IPSEC VPN

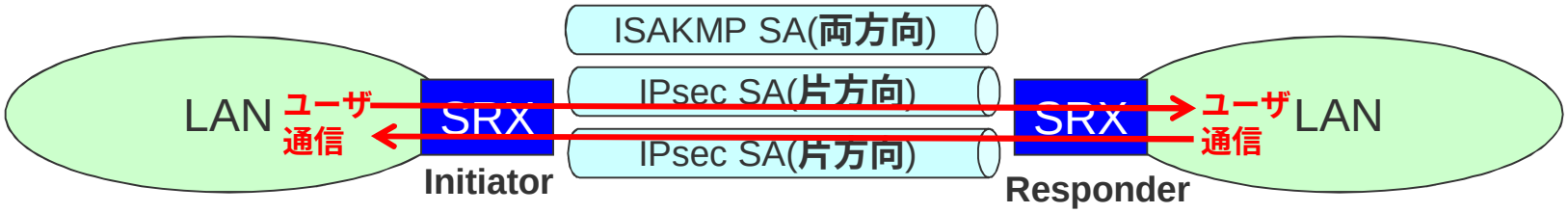
IPSEC-VPN概要

IPsec(Security Architecture for Internet Protocol)は、暗号技術を用いて、IPパケット単位でデータの改竄防止や秘匿機能を提供するプロトコルです。セキュリティゲートウェイ間でSA(Security Association, いわゆる暗号化トンネル)が作成され、SA内をユーザトラフィックが流れることとなります。

IKEにはフェーズ1とフェーズ2の2ステップがあります。IKEのフェーズ1では、1本のISAKMP SA(双方向)が生成されます。これに対し、IKEのフェーズ2では、2本のIPSec SA(片方向が1本ずつ)が生成されます。実際のユーザ通信はIPsec SAを使用して行われます。

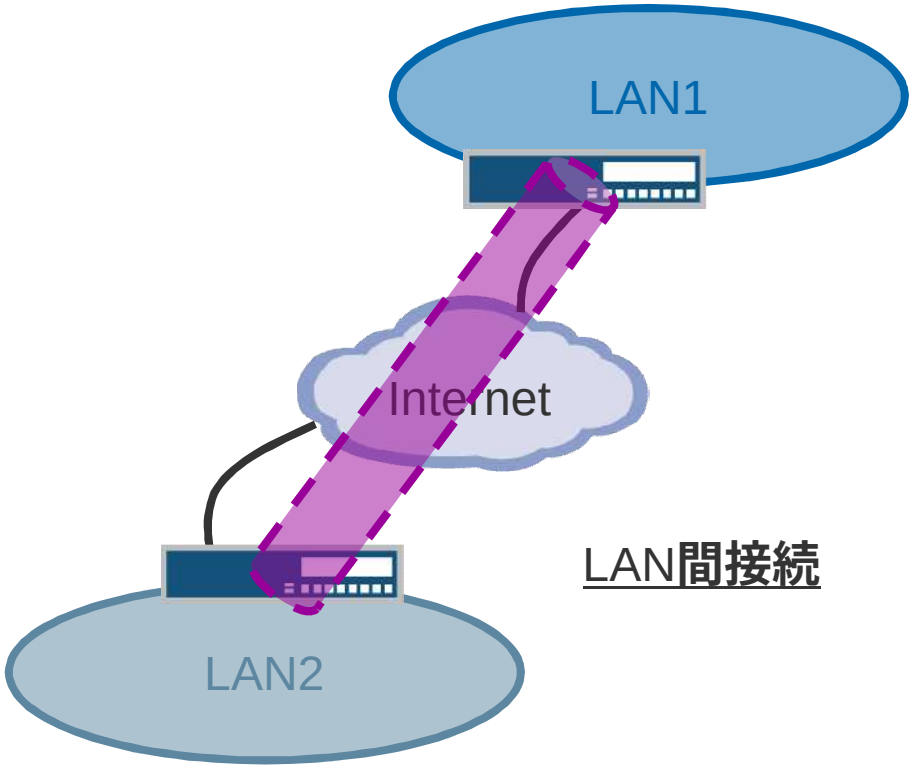
IKE折衝の開始側をInitiator、応答側をResponderと呼びます。

IPsec-VPNの概念

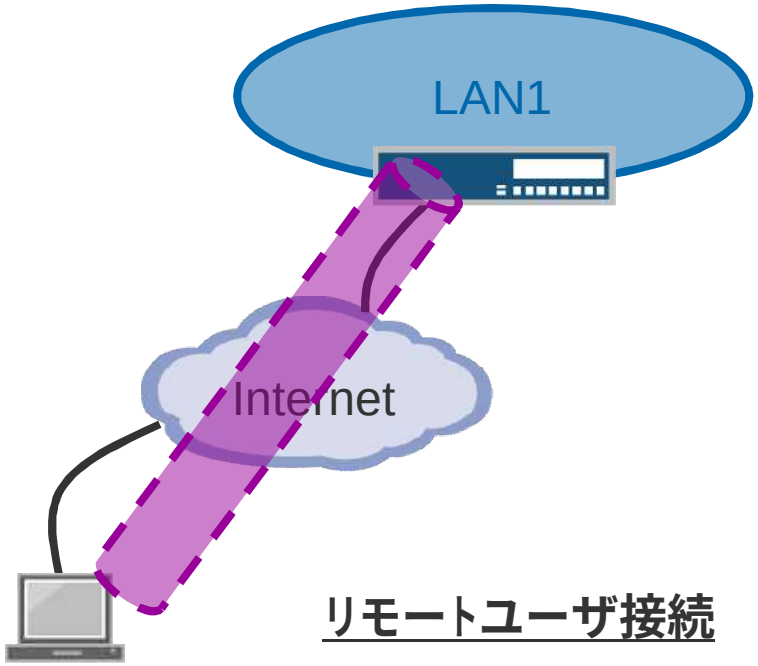


VPN接続形態(1)

VPN接続には大きく分けて下記の2通りになります。



LAN間接続



リモートユーザ接続

VPN接続形態(2)

LAN間接続

- LAN間接続にも対向のゲートウェイのIPアドレスタイプによって設定が一部異なります。
  - 両方のゲートウェイのIPアドレスが固定である（メインモード）
  - 片方のゲートウェイのIPアドレスが動的であり、特定できない（アグレッシブモード）

リモートユーザ接続

- SRXにはDynamic VPN Client という機能が実装されており、クライアントPCに予めソフトウェアをインストールすることなく、IPsec VPNが実現可能です。

LAN間接続 IPsec VPNの設定方法

SRXのLAN間接続 VPNは、以下の2つの設定方法があります。

- ルートベースVPN
  - ルーティングにマッチする全トラフィックをトンネリング
- ポリシーベースVPN
  - ポリシーにマッチするトラフィックのみをトンネリング

LAN間接続 IPsec VPN 設定の手順

LAN間接続 IPsec VPNの設定は以下のステップで行います。

1. フェーズ1 パラメーターの設定
   a. プロポーザルの設定
   b. ポリシーの設定
   c. ゲートウェイの設定
2. フェーズ2 パラメーターの設定
   a. プロポーザルの設定
   b. ポリシーの設定
   c. VPNの設定
3. ルートベースVPNの場合
   a. トンネルインタフェースの作成とゾーンの割り当て
   b. ルーティングの設定
   c. VPNへのバインディング

4. (ポリシーベースVPNの場合)
   トンネリングポリシーの作成

1-a. フェーズ1プロポーザルの設定

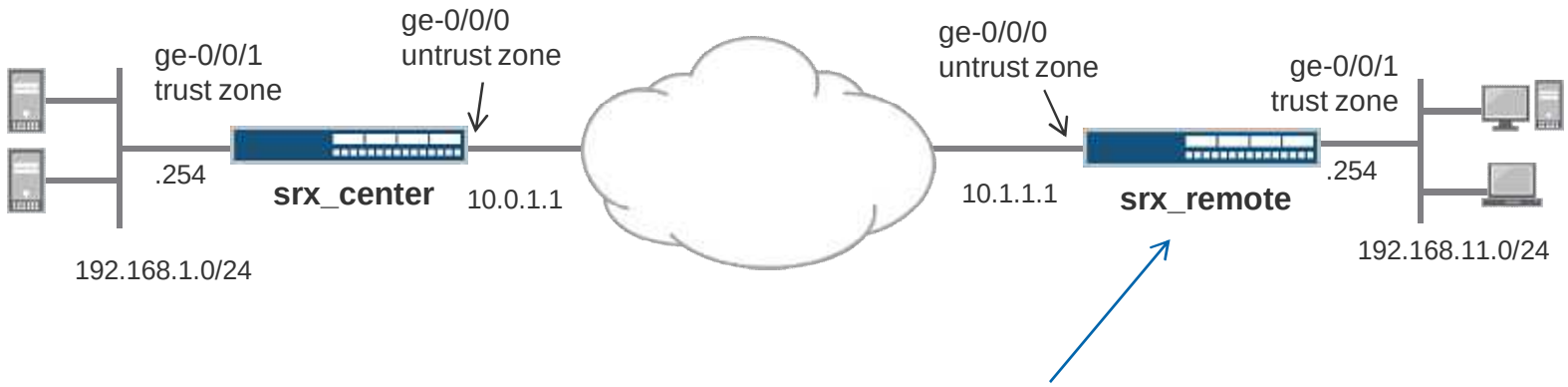
ISAKMP SAのセキュリティ属性（プロポーザル）を定義するため、認証方式、鍵交換方式(Diffie-Hellman group)、暗号化アルゴリズム、認証アルゴリズム等を指定します。

```
security {
    ike {
        proposal ike_proposal1 {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
    }
```

SRXでは、下記パラメータの組合せが予め定義されており、これを利用することもできます。

- Basic
  - Proposal 1: Preshared key, DH g1, DES, SHA1 (pre-g1-des-sha)
  - Proposal 2: Preshared key, DH g1, DES, MD5 (pre-g1-des-md5)
- Compatible
  - Proposal 1: Preshared key, DH g2, 3DES, SHA1 (pre-g2-3des-sha)
  - Proposal 2: Preshared key, DH g2, 3DES, MD5 (pre-g2-3des-md5)
  - Proposal 3: Preshared key, DH g2, DES, SHA1 (pre-g2-des-sha)
  - Proposal 4: Preshared key, DH g2, DES, MD5 (pre-g2-des-md5)
- Standard
  - Proposal 1: Preshared key, DH g2, 3DES, SHA1 (pre-g2-3des-sha)
  - Proposal 2: Preshared key, DH g2, AES128, SHA1 (pre-g2-aes128-sha)

1-b, 1-c. フェーズ1　ポリシー、ゲートウェイの設定




```
security {
    ike {
        ## ポリシーの設定
         policy ike_policy1 {
            proposals ike_proposal1;
            pre-shared-key ascii-text “juniper123"; ## SECRET-DATA
        }
        ## ゲートウェイの設定
        gateway gw1 {
            ike-policy ike_policy1;
            address 1.1.1.1;
            external-interface ge-0/0/0;
        }
    }
```

2-a. フェーズ2　プロポーザルの設定

フェーズ2 SAのセキュリティ属性（プロポーザル）を指定するため、プロトコル、暗号化アルゴリズム、認証アルゴリズム等を設定します。

```
security {
    ipsec {
        proposal ipsec-proposal1 {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
```

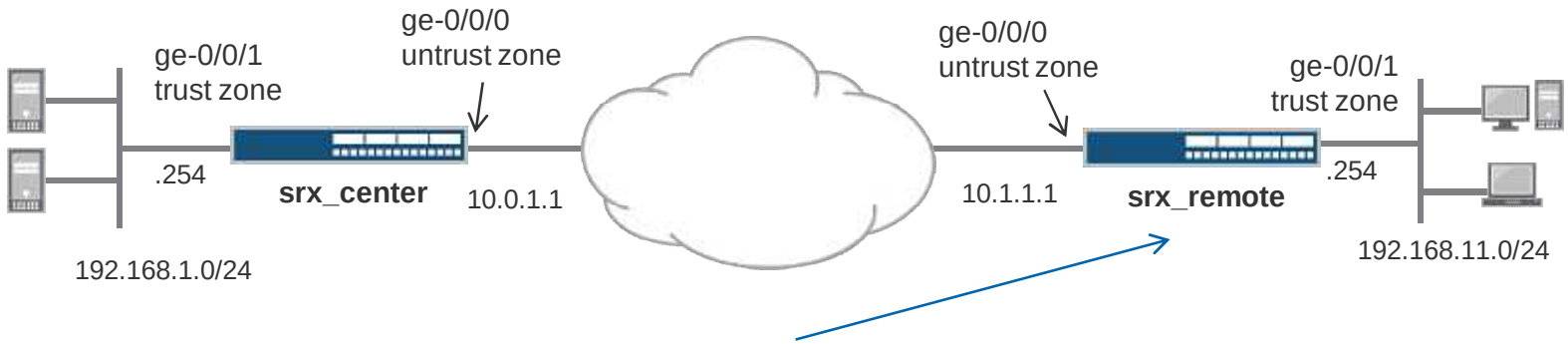
SRXでは、下記パラメータの組合せが予め定義されており、これを利用することもできます。

- Basic
  - Proposal 1: no PFS, ESP, DES, SHA1　(nopfs-esp-des-sha)
  - Proposal 2: no PFS, ESP, DES, MD5　(nopfs-esp-des-md5)
- Compatible
  - Proposal 1: no PFS, ESP, 3DES, SHA1　(nopfs-esp-3des-sha)
  - Proposal 2: no PFS, ESP, 3DES, MD5　(nopfs-esp-3des-md5)
  - Proposal 3: no PFS, ESP, DES, SHA1　(nopfs-esp-des-sha)
  - Proposal 4: no PFS, ESP, DES, MD5　(nopfs-esp-des-md5)
- Standard
  - Proposal 1: DH g2, ESP, 3DES, SHA1　(g2-esp-3des-sha)
  - Proposal 2: DH g2, ESP, AES128, SHA1　(g2-esp-aes128-sha)

2-b, 2-c. フェーズ2　ポリシーの設定、VPNの設定


```
security {
    ipsec {
        ## ポリシーの設定
        policy ipsec-policy1 {
            proposals ipsec-proposal1;
        }
        ## VPNの設定
        vpn vpn1 {
            ike {
                gateway gw1;
                ipsec-policy ipsec-policy1;
            }
            establish-tunnels immediately;
        }
    }
```

3. ルートベースVPNの設定




```
## トンネルインタフェースの作成
interfaces {
    st0 {
        unit 0 {
            family inet;
        }
    }
}
## ルーティングの設定
routing-options {
    static {
        route 192.168.1.0/24 next-hop st0.0;
    }
}
```

```
security {
    ## VPN設定との関連付け
    ipsec {
        vpn vpn1 {
            bind-interface st0.0;
        }
    }
    ## トンネルインタフェースのゾーンへの割り当て
    zones {
        security-zone vpn {
            interfaces {
                st0.0;
            }
        }
    }
}
```

4. ポリシーベースVPNの設定

アクションが “Tunnel” のセキュリティポリシーを作成します。

```
security {
    zones {
        security-zone trust {
            address-book {
                address Local-LAN 192.168.11.0/24;
            }
        security-zone untrust {
            address-book {
                address Remote-LAN 192.168.1.0/24;
            }
    policies {
        from-zone trust to-zone untrust {
            policy 100 {
                match {
                    source-address Local-LAN;
                    destination-address Remote-LAN;
                    application any;
                }
                then {
                    permit {
                        tunnel {
                            ipsec-vpn vpn1;
                        }
```

(次ページに続く)

注意：ポリシーベースVPNとルートベースVPNの混在構成(設定)は出来ません

4. ポリシーベースVPNの設定

```
security {
    policies {
        from-zone untrust to-zone trust {
            policy 200 {
                match {
                    source-address Remote-LAN;
                    destination-address Local-LAN;
                    application any;
                }
                then {
                    permit {
                        tunnel {
                            ipsec-vpn vpn1;
                        }
```

接続確認 – ISAKMP SAの確認

```
root@srx100-1# run show security ike security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
5       10.1.1.1        UP     c5a96ccb61cf85c3  fdade253ee4981bf  Main

[edit]
root@srx100-1# run show security ike security-associations detail
IKE peer 10.1.1.1, Index 5,
  Role: Responder, State: UP
  Initiator cookie: c5a96ccb61cf85c3, Responder cookie: fdade253ee4981bf
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.0.1.1:500, Remote: 10.1.1.1:500
  Lifetime: Expires in 28569 seconds
  Peer ike-id: 192.168.20.3
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : sha1
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                1076
   Output bytes  :                1212
   Input  packets:                   5
   Output packets:                   5
  Flags: Caller notification sent
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0

[edit]
root@srx100-1#
```

ここがUPにならないと接続できていない。
設定が対向側と同じになっているかを再チェック

JUNIPER NETWORKS

接続確認 – IPsec SAの確認

```
root@srx100-1# run show security ipsec security-associations
  Total active tunnels: 1
  ID    Gateway           Port  Algorithm       SPI      Life:sec/kb  Mon vsys
  <131073 10.1.1.1        500   ESP:3des/sha1   30d92a41 367/  unlim   -   root
  >131073 10.1.1.1        500   ESP:3des/sha1   a15b3df2 367/  unlim   -   root
[edit]
root@srx100-1# run show security ipsec security-associations detail
  Virtual-system: root
  Local Gateway: 10.0.1.1, Remote Gateway: 10.1.1.1
  Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    DF-bit: clear
    Direction: inbound, SPI: 30d92a41, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 364 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expired
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64

    Direction: outbound, SPI: a15b3df2, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 364 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expired
    Mode: tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Anti-replay service: counter-based enabled, Replay window size: 64
[edit]
root@srx100-1#
```

IPSec SAは片方向なので
Inbound/outboundの両方が
作成される

接続確認 - 暗号/復号トラフィックの統計確認

```
root@srx100-1# run show security ipsec statistics
ESP Statistics:
  Encrypted bytes:                680
  Decrypted bytes:                132
  Encrypted packets:                5
  Decrypted packets:             2052
AH Statistics:
  Input bytes:                      0
  Output bytes:                     0
  Input packets:                    0
  Output packets:                   0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0

[edit]
root@srx100-1#
```

IPSEC VPN トラブルシューティング

IKE のデバッグログは、/var/log/kmd 内に蓄積されます。

デバッグ用設定

```
security {
    ike {
        traceoptions {
            flag ike;
            flag all;
        }
```

デバッグログ(kmdファイル)の参照方法

> show log kmd

IKE debug log をリアルタイムにモニターする場合

> monitor start kmd (start showing ike log file in real time)

> monitor stop kmd (stop showing ike log file in real time)

http://kb.juniper.net/KB10100 もご参照ください。

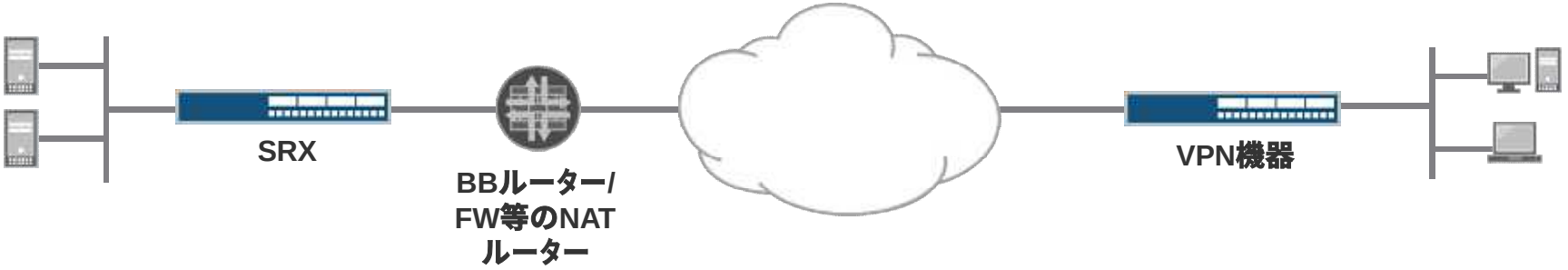
IPSEC使用時の考慮点

トンネルインタフェース (st0) のMTU値はデフォルトで9192 です。
ScreenOSとRoute-based VPNを使用して接続する場合に問題となる場合があるので注意が必要です。

IKE のエンドポイントは、inet.0 ルーティングに属します。

以下の機能はサポートされておりません。

- Tunnel Interface(st0.x) でのQoS機能
- XAuth initiator 機能
- 対向VPN機器との間にNAT装置が存在するネットワーク構成(NAT-Traverse機能)



everywhere