Juniper SRX 日本語マニュアル

4. ルートベース IPsec VPN の CLI 設定

Juniper NETWORKS | Engineering Simplicity

はじめに

ルートベースの IPsec VPN の CLI 設定について説明します。

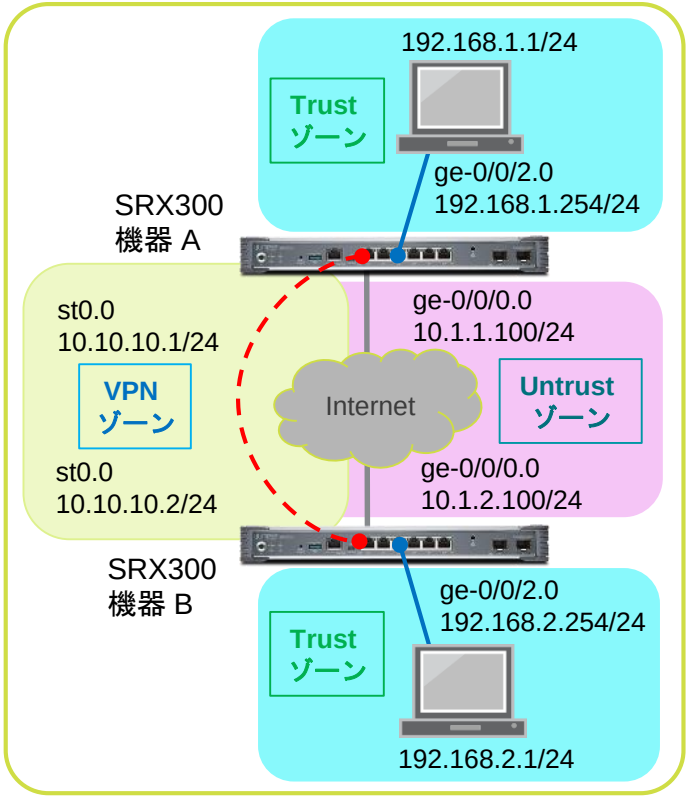
※手順内容は「SRX300」、Junos OS「15.1X49-D140」にて確認を実施しております。

2018年8月

ルートベース IPsec VPN

構成概要

- 二つの 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

① 設定初期化、root パスワードの設定、ホスト名設定

```
※機器 A、機器 B にて設定
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

② インタフェース設定

```
※機器 A の設定
user@srx# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.100/24
user@srx# set interfaces ge-0/0/2 unit 0 family inet address 192.168.1.254/24
user@srx# set interfaces st0 unit 0 family inet address 10.10.10.1/24

※機器 B の設定
user@srx# set interfaces ge-0/0/0 unit 0 family inet address 10.1.2.100/24
user@srx# set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.254/24
user@srx# set interfaces st0 unit 0 family inet address 10.10.10.2/24
```

③ デフォルトルート設定

※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 の設定
user@srx# set routing-options static route 0.0.0.0/0 next-hop 10.1.1.254

※機器 B の設定
user@srx# set routing-options static route 0.0.0.0/0 next-hop 10.1.2.254
```

ルートベース IPsec VPN

④　セキュリティゾーン設定

※機器 A の設定

```
user@srx# set security zones security-zone Trust interface ge-0/0/2.0
user@srx# set security zones security-zone Trust address-book address 192.168.1.0 192.168.1.0/24
user@srx# set security zones security-zone VPN interface st0.0
user@srx# set security zones security-zone VPN address-book address 192.168.2.0 192.168.2.0/24
user@srx# set security zones security-zone Untrust interface ge-0/0/0.0 host-inbound-traffic system-services ike
```

※機器 B の設定

```
user@srx# set security zones security-zone Trust interface ge-0/0/2.0
user@srx# set security zones security-zone Trust address-book address 192.168.2.0 192.168.2.0/24
user@srx# set security zones security-zone VPN interface st0.0
user@srx# set security zones security-zone VPN address-book address 192.168.1.0 192.168.1.0/24
user@srx# set security zones security-zone Untrust interface ge-0/0/0.0 host-inbound-traffic system-services ike
```

ルートベース IPsec VPN

⑤　セキュリティポリシー設定

※機器 A の設定

```
user@srx# set security policies from-zone Trust to-zone VPN policy TtoV match source-address 192.168.1.0
user@srx# set security policies from-zone Trust to-zone VPN policy TtoV match destination-address 192.168.2.0
user@srx# set security policies from-zone Trust to-zone VPN policy TtoV match application any
user@srx# set security policies from-zone Trust to-zone VPN policy TtoV then permit
user@srx# set security policies from-zone VPN to-zone Trust policy VtoT match source-address 192.168.2.0
user@srx# set security policies from-zone VPN to-zone Trust policy VtoT match destination-address 192.168.1.0
user@srx# set security policies from-zone VPN to-zone Trust policy VtoT match application any
user@srx# set security policies from-zone VPN to-zone Trust policy VtoT then permit
```

※機器 B の設定

```
user@srx# set security policies from-zone Trust to-zone VPN policy TtoV match source-address 192.168.2.0
user@srx# set security policies from-zone Trust to-zone VPN policy TtoV match destination-address 192.168.1.0
user@srx# set security policies from-zone Trust to-zone VPN policy TtoV match application any
user@srx# set security policies from-zone Trust to-zone VPN policy TtoV then permit
user@srx# set security policies from-zone VPN to-zone Trust policy VtoT match source-address 192.168.1.0
user@srx# set security policies from-zone VPN to-zone Trust policy VtoT match destination-address 192.168.2.0
user@srx# set security policies from-zone VPN to-zone Trust policy VtoT match application any
user@srx# set security policies from-zone VPN to-zone Trust policy VtoT then permit
```

ルートベース IPsec VPN

⑥ IKE（Phase1接続 プロファイル・ポリシー・ゲートウェイ）設定

※機器 A の設定

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

※機器 B の設定

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

ルートベース IPsec VPN

⑦　IPsec（Phase2接続 プロポーサル・ポリシー・VPN）設定

※機器 A の設定

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

※機器 B の設定

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

ルートベース IPsec VPN

⑧　ルーティング設定

```
※機器 A の設定
user@srx# set routing-options static route 192.168.2.0/24 next-hop st0.0

※機器 B の設定
user@srx# set routing-options static route 192.168.1.0/24 next-hop st0.0
```

⑨　TCP MSS 設定調整

※利用の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
user@srx# set security flow tcp-mss ipsec-vpn mss 1350
```

ルートベース IPsec VPN

設定の確認①

※機器 A

```
[edit]
root@srx# 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
"$9$qPTFCtOcyKtuLNdVY25Qz6tu"; ## 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@srx# 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
"$9$bRY4JikP36Ak.ORhclegoaUk."; ## 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

※機器 A

```
[edit]
root@srx# 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@srx# 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

※機器 A

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

[edit]
root@srx# 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;
        }
    }
```

※機器 B

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

[edit]
root@srx# 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;
        }
    }
```

ルートベース IPsec VPN

設定の確認④

※機器 A

```
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

```
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

※機器 A

```
[edit]
root@srx# 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;
    }
}
```

※※機器 B

```
[edit]
root@srx# 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;
    }
}
```

ルートベース IPsec VPN

設定の確認⑥

※機器 A

```
security-zone Untrust {
    interfaces {
        ge-0/0/0.0 {
            host-inbound-traffic {
                system-services {
                    ike;
                }
            }
        }
    }
}

[edit]
root@srx# 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

```
security-zone Untrust {
    interfaces {
        ge-0/0/0.0 {
            host-inbound-traffic {
                system-services {
                    ike;
                }
            }
        }
    }
}

[edit]
root@srx# 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

設定の確認⑦

※機器 A

```
[edit]
root@srx# 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@srx# 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;
        }
```