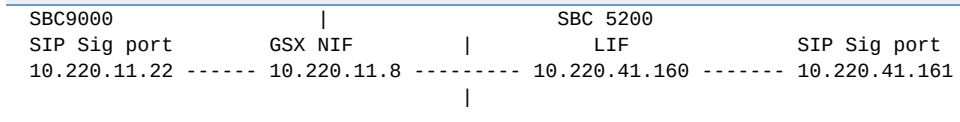
Configuring SBC for IPsec IKEv1

The following example describes a configuration of an SBC 5200 that enables IPsec encryption of SIP traffic between LABNBS1 and SBC9000.

SBC 5200-SBC 9000 Configuration Example

Network diagram showing the IP addresses used in the configuration example



SBC Core IPSEC Configuration Commands

```
### create and configure IKE and IPsec protection profiles

set profiles security ipsecProtectionProfile PRGGSX2_IPSEC_PROT_PROF saLifetimeTime 28800
set profiles security ipsecProtectionProfile PRGGSX2_IPSEC_PROT_PROF espAlgorithms integrity
hmacSha1,hmacMd5
set profiles security ipsecProtectionProfile PRGGSX2_IPSEC_PROT_PROF espAlgorithms encryption
aesCbc128,_3DesCbc

set profiles security ikeProtectionProfile PRGGSX2_IKE_PROT_PROF saLifetimeTime 28800
set profiles security ikeProtectionProfile PRGGSX2_IKE_PROT_PROF algorithms encryption
aesCbc128,_3DesCbc
set profiles security ikeProtectionProfile PRGGSX2_IKE_PROT_PROF algorithms integrity hmacSha1,hmacMd5
set profiles security ikeProtectionProfile PRGGSX2_IKE_PROT_PROF dpdInterval noDpd

### create IKE peer

set addressContext default ipsec peer PRGGSX2 ipAddress 10.220.11.8 preSharedKey
00000000000000000000000000000000 localIdentity type ipV4Addr ipAddress 10.220.41.161
set addressContext default ipsec peer PRGGSX2 remoteIdentity type ipV4Addr ipAddress 10.220.11.22
set addressContext default ipsec peer PRGGSX2 protocol ikev1 protectionProfile PRGGSX2_IKE_PROT_PROF

### create an SPD rule for this IKE peer

set addressContext default ipsec spd PRGGSX2_SPD state enabled precedence 1001
set addressContext default ipsec spd PRGGSX2_SPD localIpAddr 10.220.41.161 localIpPrefixLen 32
remoteIpAddr 10.220.11.22 remoteIpPrefixLen 32
set addressContext default ipsec spd PRGGSX2_SPD action protect
set addressContext default ipsec spd PRGGSX2_SPD protocol 0
set addressContext default ipsec spd PRGGSX2_SPD protectionProfile PRGGSX2_IPSEC_PROT_PROF
set addressContext default ipsec spd PRGGSX2_SPD mode transport
set addressContext default ipsec spd PRGGSX2_SPD peer PRGGSX2

### enable IPsec on the IP interface group

set addressContext default ipInterfaceGroup default_IP_INT_GR ipsec enabled
```

IPsec encryption works for non-media traffic only on SBC Core and SBC 9000. Only non-media traffic (signaling, ICMP) traverses through the IPsec tunnel. To encrypt media as well, use SRTP. If the media endpoint IP address is behind a NAPT, enable NaptMedia flag on the sipTrunkGroup.

IPsec using overlapped IP addressing is not supported in SBC Core releases earlier than 4.2.x; only the default addressContext is used for IPsec. In 4.2.x and later releases, the SBC supports IPsec in default and custom addressContexts.

Set all parameters identically on both sides (including timers, ciphers, SPD IP addresses, prefixes/masks, PFS, and so on).

Best Practice for IKE Peer Configuration
Set local identity to local SIP signaling port IP address and set remote identity to remote SIP signaling port IP address. The other end has to be set other way, that is, "remote identity" parameter has to match the local identity and vice versa.

Set IKE peer IP address to network interface IP address, that is, IP address of LIF or NIF/SIF.

The SBC supports a setup where the IPsec peer termination IP address (FW/IPsec GW IP address) is a public IP address and there is a SIP server or PBX with a private IP address behind this FW/GW. The SBC needs static IP routes to both termination and SIP signaling IP addresses. The static IP route to the private IP address is redundant. That means, nexthop is same as the nexthop for a public IP address. The un-encrypted traffic to the private IP address cannot be sent because the private IP address is not reachable directly from the SBC.

SPD Configuration
IP addresses of the SPDs have to be populated with SIP signaling port IP addresses. Protocol enumerations: 17 UDP, 6 TCP and so on (IANA Protocol enumerations apply).

IP addresses and prefixes (masks) in traffic selectors have to be set identically on both ends.

Ensure that the entered IP address entered for SPD entries is the subnet ID IP address and not a host IP address. For example, 192.168.1.0/29 is correct and 192.168.1.5/29 is incorrect.

To send both encrypted and unencrypted traffic through the same IP Interface Group/IP Interface, configure separate SPDs. The action type for unencrypted traffic has to be set to `bypass` and to encrypt set it to `protect`.

Enabling IPsec on an interface group that has 2 or more interfaces is not supported.

Useful CLI Commands

To retrieve the statistics and status of SA of IKE and IPsec.

```
admin@labnbs1b> show status addressContext default ipsec ikeSaStatus
ikeSaStatus 6 {
    localIpAddr      10.220.41.160;
    peerIpAddr       10.220.11.8;
    localId          10.220.41.161;
    peerId           10.220.11.22;
    encType          aes128;
    integrityType    sha1;
    secondsRemaining 28662;
}
admin@labnbs1b> show status addressContext default ipsec ikeSaStatistics
ikeSaStatistics 6 {
    localIpAddr                 10.220.41.160;
    peerIpAddr                  10.220.11.8;
    ipsecSaNegotiationsSucceeded 1;
    ipsecSaNegotiationsFailed    0;
}
[ok][2013-04-12 08:25:29]
admin@labnbs1b>

admin@labnbs1b> show status addressContext default ipsec ipsecSaStatus
ipsecSaStatus 0004BD56 {
    remoteSPI             0040D170;
    localTerminationAddr  10.220.41.160;
    remoteTerminationAddr 10.220.11.8;
    localSelector         10.220.41.161/32:*;
    remoteSelector        10.220.11.22/32:*;
    upperLayerProtocol    17;
    encType               aes128;
    integrityType         sha1;
    secondsRemaining      28612;
    bytesRemaining        -;
    selectorName          PRGGSX2_SPD;
    ikeSaIndex            6;
}
admin@labnbs1b> show status addressContext default ipsec ipsecSaStatistics
ipsecSaStatistics 0004BD56 {
    localIpAddr                   10.220.41.160;
    remoteSpi                     0040D170;
    peerIpAddr                    10.220.11.8;
    inPacketsCount                2;
    outPacketsCount               2;
    inBytesCount                  709;
    outBytesCount                 1620;
    inPacketDiscardFailedIntegrity 0;
    inPacketDiscardAntiReplay      0;
}

admin@labnbs1b> show status addressContext default ipsec systemStatistics
systemStatistics labnbs1 {
    inPacketDiscardInvalidSpi       3;
    inPacketDiscardProtected        0;
    inPacketDiscardDiscarded        0;
    outPacketDiscardProtected       3;
    outPacketDiscardDiscarded       0;
    inPacketDiscardNoState          0;
    inPacketDiscardSAExpired        0;
    inPacketDiscardSelectorMismatch 0;
    outPacketDiscardSSNWrap         0;
    outPacketDiscardSAExpired       0;
    ikeSaNegotiationsSucceeded      6;
    ikeSaNegotiationsFailed         0;
    ipsecSaNegotiationsSucceeded    7;
    ipsecSaNegotiationsFailed       32;
}
[ok][2013-04-12 08:24:29]
```