Juniper SRX 日本語マニュアル

ルートベース IPsec VPN の CLI 設定

JUNIPER NETWORKS | Driven by Experience

はじめに

- ◆ 本マニュアルは、ルートベースの IPsec VPN の CLI 設定について説明します
- ◆ 手順内容は SRX300 、Junos 21.2R3-S2 にて確認を実施しております
- ◆ 実際の設定内容やパラメータは導入する環境や構成によって異なります

  各種設定内容の詳細は下記リンクよりご確認ください

  https://www.juniper.net/documentation/

- ◆ 他にも多数の SRX 日本語マニュアルを「ソリューション＆テクニカル情報サイト」に掲載しております

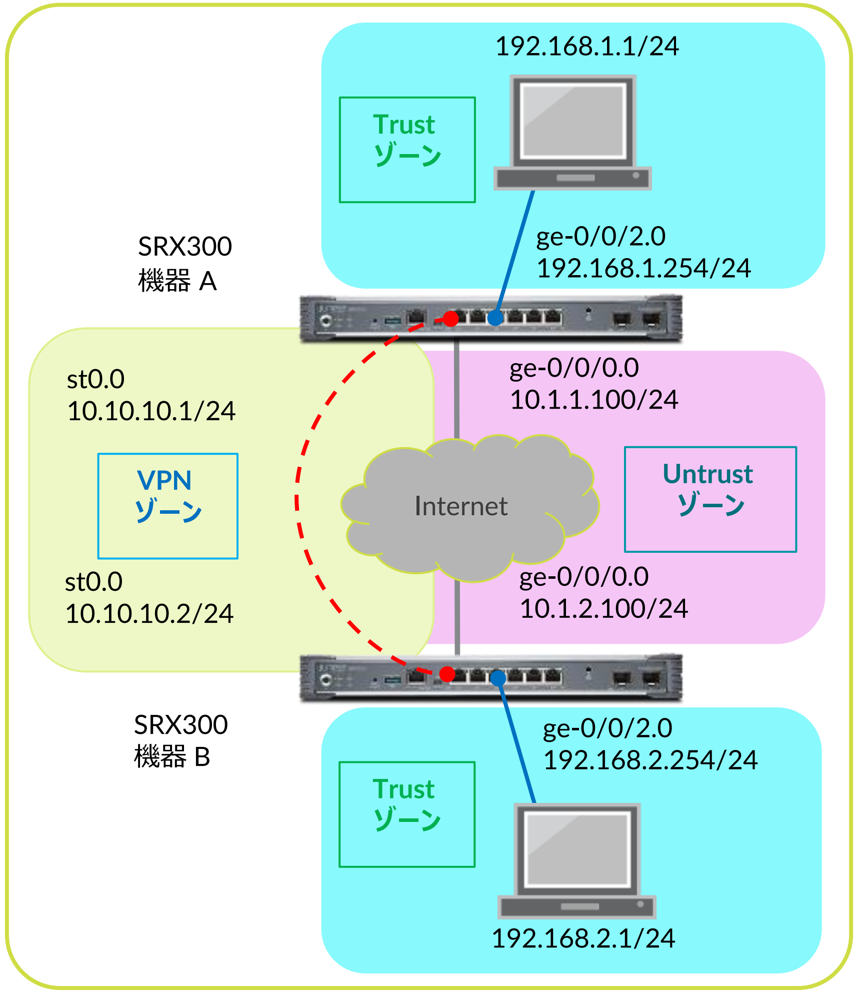
  https://www.juniper.net/jp/ja/local/solution-technical-information/security.html

2022 年 8 月

ルートベース IPsec VPN

構成概要

- 2 つの SRX300 機器間(機器 A 、機器 B)でルートベースの IPsec VPN を設定
- トンネル用の仮想インタフェース st0.0 を双方の機器に設定しセキュリティゾーン VPN に割り当てる
- Trust ゾーン / VPN ゾーン間のセキュリティポリシーを設定し通信を制御



ルートベース IPsec VPN

- 設定初期化、 root パスワードの設定、ホスト名を設定します

```
※機器 A 、機器 B それぞれの configuration モードにて実行
user@srx# delete
This will delete the entire configuration
Delete everything under this level? [yes,no] (no) yes

user@srx# set system root-authentication plain-text-password
New password: Juniper123
Retype new password: Juniper123

※機器 A にて設定
user@srx# set system  host-name SRX300-A

※機器 B にて設定
user@srx# set system  host-name SRX300-B

※機器 A 、機器 B それぞれに実行
user@srx# commit
commit completed
```

ルートベース IPsec VPN

- インタフェースを設定します

```
※機器 A にて設定
root@SRX300-A# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.100/24
root@SRX300-A# set interfaces ge-0/0/2 unit 0 family inet address 192.168.1.254/24
root@SRX300-A# set interfaces st0 unit 0 family inet address 10.10.10.1/24

※機器 B にて設定
root@SRX300-B# set interfaces ge-0/0/0 unit 0 family inet address 10.1.2.100/24
root@SRX300-B# set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.254/24
root@SRX300-B# set interfaces st0 unit 0 family inet address 10.10.10.2/24
```

- デフォルトルートを設定します
  ※構成例では 10.1.1.254 と 10.1.2.254 を Internet 側のデフォルトゲートウェイと想定

```
※機器 A にて設定
root@SRX300-A# set routing-options static route 0.0.0.0/0 next-hop 10.1.1.254

※機器 B にて設定
root@SRX300-B# set routing-options static route 0.0.0.0/0 next-hop 10.1.2.254
```

ルートベース IPsec VPN

- セキュリティゾーンを設定します

```
※機器 A にて設定
root@SRX300-A# set security zones security-zone Trust interfaces ge-0/0/2.0
root@SRX300-A# set security zones security-zone Trust address-book address 192.168.1.0 192.168.1.0/24
root@SRX300-A# set security zones security-zone VPN interfaces st0.0
root@SRX300-A# set security zones security-zone VPN address-book address 192.168.2.0 192.168.2.0/24
root@SRX300-A# set security zones security-zone Untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services ike

※機器 B にて設定
root@SRX300-B# set security zones security-zone Trust interfaces ge-0/0/2.0
root@SRX300-B# set security zones security-zone Trust address-book address 192.168.2.0 192.168.2.0/24
root@SRX300-B# set security zones security-zone VPN interfaces st0.0
root@SRX300-B# set security zones security-zone VPN address-book address 192.168.1.0 192.168.1.0/24
root@SRX300-B# set security zones security-zone Untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services ike
```

ルートベース IPsec VPN

- セキュリティポリシーを設定します

```
※機器 A にて設定
root@SRX300-A# set security policies from-zone Trust to-zone VPN policy TtoV match source-address 192.168.1.0
root@SRX300-A# set security policies from-zone Trust to-zone VPN policy TtoV match destination-address 192.168.2.0
root@SRX300-A# set security policies from-zone Trust to-zone VPN policy TtoV match application any
root@SRX300-A# set security policies from-zone Trust to-zone VPN policy TtoV then permit
root@SRX300-A# set security policies from-zone VPN to-zone Trust policy VtoT match source-address 192.168.2.0
root@SRX300-A# set security policies from-zone VPN to-zone Trust policy VtoT match destination-address 192.168.1.0
root@SRX300-A# set security policies from-zone VPN to-zone Trust policy VtoT match application any
root@SRX300-A# set security policies from-zone VPN to-zone Trust policy VtoT then permit

※機器 B にて設定
root@SRX300-B# set security policies from-zone Trust to-zone VPN policy TtoV match source-address 192.168.2.0
root@SRX300-B# set security policies from-zone Trust to-zone VPN policy TtoV match destination-address 192.168.1.0
root@SRX300-B# set security policies from-zone Trust to-zone VPN policy TtoV match application any
root@SRX300-B# set security policies from-zone Trust to-zone VPN policy TtoV then permit
root@SRX300-B# set security policies from-zone VPN to-zone Trust policy VtoT match source-address 192.168.1.0
root@SRX300-B# set security policies from-zone VPN to-zone Trust policy VtoT match destination-address 192.168.2.0
root@SRX300-B# set security policies from-zone VPN to-zone Trust policy VtoT match application any
root@SRX300-B# set security policies from-zone VPN to-zone Trust policy VtoT then permit
```

ルートベース IPsec VPN

- IKE（ Phase1 接続 プロファイル・ポリシー・ゲートウェイ)を設定します

```
※機器 A にて設定
root@SRX300-A# set security ike proposal P1 authentication-method pre-shared-keys
root@SRX300-A# set security ike proposal P1 dh-group group2
root@SRX300-A# set security ike proposal P1 authentication-algorithm sha1
root@SRX300-A# set security ike proposal P1 encryption-algorithm aes-128-cbc
root@SRX300-A# set security ike policy IKE-Policy mode main
root@SRX300-A# set security ike policy IKE-Policy proposals P1
root@SRX300-A# set security ike policy IKE-Policy pre-shared-key ascii-text “Junos123”
root@SRX300-A# set security ike gateway Gateway-A external-interface ge-0/0/0.0
root@SRX300-A# set security ike gateway Gateway-A ike-policy IKE-Policy
root@SRX300-A# set security ike gateway Gateway-A address 10.1.2.100

※機器 B にて設定
root@SRX300-B# set security ike proposal P1 authentication-method pre-shared-keys
root@SRX300-B# set security ike proposal P1 dh-group group2
root@SRX300-B# set security ike proposal P1 authentication-algorithm sha1
root@SRX300-B# set security ike proposal P1 encryption-algorithm aes-128-cbc
root@SRX300-B# set security ike policy IKE-Policy mode main
root@SRX300-B# set security ike policy IKE-Policy proposals P1
root@SRX300-B# set security ike policy IKE-Policy pre-shared-key ascii-text “Junos123”
root@SRX300-B# set security ike gateway Gateway-B external-interface ge-0/0/0.0
root@SRX300-B# set security ike gateway Gateway-B ike-policy IKE-Policy
root@SRX300-B# set security ike gateway Gateway-B address 10.1.1.100
```

ルートベース IPsec VPN

- IPsec（ Phase2 接続 プロポーサル・ポリシー・ VPN)を設定します

```
※機器 A にて設定
root@SRX300-A# set security ipsec proposal P2 protocol esp
root@SRX300-A# set security ipsec proposal P2 authentication-algorithm hmac-sha1-96
root@SRX300-A# set security ipsec proposal P2 encryption-algorithm aes-128-cbc
root@SRX300-A# set security ipsec policy IPsec-Policy proposals P2
root@SRX300-A# set security ipsec policy IPsec-Policy perfect-forward-secrecy keys group2
root@SRX300-A# set security ipsec vpn VPN-A ike gateway Gateway-A
root@SRX300-A# set security ipsec vpn VPN-A ike ipsec-policy IPsec-Policy
root@SRX300-A# set security ipsec vpn VPN-A bind-interface st0.0

※機器 B にて設定
root@SRX300-B# set security ipsec proposal P2 protocol esp
root@SRX300-B# set security ipsec proposal P2 authentication-algorithm hmac-sha1-96
root@SRX300-B# set security ipsec proposal P2 encryption-algorithm aes-128-cbc
root@SRX300-B# set security ipsec policy IPsec-Policy proposals P2
root@SRX300-B# set security ipsec policy IPsec-Policy perfect-forward-secrecy keys group2
root@SRX300-B# set security ipsec vpn VPN-B ike gateway Gateway-B
root@SRX300-B# set security ipsec vpn VPN-B ike ipsec-policy IPsec-Policy
root@SRX300-B# set security ipsec vpn VPN-B bind-interface st0.0
```

ルートベース IPsec VPN

- ルーティングを設定します

```
※機器 A にて設定
root@SRX300-A# set routing-options static route 192.168.2.0/24 next-hop st0.0

※機器 B にて設定
root@SRX300-B# set routing-options static route 192.168.1.0/24 next-hop st0.0
```

- TCP MSS 設定を調整します
  ※利用環境に合わせて調整する必要あり

```
※機器 A 、機器 B にて設定
root@SRX300# set security flow tcp-mss ipsec-vpn mss 1350
```

ルートベース IPsec VPN

設定の確認 1 (security ike)

```
※機器 A
[edit]
root@SRX300-A# show security ike
proposal P1 {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy IKE-Policy {
    mode main;
    proposals P1;
    pre-shared-key ascii-text
"$9$4GJUiP5FApB5QhreK8LGDjq5Q"; ## SECRET-DATA
}
gateway Gateway-A {
    ike-policy IKE-Policy;
    address 10.1.2.100;
    external-interface ge-0/0/0.0;
}
```

```
※機器 B
[edit]
root@SRX300-B# show security ike
proposal P1 {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy IKE-Policy {
    mode main;
    proposals P1;
    pre-shared-key ascii-text "$9$wE2oZHqfn/tqmBEcSeK4aJDqm";
## SECRET-DATA
}
gateway Gateway-B {
    ike-policy IKE-Policy;
    address 10.1.1.100;
    external-interface ge-0/0/0.0;
}
```

ルートベース IPsec VPN

設定の確認 2 (security ipsec)

```
※機器 A
[edit]
root@SRX300-A# show security ipsec
proposal P2 {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
}
policy IPsec-Policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals P2;
}
vpn VPN-A {
    bind-interface st0.0;
    ike {
        gateway Gateway-A;
        ipsec-policy IPsec-Policy;
    }
}
```

```
※機器 B
[edit]
root@SRX300-B# show security ipsec
proposal P2 {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
}
policy IPsec-Policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals P2;
}
vpn VPN-B {
    bind-interface st0.0;
    ike {
        gateway Gateway-B;
        ipsec-policy IPsec-Policy;
    }
}
```

ルートベース IPsec VPN

設定の確認 3 (security flow)

※機器 A

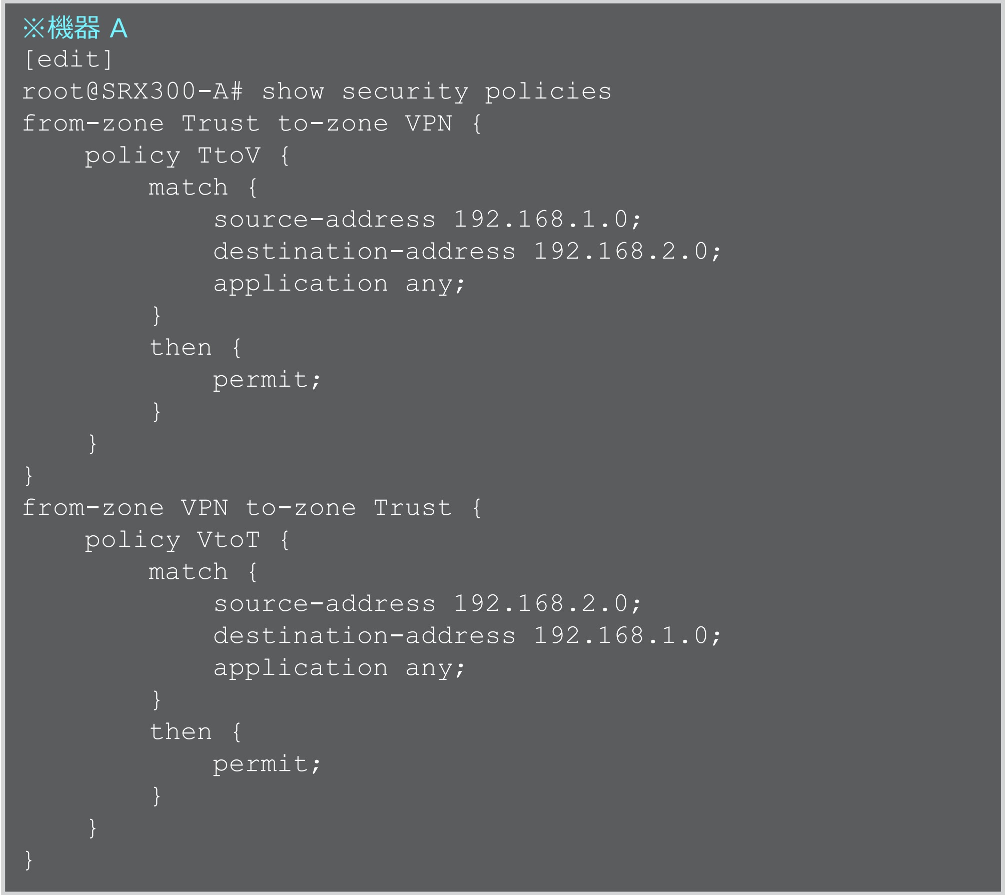
```
[edit]
root@SRX300-A# show security flow
tcp-mss {
    ipsec-vpn {
        mss 1350;
    }
}
```

※機器 B

```
[edit]
root@SRX300-B# show security flow
tcp-mss {
    ipsec-vpn {
        mss 1350;
    }
}
```

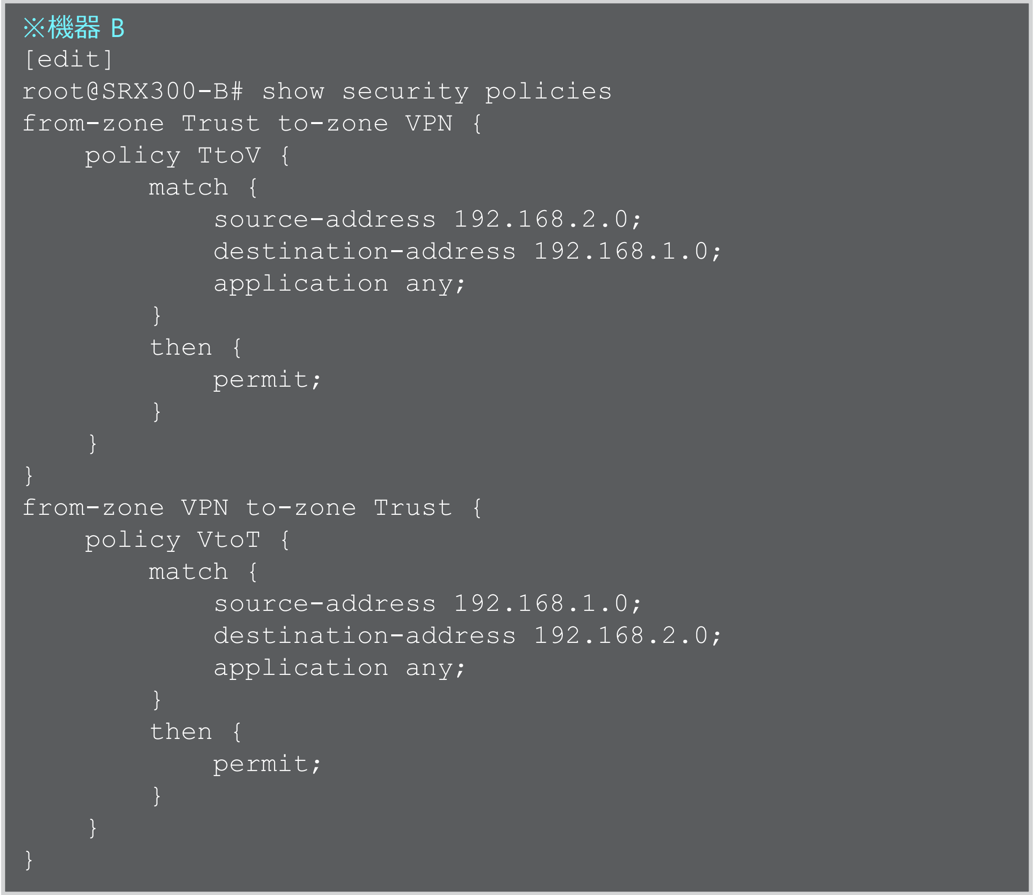
ルートベース IPsec VPN

設定の確認 4 (security policies)



※機器 A

```
[edit]
root@SRX300-A# show security policies
from-zone Trust to-zone VPN {
    policy TtoV {
        match {
            source-address 192.168.1.0;
            destination-address 192.168.2.0;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone VPN to-zone Trust {
    policy VtoT {
        match {
            source-address 192.168.2.0;
            destination-address 192.168.1.0;
            application any;
        }
        then {
            permit;
        }
    }
}
```



※機器 B

```
[edit]
root@SRX300-B# show security policies
from-zone Trust to-zone VPN {
    policy TtoV {
        match {
            source-address 192.168.2.0;
            destination-address 192.168.1.0;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone VPN to-zone Trust {
    policy VtoT {
        match {
            source-address 192.168.1.0;
            destination-address 192.168.2.0;
            application any;
        }
        then {
            permit;
        }
    }
}
```

ルートベース IPsec VPN

設定の確認 5 (security zones)

※機器 A

```
[edit]
root@SRX300-A# show security zones
security-zone Trust {
    address-book {
        address 192.168.1.0 192.168.1.0/24;
    }
    interfaces {
        ge-0/0/2.0;
    }
}
security-zone VPN {
    address-book {
        address 192.168.2.0 192.168.2.0/24;
    }
    interfaces {
        st0.0;
    }
}
security-zone Untrust {
    interfaces {
        ge-0/0/0.0 {
            host-inbound-traffic {
                system-services {
                    ike;
                }
            }
        }
    }
```

※機器 B

```
[edit]
root@SRX300-B# show security zones
security-zone Trust {
    address-book {
        address 192.168.2.0 192.168.2.0/24;
    }
    interfaces {
        ge-0/0/2.0;
    }
}
security-zone VPN {
    address-book {
        address 192.168.1.0 192.168.1.0/24;
    }
    interfaces {
        st0.0;
    }
}
security-zone Untrust {
    interfaces {
        ge-0/0/0.0 {
            host-inbound-traffic {
                system-services {
                    ike;
                }
            }
        }
    }
```

ルートベース IPsec VPN

設定の確認 6 (interfaces)

※機器 A

```
[edit]
root@SRX300-A# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.1.1.100/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 192.168.1.254/24;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.10.10.1/24;
        }
    }
}
```

※機器 B

```
[edit]
root@SRX300-B# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.1.2.100/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 192.168.2.254/24;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.10.10.2/24;
        }
    }
}
```

ルートベース IPsec VPN

設定の確認 7 (routing-options)

```
※機器 A
[edit]
root@SRX300-A# show routing-options
static {
    route 0.0.0.0/0 next-hop 10.1.1.254;
    route 192.168.2.0/24 next-hop st0.0;
}
```

```
※機器 B
[edit]
root@SRX300-B# show routing-options
static {
    route 0.0.0.0/0 next-hop 10.1.2.254;
    route 192.168.1.0/24 next-hop st0.0;
}
```

ルートベース IPsec VPN

動作の確認

```
※機器 A
root@SRX300-A> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
3899019 UP     a902482689ddf832  981e51f94d2ebac5  Main           10.1.2.100

root@SRX300-A> show security ipsec security-associations
  Total active tunnels: 1     Total Ipsec sas: 1
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <131073 ESP:aes-cbc-128/sha1 4dffda97 3564/ unlim - root 500 10.1.2.100
  >131073 ESP:aes-cbc-128/sha1 72a3b19f 3564/ unlim - root 500 10.1.2.100
```

```
※機器 B
root@SRX300-B> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
5550467 UP     a902482689ddf832  981e51f94d2ebac5  Main           10.1.1.100

root@SRX300-B> show security ipsec security-associations
  Total active tunnels: 1     Total Ipsec sas: 1
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <131073 ESP:aes-cbc-128/sha1 72a3b19f 3581/ unlim - root 500 10.1.1.100
  >131073 ESP:aes-cbc-128/sha1 4dffda97 3581/ unlim - root 500 10.1.1.100
```

Thank you

JUNIPER NETWORKS | Driven by Experience™