FlexVPN

FlexVPN Overview

FlexVPN

- Cisco’s IOS implementation of IKEv2
  - Unified configuration framework for L2L, Remote Access and Spoke - Spoke VPNs
    - Tunnel interfaces
- FlexVPN Components
  - Proposal, Policy, Credential Store, Profile
  - Tunnel interface
- Other Elements
  - IPsec Profile
  - Routing

FlexVPN/IKEv2 Proposal

- Set of algorithms used to protect IKE_SA_INIT
  - More than one function can be configured for the same security feature

```
crypto ikev2 proposal propname
  encryption  [3des|aes-cbc|aes-gcm*]
  integrity [md5|sha1|sha256|sha384|sha512]
  group [1|2|5|14|15|16|19**|20**|24]
  prf [md5|sha1|sha256|sha384|sha512]
```

  - * AES in Galois/Counter Mode (AES-GCM) is a combined-mode algorithm
    - Requires a PRF to be manually configured
  - ** DH Groups 19 and 20 are Elliptic Curve algorithms (ECDH)

FlexVPN/IKEv2 Policy

- Enables a Proposal
  - Policy can be matched based on FVRF or local IP addresses

crypto ikev2 policy *polname*
proposal *proname*
match fvrf [*fvrfname*|any]
match address local *IPv4/IPv6_address*

FlexVPN/IKEv2 Credential Store

- Stores authentication data
  - Trustpoint (**crypto pki trustpoint**)
  - Keys (can be now assymetric)
    - Keyring (**crypto ikev2 keyring**)
    - In-Profile (**authentication [local|remote] pre-share**)

crypto ikev2 keyring *kringname*
peer *peername*
hostname *name*
address *IPv4/IPv6_address*
identity [address|fqdn domain|email domain|key-id]
pre-shared-key [local|remote]

FlexVPN/IKEv2 Profile

+ Stores non-negotiable IKE parameters
  + Must be attached to an IPsec Profile

```
crypto ikev2 profile ikeprofname
  match [options]
  authentication [local|remote] [pre-share|rsa-sig|ecdsa-sig|eap]
  keyring kringname
  pki trustpoint tname [sign|verify]
  identity local [address|dn|email|fqdn|key-id]
  dpd interval [periodic|on-demand]
  virtual-template nr
  ivrf ivrfname
```

FlexVPN/IKEv2 Profile

- Profile Selection
  - Multiple „**match**” statements can be configured
    - IP address[es], certificate map, FVRF and IKEv2 ID
      - Same-type statements are ORed, different-type are ANDed
      - Certificate map and IKEv2 ID are treated as the same type

match vrf CUST1
match local address 10.1.1.1
match local address 10.2.2.1
match certificate CMAP1

  - Result : (VRF CUST1) **AND** (IP 10.1.1.1 **OR** 10.2.2.1) **AND** (cert match in CMAP1)

FlexVPN Tunnels

+ Static

interface tunnel *nr*
[ip|ipv6] address *address*
tunnel source [*interface*|*IP_address*]
tunnel destination *IP_address*
tunnel mode ipsec [ipv4|ipv6]

+ Dynamic

interface virtual-template type tunnel *nr*
[ip|ipv6] unnumbered *interface*
tunnel source [*interface*|*IP_address*]
tunnel mode ipsec [ipv4|ipv6]

IPsec Profile

- Activates IPsec
  - Requires a transform-set
  - IKEv2 Profile must be attached on the Initiator
    - Enables IKEv2

crypto ipsec transform-set *tset*
crypto ipsec profile *ipprofname*
set transform-set *tset*
set ikev2-profile *ikeprofname*

interface [tunnel *nr*|virtual-template type tunnel *nr*]
tunnel protection ipsec profile *ipprofname*

FlexVPN/IKEv2 Routing Options

- Static Routes
  - **[ip|ipv6] route**
- Dynamic Routing
  - RIP/RIPng, OSPF/OSPFv3, EIGRP/EIGRPv6, BGP/MGBP
- IKEv2 Routing
  - Implemented via IKEv2 Authorization Policy (**crypto ikev2 authorization policy**)
    - **route set [interface *ifname*|access-list *acl*|ipv6 *acl*]**
    - **route set remote [ipv4 *acl*|ipv6 *acl*]**

FlexVPN/IKEv2 Smart Defaults

- Simplifies IKEv2 Deployments
  - A group of pre-defined IKEv2 and IPsec components called „default”
    - Proposal, Policy, Transform Set, IPSec Profile, etc.
  - Verify with **show crypto ikev2 ... default** or **show run all**
    - E.g. **show crypto ikev2 proposal default**

FlexVPN

DMVPN over FlexVPN