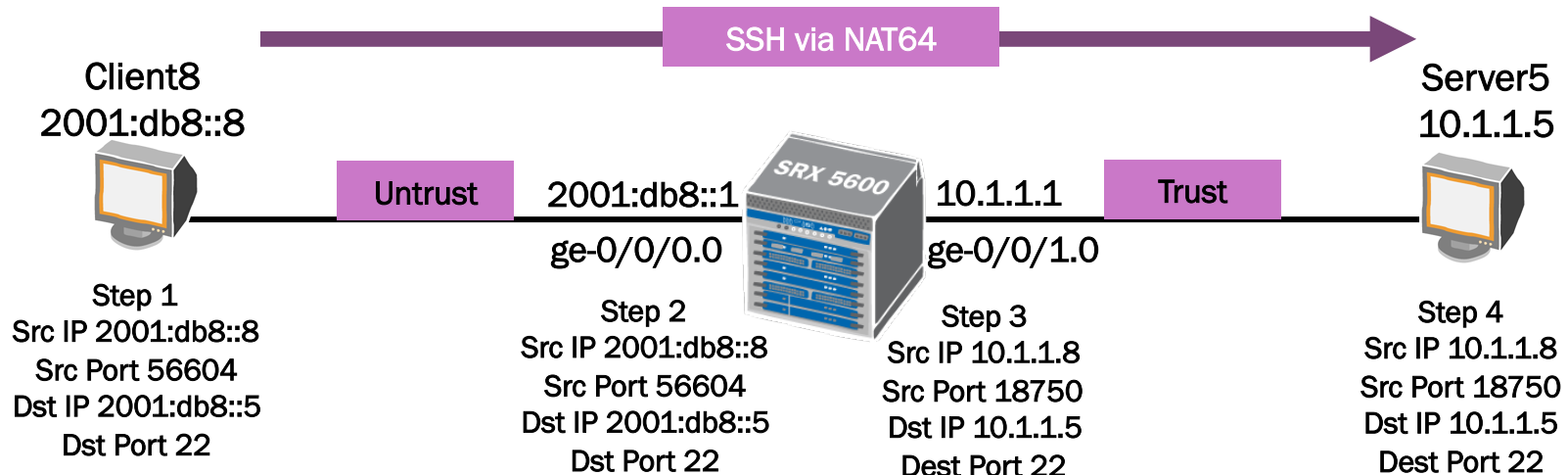


NAT64 Overview

NAT64 example

- SSH from an IPv6 client to an IPv4 server using NAT64
 - Use Static NAT on the Untrust side
 - SRX presents an IPv6 destination to the client
 - Translates the IPv6 destination address to the actual IPv4 address of server
 - Use Source NAT with Persistence
 - SRX translates the client's IPv6 address to an IPv4 address so the server can accept the connection
 - Example NATs:
 - Client8 from 2001:db8::8 to 10.1.1.8
 - Server5 from 10.1.1.5 to 2001:db8:5



NAT64 configuration example – IPv6 Flow

- Ensure the SRX is configured for IPv6 Flow Mode
 - One time setting to enable flow mode for IPv6
 - Not enabled by default
 - Requires a reboot

```
security {  
    forwarding-options {  
        family {  
            inet6 {  
                mode flow-based;  
            }  
        }  
    }  
}
```

NAT64 configuration example - Interfaces

- Configure the SRX Interfaces

- ge-0/0/0.0 = 2001:db8::164

- ge-0/0/1.0 = 10.1.1.1/24

```
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet6 {
        address 2001:db8::1/64;
      }
    }
  }
  ge-0/0/1 {
    unit 0 {
      family inet {
        address 10.1.1.1/24;
      }
    }
  }
}
```

NAT64 configuration example - zones

■ Configure the SRX Security Zones

```
security {  
    security-zone untrust {  
        address-book {  
            address client8 2001:db8::8/128;  
        }  
        interfaces {  
            ge-0/0/0.0 {  
                host-inbound-traffic {  
                    system-services {  
                        all;  
                    }  
                    protocols {  
                        all;  
                    }  
                }  
            }  
        }  
    }  
    security-zone trust {  
        address-book {  
            address server5 10.1.1.5/32;  
        }  
        interfaces {  
            ge-0/0/1.0 {  
                host-inbound-traffic {  
                    system-services {  
                        all;  
                    }  
                    protocols {  
                        all;  
                    }  
                }  
            }  
        }  
    }  
}
```

NAT64 configuration example – static nat

- Configure Static NAT for Server5
 - Traffic is coming from the client on the untrust zone
 - NAT Server5's 10.1.1.5 IPv4 address to the IPv6 2001:db8::5 address

```
security {
  nat {
    static {
      rule-set static64 {
        from zone untrust;
        rule server5 {
          match {
            destination-address 2001:db8::5/128;
          }
          then {
            static-nat prefix 10.1.1.5/32;
          }
        }
      }
    }
  }
}
```

NAT64 configuration example – source nat

■ Configure Source NAT for Client8

- Traffic is coming from the client on the untrust zone going to the server on the trust zone
- NAT Client8's 2001:db8::8 IPv6 address to the IPv4 10.1.1.8 address

```
security {  
    nat {  
        source {  
            pool client8-ipv4-pool {  
                address {  
                    10.1.1.8/32;  
                }  
            }  
            rule-set client8-rs {  
                from zone untrust;  
                to zone trust;  
                rule client8-rule {  
                    match {  
                        source-address 2001:db8::8/128;  
                        destination-address 10.1.1.5/32;  
                    }  
                    then {  
                        source-nat {  
                            pool {  
                                client8-ipv4-pool;  
                                persistent-nat {  
                                    permit any-remote-host;  
                                }  
                            }  
                        }  
                    }  
                }  
            }  
        }  
    }  
}
```

NAT64 configuration example – proxy arp

- Enable the SRX to respond to requests on behalf of the NATs
 - Both the static and source NAT IP addresses are on the same subnets as the interface IP addresses on the SRX.
 - For the IPv4 address configure Proxy ARP
 - For the IPv6 address configure Proxy NDP

```
security {  
  nat {  
    proxy-arp {  
      interface ge-0/0/1.0 {  
        address {  
          10.1.1.8/32;  
        }  
      }  
    }  
    proxy-ndp {  
      interface ge-0/0/0.0 {  
        address {  
          2001:db8::5/128;  
        }  
      }  
    }  
  }  
}
```


NAT64 configuration example – policies

- Configure a Security Policy from zone untrust to zone trust
 - Can use the key word "any"
 - Example is explicit using
 - IPv6 address 2001:db8::8 for client8
 - IPv4 address 10.1.1.5 for server5

```
security {
    policies {
        from-zone untrust to-zone trust {
            policy client8-to-server5 {
                match {
                    source-address client8;
                    destination-address server5;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-init;
                        session-close;
                    }
                    count;
                }
            }
        }
    }
}
```

NAT64 validation – session table (brief)

- Once Client8 initiates an SSH session to Server5 you can view the session entry in the flow table

```
admin@srx210> show security flow session
```

```
Session ID: 1612, Policy name: client8-to-server5/6, Timeout: 1794, Valid  
  In: 2001:db8::8/56604 --> 2001:db8::5/22;tcp, If: ge-0/0/0.0, Pkts: 24, Bytes: 3601  
  Out: 10.1.1.5/22 --> 10.1.1.8/18750;tcp, If: ge-0/0/1.0, Pkts: 17, Bytes: 3205
```

NAT64 validation – session table (detailed)

■ Detailed view of the session table

```
admin@srx210-1> show security flow session session-identifier 1612
Session ID: 1612, Status: Normal
Flag: 0x0
Policy name: client8-to-server5/6
Source NAT pool: client8-ipv4-pool
Dynamic application: junos:UNKNOWN,
Maximum timeout: 1800, Current timeout: 1746
Session State: Valid
Start time: 3476, Duration: 63
  In: 2001:db8::8/56604 --> 2001:db8::5/22;tcp,
    Interface: ge-0/0/0.0,
    Session token: 0x7, Flag: 0x0x623
    Route: 0xc0010, Gateway: 2001:db8::8, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 24, Bytes: 3601
  Out: 10.1.1.5/22 --> 10.1.1.8/18750;tcp,
    Interface: ge-0/0/1.0,
    Session token: 0x8, Flag: 0x0x620
    Route: 0xa0010, Gateway: 10.1.1.5, Tunnel: 0
    Port sequence: 0, FIN sequence: 0,
    FIN state: 0,
    Pkts: 17, Bytes: 3205
Total sessions: 1
```

NAT64 validation – static nat

■ View statistics for the Static NAT

```
admin@srx210-1> show security nat static rule all
```

```
Total static-nat rules: 1
```

```
Total referenced IPv4/IPv6 ip-prefixes: 1/1
```

```
Static NAT rule: server5           Rule-set: static64
  Rule-Id                        : 1
  Rule position                  : 1
  From zone                      : untrust
  Destination addresses          : 2001:db8::5
  Host addresses                 : 10.1.1.5
  Netmask                       : 128
  Host routing-instance          : N/A
  Translation hits               : 16
```

NAT64 validation – source nat

■ View statistics for the Source NAT

```
admin@srx210-1> show security nat source rule all
```

```
Total rules: 1
```

```
Total referenced IPv4/IPv6 ip-prefixes: 1/1
```

```
source NAT rule: client8-rule          Rule-set: client8-rs
Rule-Id                               : 1
Rule position                          : 1
From zone                             : untrust
To zone                               : trust
Match
  Source addresses                     : 2001:db8::8      - 2001:db8::8
  Destination addresses                : 10.1.1.5         - 10.1.1.5
  Destination port                     : 0                - 0
Action
  Persistent NAT type                  : client8-ipv4-pool
  Persistent NAT mapping type          : any-remote-host
  Persistent NAT mapping type         : address-port-mapping
  Inactivity timeout                   : 300
  Max session number                   : 30
Translation hits                       : 13
```

NAT64 validation – source nat

■ View statistics for the Source NAT

```
admin@srx210-1> show security nat source persistent-nat-table all
```

Internal			Reflective			Source	Type	Left_time/ Conf_time	Curr_Sess_Num/ Max_Sess_Num	Source NAT Rule
In_IP	In_Port	I_Proto	Ref_IP	Ref_Port	R_Proto	NAT Pool				
2001:db8::8	56604	tcp	10.1.1.8	18750	tcp	client8-ipv4-pool	any-remote-host	-/300	1/30	client8-rule

NAT64 validation – traffic logs

- Traffic logs are generated by the security policy (if enabled)

```
admin@srx210-1> show log traffic-log
```

```
Oct 11 22:03:22 srx210-1 RT_FLOW: RT_FLOW_SESSION_CREATE: session created  
2001:db8:0:0:0:0:8/56604->2001:0:0:0:5/22 None 10.1.1.8/18750->10.1.1.5/22 client8-rule  
server5 6 client8-to-server5 untrust trust 1612 N/A(N/A) ge-0/0/0.0
```

```
Oct 11 22:07:09 srx210-1 RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed TCP FIN:  
2001:db8:0:0:0:0:8/56604->2001:db8:0:0:0:0:5/22 None 10.1.1.8/18750->10.1.1.5/22  
client8-rule server5 6 client8-to-server5 untrust trust 1612 76(8337) 48(9057) 228  
UNKNOWN UNKNOWN N/A(N/A) ge-0/0/0.0:db8:0:0
```

NAT64 validation – NAT logs

- Below is an example of the logs generated by the persistent NATs:

```
admin@srx210-1> show log nat64-log
```

```
Oct 11 21:25:58 srx210-1 RT_NAT: RT_PST_NAT_BINDING_CREATE: Pst NAT (Active ) binding  
created, lsys_id: 0, internal ip/port/protocol: 2001:db8:0:0:0:0:0:8/56599/6, reflexive  
ip/port/protocol: 10.1.1.8/12689/6
```

```
Oct 11 21:29:10 srx210-1 RT_NAT: RT_PST_NAT_BINDING_MATCH: Pst NAT (Active ) binding  
matched, lsys_id: 0, internal ip/port/protocol: 2001:db8:0:0:0:0:0:8/56599/6, reflexive  
ip/port/protocol: 10.1.1.8/12689/6
```

```
Oct 11 21:34:20 srx210-1 RT_NAT: RT_PST_NAT_BINDING_DELETE: Pst NAT (Invalid_1) binding  
deleted, lsys_id: 0, internal ip/port/protocol: 2001:db8:0:0:0:0:0:8/56599/6, reflexive  
ip/port/protocol: 10.1.1.8/12689/6
```