APPENDIX C

Configuration Supplement—Dynamic Crypto Maps, Reverse Route Injection

This configuration supplement illustrates the head-end topology and configuration for an internal Cisco deployment of VoIP over IPSec for telecommuters in a SOHO implementation. The key features implemented in these examples include:

- Dynamic crypto maps (Digital Certificates required)
- IPSec appliances (router on a stick)
- Dual head-end routers for redundancy and availability
- Reverse Route Injection and IKE keepalive
- HSRP provides a next hop address for a firewall

An advantage of the use of dynamic crypto maps eliminates the need to make changes on the head-end routers as additional remote routers are deployed. The remote routers initiate the IPSec session to the peers defined in their configuration as devices on the remote LAN attempt to connect to resources at the corporate headquarters. In this implementation, Cisco 7960 IP Phones are installed on the SOHO LAN, their Skinny Protocol (connecting to TCP port 2000) with the headquarters CallManager generates *background* traffic, so the IKE and IPSec security associations are re-established at the end of their lifetimes. So the presence of the IP phone on the SOHO LAN allows the headquarters network administrator to telnet to the LAN interface of the SOHO router, even if the remote router is deployed in a home office and no one is home using the VPN connection.

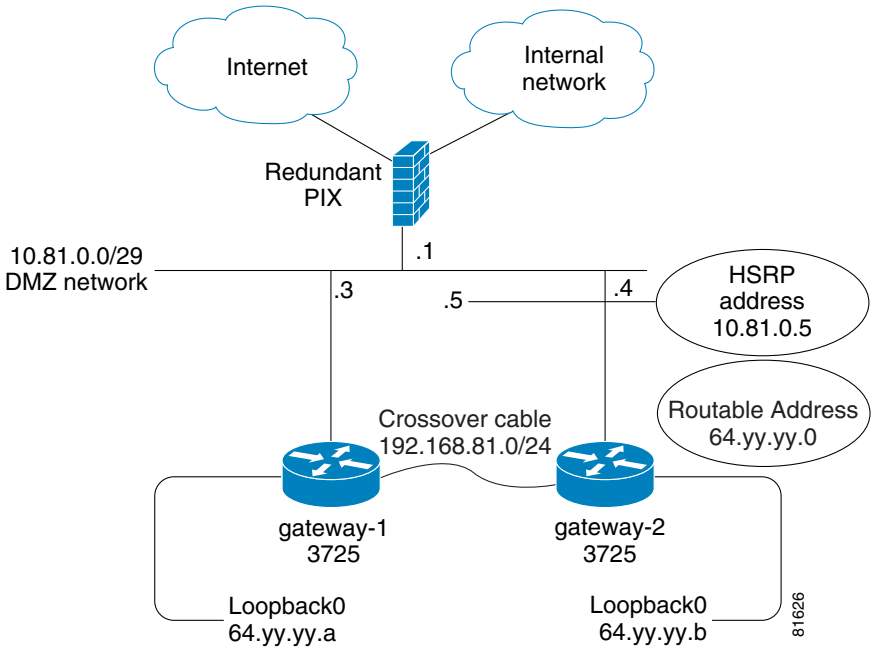
The head-end IPSec routers are configured and managed by an engineer in a separate organization from the IT support group which manages the Internet connectivity and firewall configuration. This is common in many enterprise networks, security responsibilities are routinely separated from internetworking support staff. As such, the head-end routers are truly *routers-on-a-stick*, as they have a single Fast Ethernet interface for connectivity to the enterprise core. The entire enterprise's traffic does not route through these head-end routers, only IP traffic which must be encrypted or decrypted between the headquarters and the remote SOHO users. Note the use of the **ip route-cache same-interface** command to avoid process switching in the router on a stick configuration.

The remote routers are configured with two IPSec peers defined in their crypto maps and IKE keepalives are configured to allow the remote routers a means to verify the availability of the head-end peers. During implementation it was observed that all the peers did not maintain an affinity to the first configured peer. The remote routers tend to *flip flop* between configured peers as short service disruptions to the home users cause IKE packet loss with the first configured peer. As the remote routers attempt to connect to the second peer, they often are successful with the second peer, so the IPSec session is established to that peer.

While the home user does not generally notice this *flip-flop*, it does present a routing issue if the IPSec session is established to the head-end router that is not the active HSRP router. To address this, the head-end routers are connected with a point to point Fast Ethernet interface and a simple CAT5 cross-over cable. Reverse Route Injection (RRI) is configured on the head-end crypto map and EIGRP is configured with the network address of the cross-over interfaces. Each head-end router redistributes the home user static routes inserted in the routing table by RRI. EIGRP advertises these injected routes to the other head-end router over the cross-over cable interface as an EIGRP external route (administrative distance 170).

The head-end topology is shown in Figure C-1.

Figure C-1 Head-end Topology Diagram



Note The IP addresses used in Figure C-1 and configuration examples in this section (such as 64.yy.yy.a) *must* be public, routable IP addresses. They are shown here with alphabetic characters to avoid using real public addresses in the examples.

Visualize the path of a packet from the headquarters CallManager to the remote IP phone when the IPSec session is not on the active HSRP router. The firewall forwards the packet to the HSRP active router—IP address 10.81.0.5. This router, *gateway-1,* has an EIGRP external route in the routing table for the remote user's subnet, learned over the cross-over interface from *gateway-2*. The packet are forwarded to *gateway-2*, which is the active IPSec peer for that remote subnet. The routing table for *gateway-2* includes the RRI injected static route in the routing table. These static routes are recursive routes to the 0/0 (default) route out the Fast Ethernet interface (the *stick* interface) to the firewall. This interface has a crypto map configured. The packet matches the dynamic crypto map's access list and is encrypted in the IPSec tunnel to the remote router again via the firewall shown above.

Packets from the remote IP phone to the headquarters CallManager, are encrypted in the IPSec tunnel in our example which is peered with *gateway-2* public address 64.yy.yy.b. The firewall has a static route to this public address via 10.81.0.4. The packet is decrypted and routed out the same interface and back to the firewall to be routed to the CallManager in headquarters

If the above topology is implemented as shown, the only single point of failure is the cross-over cable between the two head-end IPSec routers. If the cable is removed or the interfaces fail, IPSec traffic to the standby HSRP router is *black holed*. Using two cross-over cables and two interfaces between the two head-end IPSec routers would eliminate the single point of failure.

Configure IKE keepalives on the head-end IPSec routers and the remote routers. Missed IKE keepalives on the head-end routers trigger removal of the RRI static routes

From the firewall perspective, only ESP (protocol 50) and IKE (UDP port 500) need be permitted to the loopback (public) interfaces of the two head-end IPSec routers, all other packets can be denied from the Internet. The Internet, Internal network and firewall topology is simplified for purposes of illustration.

The following configuration example shows the relevant routing and crypto configuration for each head-end router. The certificate portion of the crypto configuration is not shown for brevity.

```
!
hostname gateway-1
!
crypto isakmp policy 1
 encr 3des
crypto isakmp keepalive 10
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode transport
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
!
crypto dynamic-map dmap 10
 set transform-set t1 t2
 reverse-route
!
crypto map test local-address Loopback0
crypto map test 1 ipsec-isakmp dynamic dmap
!
interface Loopback0
 description Public address
 ip address 64.yy.yy.a 255.255.255.255
!
interface FastEthernet0/0
 description Private
 ip address 10.81.0.3 255.255.255.248
 no ip redirects
 ip route-cache same-interface
 standby 1 ip 10.81.0.5
 standby 1 priority 120
 standby 1 preempt
 crypto map test
!
interface FastEthernet0/1
 description X-Over cable to gateway-2
 ip address 192.168.81.3 255.255.255.0
!
router eigrp 64
 redistribute static metric 1000 100 255 1 1500 route-map RRI
 passive-interface FastEthernet0/0
 network 192.168.81.0
 no auto-summary
 eigrp log-neighbor-changes
 no eigrp log-neighbor-warnings
!
ip route 0.0.0.0 0.0.0.0 10.81.0.1
!
access-list 1 remark Home user address pool(s)
```

```
access-list 1 remark 10.81.2.0 / 23
access-list 1 remark 10.81.4.0 / 22
access-list 1 permit 10.81.2.0 0.0.1.255
access-list 1 permit 10.81.4.0 0.0.3.255
access-list 1 deny any
!
route-map RRI permit 10
 description Redistribute remote subnets from RRI
 match ip address 1
!
end
```

This sample configuration is for the second head-end router. When both routers are operational, this router is the standby HSRP router, as its HSRP priority is configured as 110 verses 120 for *gateway-1*.

```
!
hostname gateway-2
!
crypto isakmp policy 1
 encr 3des
crypto isakmp keepalive 10
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode transport
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
!
crypto dynamic-map dmap 10
 set transform-set t1 t2
 reverse-route
!
crypto map test local-address Loopback0
crypto map test 1 ipsec-isakmp dynamic dmap
!
interface Loopback0
 description Public address
 ip address 64.yy.yy.b 255.255.255.255
!
interface FastEthernet0/0
 description Private
 ip address 10.81.0.4 255.255.255.248
 no ip redirects
 ip route-cache same-interface
 standby 1 ip 10.81.0.5
 standby 1 priority 110
 standby 1 preempt
 crypto map test
!
interface FastEthernet0/1
 ip address 192.168.81.4 255.255.255.0
!
router eigrp 64
 redistribute static metric 1000 100 255 1 1500 route-map RRI
 passive-interface FastEthernet0/0
 network 192.168.81.0
 no auto-summary
 eigrp log-neighbor-changes
 no eigrp log-neighbor-warnings
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.81.0.1
!
access-list 1 remark Home user address pool(s)
```

```
access-list 1 remark 10.81.2.0 / 23
access-list 1 remark 10.81.4.0 / 22
access-list 1 permit 10.81.2.0 0.0.1.255
access-list 1 permit 10.81.4.0 0.0.3.255
access-list 1 deny any
!
route-map RRI permit 10
 description Redistribute remote subnets from RRI
 match ip address 1
!
end
```

Now an example of the relevant portion of a remote SOHO router. All packets from the LAN subnet 10.81.2.0/29 are encrypted. Note the two peers defined in the crypto map, these IP addresses are the Internet routable IP addresses from the two head-end IPSec peers. IKE connections are attempted in the order the peers appear in the crypto map.

```
!
hostname soho-vp
!
crypto isakmp policy 1
encr 3des
crypto isakmp keepalive 10
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
!
crypto map test 1 ipsec-isakmp
description plain ol' ipsec
set peer 64.yy.yy.a
set peer 64.yy.yy.b
set transform-set t1
match address 101
qos pre-classify
!
access-list 101 remark ---------Crypto Map ACL------------
access-list 101 permit ip 10.81.2.0 0.0.0.7 any
!
end
!
```

Included here are displays from the remote and head-end routers to illustrate their configuration and normal state. First, the remote router. Note from the following crypto map display there are two peers defined and the current peer is indicated. In the IKE SA display, the destination (*dst)* address is the current peer's public (loopback 0) address and the source (*src*) address is the IP address on the outside Ethernet 0 interface. In this case the IP address is being assigned to this router by an upstream router that supports IPSec Pass-thru. This remote router is connected to the Internet via a 3rd party DSL modem.

```
router-vpn#show crypto map
Crypto Map "test" 1 ipsec-isakmp
        Description: plain ol' ipsec
        Peer = 64.yy.yy.a
        Peer = 64.yy.yy.b
        Extended IP access list 101
            access-list 101 permit ip 10.81.2.0 0.0.0.7 any
        Current peer: 64.yy.yy.a
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                t1,
        }
        QOS pre-classification
        Interfaces using crypto map test:
                Ethernet0
```

```
router-vpn#show crypto isakmp sa
dst             src             state          conn-id    slot
64.yy.yy.a    192.168.1.102   QM_IDLE            108       0
```

Displaying the IKE SA from the head-end peer router, notice the source address (*src*) 165.x.x.x this is the routable IP address of the above remote router, which 192.168.1.102 was translated to by the IPSec Pass-thru router.

```
gateway-1#show crypto isakmp sa
dst             src             state          conn-id    slot
64.yy.yy.a    165.x.x.x  QM_IDLE             16       0
```

From the head-end router, display the crypto map for the remote router. As this configuration uses dynamic crypto maps and the ISP assigns IP addresses for the remote routers, displaying the crypto map on the head-end router displays the access list that identifies packets to be encrypted. The access list entry identifies the remote subnet. For management and troubleshooting purposes, documenting the cross reference between remote subnet and the router's hostname is beneficial.

```
gateway-1#show crypto map
Crypto Map: "test" idb: Loopback0 local address: 64.yy.yy.a

Crypto Map "test" 1 ipsec-isakmp
        Dynamic map template tag: dmap
Crypto Map "test" 191 ipsec-isakmp
        Peer = 165.x.x.x
        Extended IP access list
            access-list  permit ip any 10.81.2.0 0.0.0.7
            dynamic (created from dynamic map dmap/10)
        Current peer: 165.x.x.x
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ t1, }
        Reverse Route Injection Enabled
```

Now look at the routing table. The RRI logic has inserted a static route for the remote subnet 10.81.2.0/29. There are two EIGRP external routes (10.81.2.24/29 and 10.81.2.48/29) learned from the second head-end router (*gateway-2*) as a result of the re-distribution of the RRI static routes. Looking at the routing table and the resulting static (or EIGRP external routes) provides a quick reference of the remote routers peered with this head-end router. Look for static routes for the remote subnets and the number of remote routers that are peered with the second head-end router (identified by the EIGRP external subnets).

```
gateway-1#show ip route

Gateway of last resort is 10.81.0.1 to network 0.0.0.0

     64.0.0.0/32 is subnetted, 1 subnets
C       64.yy.yy.a is directly connected, Loopback0
C    192.168.81.0/24 is directly connected, FastEthernet0/1
     10.0.0.0/29 is subnetted, 7 subnets
D EX    10.81.2.24 [170/2588160] via 192.168.81.4, 00:50:58, FastEthernet0/1
S       10.81.2.16 [1/0] via 0.0.0.0, FastEthernet0/0
S       10.81.2.0 [1/0] via 0.0.0.0, FastEthernet0/0
C       10.81.0.0 is directly connected, FastEthernet0/0
D EX    10.81.2.48 [170/2588160] via 192.168.81.4, 1d07h, FastEthernet0/1
S       10.81.2.40 [1/0] via 0.0.0.0, FastEthernet0/0
S       10.81.2.32 [1/0] via 0.0.0.0, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.81.0.1
```

Another perspective is found by comparing the RRI static routes on the second head-end route and the access-list entries from the crypto map.

```
gateway-2#show ip route

Gateway of last resort is 10.81.0.1 to network 0.0.0.0

     64.0.0.0/32 is subnetted, 1 subnets
C       64.yy.yy.b is directly connected, Loopback0
C    192.168.81.0/24 is directly connected, FastEthernet0/1
     10.0.0.0/29 is subnetted, 7 subnets
S       10.81.2.24 [1/0] via 0.0.0.0, FastEthernet0/0
D EX    10.81.2.16 [170/2588160] via 192.168.81.3, 1d08h, FastEthernet0/1
D EX    10.81.2.0 [170/2588160] via 192.168.81.3, 07:26:03, FastEthernet0/1
C       10.81.0.0 is directly connected, FastEthernet0/0
S       10.81.2.48 [1/0] via 0.0.0.0, FastEthernet0/0
D EX    10.81.2.40 [170/2588160] via 192.168.81.3, 05:48:36, FastEthernet0/1
D EX    10.81.2.32 [170/2588160] via 192.168.81.3, 03:51:48, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 10.81.0.1

gateway-2#show crypto map | include access-list
           access-list  permit ip any 10.81.2.48 0.0.0.7
           access-list  permit ip any 10.81.2.24 0.0.0.7
```

To test failover in the lab assessment, a remote user was in a phone conversation with an IP phone at the central site. The head-end router supporting the remote user (the standby HSRP router) was reloaded. It took approximately 23 seconds for the conversation to be audible in both directions. Then with the remote user peered with the HSRP active router, it was reloaded. It took approximately 31 seconds for the conversation to be audible in both directions. This test was conducted with only a few active remote routers. It was not a scale test, but rather a proof of concept test for this configuration.