Tunnel Templates

Tunnel templates allow a mobile router to carry multicast sessions to mobile networks as it roams. The Tunnel Templates for Multicast feature allows the configuration of multicast sessions on statically created tunnels to be applied to dynamic tunnels brought up on a home agent and a mobile router. A tunnel template is defined and applied to the tunnels between the home agent and the mobile router.

Reverse tunneling must be enabled from the mobile router to the home agent.

The following restrictions apply:

- Tunnels cannot be removed if they are being used as templates.
- This feature does not support mobile routers that are acting as mobile nodes.

Applying the Tunnel Template on the Home Agent

To apply the tunnel template to the tunnels brought up at the home agent, use the **interface tunnel** command. For example:

```
wd>enable
wd>password                                    ! If prompted
wd#configure terminal
wd(config)#ip multicast-routing          ! Enables IP multicast routing.
wd(config)#interface tunnel interfacenumber! Designates a tunnel interface and enters
interface configuration mode. This is the tunnel template that will be applied to the
mobile networks.
wd(config-in)#ip pim sparse-mode         ! Enables Protocol Independent Multicast (PIM)
on the tunnel interface in sparse mode.
wd(config)#exit
wd(config)#router mobile                 ! Enables Mobile IP on the router.
wd(config)#ip mobile mobile-networks     ! Configures mobile networks for the mobile host
and enters mobile networks configuration mode.
wd(config)#tunnel template interfacenumber! Designates the tunnel template to apply during
registration. The interfacenumber argument is set to the tunnel template.
wd(config)#end
```

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Use the **show ip mobile tunnel** command to display the active tunnels. The following example displays the active Mobile IP tunnels and the template configuration for the tunnel on the home agent:

```
Router# show ip mobile tunnel

Mobile Tunnels:

Total mobile ip tunnels 2
Tunnel1:
    src 1.1.1.1, dest 20.20.0.1
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1460 bytes
    Path MTU Discovery, mtu:0, ager:10 mins, expires:never
    outbound interface Tunnel0
    HA created, fast switching enabled, ICMP unreachable enabled
    27 packets input, 2919 bytes, 0 drops
    24 packets output, 2568 bytes
Running template configuration for this tunnel:
ip pim sparse-dense-mode

Tunnel0:
    src 1.1.1.1, dest 30.30.10.2
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu:0, ager:10 mins, expires:never
    outbound interface Ethernet1/3
    HA created, fast switching enabled, ICMP unreachable enabled
    0 packets input, 0 bytes, 0 drops
    24 packets output, 3048 bytes
```

Applying the Tunnel Template on the Mobile Router

To apply the tunnel template to the tunnels brought up at the mobile router, follow this example:

```
wd>enable
wd>password                                   ! If prompted
wd#configure terminal
wd(config)#ip multicast-routing          ! Enables IP multicast routing.
wd(config)#interface tunnel interfacenumber! Designates a tunnel interface and enters
interface configuration mode. This is the tunnel template that will be applied to the
mobile networks.
wd(config-in)#ip pim sparse-mode         ! Enables Protocol Independent Multicast (PIM)
on the tunnel interface in sparse mode.
wd(config)#exit
wd(config)#router mobile                 ! Enables Mobile IP on the router.
wd(config)#ip router mobile              ! Enables the mobile router and enters mobile
router configuration mode.
wd(config)#tunnel template interfacenumber! Designates the tunnel template to apply during
registration. The interfacenumber argument is set to the tunnel template.
wd(config)#end
```

Use the **show ip mobile tunnel** command to display the active tunnels.

Example Configuration

In the following example configuration, a tunnel template is defined and configured to be brought up at the home agent and mobile router. The foreign agent does not require any additional configuration to support the Cisco Mobile Networks—Tunnel Templates for Multicast feature.

Home Agent

```
ip multicast-routing
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
! Tunnel template to be applied to mobile networks
interface tunnel100
 ip address 13.0.0.1 255.0.0.0
 ip pim sparse-mode
!
router mobile
ip mobile mobile-networks 11.1.0.1
 description jet
 network 11.1.2.0 255.255.255.0
 network 11.1.1.0 255.255.255.0
! Select tunnel template to apply during registration
 template tunnel100
!
ip mobile secure host 11.1.0.1 spi 101 key hex 12345678123456781234567812345678 algorithm
md5 mode prefix-suffix
!
no ip mobile tunnel route-cache
```

Mobile Router

```
ip multicast-routing
!
interface Loopback0
 ip address 11.1.0.1 255.255.255.255
 ip pim sparse-mode
!
! Tunnel template to be applied to mobile networks
interface tunnel 100
 no ip address
 ip pim sparse-mode
!
interface Ethernet1/1
 ip address 20.0.0.1 255.0.0.0
 ip pim sparse-mode
 ip mobile router-service roam
!
router mobile
ip pim rp-address 7.7.7.7
ip mobile secure home-agent 1.1.1.1 spi 102 key hex 23456781234567812345678123456781
algorithm md5 mode prefix-suffix
ip mobile router
 address 11.2.0.1 255.255.0.0
 home-agent 1.1.1.1
! Select tunnel template to apply during registration
 template tunnel 100
 register extend expire 5 retry 2 interval 15
 register lifetime 10000
 reverse-tunnel
```

Applying Tunnel Templates to the IPSec Two-box Solution

Configuring IPSec in conjunction with Cisco IOS Mobile Network software requires special attention because the egress interface of the traffic can change and IPSec is typically configured on the egress interface. The previous recommendation had been to configure the crypto map on the loopback interface and to use policy routing to **set next hop loopback** for all traffic that needed encryption.

Note Applying a crypto map on a loopback interface is not a supported configuration (as documented in CSCdx79795).

Tunnel templates, introduced in Cisco IOS Release 12.2(15)T, add multicast support, but can be used to apply other parameters to the inner tunnel interface. Applying the crypto map to the tunnel template requires the **crypto map local-address** commands as shown in the following example configuration. The local address should be set to the home address interface. This recommendation eliminates the need for policy routing and allows for all traffic to be Cisco Express Forwarding (CEF) switched (which is not supported on loopback interfaces).

To be encrypted, all traffic from the mobile router must be reverse tunneled; the reverse tunnel becomes the egress interface at which the crypto map is applied.

Example Configuration

```
hostname MN
!
crypto isakmp policy 10
    encr aes
    authentication pre-share
    group 2
    lifetime 900
crypto isakmp key skeleton
!
address 192.168.1.1
crypto ipsec transform-set aes esp-aes 256 esp-sha-hmac
!
! Local-address must point to the Home Address
!
crypto map MAR_VPN local-address Loopback 0
crypto map MAR_VPN 1 ipsec-isakmp
    set peer 192.168.1.1
    set transform-set aes
    match address 110
!
interface Tunnel99
    description Mobile Networks Tunnel Template
    no ip address
    crypto map MAR_VPN
!
interface LoopbackO
    ip address 192.168.100.10 255.255.255.255
!
interface EthernetO/O
    ip address 169.254.255.1 255.255.255.255
    ip mobile router-service roam
!
interface Ethernet1/0
description Mobile Network
    ip address 192.168.124.1 255.255.255.0
!
```

```
router mobile
!
ip mobile secure home-agent 192.168.1.2 spi 100 key hex 1234567890abcdef1234567890abcdef
algorithm md5 mode prefix-suffix
ip mobile router
    address 192.168.100.10 255.255.255.0
    home-agent 192.168.1.2
    mobile-network Ethernet1/0
!
! Tunnel Template where the crypto map is applied
!
    template Tunnel99
!
! Reverse tunneling must be enabled or traffic will not exit via the tunnel
!
    reverse-tunnel
!
access-list 110 permit ip any host 192.168.2.2
!
end
```

Validating the Configuration

The configuration can be validated by using the **show ip mobile router** command to identify the tunnel interface that is being used by the mobile router, Then use the **show crypto ipsec sa interface tunnel** *n* command to verify that the relevant SAs are active. The important sections have been emphasized in the following sample output.

```
MN#show ip mobile router
Mobile Router
    Enabled 10/18/05 18:50:54
    Last redundancy state transition NEVER

Configuration:
    Home Address 192.168.100.10 Mask 255.255.255.0
    Home Agent 192.168.1.2 Priority 100 (best) (current)
    Registration lifetime 65534 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Extend Expire 120, Retry 3, Interval 10
    Reverse tunnel required
    Mobile Networks:Loopback2 (192.168.123.0/255.255.255.0)
                    Ethernet1/0 (192.168.124.0/255.255.255.0)

Monitor:
    Status -Registered
    Active foreign agent 192.168.6.1, Care-of 192.168.6.1 On interface EthernetO/O
    TunnelO mode IP/IP
```

```
MN#show crypto ipsec sa interface tunnel 0
interface: Tunnel 0
    Crypto map tag: MAR_VPN, local addr 192.168.100.10
protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.2/255.255.255.255/0/0)
current-peer 192.168.1.1 port 500
    PERMIT, flags={)
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
        local crypto endpt.: 192.168.100.10, remote crypto endpt.: 192.168.1.1
        path mtu 1514, ip mtu 1514
        current outbound spi: OxC8D41EOA(336934452~)
inbound esp sas:
    spi: OxB7BClB29 (3082558249)
        transfor.m: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:l, crypto map: MAR_VPN
        sa timdng: remaining key lifetime (k/sec): (4602927/3584) IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
inbound ah sas:
inbound pcp sas:
outbound esp sas:
    spi: OxC8D41EOA(3369344522)
        transfor.m: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: SW:2, crypto map: MAR VPN
        sa timdng: remaining key lifetime (k/sec): (4602928/3582) IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
outbound ah sas:
outbound pcp sas:
protected vrf:(none).
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.2,255.255.255.255/0/0) current-peer
192.168.1.1 port 500
        PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 8, #recv errors 0
    local crypto endpt,:192.168.100.10, remote crypto endpt.: 192.168.1.1
    path mtu 1514, ip mtu 1514
    current outbound spi: 0x0(0)

    inbound esp sas:
    inbound ah sas:
    inbound pcp sas:
    outbound esp sas:
    outbound ah sas:
    outbound pcp sas:
```

Related Documents

Cisco Mobile Networks Tunnel Templates for Multicast

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008045516 4.html

Other Configuration Tasks in the Cisco Mobile Wireless Home Agent Feature Guide

http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/products_feature_guide_chapter09186a008 05eb0d4.html