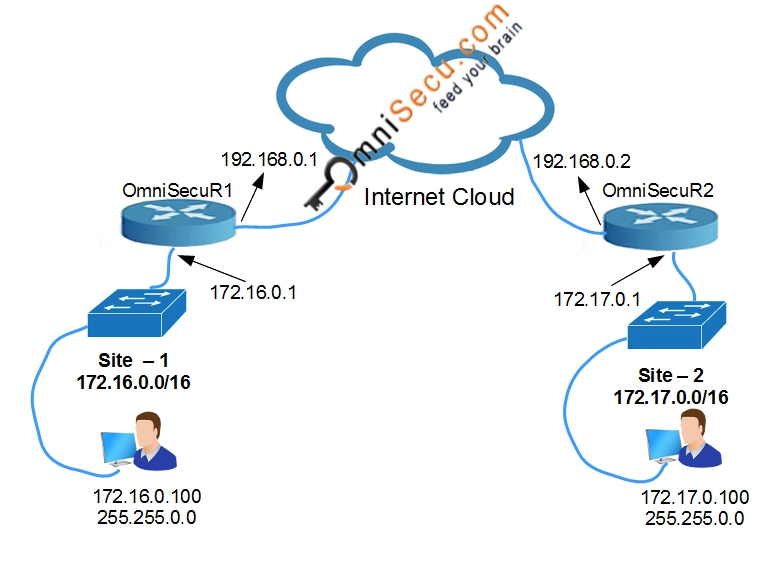
**Site-to-Site IKEv1 IPSec VPN Configuration - Lab Topology**



Note: Before proceeding, make sure that all the IP Addresses of your network devices are configured correctly. Make sure that routing is configured correctly. Make sure you can reach all the devices by pinging all IP Addresses.

### Step 1: Configure Host name and Domain name in IPSec peer Routers

To configure Hostname on aptech1 use the following commands.

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**hostname Aptech1**

**Aptech1**(config)#**exit**

**Aptech1**#

 To configure Domain name onaptech1, use the following commands.

**Aptech1**#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

**Aptech1** (config)#**ip domain-name aptechdl.com**

**Aptech1** (config)#**exit**

**Aptech1**#

To configure Hostname on Aptech2 use the following commands.

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**hostname Aptech2**

Aptech2(config)#**exit**

Aptech2#

• To configure Domain name on Aptech2, use the following commands.

Aptech2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Aptech2 (config)#**ip domain-name omnisecu.com**

Aptech2 (config)#**exit**

**Step 2: Configure Pre-Shared Key on IPSec Peers**

We have three methods of device authentication, Pre-Shared Key, RSA and Digital Certificates. Pre-Shared Key is the simplest among the three to set-up. The term Pre-Shared Key means a common key pre configured on both IPSec peers. We use Pre-Shared keys only if we have small number of IPSec devices. As the number IPSec devices grow, we may move to Digital Certificates for better scalability and security.

• To configure a Pre-Shared Key inaptech1 (for Aptech2), use the following commands.

Aptech1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Aptech1(config)#**crypto isakmp key 0 OmniSecuDotCom address 192.168.0.2**

Aptech1(config)#**exit**

Aptech1#

Please note that the Pre-Shared key we are using here is**OmniSecuDotCom**

The 0 before the Pre-Shared key specifies that the key is not encrypted.

• To configure a Pre-Shared Key in Aptech2 (foraptech1), use the following commands.

Aptech2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Aptech2(config)#**crypto isakmp key 0 OmniSecuDotCom address 192.168.0.1**

Aptech2(config)#**exit**

Aptech2#

**Step 3: Define one or more ISAKMP Policies**

An ISAKMP (IKE) policy is used to define the components of Phase1 ISAKMP management connection. An ISAKMP policy defines how Phase1 ISAKMP (IKE) tunnel is to be created, authenticated, and protected. It is possible to have more than one ISAKMP policy on a Router. If we have multiple IPSec connection to multiple sites and the Routers on different sites have different specifications and different abilities we must define multiple ISAKMP policies for different sites.

In this example we are going to define only one policy.

An ISAKMP (IKEv1) policy contains the parameters used for IKEv1 Phase 1 negotiation. Following are the Parameters and the selected Parameters which we are going to configure for this example.

Please note that the available Parameters may change depending on the version of IOS which you use. I am using IOS Version 15.2(4).

|  |  |  |
| --- | --- | --- |
| **Type** | **Possible Parameters** | **Selected Parameter** |
| Priority Number | 1-10000 | 1 |
| Encryption Algorithm | DES, 3DES, AES128, AES192, AES256 | AES256 |
| Hashing Algorithm | MD5, SHA1, SHA256, SHA384, SHA512 | SHA512 |
|  |  |  |
| Diffie-Hellman Group | 1, 2, 5, 14, 15, 16, 19, 20, 21, 24 | 24 |
| Authentication Method | PRE-SHARE, RSA-ENCR, RSA-SIG | PRE-SHARE |
| Connection lifetime (Seconds) | 60-86400 | 21600 |

• To configure a ISKAMP policy inaptech1 (with the selected values as in above table), use the following commands.

Aptech1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Aptech1(config)#**crypto isakmp policy 1**

Aptech1(config-isakmp)#**encryption aes 256**

Aptech1(config-isakmp)#**hash sha512**

Aptech1(config-isakmp)#**group 24**

Aptech1(config-isakmp)#**authentication pre-share**

Aptech1(config-isakmp)#**lifetime 21600**

Aptech1(config-isakmp)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To configure a ISKAMP policy in Aptech2 (with the selected values as in above table), use the following commands.

Aptech2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Aptech2(config)#**crypto isakmp policy 1**

Aptech2(config-isakmp)#**encryption aes 256**

Aptech2(config-isakmp)#**hash sha512**

Aptech2(config-isakmp)#**group 24**

Aptech2(config-isakmp)#**authentication pre-share**

Aptech2(config-isakmp)#**lifetime 21600**

Aptech2(config-isakmp)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 4: Define Crypto ACL to identify IPSec secured traffic

Crypto ACL is just an ACL created using normal ACL syntax, with permit or deny statements. Crypto ACLs are not used to permit or deny traffic similar to normal ACLs. In Crypto ACL, a permit statement is used to identify the traffic which is to be secured using IPSec and a deny statement is used to identify the traffic whish doesn't need to be secured. Here we are using "named extended access lists".

To configure a Crypto ACL inaptech1 (to identify the traffic to Aptech2), use the following commands.

Aptech1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Aptech1(config)#**ip access-list extended SITE1-SITE2-CACL**

Aptech1(config-ext-nacl)#**permit ip 172.16.0.0 0.0.255.255 172.17.0.0 0.0.255.255**

Aptech1(config-ext-nacl)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To configure a Crypto ACL in Aptech2 (to identify the traffic toaptech1), use the following commands.

Aptech2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Aptech2(config)#**ip access-list extended SITE2-SITE1-CACL**

Aptech2(config-ext-nacl)#**permit ip 172.17.0.0 0.0.255.255 172.16.0.0 0.0.255.255**

Aptech2(config-ext-nacl)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 5: Define Transform Sets for Phase 2 negotiation

A Transform set is used to define how the data traffic between IPSec peers is going to be protected in Phase 2. It is possible to have more than one Transform Set on a Router. If we have multiple IPSec connection to multiple sites and the Routers on different sites have different specifications and different abilities we must define multiple Transform Sets for different sites.

A Transform Set must have a unique identifier name. A Transform Set can contain up to four transforms. Following are the parameters possible for a Transform Set.

To define a Transform Set inaptech1 (for securing Phase 2 with Aptech2), use the following commands.

Aptech1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Aptech1(config)#**crypto ipsec transform-set SITE2TS esp-sha512-hmac esp-aes**

Aptech1(cfg-crypto-trans)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To define a Transform Set in Aptech2 (for securing Phase 2 withaptech1), use the following commands.

Aptech2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Aptech2(config)#**crypto ipsec transform-set SITE1TS esp-sha512-hmac esp-aes**

Aptech2(cfg-crypto-trans)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 6: Define Crypto Maps

Crypto Maps are used to connect all the pieces of IPSec configuration together. A Crypto Map consists of one or more entries. A Crypto Map is made up of Crypto ACL, Transform Set, Remote Peer, the lifetime of the data connections etc.

• To define a Crypto Map inaptech1, use the following commands.

Aptech1(config)#**crypto map SITE2CMAP 10 ipsec-isakmp**

Aptech1(config-crypto-map)#**set security-association lifetime seconds 3600**

Aptech1(config-crypto-map)#**set peer 192.168.0.2**

Aptech1(config-crypto-map)#**set transform-set SITE2TS**

Aptech1(config-crypto-map)#**set pfs group16**

Aptech1(config-crypto-map)#**match address SITE2CACL**

Aptech1(config-crypto-map)#**exit**

Aptech1(config)#**exit**

• To define a Crypto Map in Aptech2, use the following commands.

Aptech2#**configure terminal**

Aptech2(config)#**crypto map SITE1CMAP 10 ipsec-isakmp**

Aptech2(config-crypto-map)#**set security-association lifetime seconds 3600**

Aptech2(config-crypto-map)#**set peer 192.168.0.1**

Aptech2(config-crypto-map)#**set transform-set SITE1TS**

Aptech2(config-crypto-map)#**set pfs group16**

Aptech2(config-crypto-map)#**match address SITE1CACL**

Aptech2(config-crypto-map)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 7: Activate Crypto Maps by applying the Crypto Map to Router's Interface

• To apply Crypto Map to the WAN Interface onaptech1, use following commands.

Aptech1#**configure terminal**

Aptech1(config)#**interface gi0/0**

Aptech1(config-if)#**crypto map SITE2CMAP**

Aptech1(config-if)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To apply Crypto Map to the WAN Interface on Aptech2, use following commands.

Aptech2#**configure terminal**

Aptech2(config)#**interface gi0/0**

Aptech2(config-if)#**crypto map SITE1CMAP**

Aptech2(config-if)#**exit**

Aptech2(config)#**exit**

Aptech2#

After configuring, initiate an IP traffic from device inside at Site-1 network to reach a device at Site-2 network. Your IPSec VPN Main mode IPSec tunnel will be built when any router find interesting traffic.

That is it ……………

## How to configure Site-to-Site IKEv2 IPSec VPN using Pre-Shared Key Authentication

Following are the main components which are used to construct Site-to-Site IKEv2 IPSec VPN.

• IKEv2 Proposal

• IKEv2 Policy

• IKEv2 Profile

• IKEv2 Keyring

• Crypto Map

### Step 2: Define IKEv2 Keyring

An IKEv2 keyring consists of preshared keys associated with an IKEv2 profile. Authentication is performed by Pre-Shared Keys defined inside an IKEv2 keyring.

• To define a IKEv2 Keyring in aptech1, use following commands.

Aptech1#**configure terminal**

Aptech1(config)#**crypto ikev2 keyring KR-1**

Aptech1(config-ikev2-keyring)#**peer SITE-2**

Aptech1(config-ikev2-keyring-peer)#**address 192.168.0.2**

Aptech1(config-ikev2-keyring-peer)#**pre-shared-key dell@123**

Aptech1(config-ikev2-keyring-peer)#**exit**

Aptech1(config-ikev2-keyring)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To define a IKEv2 Keyring in Aptech2, use following commands.

Aptech2#**configure terminal**

Aptech2(config)#**crypto ikev2 keyring KR-1**

Aptech2(config-ikev2-keyring)#**peer SITE-1**

Aptech2(config-ikev2-keyring-peer)#**address 192.168.0.1**

Aptech2(config-ikev2-keyring-peer)#**pre-shared-key dell@123**

Aptech2(config-ikev2-keyring-peer)#**exit**

Aptech2(config-ikev2-keyring)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 3: Define IKEv2 Proposal

An IKEv2 proposal consists of transforms which are used in the negotiation of IKE SAs, in [IKE\_SA\_INIT](http://www.omnisecu.com/tcpip/ikev2-phase-1-and-phase-2-message-exchanges.php) exchange. Following parameters are defined.

• Encryption Algorithm

• Integrity Algorithm

• Pseudo-Random Function (PRF) algorithm

• Diffie-Hellman (DH) Group

• To define an IKEv2 Proposal inaptech1, use following commands.

Aptech1#**configure terminal**

Aptech1(config)#**crypto ikev2 proposal PROP-SITE2**

Aptech1(config-ikev2-proposal)#**encryption aes-cbc-256**

Aptech1(config-ikev2-proposal)#**integrity sha512**

Aptech1(config-ikev2-proposal)#**group 24**

Aptech1(config-ikev2-proposal)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To define a IKEv2 Proposal in Aptech2, use following commands.

Aptech2#**configure terminal**

Aptech2(config)#**crypto ikev2 proposal PROP-SITE1**

Aptech2(config-ikev2-proposal)#**encryption aes-cbc-256**

Aptech2(config-ikev2-proposal)#**integrity sha512**

Aptech2(config-ikev2-proposal)#**group 24**

Aptech2(config-ikev2-proposal)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 4: Define IKEv2 Policies

An IKEv2 Policy contains IKEv2 Proposals (defined in above step) which are used to negotiate the [Encryption Algorithm](http://www.omnisecu.com/tcpip/important-symmetric-and-assymmetric-encryption-algorithms.php),[Integrity Algorithm](http://www.omnisecu.com/tcpip/how-hash-values-can-be-used-to-determine-integrity-of-data.php), PRF Algorithms, and [Diffie-Hellman (DH) Group](http://www.omnisecu.com/tcpip/what-is-diffie-hellman-group.php) in [IKE\_SA\_INIT](http://www.omnisecu.com/tcpip/ikev2-phase-1-and-phase-2-message-exchanges.php) exchange.

• To define IKEv2 Policy inaptech1, use following commands.

Aptech1#**configure terminal**

Aptech1(config)#**crypto ikev2 policy POL-SITE2**

Aptech1(config-ikev2-policy)#**proposal PROP-SITE2**

Aptech1(config-ikev2-policy)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To define IKEv2 Policy in Aptech2, use following commands.

Aptech2#**configure terminal**

Aptech2(config)#**crypto ikev2 policy POL-SITE1**

Aptech2(config-ikev2-policy)#**proposal PROP-SITE1**

Aptech2(config-ikev2-policy)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 5: Define Crypto ACL to identify IPSec secured traffic

Crypto ACL is just an ACL created using normal ACL syntax, with permit or deny statements. Crypto ACLs are not used to permit or deny traffic similar to normal ACLs. In Crypto ACL, a permit statement is used to identify the traffic which is to be secured using IPSec and a deny statement is used to identify the traffic whish doesn't need to be secured. Here we are using "named extended access lists".

New to Access Control Lists (ACLs)? Please refer below lessons if you wish.

To configure a Crypto ACL inaptech1 (to identify the traffic to Aptech2), use the following commands.

Aptech1#**configure terminal**

Aptech1(config)#**ip access-list extended SITE1-SITE2-CACL**

Aptech1(config-ext-nacl)#**permit ip 172.16.0.0 0.0.255.255 172.17.0.0 0.0.255.255**

Aptech1(config-ext-nacl)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To configure a Crypto ACL in Aptech2 (to identify the traffic toaptech1), use the following commands.

Aptech2#**configure terminal**

Aptech2(config)#**ip access-list extended SITE2-SITE1-CACL**

Aptech2(config-ext-nacl)#**permit ip 172.17.0.0 0.0.255.255 172.16.0.0 0.0.255.255**

Aptech2(config-ext-nacl)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 6: Define Transform Sets

A Transform Set is used to define how the data traffic between IPSec peers is going to be protected in Child Tunnel (IPSec Tunnel).

• To configure Transform Set inaptech1, use following commands.

Aptech1#**configure terminal**

Aptech1(config)#**crypto ipsec transform-set SITE2-TS esp-aes esp-sha512-hmac**

Aptech1(cfg-crypto-trans)#**exit**

Aptech1(config)#**exit**

Aptech1#f

• To configure Transform Set in Aptech2, use following commands.

Aptech2#**configure terminal**

Aptech2(config)#**crypto ipsec transform-set SITE1-TS esp-aes esp-sha512-hmac**

Aptech2(cfg-crypto-trans)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 7: Define IKEv2 Profiles

IKEv2 Profiles are similar to IKEv1 ISAKMP Profile.

• To configure IKEv2 Profiles inaptech1, use following commands.

Aptech1#**configure terminal**

Aptech1(config)#**crypto ikev2 profile SITE2-PROFILE**

Aptech1(config-ikev2-profile)#**match identity remote address 192.168.0.2 255.255.255.255**

Aptech1(config-ikev2-profile)#**authentication local pre-share**

Aptech1(config-ikev2-profile)#**authentication remote pre-share**

Aptech1(config-ikev2-profile)#**keyring local KR-1**

Aptech1(config-ikev2-profile)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To configure IKEv2 Profiles in Aptech2, use following commands.

Aptech2#**configure terminal**

Aptech2(config)#**crypto ikev2 profile SITE1-PROFILE**

Aptech2(config-ikev2-profile)#**match identity remote address 192.168.0.1 255.255.255.255**

Aptech2(config-ikev2-profile)#**authentication local pre-share**

Aptech2(config-ikev2-profile)#**authentication remote pre-share**

Aptech2(config-ikev2-profile)#**keyring local KR-1**

Aptech2(config-ikev2-profile)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 8: Define Crypto Maps

Crypto Maps are used to connect all the pieces of IPSec configuration together. A Crypto Map consists of one or more entries. A Crypto Map is made up of Crypto ACL, Transform Set, Remote Peer, the lifetime of the data connections etc.

� To define Crypto Map inaptech1, use following commands.

Aptech1#**configure terminal**

Aptech1(config)#**crypto map CMAP-SITE2 10 ipsec-isakmp**

Aptech1(config-crypto-map)#**set peer 192.168.0.2**

Aptech1(config-crypto-map)#**set pfs group24**

Aptech1(config-crypto-map)#**set security-association lifetime seconds 3600**

Aptech1(config-crypto-map)#**set transform-set SITE2-TS**

Aptech1(config-crypto-map)#**set ikev2-profile SITE2-PROFILE**

Aptech1(config-crypto-map)#**match address SITE1-SITE2-CACL**

Aptech1(config-crypto-map)#**exit**

Aptech1(config)#**exit**

� To define Crypto Map in Aptech2, use following commands.

Aptech2#**configure terminal**

Aptech2(config)#**crypto map CMAP-SITE1 10 ipsec-isakmp**

Aptech2(config-crypto-map)#**set peer 192.168.0.1**

Aptech2(config-crypto-map)#**set pfs group24**

Aptech2(config-crypto-map)#**set security-association lifetime seconds 3600**

Aptech2(config-crypto-map)#**set transform-set SITE1-TS**

Aptech2(config-crypto-map)#**set ikev2-profile SITE1-PROFILE**

Aptech2(config-crypto-map)#**match address SITE2-SITE1-CACL**

Aptech2(config-crypto-map)#**exit**

Aptech2(config)#**exit**

Aptech2#

### Step 9: Activate Crypto Maps by applying the Crypto Map to Router's Interface

• To apply Crypto Map to the WAN Interface onaptech1, use following commands.

Aptech1#**configure terminal**

Aptech1(config)#**interface gi0/0**

Aptech1(config-if)#**crypto map CMAP-SITE2**

Aptech1(config-if)#**exit**

Aptech1(config)#**exit**

Aptech1#

• To apply Crypto Map to the WAN Interface on Aptech2, use following commands.

Aptech2#**configure terminal**

Aptech2(config)#**interface gi0/0**

Aptech2(config-if)#**crypto map CMAP-SITE1**

Aptech2(config-if)#**exit**

Aptech2(config)#**exit**

Aptech2#

After configuring, initiate an IP traffic from device inside at Site-1 network to reach a device at Site-2 network. Your IPSec VPN Main mode IPSec tunnel will be built when any router find interesting traffic.