Juniper SRX 日本語マニュアル

Hub-and-Spoke VPN の CLI 設定

JUNIPER NETWORKS | Driven by Experience

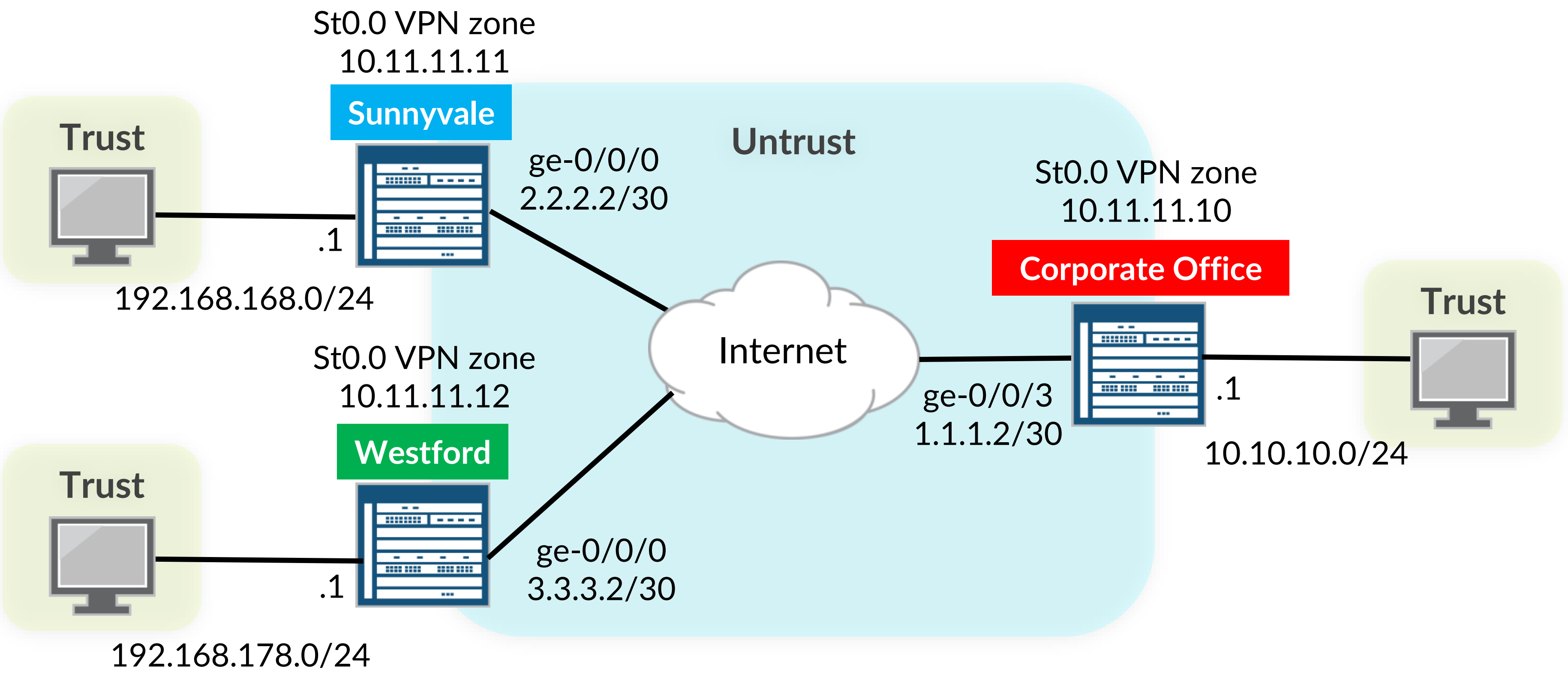
はじめに

- ◆ 本マニュアルは、Hub-and-Spoke 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

Hub-and-Spoke VPN

構成概要



Hub-and-Spoke VPN (Corporate office)

1. インタフェースを設定します

```
user@SRX-Corporate# set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/24
user@SRX-Corporate# set interfaces ge-0/0/3 unit 0 family inet address 1.1.1.2/30
user@SRX-Corporate# set interfaces st0 unit 0 family inet address 10.11.11.10/24
```

2. インタフェースをセキュリティゾーンにバインドします

```
user@SRX-Corporate# set security zones security-zone untrust interfaces ge-0/0/3.0
user@SRX-Corporate# set security zones security-zone untrust host-inbound-traffic system-services ike
user@SRX-Corporate# set security zones security-zone trust interfaces ge-0/0/0.0
user@SRX-Corporate# set security zones security-zone trust host-inbound-traffic system-services all
user@SRX-Corporate# set security zones security-zone vpn interfaces st0.0
```

3. ルーティングを設定します

```
user@SRX-Corporate# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
user@SRX-Corporate# set routing-options static route 192.168.168.0/24 next-hop 10.11.11.11
user@SRX-Corporate# set routing-options static route 192.168.178.0/24 next-hop 10.11.11.12
```

4. アドレスブックを設定します

```
user@SRX-Corporate# set security address-book book1 address local-net 10.10.10.0/24
user@SRX-Corporate# set security address-book book1 attach zone trust
user@SRX-Corporate# set security address-book book2 address sunnyvale-net 192.168.168.0/24
user@SRX-Corporate# set security address-book book2 address westford-net 192.168.178.0/24
user@SRX-Corporate# set security address-book book2 attach zone vpn
```

Hub-and-Spoke VPN (Corporate office)

5. 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

```
user@SRX-Corporate# set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
user@SRX-Corporate# set security ike proposal ike-phase1-proposal dh-group group2
user@SRX-Corporate# set security ike proposal ike-phase1-proposal authentication-algorithm sha1
user@SRX-Corporate# set security ike proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
user@SRX-Corporate# set security ike policy ike-phase1-policy mode main
user@SRX-Corporate# set security ike policy ike-phase1-policy proposals ike-phase1-proposal
user@SRX-Corporate# set security ike policy ike-phase1-policy pre-shared-key ascii-text “$ABC123”
user@SRX-Corporate# set security ike gateway gw-westford external-interface ge-0/0/3.0
user@SRX-Corporate# set security ike gateway gw-westford ike-policy ike-phase1-policy
user@SRX-Corporate# set security ike gateway gw-westford address 3.3.3.2
user@SRX-Corporate# set security ike gateway gw-sunnyvale external-interface ge-0/0/3.0
user@SRX-Corporate# set security ike gateway gw-sunnyvale ike-policy ike-phase1-policy
user@SRX-Corporate# set security ike gateway gw-sunnyvale address 2.2.2.2
```

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

```
user@SRX-Corporate# set security ipsec proposal ipsec-phase2-proposal protocol esp
user@SRX-Corporate# set security ipsec proposal ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
user@SRX-Corporate# set security ipsec proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
user@SRX-Corporate# set security ipsec policy ipsec-phase2-policy proposals ipsec-phase2-proposal
user@SRX-Corporate# set security ipsec policy ipsec-phase2-policy perfect-forward-secrecy keys group2
user@SRX-Corporate# set security ipsec vpn vpn-westford ike gateway gw-westford
user@SRX-Corporate# set security ipsec vpn vpn-westford ike ipsec-policy ipsec-phase2-policy
user@SRX-Corporate# set security ipsec vpn vpn-westford bind-interface st0.0
user@SRX-Corporate# set security ipsec vpn vpn-sunnyvale ike gateway gw-sunnyvale
user@SRX-Corporate# set security ipsec vpn vpn-sunnyvale ike ipsec-policy ipsec-phase2-policy
user@SRX-Corporate# set security ipsec vpn vpn-sunnyvale bind-interface st0.0
user@SRX-Corporate# set interfaces st0 unit 0 multipoint
user@SRX-Corporate# set interfaces st0 unit 0 family inet next-hop-tunnel 10.11.11.11 ipsec-vpn vpn-sunnyvale
user@SRX-Corporate# set interfaces st0 unit 0 family inet next-hop-tunnel 10.11.11.12 ipsec-vpn vpn-westford
```

Hub-and-Spoke VPN (Corporate office)

7. 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

```
user@SRX-Corporate# set security flow tcp-mss ipsec-vpn mss 1350
```

8. セキュリティポリシーを設定します

```
user@SRX-Corporate# set security policies from-zone trust to-zone vpn policy local-to-spokes match source-address local-net
user@SRX-Corporate# set security policies from-zone trust to-zone vpn policy local-to-spokes match destination-address sunnyvale-net
user@SRX-Corporate# set security policies from-zone trust to-zone vpn policy local-to-spokes match destination-address westford-net
user@SRX-Corporate# set security policies from-zone trust to-zone vpn policy local-to-spokes match application any
user@SRX-Corporate# set security policies from-zone trust to-zone vpn policy local-to-spokes then permit
user@SRX-Corporate# set security policies from-zone vpn to-zone trust policy spokes-to-local match source-address sunnyvale-net
user@SRX-Corporate# set security policies from-zone vpn to-zone trust policy spokes-to-local match source-address westford-net
user@SRX-Corporate# set security policies from-zone vpn to-zone trust policy spokes-to-local match destination-address local-net
user@SRX-Corporate# set security policies from-zone vpn to-zone trust policy spokes-to-local match application any
user@SRX-Corporate# set security policies from-zone vpn to-zone trust policy spokes-to-local then permit
user@SRX-Corporate# set security policies from-zone vpn to-zone vpn policy spoke-to-spoke match source-address any
user@SRX-Corporate# set security policies from-zone vpn to-zone vpn policy spoke-to-spoke match destination-address any
user@SRX-Corporate# set security policies from-zone vpn to-zone vpn policy spoke-to-spoke match application any
user@SRX-Corporate# set security policies from-zone vpn to-zone vpn policy spoke-to-spoke then permit
```

Hub-and-Spoke VPN (Westford)

1. インタフェースを設定します

```
user@SRX-Westford# set interfaces ge-0/0/0 unit 0 family inet address 3.3.3.2/30
user@SRX-Westford# set interfaces ge-0/0/3 unit 0 family inet address 192.168.178.1/24
user@SRX-Westford# set interfaces st0 unit 0 family inet address 10.11.11.12/24
```

2. インタフェースをセキュリティゾーンにバインドします

```
user@SRX-Westford# set security zones security-zone untrust interfaces ge-0/0/0.0
user@SRX-Westford# set security zones security-zone untrust host-inbound-traffic system-services ike
user@SRX-Westford# set security zones security-zone trust interfaces ge-0/0/3.0
user@SRX-Westford# set security zones security-zone trust host-inbound-traffic system-services all
user@SRX-Westford# set security zones security-zone vpn interfaces st0.0
```

3. ルーティングを設定します

```
user@SRX-Westford# set routing-options static route 0.0.0.0/0 next-hop 3.3.3.1
user@SRX-Westford# set routing-options static route 10.10.10.0/24 next-hop 10.11.11.10
user@SRX-Westford# set routing-options static route 192.168.168.0/24 next-hop 10.11.11.10
```

4. アドレスブックを設定します

```
user@SRX-Westford# set security address-book book1 address local-net 192.168.178.0/24
user@SRX-Westford# set security address-book book1 attach zone trust
user@SRX-Westford# set security address-book book2 address corp-net 10.10.10.0/24
user@SRX-Westford# set security address-book book2 address sunnyvale-net 192.168.168.0/24
user@SRX-Westford# set security address-book book2 attach zone vpn
```

Hub-and-Spoke VPN (Westford)

5. 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

```
user@SRX-Westford# set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
user@SRX-Westford# set security ike proposal ike-phase1-proposal dh-group group2
user@SRX-Westford# set security ike proposal ike-phase1-proposal authentication-algorithm sha1
user@SRX-Westford# set security ike proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
user@SRX-Westford# set security ike policy ike-phase1-policy mode main
user@SRX-Westford# set security ike policy ike-phase1-policy proposals ike-phase1-proposal
user@SRX-Westford# set security ike policy ike-phase1-policy pre-shared-key ascii-text “$ABC123”
user@SRX-Westford# set security ike gateway gw-corporate external-interface ge-0/0/0.0
user@SRX-Westford# set security ike gateway gw-corporate ike-policy ike-phase1-policy
user@SRX-Westford# set security ike gateway gw-corporate address 1.1.1.2
```

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

```
user@SRX-Westford# set security ipsec proposal ipsec-phase2-proposal protocol esp
user@SRX-Westford# set security ipsec proposal ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
user@SRX-Westford# set security ipsec proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
user@SRX-Westford# set security ipsec policy ipsec-phase2-policy proposals ipsec-phase2-proposal
user@SRX-Westford# set security ipsec policy ipsec-phase2-policy perfect-forward-secrecy keys group2
user@SRX-Westford# set security ipsec vpn vpn-corporate ike gateway gw-corporate
user@SRX-Westford# set security ipsec vpn vpn-corporate ike ipsec-policy ipsec-phase2-policy
user@SRX-Westford# set security ipsec vpn vpn-corporate bind-interface st0.0
```

Hub-and-Spoke VPN (Westford)

7. TCP MSS 設定を調整します

```
user@SRX-Westford# set security flow tcp-mss ipsec-vpn mss 1350
```

8. セキュリティポリシーを設定します

```
user@SRX-Westford# set security policies from-zone trust to-zone vpn policy to-corporate match source-address local-net
user@SRX-Westford# set security policies from-zone trust to-zone vpn policy to-corporate match destination-address corp-net
user@SRX-Westford# set security policies from-zone trust to-zone vpn policy to-corporate match destination-address sunnyvale-net
user@SRX-Westford# set security policies from-zone trust to-zone vpn policy to-corporate match application any
user@SRX-Westford# set security policies from-zone trust to-zone vpn policy to-corporate then permit
user@SRX-Westford# set security policies from-zone vpn to-zone trust policy from-corporate match source-address corp-net
user@SRX-Westford# set security policies from-zone vpn to-zone trust policy from-corporate match source-address sunnyvale-net
user@SRX-Westford# set security policies from-zone vpn to-zone trust policy from-corporate match destination-address local-net
user@SRX-Westford# set security policies from-zone vpn to-zone trust policy from-corporate match application any
user@SRX-Westford# set security policies from-zone vpn to-zone trust policy from-corporate then permit
```

Hub-and-Spoke VPN (Sunnyvale)

1. インタフェースを設定します

```
user@SRX-Sunnyvale# set interfaces ge-0/0/0 unit 0 family inet address 2.2.2.2/30
user@SRX-Sunnyvale# set interfaces ge-0/0/3 unit 0 family inet address 192.168.168.1/24
user@SRX-Sunnyvale# set interfaces st0 unit 0 family inet address 10.11.11.11/24
```

2. インタフェースをセキュリティゾーンにバインドします

```
user@SRX-Sunnyvale# set security zones security-zone untrust interfaces ge-0/0/0.0
user@SRX-Sunnyvale# set security zones security-zone untrust host-inbound-traffic system-services ike
user@SRX-Sunnyvale# set security zones security-zone trust interfaces ge-0/0/3.0
user@SRX-Sunnyvale# set security zones security-zone trust host-inbound-traffic system-services all
user@SRX-Sunnyvale# set security zones security-zone vpn interfaces st0.0
```

3. ルーティングを設定します

```
user@SRX-Sunnyvale# set routing-options static route 0.0.0.0/0 next-hop 2.2.2.1
user@SRX-Sunnyvale# set routing-options static route 10.10.10.0/24 next-hop 10.11.11.10
user@SRX-Sunnyvale# set routing-options static route 192.168.178.0/24 next-hop 10.11.11.10
```

4. アドレスブックを設定します

```
user@SRX-Sunnyvale# set security address-book book1 address local-net 192.168.168.0/24
user@SRX-Sunnyvale# set security address-book book1 attach zone trust
user@SRX-Sunnyvale# set security address-book book2 address corp-net 10.10.10.0/24
user@SRX-Sunnyvale# set security address-book book2 address westford-net 192.168.178.0/24
user@SRX-Sunnyvale# set security address-book book2 attach zone vpn
```

Hub-and-Spoke VPN (Sunnyvale)

5. 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

```
user@SRX-Sunnyvale# set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
user@SRX-Sunnyvale# set security ike proposal ike-phase1-proposal dh-group group2
user@SRX-Sunnyvale# set security ike proposal ike-phase1-proposal authentication-algorithm sha1
user@SRX-Sunnyvale# set security ike proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
user@SRX-Sunnyvale# set security ike policy ike-phase1-policy mode main
user@SRX-Sunnyvale# set security ike policy ike-phase1-policy proposals ike-phase1-proposal
user@SRX-Sunnyvale# set security ike policy ike-phase1-policy pre-shared-key ascii-text “$ABC123”
user@SRX-Sunnyvale# set security ike gateway gw-corporate external-interface ge-0/0/0.0
user@SRX-Sunnyvale# set security ike gateway gw-corporate ike-policy ike-phase1-policy
user@SRX-Sunnyvale# set security ike gateway gw-corporate address 1.1.1.2
```

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

```
user@SRX-Sunnyvale# set security ipsec proposal ipsec-phase2-proposal protocol esp
user@SRX-Sunnyvale# set security ipsec proposal ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
user@SRX-Sunnyvale# set security ipsec proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
user@SRX-Sunnyvale# set security ipsec policy ipsec-phase2-policy proposals ipsec-phase2-proposal
user@SRX-Sunnyvale# set security ipsec policy ipsec-phase2-policy perfect-forward-secrecy keys group2
user@SRX-Sunnyvale# set security ipsec vpn vpn-corporate ike gateway gw-corporate
user@SRX-Sunnyvale# set security ipsec vpn vpn-corporate ike ipsec-policy ipsec-phase2-policy
user@SRX-Sunnyvale# set security ipsec vpn vpn-corporate bind-interface st0.0
```

Hub-and-Spoke VPN (Sunnyvale)

7. TCP MSS 設定を調整します

```
user@SRX-Sunnyvale# set security flow tcp-mss ipsec-vpn mss 1350
```

8. セキュリティポリシーを設定します

```
user@SRX-Sunnyvale# set security policies from-zone trust to-zone vpn policy to-corporate match source-address local-net
user@SRX-Sunnyvale# set security policies from-zone trust to-zone vpn policy to-corporate match destination-address corp-net
user@SRX-Sunnyvale# set security policies from-zone trust to-zone vpn policy to-corporate match destination-address westford-net
user@SRX-Sunnyvale# set security policies from-zone trust to-zone vpn policy to-corporate match application any
user@SRX-Sunnyvale# set security policies from-zone trust to-zone vpn policy to-corporate then permit
user@SRX-Sunnyvale# set security policies from-zone vpn to-zone trust policy from-corporate match source-address corp-net
user@SRX-Sunnyvale# set security policies from-zone vpn to-zone trust policy from-corporate match source-address westford-net
user@SRX-Sunnyvale# set security policies from-zone vpn to-zone trust policy from-corporate match destination-address local-net
user@SRX-Sunnyvale# set security policies from-zone vpn to-zone trust policy from-corporate match application any
user@SRX-Sunnyvale# set security policies from-zone vpn to-zone trust policy from-corporate then permit
```

Hub-and-Spoke VPN (Corporate office)

設定の確認 1

```
user@SRX-Corporate# show
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
            mode main;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$jzik.PfQ3n9p08XN-wsfTQ"; ## SECRET-DATA
        }
        gateway gw-westford {
            ike-policy ike-phase1-policy;
            address 3.3.3.2;
            external-interface ge-0/0/3.0;
        }
        gateway gw-sunnyvale {
            ike-policy ike-phase1-policy;
            address 2.2.2.2;
            external-interface ge-0/0/3.0;
        }
    }
```

Hub-and-Spoke VPN (Corporate office)

設定の確認 2

```
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
        policy ipsec-phase2-policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec-phase2-proposal;
        }
        vpn vpn-westford {
            bind-interface st0.0;
            ike {
                gateway gw-westford;
                ipsec-policy ipsec-phase2-policy;
            }
        }
        vpn vpn-sunnyvale {
            bind-interface st0.0;
            ike {
                gateway gw-sunnyvale;
                ipsec-policy ipsec-phase2-policy;
            }
        }
    }
```

Hub-and-Spoke VPN (Corporate office)

設定の確認 3

```
    address-book {
        book1 {
            address local-net 10.10.10.0/24;
            attach {
                zone trust;
            }
        }
        book2 {
            address sunnyvale-net 192.168.168.0/24;
            address westford-net 192.168.178.0/24;
            attach {
                zone vpn;
            }
        }
    }
    flow {
        tcp-mss {
            ipsec-vpn {
                mss 1350;
            }
        }
    }
```

Hub-and-Spoke VPN (Corporate office)

設定の確認 4

```
    policies {
        from-zone trust to-zone vpn {
            policy local-to-spokes {
                match {
                    source-address local-net;
                    destination-address [ sunnyvale-net westford-net ];
                    application any;
                }
                then {
                    permit;
                }
                from-zone vpn to-zone trust {
            policy spokes-to-local {
                match {
                    source-address [ sunnyvale-net westford-net ];
                    destination-address local-net;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
```

Hub-and-Spoke VPN (Corporate office)

設定の確認 5

```
        from-zone vpn to-zone vpn {
            policy spoke-to-spoke {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
    zones {
        security-zone untrust {
            host-inbound-traffic {
                system-services {
                    ike;
                }
            }
            interfaces {
                ge-0/0/3.0;
            }
        }
```

Hub-and-Spoke VPN (Corporate office)

設定の確認 6

```
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
            }
            interfaces {
                ge-0/0/0.0;
            }
        }
        security-zone vpn {
            interfaces {
                st0.0;
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.10.10.1/24;
            }
        }
    }
```

Hub-and-Spoke VPN (Corporate office)

設定の確認 7

```
    ge-0/0/3 {
        unit 0 {
            family inet {
                address 1.1.1.2/30;
            }
        }
    }
    st0 {
        unit 0 {
            multipoint;
            family inet {
                next-hop-tunnel 10.11.11.11 ipsec-vpn vpn-sunnyvale;
                next-hop-tunnel 10.11.11.12 ipsec-vpn vpn-westford;
                address 10.11.11.10/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 1.1.1.1;
        route 192.168.168.0/24 next-hop 10.11.11.11;
        route 192.168.178.0/24 next-hop 10.11.11.12;
    }
}
```

Hub-and-Spoke VPN (Westford)

設定の確認 1

```
user@SRX-Westford# show
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
            mode main;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$piWhuO1RESleMX7Diq.5TEcS"; ## SECRET-DATA
        }
        gateway gw-corporate {
            ike-policy ike-phase1-policy;
            address 1.1.1.2;
            external-interface ge-0/0/0.0;
        }
    }
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
```

Hub-and-Spoke VPN (Westford)

設定の確認 2

```
        policy ipsec-phase2-policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec-phase2-proposal;
        }
        vpn vpn-corporate {
            bind-interface st0.0;
            ike {
                gateway gw-corporate;
                ipsec-policy ipsec-phase2-policy;
            }
        }
    }
    address-book {
        book1 {
            address local-net 192.168.178.0/24;
            attach {
                zone trust;
            }
        }
        book2 {
            address corp-net 10.10.10.0/24;
            address sunnyvale-net 192.168.168.0/24;
            attach {
                zone vpn;
            }
        }
    }
```

Hub-and-Spoke VPN (Westford)

設定の確認 3

```
    flow {
        tcp-mss {
            ipsec-vpn {
                mss 1350;
            }
        }
    }
    policies {
        from-zone trust to-zone vpn {
            policy to-corporate {
                match {
                    source-address local-net;
                    destination-address [ corp-net sunnyvale-net ];
                    application any;
                }
                then {
                    permit;
                }
            }
        }
```

Hub-and-Spoke VPN (Westford)

設定の確認 4

```
        from-zone vpn to-zone trust {
            policy from-corporate {
                match {
                    source-address [ corp-net sunnyvale-net ];
                    destination-address local-net;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
    zones {
        security-zone untrust {
            host-inbound-traffic {
                system-services {
                    ike;
                }
            }
            interfaces {
                ge-0/0/0.0;
            }
        }
```

Hub-and-Spoke VPN (Westford)

設定の確認 5

```
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
            }
            interfaces {
                ge-0/0/3.0;
            }
        }
        security-zone vpn {
            interfaces {
                st0.0;
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 3.3.3.2/30;
            }
        }
    }
```

Hub-and-Spoke VPN (Westford)

設定の確認 6

```
    ge-0/0/3 {
        unit 0 {
            family inet {
                address 192.168.178.1/24;
            }
        }
    }
    st0 {
        unit 0 {
            family inet {
                address 10.11.11.12/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 3.3.3.1;
        route 10.10.10.0/24 next-hop 10.11.11.10;
        route 192.168.168.0/24 next-hop 10.11.11.10;
    }
}
```

Hub-and-Spoke VPN (Sunnyvale)

設定の確認 1

```
user@SRX-Sunnyvale# show
security {
    ike {
        proposal ike-phase1-proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-phase1-policy {
            mode main;
            proposals ike-phase1-proposal;
            pre-shared-key ascii-text "$9$eEPKM8Xx-bw2aZ36CA0OxN-"; ## SECRET-DATA
        }
        gateway gw-corporate {
            ike-policy ike-phase1-policy;
            address 1.1.1.2;
            external-interface ge-0/0/0.0;
        }
    }
    ipsec {
        proposal ipsec-phase2-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
```

Hub-and-Spoke VPN (Sunnyvale)

設定の確認 2

```
        policy ipsec-phase2-policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec-phase2-proposal;
        }
        vpn vpn-corporate {
            bind-interface st0.0;
            ike {
                gateway gw-corporate;
                ipsec-policy ipsec-phase2-policy;
            }
        }
    }
    address-book {
        book1 {
            address local-net 192.168.168.0/24;
            attach {
                zone trust;
            }
        }
        book2 {
            address corp-net 10.10.10.0/24;
            address westford-net 192.168.178.0/24;
            attach {
                zone vpn;
            }
        }
    }
```

Hub-and-Spoke VPN (Sunnyvale)

設定の確認 3

```
    flow {
        tcp-mss {
            ipsec-vpn {
                mss 1350;
            }
        }
    }
    policies {
        from-zone trust to-zone vpn {
            policy to-corporate {
                match {
                    source-address local-net;
                    destination-address [ corp-net westford-net ];
                    application any;
                }
                then {
                    permit;
                }
            }
        }
```

Hub-and-Spoke VPN (Sunnyvale)

設定の確認 4

```
        from-zone vpn to-zone trust {
            policy from-corporate {
                match {
                    source-address [ corp-net westford-net ];
                    destination-address local-net;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
    }
    zones {
        security-zone untrust {
            host-inbound-traffic {
                system-services {
                    ike;
                }
            }
            interfaces {
                ge-0/0/0.0;
            }
        }
```

Hub-and-Spoke VPN (Sunnyvale)

設定の確認 5

```
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
            }
            interfaces {
                ge-0/0/3.0;
            }
        }
        security-zone vpn {
            interfaces {
                st0.0;
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 2.2.2.2/30;
            }
        }
    }
```

Hub-and-Spoke VPN (Sunnyvale)

設定の確認 6

```
    ge-0/0/3 {
        unit 0 {
            family inet {
                address 192.168.168.1/24;
            }
        }
    }
    st0 {
        unit 0 {
            family inet {
                address 10.11.11.11/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 2.2.2.1;
        route 10.10.10.0/24 next-hop 10.11.11.10;
        route 192.168.178.0/24 next-hop 10.11.11.10;
    }
}
```

Hub-and-Spoke VPN

VPN ステータスの確認 (Corporate office)

- Phase1

```
user@SRX-Corporate> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
3899021 UP     bb4e1be49797023f  a5ee77e510e4d0df  Main           2.2.2.2
3899022 UP     b003df2c9ebf11be  f1d7ba2fad1dec63  Main           3.3.3.2
```

- Phase2

```
user@SRX-Corporate> show security ipsec security-associations
  Total active tunnels: 2     Total Ipsec sas: 2
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <131074 ESP:aes-cbc-128/sha1 94565f5a 3575/ unlim - root 500 2.2.2.2
  >131074 ESP:aes-cbc-128/sha1 cf53d3dd 3575/ unlim - root 500 2.2.2.2
  <131073 ESP:aes-cbc-128/sha1 3eafcdad 3575/ unlim - root 500 3.3.3.2
  >131073 ESP:aes-cbc-128/sha1 776fffb5 3575/ unlim - root 500 3.3.3.2
```

Thank you

JUNIPER NETWORKS

Driven by Experience™