NAT

NETWORK ADDRESS TRANSLATION

SCREENOSとのNAT実装の違い

ScreenOSとJ-Series(JUNOS9.5以前)では、NAT処理をポリシーにバインドすることにより処理。

ScreenOSとJ-Series(JUNOS9.5以前)では、ポリシールックアップを実施後、その結果を元にどのようにNATするかを決定される。

このモデルの場合、以下のような制限事項あり:

- Destination NATの場合、ポリシールックアップは、ルーティング処理の後に行われる為、作為的なルートが追加される必要があり
  - 変換後のアドレスがZoneに紐づけるためのルーティング
- NAT Pool (DIP) はIFと関連付けられている為、同じNAT Poolが二つ以上のEgress IFで使用される場合、Loopback Groupを利用する必要があり(ScreenOSなど)

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

SRXでのNAT実装

SRXでは、NAT処理をセキュリティポリシーから分離

複数のMatch Conditionにより、複雑なトラフィックパターンを容易に表現可能な、きめ細かいポリシーの作成が可能

NAT設定やネットワークトポロジ変更に際して、セキュリティポリシーの変更が不要

- NATルールとFWポリシーが混同しない

Loopback GroupやDummy Static Routeが不要

- 設定がシンプルに

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

SCREENOSのNAT機能との対比

ScreenOSが実装していた全てのNATタイプは、SRXのNATで
すべて対応可能

ScreenOS	SRX
DIP (Src-NAT)	Source NAT using an address Pool
Interface NAT	Source NAT
MIP	Static NAT
VIP	Destination NAT
DIP (Dst-NAT)	Destination NAT

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

独立したNATルール

セキュリティポリシーはNATを管理しない

- **独立したNATルールはアドレス変換処理の実行に必要**

Source NAT

- **インターフェースベースNAT**
- **プールベースNAT（オプション：ポート番号変換 有/無）**
- **IPアドレスシフト**

Destination NAT

- **宛先IP（オプション：ポート番号変換 有/無）**
- **IPアドレスシフト**

Static NAT

- **1：1 アドレスマッピング**

Copyright © 2010 Juniper Networks, Inc.

DESTINATION NAT と STATIC NAT

Destination NAT:

- Ingress IFでのDestination IP/Portのトランスレーション
- 2種類のDestination NATオプション
  - M → 1 (M=1,2,…)
  - M → N (M,N>1, better M<=N)

Static NAT

- Double-IP-NAT
  - IngressでDestination NATかつEgressでSource NAT（このとき逆方向パケット転送についても、1st パケットと同一セッションであることを保障）
  - Port Translationには未対応
- 2種類のNATオプション
  - 1 to 1
  - Subnet to Subnet

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

CONE NAT

Full cone NATで定義される構成は4種類

- Full cone NAT
- Restricted cone NAT
- Port restricted cone NAT
- Symmetric NAT

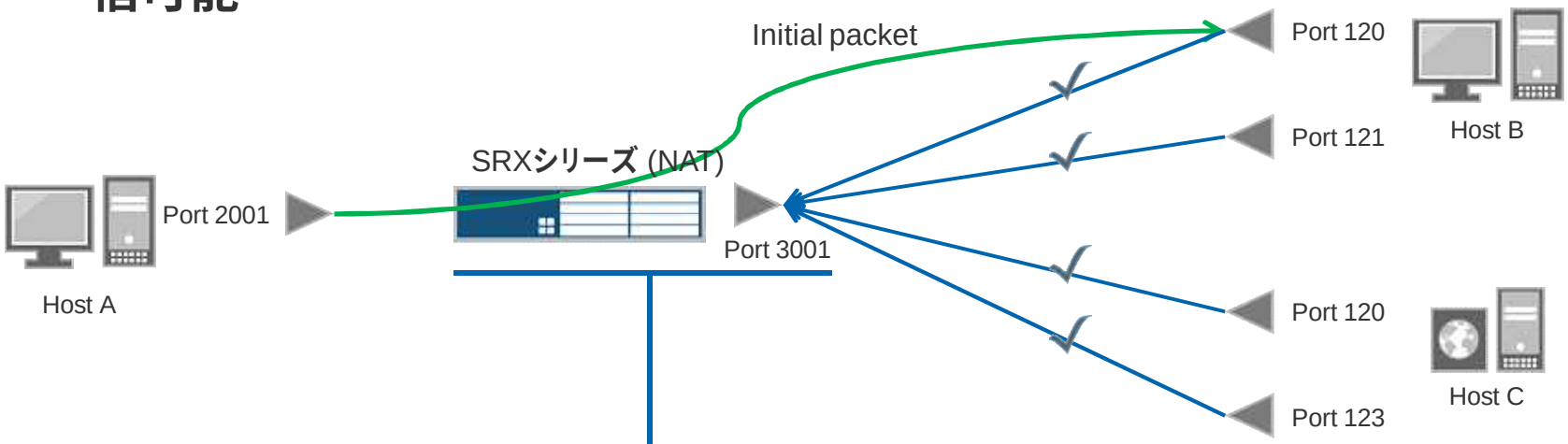
SRXシリーズではJUNOS 10.0からサポート

Copyright © 2010 Juniper Networks, Inc.

FULL CONE NAT

Full cone NATとは

- **内部のIPとポート番号が外部のIPとポート番号に1:1でマッピングされる**
- **マッピングされたアドレスには外部のどのホストやポート番号からでも通信可能**



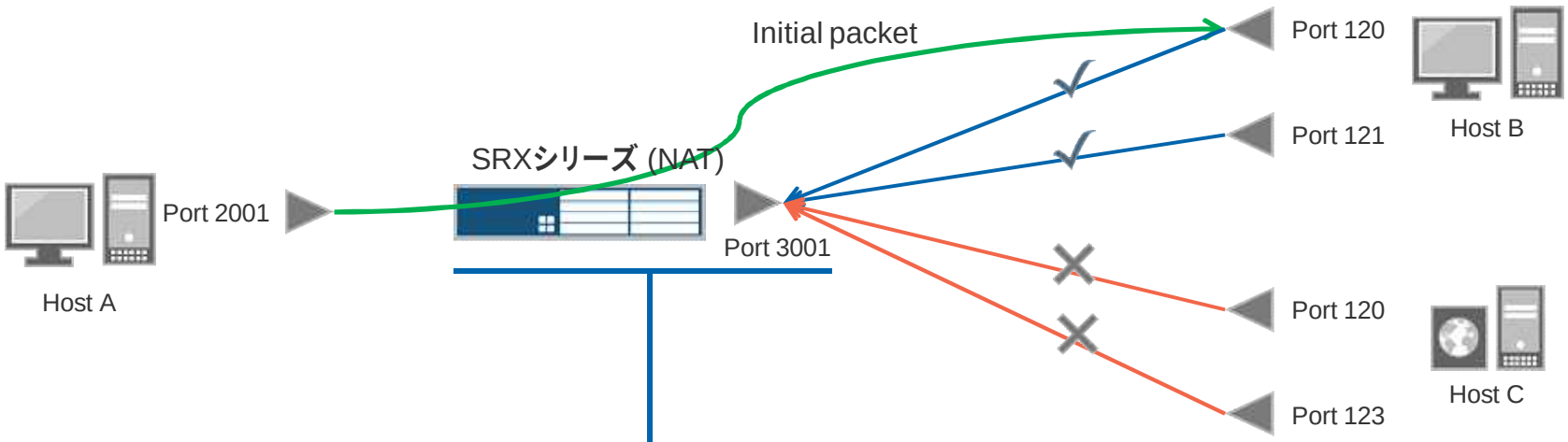
ローカルアドレス:ポート	外部アドレス:ポート	外部アクセスフィルタ
Host A:2001	Z:3001	*:* (Any)

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

RESTRICTED CONE NAT

Restricted cone NATとは

- 内部のIPとポート番号が外部のIPとポート番号に1:1でマッピングされる
- マッピングされたアドレスには接続したホストからのみ通信可能



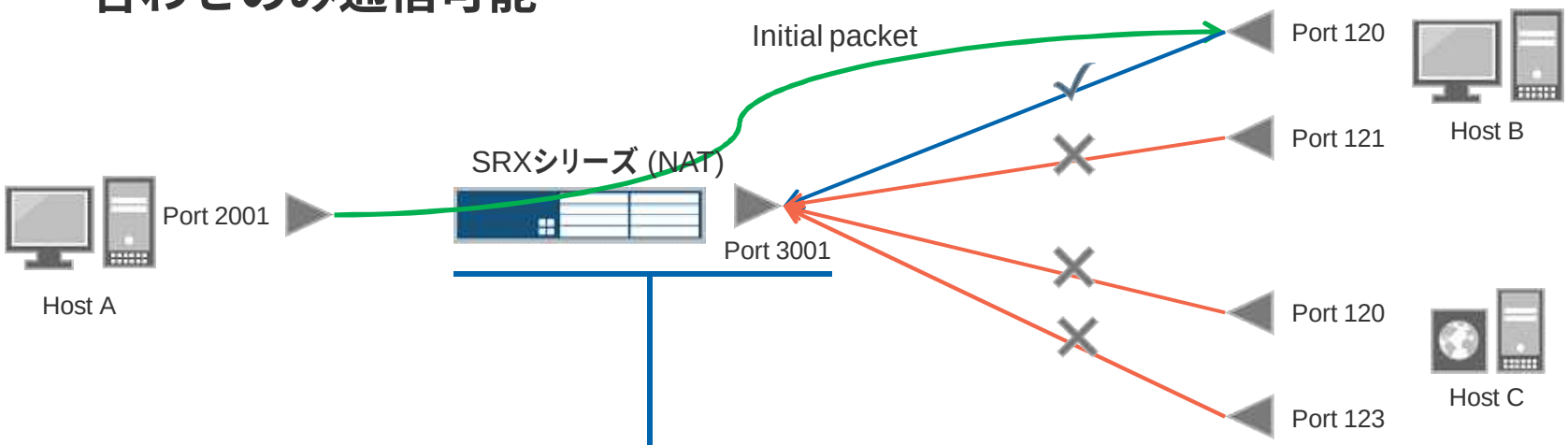
ローカルアドレス:ポート	外部アドレス:ポート	外部アクセスフィルタ
Host A:2001	Z:3001	Host B:* (Port any)

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

PORT RESTRICTED CONE NAT

Port restricted cone NATとは

- 内部のIPとポート番号が外部のIPとポート番号に1：1でマッピングされる
- マッピングされたアドレスには最初に接続したホストとポート番号の組み合わせのみ通信可能



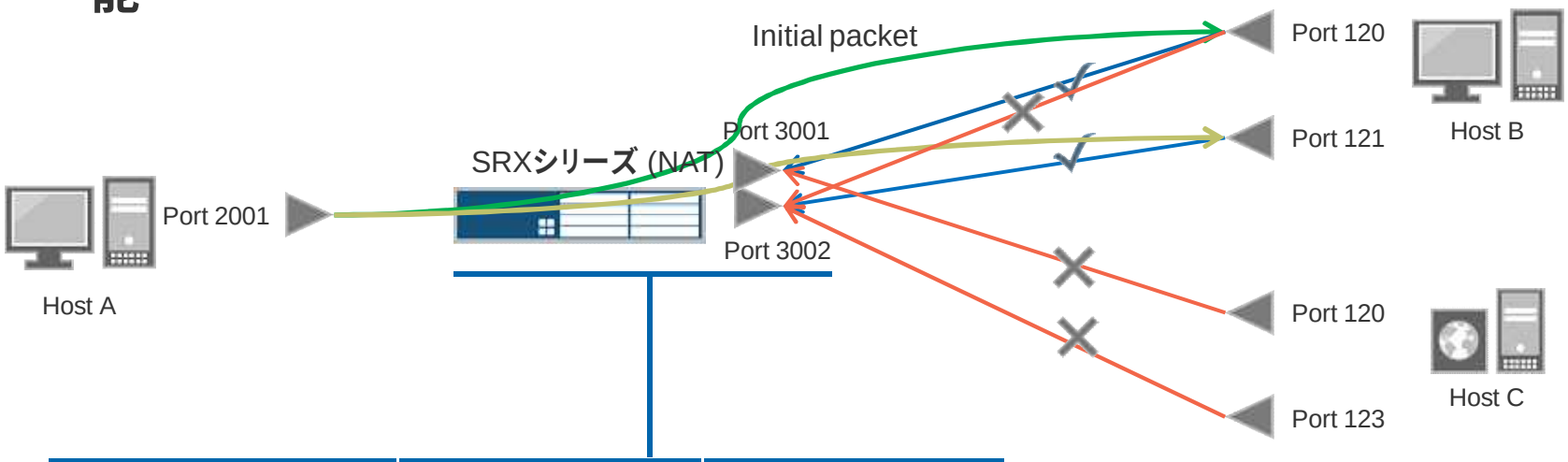
ローカルアドレス：ポート	外部アドレス：ポート	外部アクセスフィルタ
Host A:2001	IP Z:3001	Host B：120

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

SYMMETRIC NAT

Symmetric NATとは

- **接続先のアドレスとポート番号の組み合わせ毎に外部アドレスがマッピングされる**
- **マッピングされたアドレスには接続したホストとポート番号のみ通信可能**



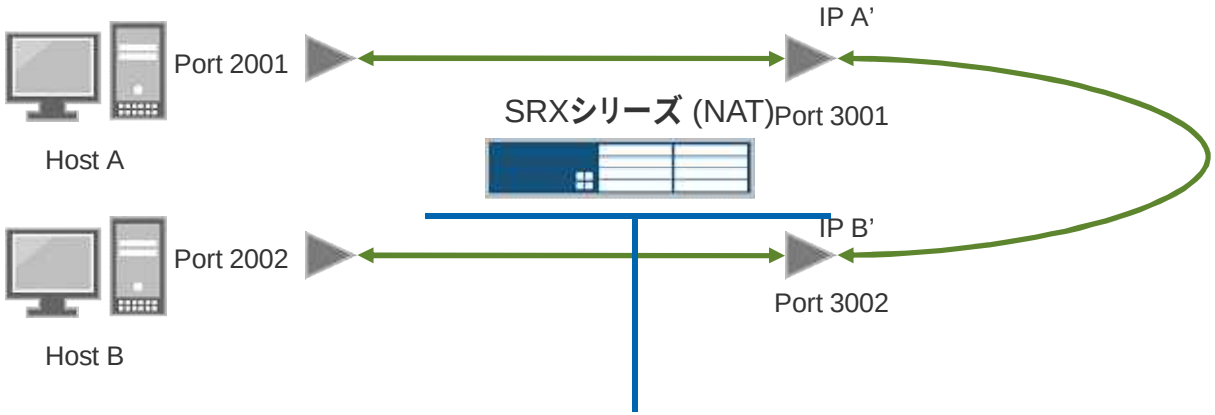
ローカルアドレス:ポート	外部アドレス:ポート	外部アクセスフィルタ
Host A:2001	IP Z:3001	Host B:120
Host A:2001	IP Z:3002	Host B:121

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

HAIRPINNING BEHAVIOR

Hairpinning behavior (**ヘアピンNAT)とは**

- **NATされるホスト同士が、NATされたアドレスを利用して通信を行えるようにする動作**
- **相互通信はNATされたアドレスを介して行う(ローカルIPでは通信しない)**



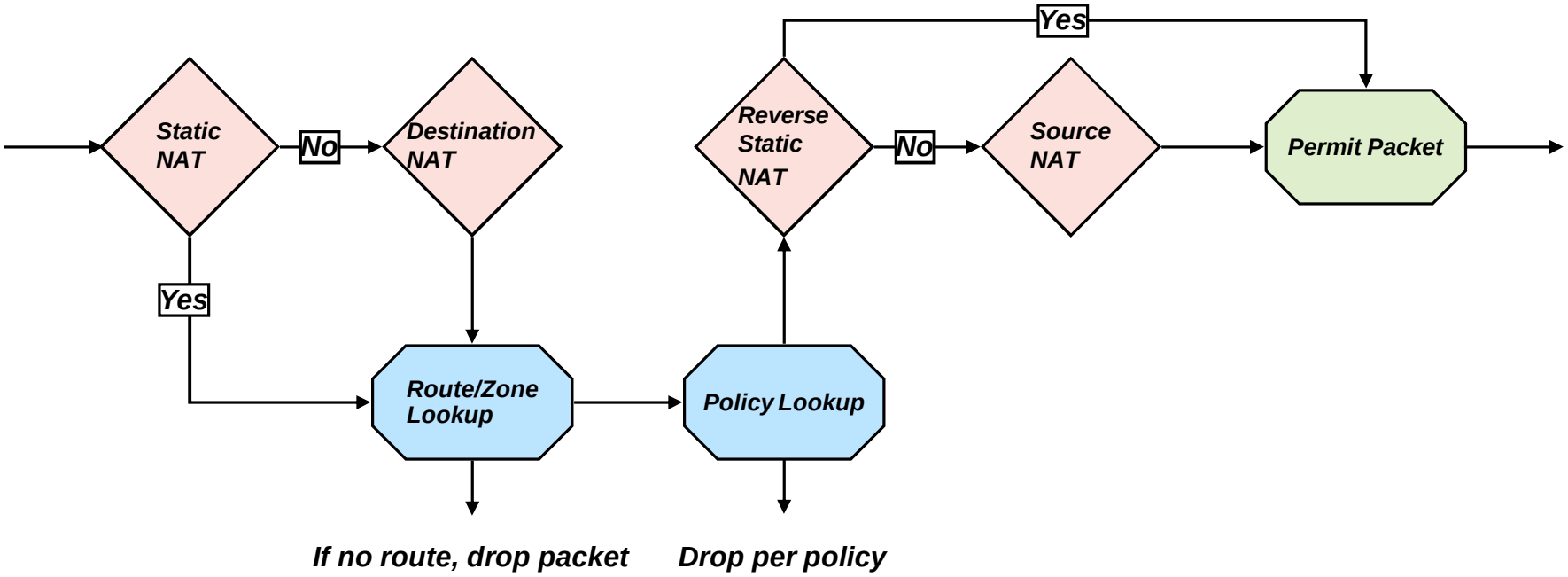
ローカルアドレス:ポート	外部アドレス:ポート	外部アクセス
Host A:2001	IP A':3001	IP B':3002
Host B:2002	IP B':3002	IP A':3001

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

NAT 処理

Static & destination NATは、セキュリティポリシー適用の前に実施

Reverse static & source NATは、セキュリティポリシー適用後に実施



Copyright © 2010 Juniper Networks, Inc. www.juniper.net

ルールセット

ルールセットとは
- NATルールをまとめたグループ

各ルールセットは、宛先や送信元に基づいた適用条件のセットを持つ
- Interface
- Zone
- Routing-Instance

特定のルールセットが適用後、ルールセット中のルールが順番に評価される

各ルールは、マッチしたトラフィックがどのように処理されるかを以下のオプションの中から指示:
- Poolを利用してトランスレーション
- Egress IFのIPアドレスへトランスレーション (Source NATのみ)
- なんらトランスレーションを実施せずフォワーディング実施

ルールセット内に定義可能な最大ルール数は下記の通り (JUNOS 10.2)

Type/Platform	SRX100	SRX210	SRX240	SRX650	SRX-HE
Src-NAT	512	512	1024	1024	8192
Dst-NAT	512	512	1024	1024	8192
Static NAT	512	512	1024	1024	8192

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

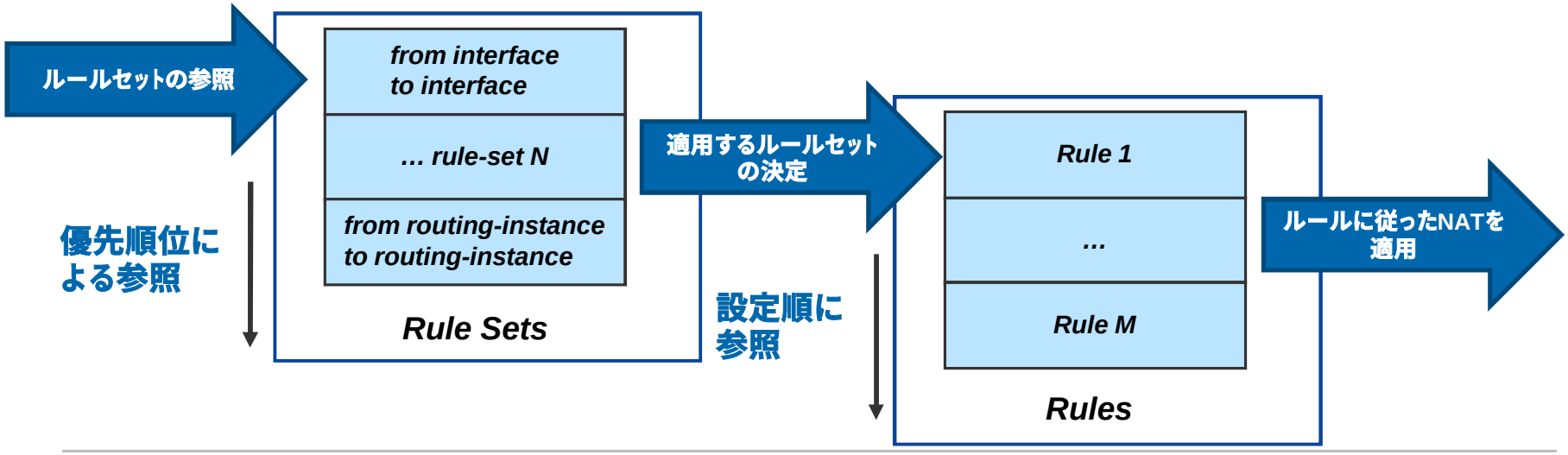
ルールセットの優先順位

パケットが複数のルールセットにマッチした場合、最も詳細にマッチしたルールが優先される

優先順位 (高から低)

- Interface
- Zone
- Routing-Instance

ルールセット中のルールは順番にマッチ評価される



Copyright © 2010 Juniper Networks, Inc. www.juniper.net

アドレスプール設定

アドレスプールの形態

- 単一のIPアドレス
- IPアドレスレンジ
- Interface (source NATのみ)

オプション

- ポート変換無し (PAT無効)

Overflow pools

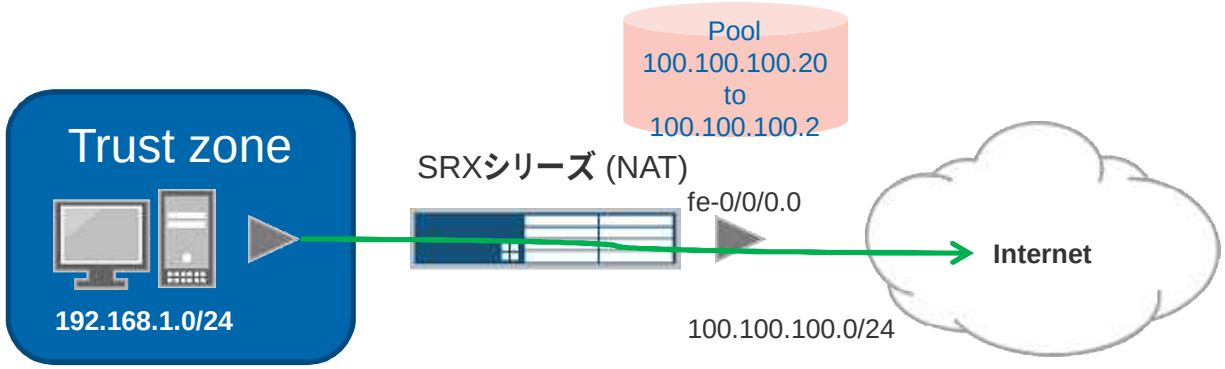
- フォールバック時の為に設定
- ポートトランスレーション無しのPoolが必要

```
regress@limebert# show pool 666
address {
    222.1.1.1/32 to 222.1.1.14/32;
}
port no-translation;
```

```
[edit security nat source]
regress@limebert# show pool 666
address {
    222.1.1.1/32 to 222.1.1.14/32;
}
port no-translation;
overflow-pool interface;
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

SOURCE NAT (PAT有り)



SRX100-vpn# run show security flow session
Session ID: 11010, Policy name: trust-to-untrust/4, Timeout: 1792, Valid
In: 192.168.1.22/57842 --> 100.100.100.254/23;tcp, If: vlan.0, Pkts: 5, Bytes: 227
Out: 100.100.100.254/23 --> 100.100.100.26/21626;tcp, If: fe-0/0/0.0, Pkts: 5, Bytes: 259

NAPTされている

SRX100-vpn# run show security nat source summary
Total pools: 1

Pool Name	Address Range	Routing Instance	PAT	Total Address
src_nat_pool_napt	100.100.100.20-100.100.100.29	default	yes	10

Total rules: 1

Rule name	Rule set	From	To	Action
napt_1	src_nat_napt	trust	fe-0/0/0.0	src_nat_pool_napt

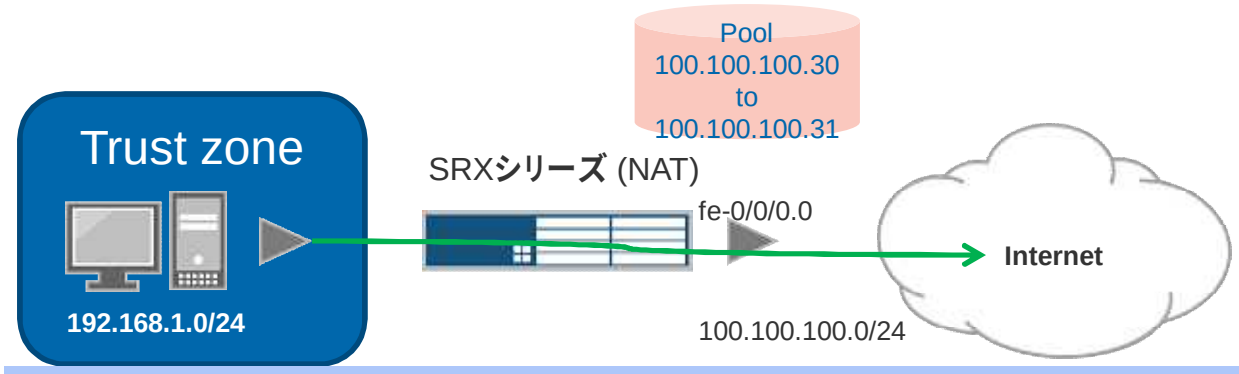
Copyright © 2010 Juniper Networks, Inc. www.juniper.net

SOURCE NAT 設定例 (PAT有り) 設定

```
nat {
    source {
        pool src_nat_pool_napt {
            address {
                100.100.100.20/32 to 100.100.100.29/32;
            }
        }
        rule-set src_nat_napt {
            from zone trust;
            to interface fe-0/0/0.0;
            rule napt_1 {
                match {
                    source-address 192.168.1.0/24;
                }
                then {
                    source-nat {
                        pool {
                            src_nat_pool_napt;
                        }
                    }
                }
            }
        }
    }
    proxy-arp {
        interface fe-0/0/0.0 {
            address {
                100.100.100.20/32 to 100.100.100.50/32;
            }
        }
    }
}
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

SOURCE NAT (PAT無し, OVER FLOW POOL有り)



SRX100-vpn# run show security flow session
Session ID: 11120, Policy name: trust-to-untrust/4, Timeout: 1580, Valid
In: 192.168.1.22/21003 --> 100.100.100.254/23;tcp, If: vlan.0, Pkts: 36, Bytes: 1481
Out: 100.100.100.254/23 --> 100.100.100.30/21003;tcp, If: fe-0/0/0.0, Pkts: 36, Bytes: 1523

Session ID: 11127, Policy name: trust-to-untrust/4, Timeout: 1790, Valid
In: 192.168.1.23/1267 --> 100.100.100.254/22;tcp, If: vlan.0, Pkts: 17, Bytes: 1673
Out: 100.100.100.254/22 --> 100.100.100.31/1267;tcp, If: fe-0/0/0.0, Pkts: 18, Bytes: 1767

NATされているがポート変換されていない

Session ID: 11159, Policy name: trust-to-untrust/4, Timeout: 1794, Valid
In: 192.168.1.24/1044 --> 100.100.100.254/80;tcp, If: vlan.0, Pkts: 22, Bytes: 1680
Out: 100.100.100.254/80 --> 100.100.100.1/64506;tcp, If: fe-0/0/0.0, Pkts: 43, Bytes: 40039

SRX100-vpn# run show security nat source summary
Total pools: 2

Pool Name	Address Range	Routing Instance	PAT	Total Address
src_nat_pool_napt	100.100.100.20-100.100.100.29	default	yes	10
src_nat_pool_nat	100.100.100.30-100.100.100.31	default	no	2

Poolを超過したためIFアドレスでNAPTされている

Total rules: 1

Rule name	Rule set	From	To	Action
nat_over_flow_pool	src_nat_napt	trust	fe-0/0/0.0	src_nat_pool_nat

SOURCE NAT 設定例 (PAT無し, OVER FLOW POOL有り)

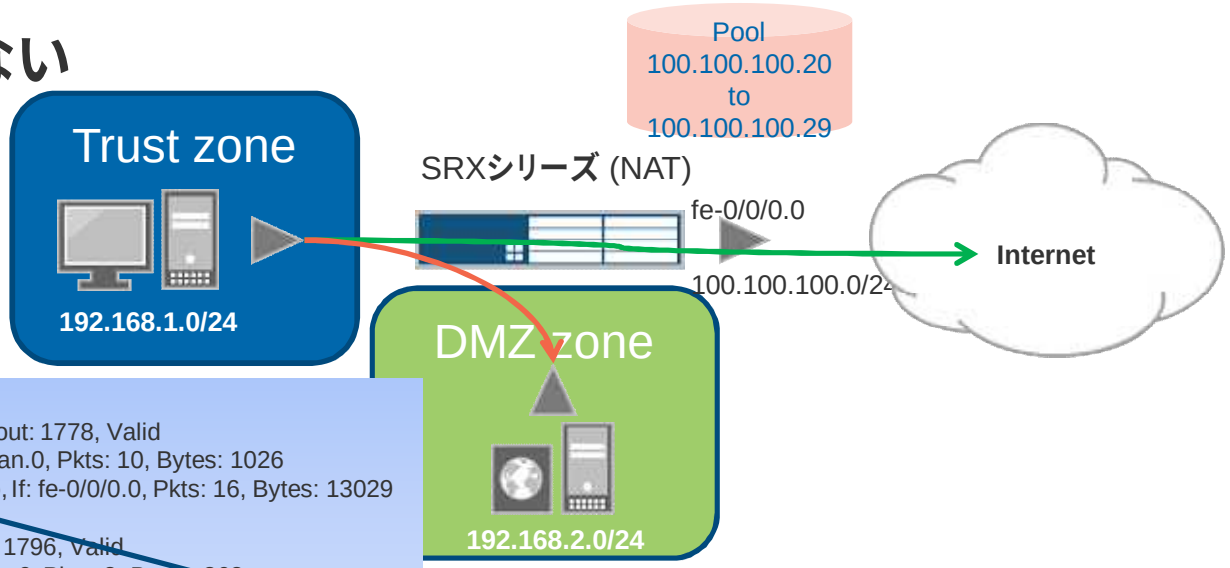
```
nat {
    source {
        pool src_nat_pool_nat {
            address {
                100.100.100.30/32 to 100.100.100.31/32;
            }
            port no-translation;
            overflow-pool interface;
        }
        rule nat_over_flow_pool {
            match {
                source-address 192.168.1.0/24;
            }
            then {
                source-nat {
                    pool {
                        src_nat_pool_nat;
                    }
                }
            }
        }
    }
    proxy-arp {
        interface fe-0/0/0.0 {
            address {
                100.100.100.20/32 to 100.100.100.50/32;
            }
        }
    }
}
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

複数NATルールの適用例

Internet向けにはNATする

DMZ向けにはNATしない




```
SRX100-vpn# run show security flow session
Session ID: 11254, Policy name: trust-to-untrust/4, Timeout: 1778, Valid
  In: 192.168.1.24/1045 --> 100.100.100.254/80;tcp, If: vlan.0, Pkts: 10, Bytes: 1026
  Out: 100.100.100.254/80 --> 100.100.100.24/18416;tcp, If: fe-0/0/0.0, Pkts: 16, Bytes: 13029

Session ID: 11255, Policy name: any_permit/6, Timeout: 1796, Valid
  In: 192.168.1.22/57601 --> 192.168.2.254/23;tcp, If: vlan.0, Pkts: 8, Bytes: 368
  Out: 192.168.2.254/23 --> 192.168.1.22/57601;tcp, If: fe-0/0/1.0, Pkts: 7, Bytes: 360

SRX100-vpn# run show security nat source summary
Total pools: 2
Pool              Address                Routing          PAT  Total
Name              Range                  Instance              Address
src_nat_pool_napt   100.100.100.20-100.100.100.29 default       yes  10
src_nat_pool_nat    100.100.100.30-100.100.100.31 default       no   2

Total rules: 2
Rule name         Rule set       From          To              Action
napt_1            src_nat_napt   trust         fe-0/0/0.0      src_nat_pool_napt
NO_nat            NO_nat_for_DMZ trust         DMZ             off
```

Internet向けにはNATされている

DMZにはNATされていない

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

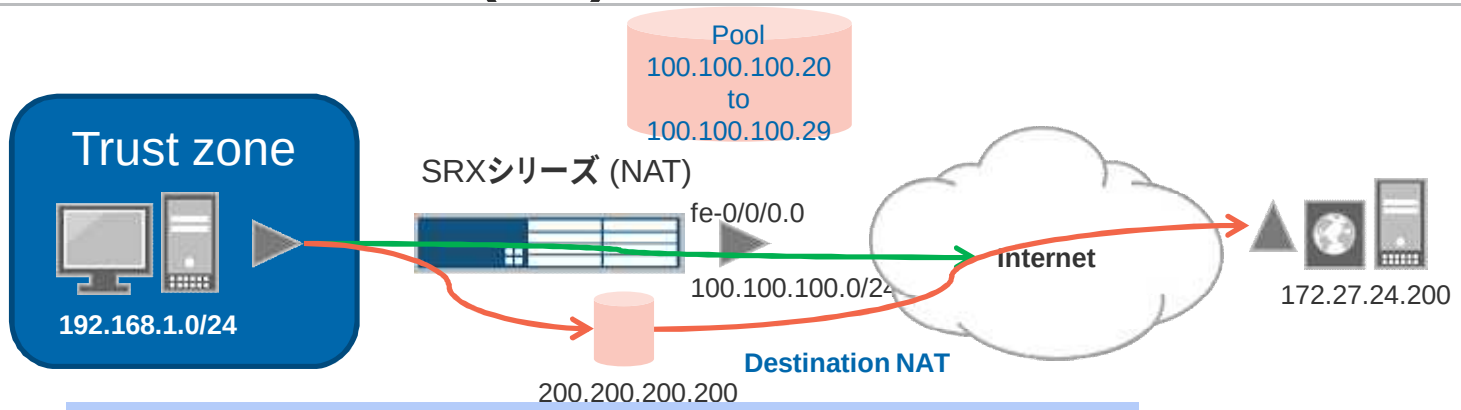
複数NATルールの適用例 (CONFIG)

```
nat {
    source {
        pool src_nat_pool_napt {
            address {
                100.100.100.20/32 to
100.100.100.29/32;
            }
        }
        rule-set src_nat_napt {
            from zone trust;
            to interface fe-0/0/0.0;
            rule napt_1 {
                match {
                    source-address 192.168.1.0/24;
                }
                then {
                    source-nat {
                        pool {
                            src_nat_pool_napt;
                        }
                    }
                }
            }
        }
```

```
        rule-set NO_nat_for_DMZ {
            from zone trust;
            to zone DMZ;
            rule NO_nat {
                match {
                    source-address 192.168.1.0/24;
                }
                then {
                    source-nat {
                        off;
                    }
                }
            }
        }
    }
    proxy-arp {
        interface fe-0/0/0.0 {
            address {
                100.100.100.20/32 to
100.100.100.50/32;
            }
        }
    }
}
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

DESTINATION NAT (1:1)



SRX100-vpn# run show security flow session
Session ID: 11649, Policy name: trust-to-untrust/4, Timeout: 1796, Valid
In: 192.168.1.22/34367 --> 200.200.200.200/23;tcp, If: vlan.0, Pkts: 9, Bytes: 402
Out: 172.27.24.200/23 --> 100.100.100.28/29684;tcp, If: fe-0/0/0.0, Pkts: 8, Bytes: 436

SRX100-vpn# run show security nat source summary
Total pools: 2

Pool Name	Address Range	Routing Instance	PAT	Total Address
src_nat_pool_napt	100.100.100.20-100.100.100.29	default	yes	
src_nat_pool_nat	100.100.100.30-100.100.100.31	default	no	

Src-NATされている

Dst-NATされている

Total rules: 1

Rule name	Rule set	From	To	Action
nat_over_flow_pool	src_nat_napt	trust	fe-0/0/0.0	src_nat_pool_nat

SRX100-vpn# run show security nat destination summary
Total pools: 1

Pool name	Address Range	Routing Instance	Port	Total Address
application_srv	172.27.24.200 - 172.27.24.200	default	0	1

Total rules: 1

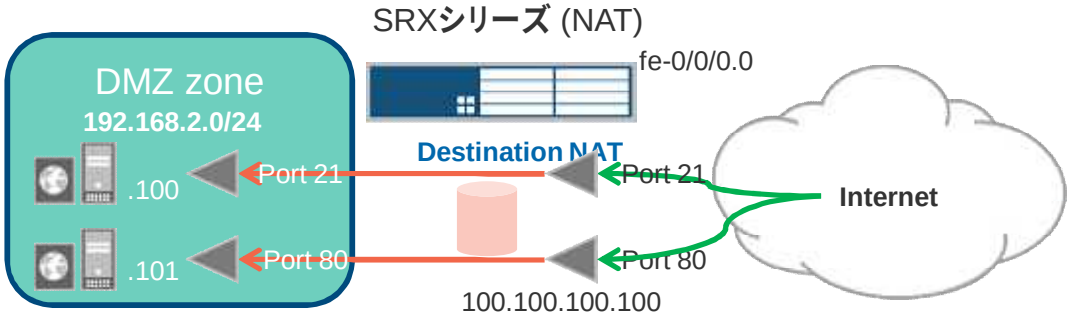
Rule name	Rule set	From	Action
app_srv	one_to_one_dst_nat	trust	application_srv

DESTINATION NAT (1:1) 設定例

```
nat {
destination {
    pool application_srv {
        address 172.27.24.200/32;
    }
    rule-set one_to_one_dst_nat {
        from zone trust;
        rule app_srv {
            match {
                source-address 192.168.1.0/24;
                destination-address 200.200.200.200/32;
            }
            then {
                destination-nat pool application_srv;
            }
        }
    }
}
}
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

DESTINATION NAT (1:N)



SRX100-vpn# run show security flow session
Session ID: 11866, Policy name: srv_permit/7, Timeout: 12, Valid
In: 172.27.23.20/1492 --> 100.100.100.100/21;tcp, If: fe-0/0/0.0, Pkts: 2, Bytes: 96
Out: 192.168.2.100/21 --> 172.27.23.20/1492;tcp, If: fe-0/0/1.0, Pkts: 0, Bytes: 0

Session ID: 11867, Policy name: srv_permit/7, Timeout: 1796, Valid
In: 172.27.23.20/1493 --> 100.100.100.100/80;tcp, If: fe-0/0/0.0, Pkts: 18, Bytes: 1428
Out: 192.168.2.101/80 --> 172.27.23.20/1493;tcp, If: fe-0/0/1.0, Pkts: 17, Bytes: 13075

SRX100-vpn# run show security nat destination summary
Total pools: 2

Pool name	Address Range		Routing Instance	Port	Total Address
multiple_appli_srv1	192.168.2.100	- 192.168.2.100	default	21	1
multiple_appli_srv2	192.168.2.101	- 192.168.2.101	default	80	1

Total rules: 2

Rule name	Rule set	From	Action
ftp_srv	one_to_N_dst_nat	untrust	multiple_appli_srv1
web_srv	one_to_N_dst_nat	untrust	multiple_appli_srv2

宛先ポート単位で
NATを振り分けている

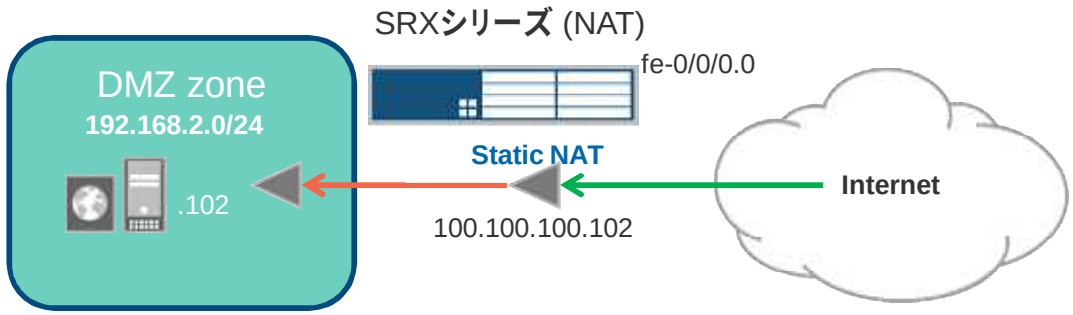
DESTINATION NAT (1:N) 設定例

```
destination {
 pool multiple_appli_srv1 {
       address 192.168.2.100/32 port 21;
   }
   pool multiple_appli_srv2 {
       address 192.168.2.101/32 port 80;
   }
rule-set one_to_N_dst_nat {
       from zone untrust;
       rule ftp_srv {
          match {
             source-address 0.0.0.0/0;
             destination-address 100.100.100.100/32;
             destination-port 21;
          }
          then {
             destination-nat pool multiple_appli_srv1;
          }
```

```
}
       rule web_srv {
          match {
             source-address 0.0.0.0/0;
             destination-address 100.100.100.100/32;
             destination-port 80;
          }
          then {
             destination-nat pool multiple_appli_srv2;
          }
       }
   }
}
proxy-arp {
   interface fe-0/0/0.0 {
       address {
          100.100.100.100/32;
       }
   }
}
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

STATIC NAT



SRX100-vpn# run show security flow session
Session ID: 11875, Policy name: srv_permit/7, Timeout: 1790, Valid
In: 172.27.23.20/1709 --> 100.100.100.102/80;tcp, If: fe-0/0/0.0, Pkts: 28, Bytes: 1491
Out: 192.168.2.102/80 --> 172.27.23.20/1709;tcp, If: fe-0/0/1.0, Pkts: 27, Bytes: 25498
w
Session ID: 11883, Policy name: any_permit/8, Timeout: 1790, Valid
In: 192.168.2.102/4339 --> 100.100.100.254/23;tcp, If: fe-0/0/1.0, Pkts: 5, Bytes: 221
Out: 100.100.100.254/23 --> 100.100.100.102/4339;tcp, If: fe-0/0/0.0, Pkts: 5, Bytes: 25

SRX100-vpn# run show security nat static rule all
Total static-nat rules: 1

Static NAT rule: srv1 Rule-set: static_nat
Rule-Id : 1
Rule position : 1
From zone : untrust
Destination addresses : 100.100.100.102
Host addresses : 192.168.2.102
Netmask : 255.255.255.255
Host routing-instance : N/A
Translation hits : 3

アドレスを1:1でマッピング

Static NATで登録されたIPからの通信も自動的にSrc-NATされる

juniper NETWORKS

STATIC NAT 設定例

```
static {
    rule-set static_nat {
        from zone untrust;
        rule srv1 {
            match {
                destination-address 100.100.100.102/32;
            }
            then {
                static-nat prefix 192.168.2.102/32;
            }
        }
    }
}
proxy-arp {
    interface fe-0/0/0.0 {
        address {
            100.100.100.102/32;
        }
    }
}
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

PERSISTENT NAT (CONE NAT)

Persistent NATは下記のCone NATタイプに適合する

- Any remote host
  - Full cone NAT
- Target host
  - Restricted cone NAT
- Target host port
  - Port restricted cone NAT

設定はSource NATルール配下で指定する

- any-remote-host　Permit any remote host
- target-host　Permit target host
- target-host-port　Permit target host port

```
rule rule_01 {
    match {
        source-address 192.168.1.0/24;
    }
    then {
        source-nat {
            pool {
                persistent_nat;
                persistent-nat {
                    permit any-remote-host;
                    inactivity-timeout 600;
                }
            }
        }
    }
}
```

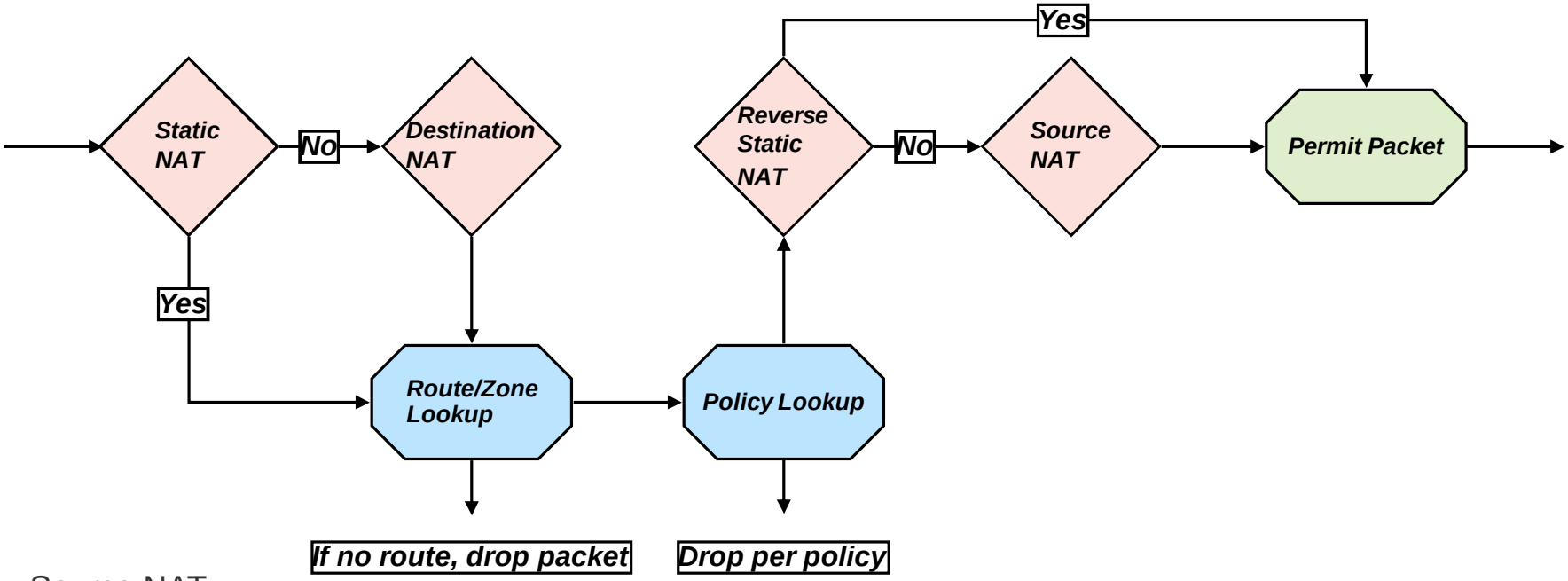
```
Session ID: 11936, Policy name: trust-to-untrust/4, Timeout: 1672, Valid
  In: 192.168.1.22/31473 --> 100.100.100.254/23;tcp, If: vlan.0, Pkts: 38, Bytes: 1568
  Out: 100.100.100.254/23 --> 100.100.100.191/27597;tcp, If: fe-0/0/0.0, Pkts: 38, Bytes: 1618

Session ID: 11941, Policy name: any_permit/9, Timeout: 6, Valid
  In: 172.27.23.20/3097 --> 100.100.100.191/27597;tcp, If: fe-0/0/0.0, Pkts: 3, Bytes: 144
  Out: 192.168.1.22/31473 --> 172.27.23.20/3097;tcp, If: vlan.0, Pkts: 0, Bytes: 0
```

マッピングされたアドレス宛の通信はInbound通信も受け入れられる

Copyright © 2010 Juniper Networks, Inc.　www.juniper.net

POLICYとNATの相互関係動作



Source NAT

- ポリシーは、プライベート送信元アドレスとパブリック送信先アドレスにマッチ
- もしくは、単純にセキュリティポリシーはNATルールセット前に評価される

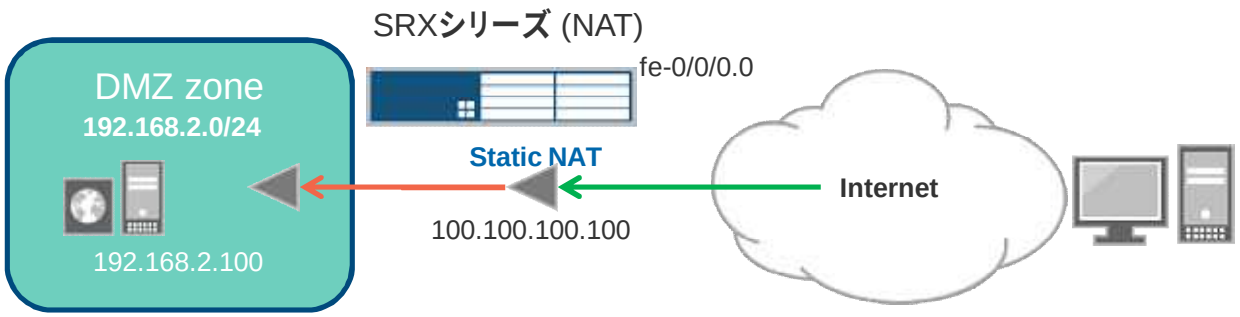
Destination NAT/Static NAT

- ポリシーは、変換された送信先アドレスとオリジナルの送信元アドレスにマッチ
- セキュリティポリシーは、Destination/Static NATルール後に評価される

従って、ポリシーは常にエンドポイントの実際のアドレスを参照することになる

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

NAT時のPOLICY動作



NAT適応時のポリシー条件について

1. Internet上のホスト(200.200.200.200)からNAT用のアドレス(100.100.100.100)に通信が行われる
2. 100.100.100.100への通信はSRXでNATされ、実際のホスト(192.168.2.100)へ変換される
3. ポリシーエンジンは実アドレスを評価するので、Src:200.200.200.200, Dst:192.168.2.100の条件にマッチ
4. 200.200.200.200から192.168.2.100への通信(到達が可能と仮定)も同じポリシー条件にマッチする
5. ポリシーエンジンはNATされたトラフィックか否かを判断し、Permit/Denyを適用できます

```
from-zone untrust to-zone DMZ {
    policy srv_permit {
        match {
            source-address any;
            destination-address 192.168.2.0/24;
            application [ junos-http junos-ftp ];
        }
        then {
            permit {
                destination-address {
                    drop-untranslated
                }
            }
        }
    }
}
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net

設定確認 (SOURCE NAT)

Source NAT

- show security nat source pool <pool-name | all>
- show security nat source rule <rule-name | all>
- show security nat source summary
- show security nat interface-nat-ports
- show security nat translation-context (*)
- show security nat incoming-nat (*)

- Note: (*) not available now

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

設定確認 (DESTINATION NAT)

Destination NAT

- show security nat destination pool <pool-name | all>
- show security nat destination rule <rule-name | all>
- show security nat destination summary

Copyright © 2010 Juniper Networks, Inc. www.juniper.net

設定確認 (STATIC NAT)

Static NAT

- show security nat static rule <rule-name | all>

Copyright © 2010 Juniper Networks, Inc.

設定確認 (PERSISTENT NAT)

Persistent NAT

- show security nat source persistent-nat-table summary
- show security nat source persistent-nat-table pool <pool-name>
- show security nat source persistent-nat-table all

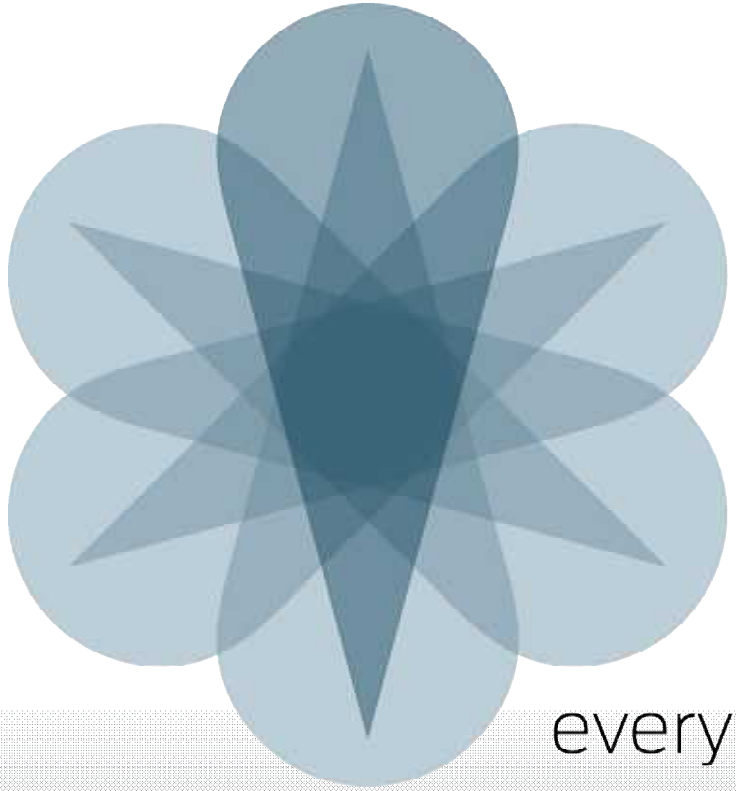
Copyright © 2010 Juniper Networks, Inc. www.juniper.net

デバック取得(TRACEOPTION設定)

```
root@SRX100-1# set security nat traceoptions flag ?
Possible completions:
  all                  Trace everything
  destination-nat-pfe  Trace destination nat events on PFE-ukernel side
  destination-nat-re   Trace destination nat events on RE side
  destination-nat-rt   Trace destination nat events on PFE-RT side
  source-nat-pfe       Trace source nat events on PFE-ukernel side
  source-nat-re        Trace source nat events on RE side
  source-nat-rt        Trace source nat events on PFE-RT side
  static-nat-pfe       Trace static nat events on PFE-ukernel side
  static-nat-re        Trace static nat events on RE side
  static-nat-rt        Trace static nat events on PFE-RT side

root@SRX100-1# set security nat traceoptions file <name>
                 [match <match>] [size <size>] [files <number>] |
                 [world-readable | no-world-readable];
```


Copyright © 2010 Juniper Networks, Inc. www.juniper.net



everywhere