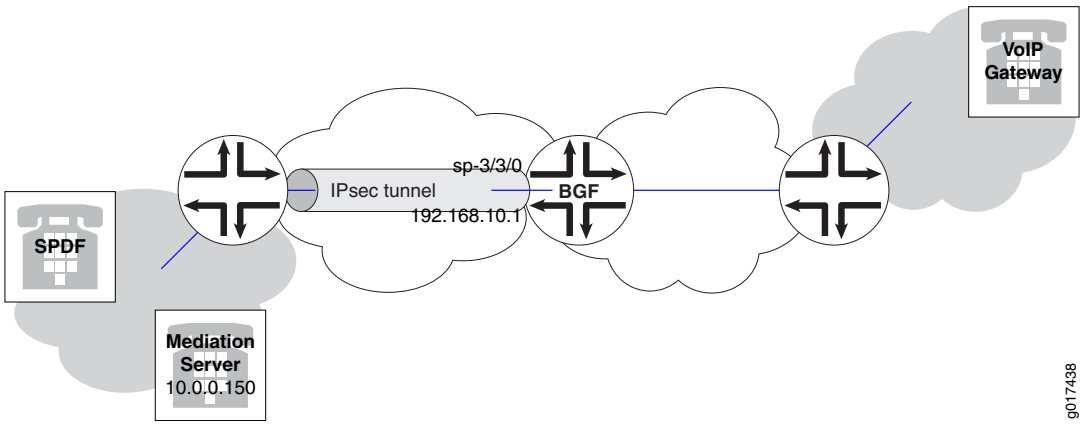
Configuring IPsec to Protect Mirrored Sessions in Tunnel Mode

Figure 1 shows a sample configuration that protects session mirroring call content (that is, the X3 interface) using IPsec tunnel mode.

Figure 1: Protecting Session Mirroring Call Content Using IPsec Tunnel Mode



To configure IPsec to protect session mirroring call content as shown in Figure 1:

1. Configure the service PIC that you want IPsec to use. IPsec can use the same service PIC that the BGF uses, or it can have a dedicated service PIC.

   Assign a logical interface for incoming traffic to the IPsec tunnel and a logical interface for outgoing traffic from the IPsec tunnel. For example:

```
[edit interfaces sp-3/3/0]
unit 0 {
    family inet;
}
unit 10 {
    family inet;
    service-domain inside;
}
unit 20 {
    family inet;
    service-domain outside;
}
unit 50 {
    description IPsec-tunnel-incoming;
    family inet;
    service-domain inside;
}
unit 60 {
    description IPsec-tunnel-outgoing;
    family inet;
    service-domain outside;
}
```

2. Configure a service set that has the following characteristics:

   - Next hop service that contains the inside and outside interfaces that you configured for IPsec.
   - The local IP address for IPsec traffic.
   - The IPsec rule or rule set applied to the tunnel. This is a rule or rule set that you configure at the [edit services ipsec-vpn] hierarchy level.

```
[edit services service-set ipsec-tunnel-for-bgf]
next-hop-service {
    inside-service-interface sp-3/3/0.50;
    outside-service-interface sp-3/3/0.60;
}
ipsec-vpn-options {
    local-gateway 192.168.10.1;
}
ipsec-vpn-rules rule-ike;
```

3. Configure a static route to the mediation server with the IPsec interface as the next hop.

```
[edit routing-options]
static {
    route 10.0.0.150/32 next-hop sp-3/3/0.50;
}
```

Published: 2010-04-13