DEPLOYMENT GUIDE

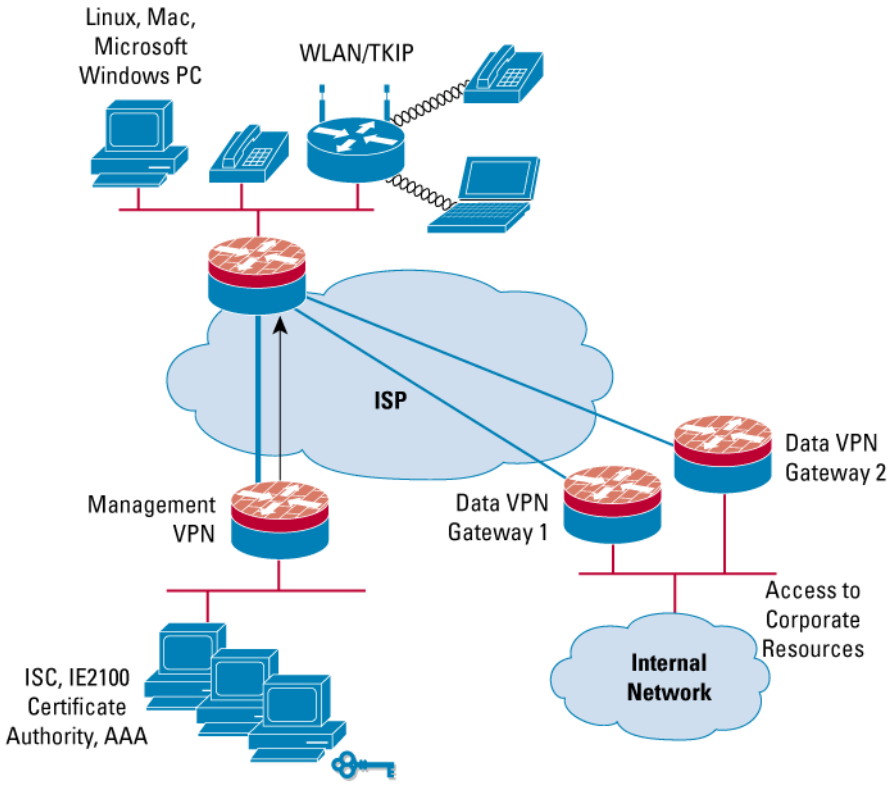
CISCO IOS IPSEC HIGH AVAILABILITY

The Cisco IOS® IPsec High Availability (IPsec HA) Enhancements feature provides an infrastructure for reliable and secure networks to provide transparent availability of the VPN gateways---that is, Cisco IOS Software–based routers. This feature works well for all IP Security (IPsec)-based networks. In an Enterprise-Class Teleworker (ECT) solution, which encompasses a Dynamic Multipoint VPN (DMVPN) architecture for data gateway infrastructure and plain IPsec for management gateway infrastructure, IPsec HA can be used to provide redundancy---that is, stateful failover and rollback of the gateways to provide uninterrupted management connectivity to the spokes. For more details about ECT deployment, please refer to the link given in the references section.

TOPOLOGY

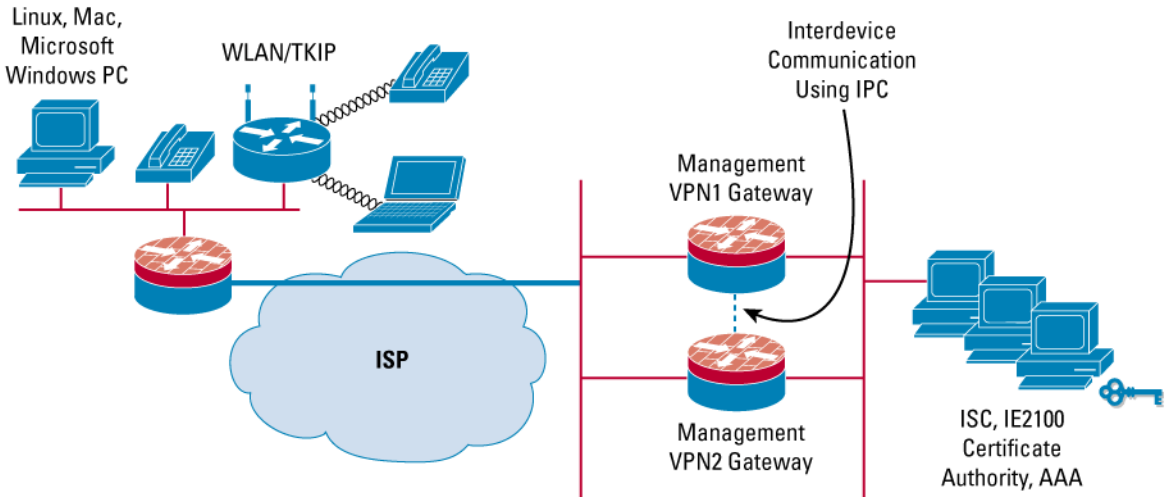
In a DMVPN deployment, IPsec HA can be incorporated in the management gateways. The topology shown in Figure 1 indicates the connectivity between spokes and management gateways. The current topology for a DMVPN deployment is given in Figure 1.

Figure 1. Original ECT Topology



Redundant management gateways can be deployed using IPsec HA as illustrated by the topology shown in Figure 2.

Figure 2. Deploying Redundant Management Gateways Using IPsec HA



The Hot Standby Router Protocol (HSRP) is used to achieve the redundancy between the management gateways. The spoke views the virtual IP address of the HSRP as the IP address of the management gateway. This setup allows any failover on management gateways to be transparent to the spoke. Once an IPsec session is established with the active router (management gateway), the corresponding session's Internet Key Exchange (IKE) Security Association (SAs) and IPsec SAs are sent to a standby router using IPC (Inter-Process Communication) and both active and standby routers maintain the spoke's session information. When the active management gateway goes down, the standby gateway becomes the active gateway and handles the IPsec sessions transparently. This arrangement avoids the need for session reestablishment.

IMAGES

IPsec HA is supported only on limited hardware. The hardware list includes Cisco 7200 VXR (NPE-400, NPE-G1) Series router, Cisco 7301 Router, and Cisco 3725 and 3745 multiservice access routers.

- Image on management gateway: Cisco IOS Software Release 12.3(11)T4; c3725-advipservicesk9-mz
- Image on spoke: Cisco IOS Software Release 12.3(8)T5; c831-k9o3sy6-mz.123-8.T5

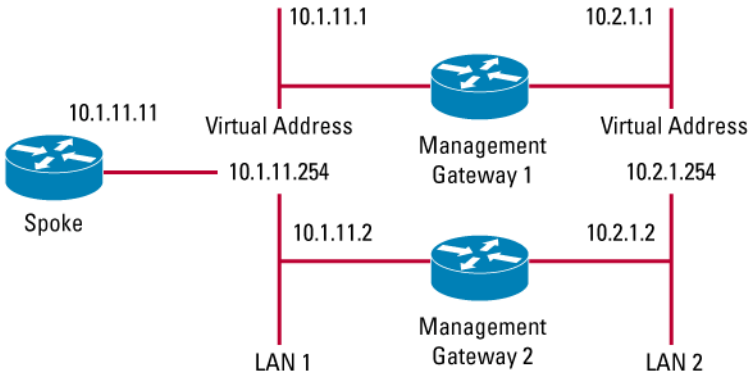
LIMITATIONS

- When a router is first configured for interdevice redundancy, the router must be reloaded for the configuration to take effect.
- The current configuration does not allow the user to use the peer's loopback address. Enchancement for this configuration has been requested and may eventually be resolved.
- When one of the interfaces of an active router goes down, the standby router takes over as active and handles all the operations. However, the previous active router undergoes a reload and eventually stabilizes as the standby router (if the priority of the router is at or below that of the current active router).
- Routers must be connected using a hub or a switch. If routers are connected back to back, any time the active router reloads, the standby router also reloads. This arrangement defeats the purpose of IPsec HA.

CONFIGURATION

Figure 3 shows the short version of the topology to map the IP addressing with configuration examples below.

Figure 3. Simplified Topology---Sample IPO Addresses Corresponding to Configuration



Configuration on Management Gateway 1

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dt1-72a-hub2
!
boot-start-marker
boot-end-marker
!
! Configures redundancy and enters inter-device configuration mode. Currently only “standby”
! scheme is supported. Note that the name of the standby “ha-in” must match with the standby
! group name defined under the interface.
!
redundancy inter-device
 scheme standby ha-in
!
logging snmp-authfail
no logging console
!
! The commands below configure inter-device communication protocol (IPC) between the two
! gateways. “IPC zone default” initiates communication link between active and standby routers.
! The subcommand association, sets up association between active and standby routers and uses
! the transport protocol sctp. The next few lines define the local and remote SCTP port and ip
! address. Note though that local port defined on this router should match the remote port
```

```
! configured on peer router. The local and remote ip address should NOT be virtual ip address.
! The path-retransmit defines number of sctp retries before failing an association and retransmit
! timeot defines maximum amount of time SCTP waits before retransmitting data
!
!
ipc zone default
 association 1
no shutdown
protocol sctp
    local-ip 10.2.1.2
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 20
   remote-port 5000
    remote-ip 10.2.1.1
!
no aaa new-model
ip subnet-zero
!
!
ip cef
no ip dhcp conflict logging
!
!
!
!

!
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec security-association lifetime kilobytes 2560
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
!
crypto dynamic-map ha_dynamic 1
set transform-set t2
!
```

```
! This command allows the user to modify the interval in which an IP redundancy-enabled crypto
! map sends anti-replay updates from the active router to the standby router.
!

crypto map ha_dynamic redundancy replay-interval inbound 10 outbound 1000
crypto map ha_dynamic 1 ipsec-isakmp dynamic ha_dynamic
!
!
!
!
interface Loopback0
 ip address 30.1.0.1 255.255.255.255
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
speed auto
 media-type rj45
 no negotiation auto
!
! This interface redundancy is configured using HSRP. This interface is used for inter-device
! communication using SCTP protocol between Active and Standby gateways.
!
interface GigabitEthernet0/3
 ip address 10.2.1.2 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 duplex auto
 speed 10
 media-type rj45
 no negotiation auto
 standby delay minimum 30 reload 60
 standby 2 ip 10.2.1.254
 standby 2 timers 1 10
 standby 2 preempt
 standby 2 name ha-in
```

```
 standby 2 track Ethernet1/1
!

interface Ethernet1/0
no ip address
 no ip mroute-cache
 shutdown
 duplex half
!
! This interface is configured for redundancy using HSRP. The spoke communicates with the
! active management gateway using the virtual-ip address of this interface.
!
interface Ethernet1/1
 ip address 10.1.11.2 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 duplex half
 standby delay minimum 30 reload 60
 standby 1 ip 10.1.11.254
 standby 1 timers 1 10
 standby 1 preempt
 standby 1 name ha-out
 standby 1 track GigabitEthernet0/3
 crypto map ha_dynamic redundancy ha-out stateful
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex half
no ip address
 shutdown
 duplex half
!
ip classless
ip route 10.1.11.11 255.255.255.255 Ethernet1/1
!
no ip http server
no ip http secure-server
!
!
!
```

```
ip access-list extended peer-outside
 permit ip host 10.1.11.254 host 10.1.11.1
!
!
!
!
control-plane
!
dial-peer cor custom
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 transport preferred all
 transport output all
 stopbits 1
line aux 0
 transport preferred all
 transport output all
 stopbits 1
line vty 0 4
 login
transport preferred all
 transport input all
 transport output all
!
!
end

dt1-72a-hub2#
```

Configuration on Management Gateway 2

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dt1-72a-hub2
```

```
!
boot-start-marker
boot-end-marker
!
! Configures redundancy and enters inter-device configuration mode.
!

redundancy inter-device
 scheme standby ha-in
!
logging snmp-authfail
no logging console
!
! Configures inter-device communication and uses SCTP transport protocol to communicate
! between active and standby association.
!
ipc zone default
 association 1
no shutdown
protocol sctp
    local-ip 10.2.1.1
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 20
    remote-port 5000
    remote-ip 10.2.1.2
!
no aaa new-model
ip subnet-zero
!
!
ip cef
no ip dhcp conflict logging
!
!
!
!

!
!
!
```

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec security-association lifetime kilobytes 2560
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
!
crypto dynamic-map ha_dynamic 1
set transform-set t2
!
! This command allows the user to modify the interval in which an IP redundancy-enabled crypto
! map sends anti-replay updates from the active router to the standby router.
!
crypto map ha_dynamic redundancy replay-interval inbound 10 outbound 1000
crypto map ha_dynamic 1 ipsec-isakmp dynamic ha_dynamic
!
!
!
!
interface Loopback0
 ip address 30.1.0.1 255.255.255.255
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
speed auto
 media-type rj45
 no negotiation auto
!
! This interface redundancy is configured using HSRP. This interface is used for inter-device
! communication using SCTP protocol between Active and Standby gateways.
!
```

```
interface GigabitEthernet0/3
 ip address 10.2.1.1 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 duplex auto
 speed 10
 media-type rj45
 no negotiation auto
 standby delay minimum 30 reload 60
 standby 2 ip 10.2.1.254
 standby 2 timers 1 10
 standby 2 preempt
 standby 2 name ha-in
 standby 2 track Ethernet1/1
!
interface Ethernet1/0
 ip address 10.2.11.251 255.255.255.0
 no ip mroute-cache
 shutdown
 duplex half
!
! This interface is configured for redundancy using HSRP. The spoke communicates with the
! active management gateway using the virtual-ip address of this interface.
!
!
interface Ethernet1/1
 ip address 10.1.11.1 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 duplex half
 standby delay minimum 30 reload 60
 standby 1 ip 10.1.11.254
 standby 1 timers 1 10
 standby 1 preempt
 standby 1 name ha-out
 standby 1 track GigabitEthernet0/3
 crypto map ha_dynamic redundancy ha-out stateful
!
interface Ethernet1/2
 no ip address
 shutdown
 duplex half
```

```
no ip address
 shutdown
 duplex half
!
ip classless
ip route 10.1.11.11 255.255.255.255 Ethernet1/1
!
no ip http server
no ip http secure-server
!
!
!

ip access-list extended peer-outside
 permit ip host 10.1.11.254 host 10.1.11.1
!
!
!
control-plane
!
dial-peer cor custom
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 transport preferred all
 transport output all
 stopbits 1
line aux 0
 transport preferred all
 transport output all
 stopbits 1
line vty 0 4
 login
transport preferred all
 transport input all
 transport output all
!
```

```
!
end

dt1-72a-hub2#
```

Configuration on Spoke

```
dt1-831a#sh run
Building configuration...

Current configuration : 1969 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
|no service password-encryption
!
hostname dt1-831a
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Eymz$CQY6Kt/dazhZsOgI83la..
!
username lab password 0 lab
clock timezone PST -8
clock summer-time PDT recurring
no aaa new-model
ip subnet-zero
!
!
!
!
no ip domain lookup
ip cef
ip ips po max-events 100
no ftp-server write-enable
!
!
!
! Specify the peer address as the virtual ip address of management gateway.
!
crypto isakmp policy 1
```

```
 authentication pre-share
crypto isakmp key cisco123 address 10.1.11.254
!
crypto ipsec security-association lifetime kilobytes 536870912
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
!
crypto map test_1 1 ipsec-isakmp
 set peer 10.1.11.254
 set transform-set t2
 match address test_1
!
!
!
interface Ethernet0
 no ip address
 shutdown
!
interface Ethernet1
 ip address 110.1.11.11 255.255.0.0
 duplex auto
 crypto map test_1
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!

interface FastEthernet4
 no ip address
```

```
 duplex auto
 speed auto
!
ip classless
ip route 10.2.1.254 255.255.255.255 Ethernet1
!
ip http server
no ip http secure-server
!
!
ip access-list extended test_1
 permit ip host 10.1.11.11 host 10.2.1.254
 permit ip host 10.2.11.11 host 10.1.11.254
 no cdp log mismatch duplex
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 login
 transport preferred all
 transport input all
 transport output all
!
scheduler max-task-time 5000
end

dt1-831a#
```

Note: The configuration examples provided here use preshared keys. IPsec HA works even with PKI.

Other Configuration Combinations

Configuration for other scenarios that will be updated on ongoing basis:

- IPsec HA on Cisco Catalyst® 6500 Series switch with VPNSM
- IPsec HA with SSO

TROUBLESHOOTING AND SHOW COMMANDS

To help troubleshoot possible HSRP-related configuration problems, issue any of the following HSRP-related debug commands

- debug standby errors
- debug standby events
- debug standby packets [terse]

To help troubleshoot possible inter-device configuration problems, issue

- debug redundancy command

To help troubleshoot possible IPsec HA-related problems, issue

- debug crypto ha
- debug crypto ipsec ha [detail] [update] command
- debug crypto isakmp ha

To disable debugging, use the “no” form of this command.

The following show and clear commands display state of the devices and state of crypto sessions

- show redundancy [states | inter-device]
- show standby
- show crypto isakmp sa [active | standby]
- show crypto ipsec sa [active | standby]
- show crypto session [active | standby]
- show crypto ha
- clear crypto isakmp [active | standby]
- clear crypto sa [active | standby]
- clear crypto session [active | standby]

REFERENCES

- Configuration guide for Stateful Failover for IPsec:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802d03f2.html

- Hot Standby Router Protocol FAQ:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800a9679.shtml

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.**