Cisco IOS Server Load Balancer Configuration for Dynamic Virtual Tunnel Interface Hub

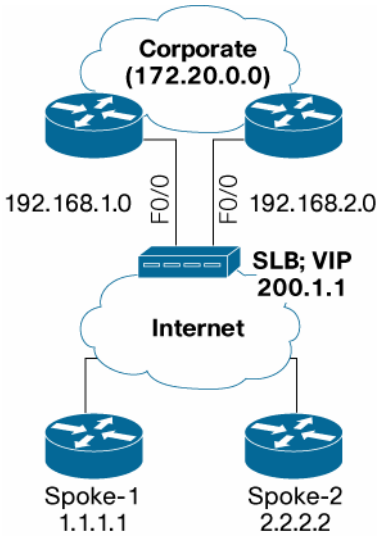
This document provides configuration guidance for configuring the Cisco IOS® Server Load Balancer (SLB) feature to distribute large numbers of IP Security (IPsec) tunnels onto a Cisco® 7200/7301 IPsec server farm. The server farm hubs are configured with dynamic Virtual Tunnel Interface (VTI) while the remote spokes can be configured using VTI or crypto maps (supporting single proxy).

1. Audience

This configuration guide is intended to provide best practices and configuration guidelines for Cisco customers, Systems® engineers and customer support engineers.

2. Network Topology

Figure 1. Topology



3. System Components

- Tested version on IPsec hubs: Cisco IOS Software Release 12.4(4)T1
- Tested version on 6500 SLB: Cisco IOS Software Release 12.2(18)SXF
- Tested version on the spokes (crypto maps): Cisco IOS Software Release 12.2(15)T14

4. SLB Configuration

```
!
! Failure detection mechanism is set to ICMP. Failure to respond to
! three pings will change the status of IPsec server to DOWN
!
ip slb probe PING-PROBE ping
 faildetect 3
!
! Define the REAL servers in the server farm. Least loaded server
! will accept new connection. If the server fails, all the connection
! entries will be purged. Max Connections on the servers are set to
! 500 (per server).
!
ip slb serverfarm 7301-FARM
 predictor leastconns
 failaction purge
 probe PING-PROBE
 !
 real 192.168.1.1
  weight 1
  maxconns 500
  inservice
 !
 real 192.168.2.1
  weight 1
  maxconns 500
  inservice
!
! Define ESP and ISAKMP (500 and 4500) to be load balanced on these
! servers. To add stickiness between ISAKMP and IPsec, “sticky”
! command is used. IKE and IPsec sessions should never go to two
! different servers. This stickiness should be maintained more than
! the IPsec re-key interval. If the stickiness time is not long
! enough, both the sessions might initially go to same routers but
! when IPsec re-keys after 1 hour, IPsec session can end up on wrong
! server. Similarly idle time is set to a little more than IPsec
! re-key interval to avoid accidental clearance of the connection on
! the SLB. Virtual IP address defined is 200.1.1.1.
!
ip slb vserver ESP
 virtual 200.1.1.1 esp
 serverfarm 7301-FARM
 sticky 3650 group 1
 idle 3660
 inservice
!
ip slb vserver ISAKMP
 virtual 200.1.1.1 udp isakmp
```

```
 serverfarm 7301-FARM
 sticky 3650 group 1
 idle 3660
 inservice
!
ip slb vserver NAT-T
 virtual 200.1.1.1 udp 4500
 serverfarm 7301-FARM
 sticky 3650 group 1
 idle 3660
 inservice
!
```

5. Dynamic VTI Configuration

5.1. Basic IPsec Configuration

```
crypto keyring all
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 60
!
crypto ipsec transform-set SHA_3DES esp-3des esp-sha-hmac
!
crypto ipsec profile vti
 set transform-set SHA_3DES
!
```

5.2. ISAKMP Profile Configuration

```
crypto isakmp profile IPSEC-DVTI
   keyring all
   match identity address 0.0.0.0
   virtual-template 1
!
```

5.3. Virtual Tunnel Interface Configuration

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vti
```

5.4. Loopback Interface

```
!
! The VIP address on the SLB is defined as the Loopback address on the
IPsec Server
! IPsec tunnels are sourced from this address and SLB pings this
address to
! determine IPsec Server availability.
!
interface Loopback0
 ip address 200.1.1.1 255.255.255.255
!
```

6. SLB Verification

6.1. Show Commands on SLB (No Connections)

SLB#sh ip slb serverfarms

```
server farm    predictor         nat   reals   bind id  interface(s)
-------------------------------------------------------------------------
7301-FARM      LEASTCONNS        none  2       0        <any>
```

SLB#sh ip slb reals

```
Real                  farm name       weight   state          conns
-------------------------------------------------------------------
192.168.1.1           7301-FARM        1       OPERATIONAL    0
192.168.2.1           7301-FARM        1       OPERATIONAL    0
```

SLB#sh ip slb vservers

```
slb vserver  prot  virtual            state        cons  interface(s)
-------------------------------------------------------------------------
ESP          ESP   200.1.1.1/32:0     OPERATIONAL  0     <any>
ISAKMP       UDP   200.1.1.1/32:500   OPERATIONAL  0     <any>
NAT-T        UDP   200.1.1.1/32:4500  OPERATIONAL  0     <any>
```

SLB#sh ip slb conn

```
Vserver       prot client            real          state          nat
-------------------------------------------------------------------------
```

6.2. Show Commands on SLB (With Connections)

SLB#sh ip slb conn

```
Vserver       prot client           real          state         nat
---------------------------------------------------------------------
ESP           ESP  1.1.1.1:0        192.168.1.1   ESTAB         none
ISAKMP        UDP  1.1.1.1:500      192.168.1.1   ESTAB         none
ESP           ESP  2.2.2.2:0        192.168.2.1   ESTAB         none
ISAKMP        UDP  2.2.2.2:500      192.168.2.1   ESTAB         none
```

SLB#sh ip slb vserver

```
slb vserver  prot  virtual            state        cons  interface(s)
---------------------------------------------------------------------
ESP          ESP   200.1.1.1/32:0     OPERATIONAL   2     <any>
ISAKMP       UDP   200.1.1.1/32:500   OPERATIONAL   2     <any>
NAT-T        UDP   200.1.1.1/32:4500  OPERATIONAL   0     <any>
```

SLB#sh ip slb reals

```
Real                 farm name       weight   state         conns
---------------------------------------------------------------------
192.168.1.1          7301-FARM        1       OPERATIONAL    2
192.168.2.1          7301-FARM        1       OPERATIONAL    2
```

SLB#sh ip slb stick

```
        ip/netmask    id       cons    server real      firewall real
---------------------------------------------------------------------
        1.1.1.1/32    1        2       192.168.1.1
        2.2.2.2/32    1        2       192.168.2.1
```

7. IPsec Verification

7.1. IPsec-1 Show Commands

```
IPsec-1#sh cry isa sa

IPv4 Crypto ISAKMP SA
Dst             src             state          conn-id slot status
200.1.1.1       1.1.1.1         QM_IDLE           1009    0 ACTIVE

IPsec-1#sh cry ipsec sa

interface: Virtual-Access2
    Crypto map tag: Virtual-Access2-head-0, local addr 200.1.1.1

   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): (10.1.1.0/255.255.255.0/0/0)
   current_peer 1.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #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.: 200.1.1.1, remote crypto endpt.: 1.1.1.1
     path mtu 1514, ip mtu 1514
     current outbound spi: 0x43C4D43C(1136972860)

     inbound esp sas:
      spi: 0x6961ED15(1768025365)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 15, flow_id: SW:15,
        crypto map: Virtual-Access2-head-0
        sa timing: remaining key lifetime (k/sec): (4435562/3364)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x43C4D43C(1136972860)
```

```
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 16, flow_id: SW:16,
        crypto map: Virtual-Access2-head-0
        sa timing: remaining key lifetime (k/sec): (4435562/3363)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

IPsec-1#sh ip rou

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
       L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.1.254 to network 0.0.0.0

     200.1.1.0/32 is subnetted, 1 subnets
C       200.1.1.1 is directly connected, Loopback0
     172.20.0.0/24 is subnetted, 1 subnets
C       172.20.1.0 is directly connected, FastEthernet0/1
     10.0.0.0/24 is subnetted, 1 subnets
S       10.1.1.0 [1/0] via 0.0.0.0, Virtual-Access2
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.1.254
```

IPsec-1#sh int virtual-access 2

```
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback0 (200.1.1.1)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x0, loopback not set
  Keepalive not set
  Tunnel source 200.1.1.1 (Loopback0), destination 1.1.1.1
  Tunnel protocol/transport IPSEC/IP
```

```
Tunnel TTL 255
Fast tunneling enabled
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPsec (profile “vti”)
Last input never, output never, output hang never
Last clearing of “show interface” counters 22:36:02
Input queue: 0/75/0/0 (size/max/drops/flushes);
Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   46 packets input, 4600 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   21 packets output, 2100 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
```

7.2. IPsec-2 Show Commands

```
IPsec-2#sh cry isa sa

IPv4 Crypto ISAKMP SA
Dst             src             state          conn-id slot status
200.1.1.1       2.2.2.2         QM_IDLE          13002    0 ACTIVE

IPsec-2#sh cry ipsec sa

interface: Virtual-Access2
    Crypto map tag: Virtual-Access2-head-0, local addr 200.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.20.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
   current_peer 2.2.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #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.: 200.1.1.1, remote crypto endpt.: 2.2.2.2
     path mtu 1514, ip mtu 1514
     current outbound spi: 0xA39C41F0(2744926704)
```

```
     inbound esp sas:
      spi: 0xF3B45D4(255542740)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: VAM2:7,
        crypto map: Virtual-Access2-head-0
        sa timing: remaining key lifetime (k/sec): (4392505/3072)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xA39C41F0(2744926704)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: VAM2:8,
        crypto map: Virtual-Access2-head-0
        sa timing: remaining key lifetime (k/sec): (4392505/3071)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

IPsec-2#sh ip rou

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
       L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.2.254 to network 0.0.0.0

     200.1.1.0/32 is subnetted, 1 subnets
C       200.1.1.1 is directly connected, Loopback0
     172.20.0.0/24 is subnetted, 1 subnets
C       172.20.1.0 is directly connected, FastEthernet0/1
     10.0.0.0/24 is subnetted, 1 subnets
```

```
S       10.1.2.0 [1/0] via 0.0.0.0, Virtual-Access2
C    192.168.2.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.2.254

IPsec-2#sh int virtual-access 2

Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback0 (200.1.1.1)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x0, loopback not set
  Keepalive not set
  Tunnel source 200.1.1.1 (Loopback0), destination 2.2.2.2
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPsec (profile “vti”)
  Last input never, output never, output hang never
  Last clearing of “show interface” counters 22:43:38
  Input queue: 0/75/0/0 (size/max/drops/flushes);
  Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     8 packets input, 800 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     8 packets output, 800 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

8. Related Documents

CDC Documentation:
http://www.cisco.com/en/US/netsol/ns482/networking_solutions_sub_solution.html

9. Appendix A

9.1. SLB Version

```
Cisco IOS Software
Cisco IOS s72033_rp Software (s72033_rp-ADVENTERPRISEK9_WAN-M),
Version 12.2(18)SXF, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Sat 10-Sep-05 00:33 by ccai
Image text-base: 0x40101040, data-base: 0x42D60000


ROM: System Bootstrap, Version 12.2(17r)S2, RELEASE SOFTWARE (fc1)
BOOTLDR: s72033_rp Software (s72033_rp-ADVENTERPRISEK9_WAN-M), Version
12.2(18)SXF, RELEASE SOFTWARE (fc1)


SLB uptime is 22 hours, 29 minutes
Time since SLB switched to active is 22 hours, 28 minutes
System returned to ROM by power cycle (SP by power on)
System restarted at 18:59:07 EST Wed Feb 1 2006
System image file is “disk0:s72033-adventerprisek9_wan-mz.122-18.SXF”


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply third-
party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are
unable to comply with U.S. and local laws, return this product
immediately.


A summary of U.S. laws governing Cisco cryptographic products may be
found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html


If you require further assistance please contact us by sending email
to export@cisco.com.


Cisco WS-C6506-E (R7000) processor (revision 1.0) with 983008K/65536K
bytes of memory
Processor board ID SAL08404LV3
SR71000 CPU at 600MHz, Implementation 0x504, Rev 1.2, 512 KB Layer 2
Cache
Last reset from power-on
SuperLAT software (copyright 1990 by Meridian Technology Corp)
X.25 software, Version 3.0.0
Bridging software
TN3270 emulation software
1 FlexWAN controller (2 FastEthernet)
2 Virtual Ethernet/IEEE 802.3 interfaces
2 FastEthernet/IEEE 802.3 interfaces
2 Gigabit Ethernet/IEEE 802.3 interfaces
1917 KB of nonvolatile configuration memory
```

```
8192 KB of packet buffer memory

65536 KB of flash internal SIMM (sector size 512 KB)
Configuration register is 0x2102
```

9.2. SLB Configuration

```
version 12.2
!
service counters max age 10
!
hostname SLB

!boot system disk0:s72033-adventerprisek9_wan-mz.122-18.SXF
!
no aaa new-model
ip subnet-zero
!
ip slb probe PING-PROBE ping
 faildetect 3
!
ip slb serverfarm 7301-FARM
 predictor leastconns
 failaction purge
 probe PING-PROBE
 !
 real 192.168.1.1
  weight 1
  maxconns 500
  inservice
 !
 real 192.168.2.1
  weight 1
  maxconns 500
 inservice
!
ip slb vserver ESP
 virtual 200.1.1.1 esp
 serverfarm 7301-FARM
 sticky 3650 group 1
 idle 3660
 inservice
!
ip slb vserver ISAKMP
 virtual 200.1.1.1 udp isakmp
 serverfarm 7301-FARM
 sticky 3650 group 1
 idle 3660
 inservice
!
```

```
ip slb vserver NAT-T
 virtual 200.1.1.1 udp 4500
 serverfarm 7301-FARM
 sticky 3650 group 1
 idle 3660
 inservice
!
ipv6 mfib hardware-switching replication-mode ingress
mls ip multicast flow-stat-timer 9
mls aging slb normal 20000
no mls flow ip
no mls flow ipv6
no mls acl tcam share-global
mls cef error action freeze
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
port-channel per-module load-balance
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
interface FastEthernet2/0/0
 description TO IPsec-1
 ip address 192.168.1.254 255.255.255.0
 full-duplex
!
interface FastEthernet2/1/0
 description TO IPsec-2
 ip address 192.168.2.254 255.255.255.0
 full-duplex
!
interface GigabitEthernet6/1
 description TO INTERNET
 ip address 110.1.1.1 255.255.255.0
 speed nonegotiate
!
interface GigabitEthernet6/2
 no ip address
 media-type rj45
 speed 100
 duplex full
!
```

```
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 110.1.1.2
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
 password lab
 login
!
no cns aaa enable
end
```

10. Appendix B

10.1 IPsec-1 Version

```
Cisco IOS Software, 7200 Software (C7200-JK9S-M), Version 12.4(4)T1,
RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 21-Dec-05 22:58 by ccai


ROM: System Bootstrap, Version 12.0(19990210:195103) [12.0XE 105],
DEVELOPMENT SOFTWARE
BOOTLDR: 7200 Software (C7200-BOOT-M), Version 12.0(10)S, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)


IPsec-1 uptime is 23 hours, 14 minutes
System returned to ROM by reload at 17:54:32 UTC Wed Feb 1 2006
Running default software
Last reload reason: Reload Command


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply third-
party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are
unable to comply with U.S. and local laws, return this product
immediately.


A summary of U.S. laws governing Cisco cryptographic products may be
found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html


If you require further assistance please contact us by sending email
to export@cisco.com.


Cisco 7206VXR (NPE300) processor (revision D) with 122880K/40960K
bytes of memory.
Processor board ID 20390414
R7000 CPU at 262 MHz, Implementation 39, Rev 1.0, 256 KB Layer 2 Cache
6 slot VXR midplane, Version 2.0


Last reset from power-on


PCI bus mb0_mb1 (Slots 0, 1, 3 and 5) has a capacity of 600 bandwidth
points.
Current configuration on bus mb0_mb1 has a total of 200 bandwidth
points.
This configuration is within the PCI bus capacity and is supported.


PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 0 bandwidth points.
This configuration is within the PCI bus capacity and is supported.
```

```
Please refer to the following document “Cisco 7200 Series Port Adaptor
Hardware Configuration Guidelines” on Cisco.com http://www.cisco.com
for Cisco 7200 Series Router bandwidth points oversubscription and
usage  guidelines.


2 FastEthernet interfaces
125 KB of NVRAM


47040 KB of ATA PCMCIA card at slot 0 (sector size 512 KB)
20480 KB of flash PCMCIA card at slot 1 (sector size 128 KB)
4096 KB of flash internal SIMM (sector size 256 KB)
Configuration register is 0x2102
```

10.2 IPsec-1 Configuration

```
version 12.4
no service password-encryption
!
hostname IPsec-1
!
boot-start-marker
boot system disk0:c7200-jk9s-mz.124-4.T1
boot-end-marker
!
!
no aaa new-model
!
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
crypto keyring all
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 60
crypto isakmp profile IPSEC-DVTI
   keyring all
   match identity address 0.0.0.0
   virtual-template 1
!
crypto ipsec transform-set SHA_3DES esp-3des esp-sha-hmac
!
crypto ipsec profile vti
```

```
 set transform-set SHA_3DES
!
interface Loopback0
 ip address 200.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex full
!
interface FastEthernet0/1
 ip address 172.20.1.1 255.255.255.0
 duplex full

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vti
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end
```

11. Appendix C

11.1 IPsec-2 Version

```
Cisco IOS Software, 7200 Software (C7200-JK9S-M), Version 12.4(4)T1,
RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 21-Dec-05 22:58 by ccai


ROM: System Bootstrap, Version 12.2(4r)B, RELEASE SOFTWARE (fc1)


IPsec-2 uptime is 1 day, 1 hour, 13 minutes
System returned to ROM by error - an Error Interrupt, PC 0x628F59A0 at
16:39:28 UTC Wed Feb 1 2006
System image file is “disk0:c7200-jk9s-mz.124-4.T1”



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply third-
party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are
unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be
found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html


If you require further assistance please contact us by sending email
to export@cisco.com.


Cisco 7206VXR (NPE400) processor (revision A) with 229376K/32768K
bytes of memory.
Processor board ID 23655916
R7000 CPU at 350 MHz, Implementation 39, Rev 3.3, 256 KB Layer 2 Cache
6 slot VXR midplane, Version 2.1


Last reset from power-on


PCI bus mb0_mb1 (Slots 0, 1, 3 and 5) has a capacity of 600 bandwidth
points.
Current configuration on bus mb0_mb1 has a total of 200 bandwidth
points.
This configuration is within the PCI bus capacity and is supported.


PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 600 bandwidth points
This configuration is within the PCI bus capacity and is supported.


Please refer to the following document “Cisco 7200 Series Port Adaptor
Hardware Configuration Guidelines” on Cisco.com http://www.cisco.com
```

```
for Cisco 7200 Series Router bandwidth points oversubscription and
usage guidelines.

2 FastEthernet interfaces
1 Virtual Private Network (VPN) Module
125 KB of NVRAM

46976 KB of ATA PCMCIA card at slot 0 (sector size 512 KB)
4096 KB of flash internal SIMM (sector size 256 KB)
Configuration register is 0x0 (will be 0x2102 at next reload)

IPsec-2#
```

11.2. IPsec-2 Version

```
version 12.4
no service password-encryption
!
hostname IPsec-2
!
boot-start-marker
boot system disk0:c7200-jk9s-mz.124-4.T1
boot-end-marker
!
no aaa new-model
!
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
!
controller ISA 4/1
!
crypto keyring all
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60
crypto isakmp profile IPSEC-DVTI
   keyring all
   match identity address 0.0.0.0
   virtual-template 1
!
!
```

```
crypto ipsec transform-set SHA_3DES esp-3des esp-sha-hmac
!
crypto ipsec profile vti
 set transform-set SHA_3DES
!
interface Loopback0
 ip address 200.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 description TO SLB
 ip address 192.168.2.1 255.255.255.0
 duplex full
!
interface FastEthernet0/1
 ip address 172.20.1.2 255.255.255.0
 duplex full
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vti
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.2.254
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end
```

12. Appendix D

12.1. Spoke Version

```
Cisco IOS Software
Cisco IOS Software for Cisco 2600 Series Routers (C2600-IK9O3S3-M),
Version 12.2(15)T14, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Sat 28-Aug-04 06:47 by cmong
Image text-base: 0x80008098, data-base: 0x81942B30


ROM: System Bootstrap, Version 12.2(7r) [cmong 7r], RELEASE SOFTWARE
(fc1)
ROM: C2600 Software (C2600-IK9O3S3-M), Version 12.2(15)T14, RELEASE
SOFTWARE (fc4)


S1 uptime is 24 weeks, 5 days, 2 hours, 3 minutes
System returned to ROM by power-on
System image file is "flash:c2600-ik9o3s3-mz.122-15.T14"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply third-
party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are
unable to comply with U.S. and local laws, return this product
immediately.


A summary of U.S. laws governing Cisco cryptographic products may be
found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html


If you require further assistance please contact us by sending email
to export@cisco.com.


Cisco 2651XM (MPC860P) processor (revision 0x100) with 125952 KB/5120
KB of memory
Processor board ID JAE07350BC0 (2764185207)
M860 processor: part number 5, mask 2
Bridging software
X.25 software, Version 3.0.0
2 FastEthernet/IEEE 802.3 interface(s)
1 serial network interface(s)
32 KB of nonvolatile configuration memory
32768 KB of processor board system flash (read/write)


Configuration register is 0x2102
```

12.2. Spoke Configuration

```
version 12.2
no service password-encryption
!
hostname S1
!
ip subnet-zero
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60
!
!
crypto ipsec transform-set SHA_3DES esp-3des esp-sha-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set SHA_3DES
 match address 100
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 speed 100
 full-duplex
 no keepalive
!
interface Serial0/0
 ip address 1.1.1.1 255.255.255.252
 crypto map mymap
!
ip classless
ip route 0.0.0.0 0.0.0.0 1.1.1.2
!
access-list 100 permit ip 10.1.1.0 0.0.0.255 any
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
end
```

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-342685-02 07/07

