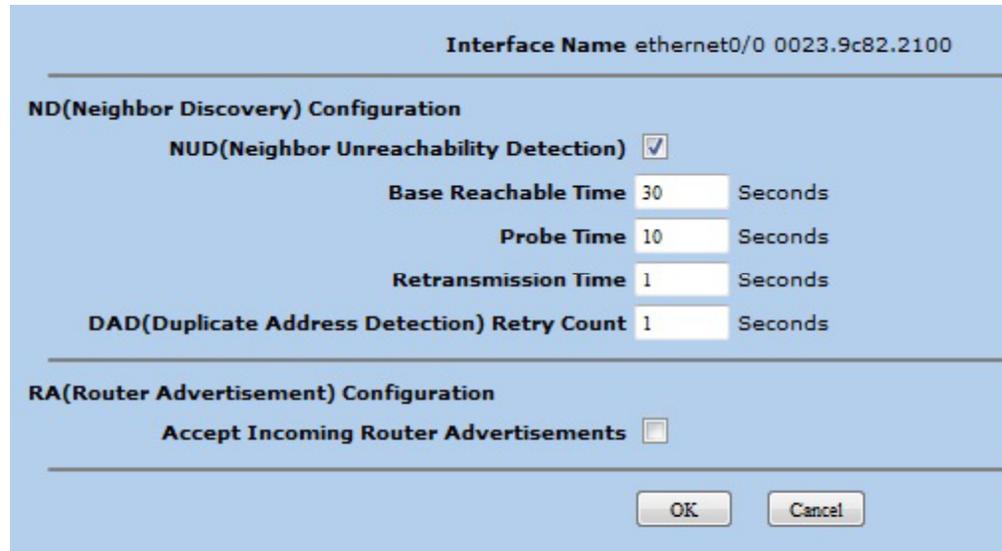
Node Configuration

[ND/RA Settings](#)

[Prefix list](#)

Netscreen – ND/RA Settings (Host)

- If using Host Mode, determine if you would like to accept incoming router advertisements.
- Accept Incoming Router Advertisements learns of the existence and identity of IPv6 routers by accepting Router Advertisement (RA) messages.



Interface Name ethernet0/0 0023.9c82.2100

ND(Neighbor Discovery) Configuration

NUD(Neighbor Unreachability Detection)

Base Reachable Time 30 Seconds

Probe Time 10 Seconds

Retransmission Time 1 Seconds

DAD(Duplicate Address Detection) Retry Count 1 Seconds

RA(Router Advertisement) Configuration

Accept Incoming Router Advertisements

OK Cancel

Netscreen – ND/RA Settings (Router)

- Use RA Transmission to learn of the existence and identity of other IPv6 routers.
- Link MTU advertises the link-MTU in router advertisements.
- Link Layer Address enables the Link Layer Address flag, which includes the link-layer (MAC) address of the router in outgoing RA messages.

Interface Name ethernet0/0 0023.9c82.2100

ND(Neighbor Discovery) Configuration

NUD(Neighbor Unreachability Detection)

Base Reachable Time Seconds

Probe Time Seconds

Retransmission Time Seconds

DAD(Duplicate Address Detection) Retry Count Seconds

RA(Router Advertisement) Configuration

Allow RA Transmission

Link MTU

Link Layer Address

Managed Configuration Flag

Other Parameters Configuration Flag

Reachable Time

Retransmission Time

Current Hop Limit

Maximum Advertisement Interval Seconds

Minimum Advertisement Interval Seconds

Default Router Lifetime Seconds

Advertised Router Preference High Medium Low

OK Cancel

Netscreen –IPv6 Route Table

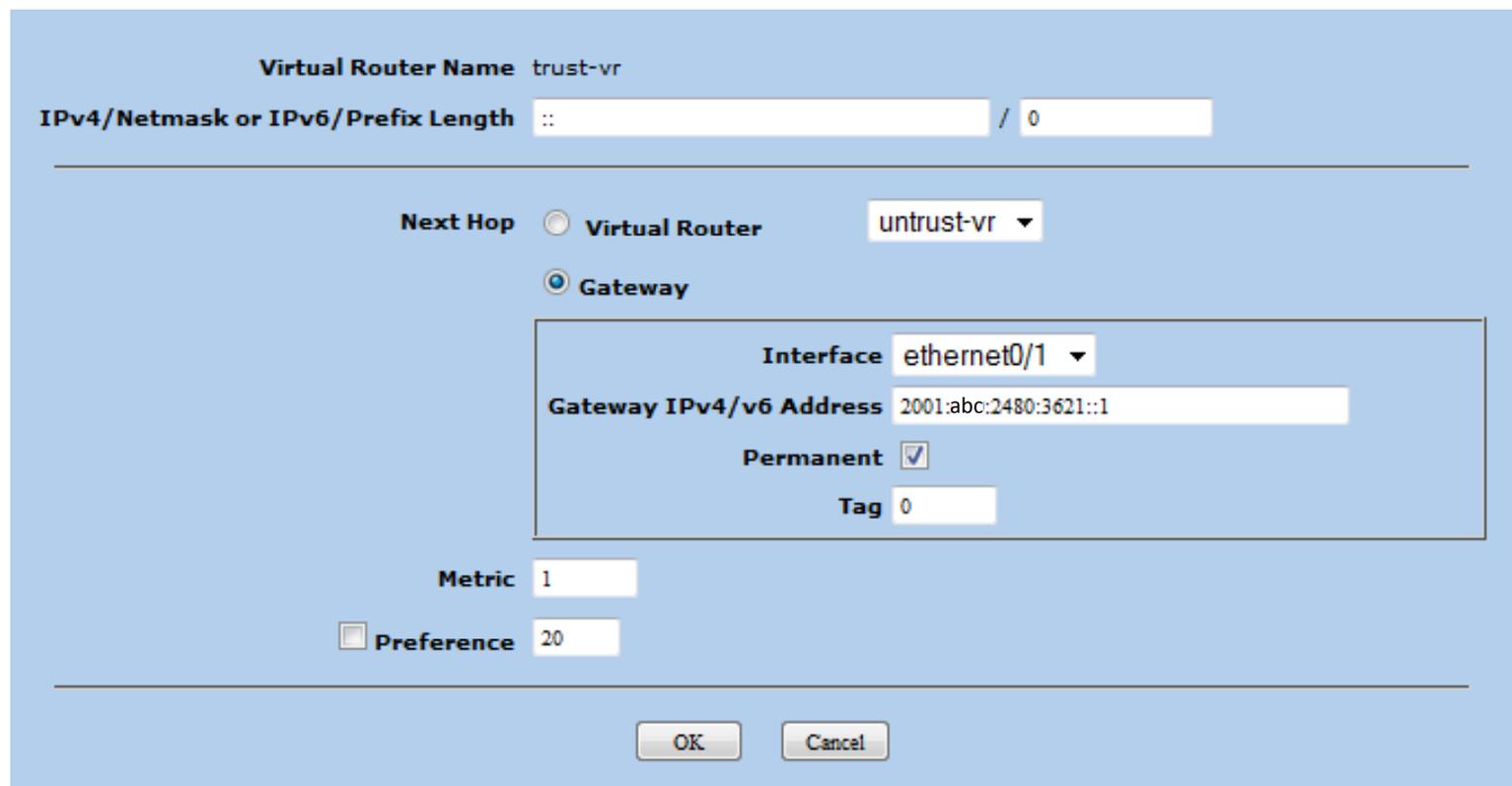
- Text

IPv6 Routing Table -- trust-vr								
	IP/Prefix	Gateway	Interface	Protocol	Preference	Metric	Vsys	Configure
*	2001:abc:2480:3621::3/64	::	ethernet0/1	C			Root	-
*	2001:abc:2480:3621::3/128	::	ethernet0/1	H			Root	-
*	2001:abc:2480:3627::1/64	::	ethernet0/2	C			Root	-
*	2001:abc:2480:3627::1/128	::	ethernet0/2	H			Root	-
*	2001:abc:2480:36f7::254/128	::	loopback.1	C			Root	-
*	2001:abc:2480:36f7::254/128	::	loopback.1	H			Root	-
*	2001:abc:2480:36aa::7/64	::	ethernet0/0	C			Root	-
*	2001:abc:2480:36aa::7/128	::	ethernet0/0	H			Root	-

* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1 H Host Route
 P Permanent S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2
 D Dynamic N NHRP

Netscreen – Add IPv6 Default Route

- Add ‘`:::/0`’ to denote default route (all IPv6 addresses)
- Add next-hop IPv6 address



The screenshot shows the configuration window for a Virtual Router. The Virtual Router Name is 'trust-vr'. The IPv4/Netmask or IPv6/Prefix Length is set to '::' / '0'. The Next Hop is configured as a Gateway on the 'untrust-vr' interface. The Gateway IPv4/v6 Address is '2001:abc:2480:3621::1'. The Permanent checkbox is checked, and the Tag is set to 0. The Metric is 1, and the Preference is 20. The OK and Cancel buttons are visible at the bottom.

Virtual Router Name trust-vr

IPv4/Netmask or IPv6/Prefix Length :: / 0

Next Hop Virtual Router untrust-vr Gateway

Interface ethernet0/1

Gateway IPv4/v6 Address 2001:abc:2480:3621::1

Permanent

Tag 0

Metric 1

Preference 20

OK Cancel

Netscreen – Verify Default IPv6 Route

- Verify the newly added IPv6 default route is now in the routing table and is active.

IPv6 Routing Table -- trust-vr								
	IP/Prefix	Gateway	Interface	Protocol	Preference	Metric	Vsys	Configure
*	2001:abc:2480:3621::3/64	::	ethernet0/1	C			Root	-
*	2001:abc:2480:3621::3/128	::	ethernet0/1	H			Root	-
*	2001:abc:2480:3627::1/64	::	ethernet0/2	C			Root	-
*	2001:abc:2480:3627::1/128	::	ethernet0/2	H			Root	-
*	2001:abc:2480:36f7::254/128	::	loopback.1	C			Root	-
*	2001:abc:2480:36f7::254/128	::	loopback.1	H			Root	-
*	2001:abc:2480:36aa::7/64	::	ethernet0/0	C			Root	-
*	2001:abc:2480:36aa::7/128	::	ethernet0/0	H			Root	-
*	::/0	2001:abc:2480:3621::1	ethernet0/1	SP	20	1	Root	Remove

* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1 H Host Route
 P Permanent S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2
 D Dynamic N NHRP

Netscreen Policies – Allow ICMP6

- **As with IPv4, do not block all ICMP6!**
- **See RFC4890 - Recommendations for Filtering ICMPv6 Messages in Firewalls**
- **Traffic That Must Not Be Dropped**
 - Destination Unreachable (Type 1) - All codes
 - Packet Too Big (Type 2)
 - Time Exceeded (Type 3) - Code 0 only
 - Parameter Problem (Type 4) - Codes 1 and 2 only
 - Echo Request (Type 128)
 - Echo Response (Type 129)
- **This is not all inclusive, there are other recommendations in RFC.**

Netscreen IPv6 Policies

- IPv6 policies are separate policies from IPv4.
- Can add policy elements & groups for IPv6 just as IPv4.
- Implement policies for IPv6 the same as for IPv4.

From SAN_Zone To Untrust, total policy: 6

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
994276	Any-IPv4	127.32.148.160/28	Good ICMP and Traceroute			Edit Clone Remove	<input checked="" type="checkbox"/>	
994275	Any-IPv6	2001:abc:2480:a000::/64	Good ICMP6 and Traceroute			Edit Clone Remove	<input checked="" type="checkbox"/>	
994272	Any5 IPv4 - 127.32.148.172/32 Any IPv4 - 127.32.148.175/32 Any6 IPv4 - 127.32.148.174/32 Any7 IPv4 - 127.32.148.173/32	Any4 IPv4 - 127.32.240.95/32 Any3 IPv4 - 127.32.240.19/32 Any1 IPv4 - 127.32.240.138/32 Any2 IPv4 - 127.32.240.120/32	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	
994269	Any-IPv4	Any-IPv4	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	
994274	Any5 IPv6 - 2001:abc:2480:a000::90/64 Any IPv6 - 2001:abc:2480:a000::93 Any6 IPv6 - 2001:abc:2480:a000::92 Any7 IPv6 - 2001:abc:2480:a000::91/64	Any4 IPv6 - 2001:abc:430::240:95/64 Any3 IPv6 - 2001:abc:430::240:119/64 Any1 IPv6 - 2001:abc:430::240:138/64 Any2 IPv6 - 2001:abc:430::240:120	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	
994270	Any-IPv6	Any-IPv6	ANY			Edit Clone Remove	<input checked="" type="checkbox"/>	

Netscreen CLI – Verify Routing

- Use the ‘get route v6’ to view IPv6 routing table.

```

10.10.1238 - PuTTY
FW_Sitel-> get route v6

IPv6 Dest-Routes for <untrust-vr> (0 entries)
-----
H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
N: NHRP
1B: IBGP eB: EBGp O: OSPF E1: OSPF external type 1
E2: OSPF external type 2 trailing B: backup route

IPv6 Dest-Routes for <trust-vr> (9 entries)
-----
      ID                IP-Prefix          Interface
      Gateway          P Pref      Mtr      Vsys
-----
*      1                ::0                eth0/1
      2001:abc:2480:3621::1 SP  20      1      Root
*      6                2001:abc:2480:3627::/64
      :: C      0      0      Root
*      7                2001:abc:2480:3627::1/128
      :: H      0      0      Root
*      5                2001:abc:2480:3621::3/128
      :: H      0      0      Root
*      4                2001:abc:2480:3621::/64
      :: C      0      0      Root
*      8                2001:abc:2480:36f7::254/128
      :: C      0      0      Root
*      9                2001:abc:2480:36f7::254/128
      :: H      0      0      Root
*     15                2001:abc:2480:36aa::7/128
      :: H      0      0      Root
*     14                2001:abc:2480:36aa::/64
      :: C      0      0      Root

FW_Sitel->
  
```

Netscreen CLI – Verify IPv6 Neighbors

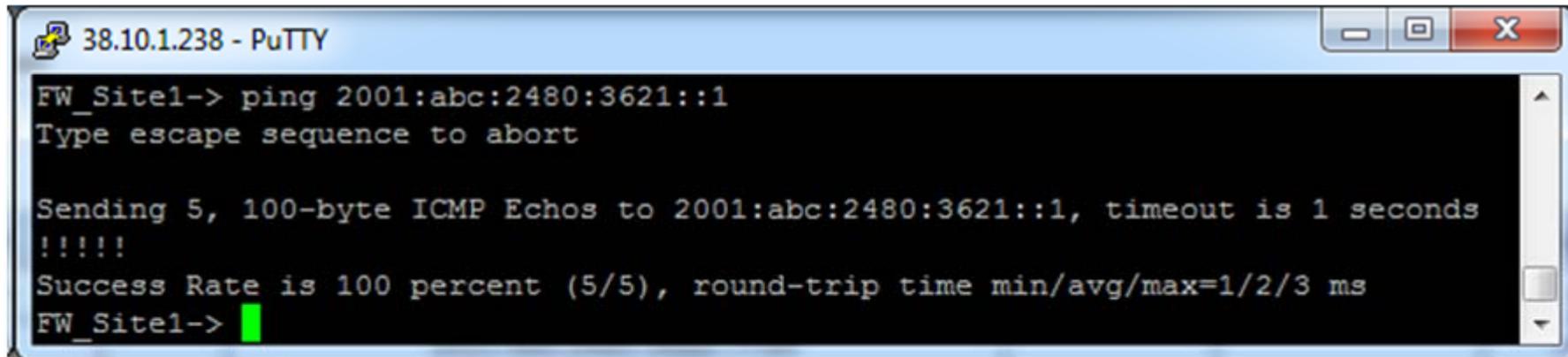


- Use 'get ndp' to determine IPv6 neighbors.

```
38.10.1.238 - PuTTY
FW_Site1-> get nd
usage: 4/4096 miss: 0 always-on-dest: disabled
states(S): N Undefined, X Deleted, I Incomplete, R Reachable, L Stale, D Delay,
P Probe, F Probe forever S Static, A Active, I Inactive, * persistent
-----
IPv6 Address                Link-Layer Addr S Interface    Age          Pk
2001:abc:2480:3627::10      000c29614c22   L ethernet0/2  01h36m26s  0
2001:abc:2480:3621::1      0024dc0cab02   L ethernet0/1  01h46m45s  0
fe80::110a:438:2dd9:3b8e    000c29614c22   L ethernet0/2  01h36m26s  0
fe80::224:dcff:fe0c:ab02    0024dc0cab02   L ethernet0/1  01h48m39s  0
FW_Site1->
```

Netscreen CLI – Verify Reachability

- Use the Ping command to ping the upstream router.

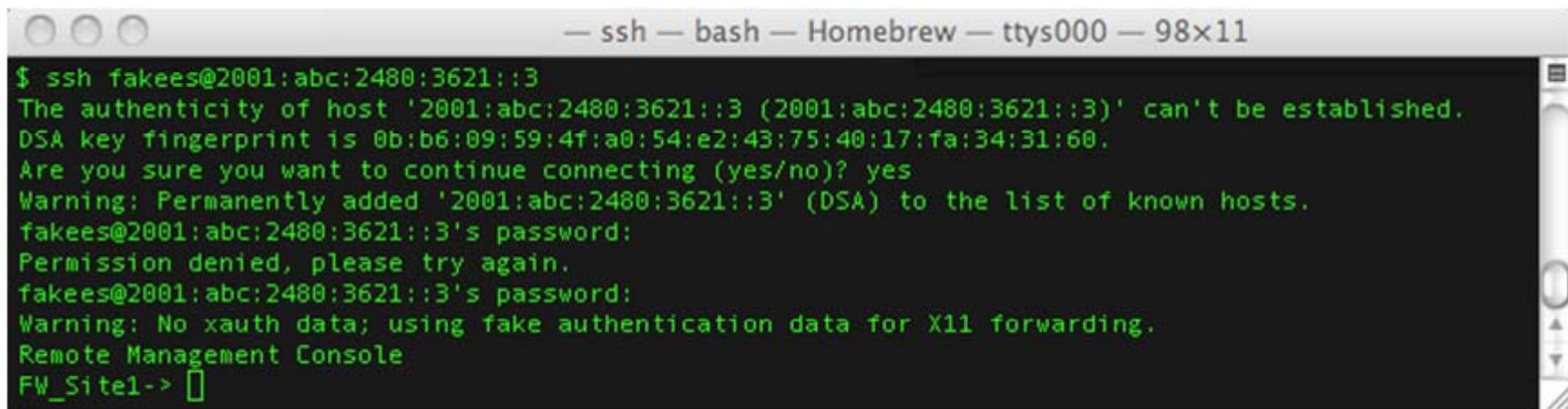


```

38.10.1.238 - PuTTY
FW_Site1-> ping 2001:abc:2480:3621::1
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 2001:abc:2480:3621::1, timeout is 1 seconds
!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=1/2/3 ms
FW_Site1->
  
```

- SSH to the IPv6 Firewall Address.



```

— ssh — bash — Homebrew — ttys000 — 98x11
$ ssh fakees@2001:abc:2480:3621::3
The authenticity of host '2001:abc:2480:3621::3 (2001:abc:2480:3621::3)' can't be established.
DSA key fingerprint is 0b:b6:09:59:4f:a0:54:e2:43:75:40:17:fa:34:31:60.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '2001:abc:2480:3621::3' (DSA) to the list of known hosts.
fakees@2001:abc:2480:3621::3's password:
Permission denied, please try again.
fakees@2001:abc:2480:3621::3's password:
Warning: No xauth data; using fake authentication data for X11 forwarding.
Remote Management Console
FW_Site1->
  
```

Netscreen CLI - Commands

IPv6 Interface Configuration –

```
set interface ethernet0/1 ip 168.168.201.3/29
set interface "ethernet0/1" ipv6 mode "router"
set interface "ethernet0/1" ipv6 ip 2001:abc:2480:3621::3/64
set interface "ethernet0/1" ipv6 enable
set interface ethernet0/1 route
```

IPv6 Router Advertisement Settings –

```
set interface ethernet0/1 ipv6 ra prefix 2001:abc:2480:3621::/64 autonomous onlink
set interface ethernet0/1 ipv6 ra link-address
set interface ethernet0/1 ipv6 ra transmit
set interface ethernet0/1 ipv6 ra link-mtu
set interface ethernet0/1 ipv6 nd nud
```

IPv6 Default Route –

```
set route ::/0 interface ethernet0/1 gateway 2001:abc:2480:3621::1 permanent
```

Policy Using 'Multiple' Source and 'Multiple' Destination –

```
set policy id 994274 from "SAN_Zone" to "Untrust" "Any9 IPv6 - 2001:abc:2480:a000::90/64" "Any10 IPv6 - 2001:abc:4300::240:95/64" "ANY" permit
set policy id 994274
set src-address "Any11 IPv6 - 2001:abc:2480:a000::93"
set src-address "Any12 IPv6 - 2001:abc:2480:a000::92"
set src-address "Any13 IPv6 - 2001:abc:2480:a000::91/64"
set dst-address "Any14 IPv6 - 2001:abc:4300::2400:119/64"
set dst-address "Any15 IPv6 - 2001:abc:4300::2400:138/64"
set dst-address "Any16 IPv6 - 2001:abc:4300::2400:120"
```

Set Policy Group –

```
set group address "SAN_Zone" "SAN_Servers"
set group address "SAN_Zone" "SAN_Servers" add "Any11 IPv4 - 127.32.148.172/32"
set group address "SAN_Zone" "SAN_Servers" add "Any12 IPv4 - 127.32.148.175/32"
set group address "SAN_Zone" "SAN_Servers" add "Any13 IPv4 - 127.32.148.174/32"
set group address "SAN_Zone" "SAN_Servers" add "Any14 IPv4 - 127.32.148.173/32"
```