CHAPTER 5

Small Branch—Dial Backup to Cisco VPN 3000 Concentrator

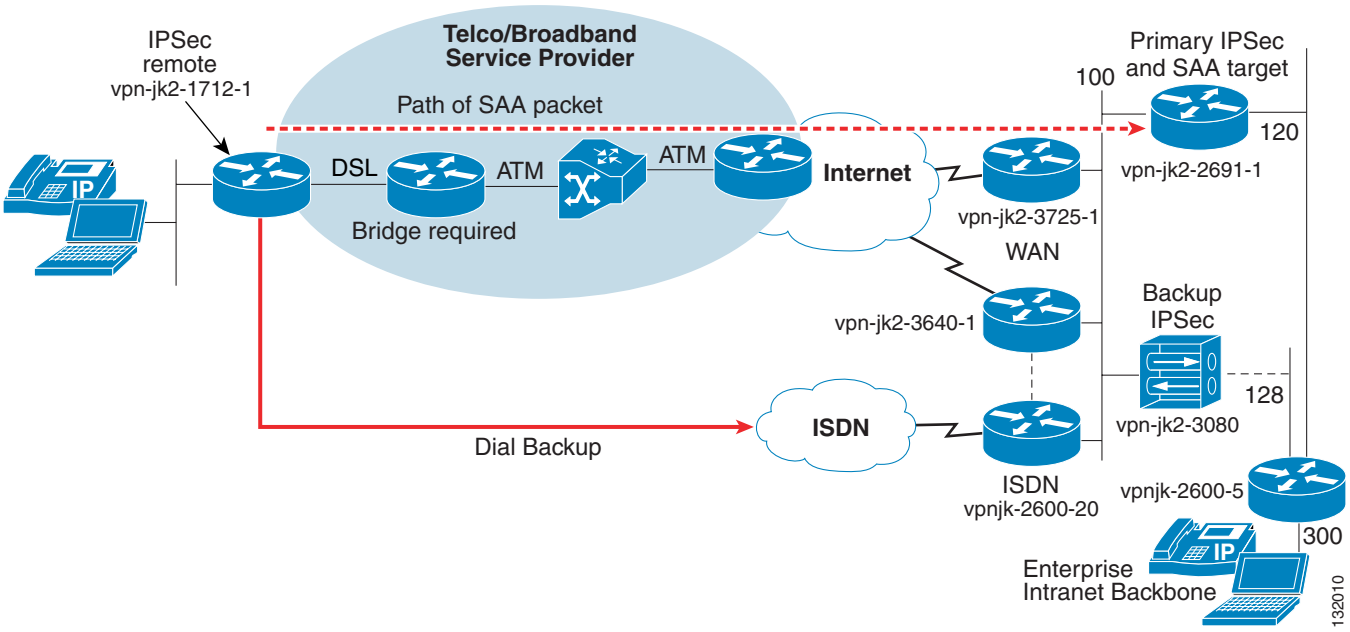
This design was proposed to meet the requirements for a national catalog retail business that has approximately 60 retail stores in addition to the direct mail and Internet web business model. The retailer has an existing Cisco VPN 3000 Concentrator that supports remote access software clients, and wants to use that device as an IPSec head end to serve as a crypto peer for dial backup if the primary path over the Internet fails. The application supported is primarily point-of-sale transactions.

This chapter contains the following sections:

Topology

The topology in Figure 5-1 shows the use of a Cisco 1712 router that includes a Basic Rate ISDN interface; however, the design can be adapted to use a Cisco 1711 and to dial either the access server of an Internet Service Provider or an access server provisioned by the enterprise.

Figure 5-1 Topology Dial Backup to Cisco VPN 3000



The design shows the use of one Cisco IOS head-end IPSec peer that is also the SAA target device for the Reliable Static Routing Backup Using Object Tracking feature in Cisco IOS Software.

The enterprise intranet backbone router is configured to route packets to the remote subnets using the IPSec primary router if the Reverse Route Injection (RRI) network advertisements appear in its routing table; otherwise, the packets are routed to the Cisco VPN 3000 Concentrator.

The VPN 3000 Concentrator is configured with a default route to the ISDN WAN router; however, for higher availability, a customer deployment might use a Hot Standby Router Protocol (HSRP) address shared between a pair of WAN routers, or enable OSPF or RIP on the outside interface and participate in a dynamic routing protocol with the various WAN routers.

Failover/Recovery Time

Failover and recovery times are similar to the results described in two earlier chapters: Small Branch—DSL with ISDN Backup and Small Branch—Cable with DSL Backup.

There is a difference in configuration between the ISDN backup in the previous section and this configuration. As previously described, the Basic Rate ISDN interface is a backup interface for a tunnel interface, and the interface up/down state is keyed off the tunnel interface state. In this configuration, a **dialer idle-timeout** is configured as well as **dialer-list** that excludes IKE packets as interesting traffic.

```
access-list 100 remark DIALER LIST, IKE traffic should not be interesting
access-list 100 deny   icmp any any
access-list 100 deny   udp any eq isakmp any eq isakmp
access-list 100 permit ip any any
dialer-list 2 protocol ip list 100
```

Note For more information regarding dialer interfaces, see the *Cisco IOS Dial Technologies Configuration Guide* at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080393bf3.html.

Caveats

This section describes the caveats associated with this design, and includes the following topics:

- EZVPN—Tunnel Goes to SS_OPEN State on Re-establishing Connection
- RRI Fails to Insert the Appropriate Static Route

EZVPN—Tunnel Goes to SS_OPEN State on Re-establishing Connection

It appears in some instances that the Cisco 1712 is exposed to the following condition: CSCin53097 EZVPN—tunnel goes to SS_OPEN state on re-establishing connection. The following is a successful and unsuccessful initiation of the EZVPN tunnel to the VPN Concentrator. To force the primary path down, an ISP link failure was simulated.

This is a successful dial backup and tunnel establishment.

```
vpn-jk2-1712-1#debug track
Jan 21 16:07:47.717 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.4:500       Id: vpn-jk-2691-1.ese.ciscom
Jan 21 16:07:51.289 est: Track: 123 Down change delayed for 60 secs
vpn-jk2-1712-1#
Jan 21 16:08:51.301 est: Track: 123 Down change delay expired
Jan 21 16:08:51.301 est: Track: 123 Change #50 rtr 233, reachability Up->Down
vpn-jk2-1712-1#
Jan 21 16:08:59.489 est: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
Jan 21 16:08:59.625 est: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan 21 16:09:00.545 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
state to up
Jan 21 16:09:00.641 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
Jan 21 16:09:02.229 est: %LINK-3-UPDOWN: Interface BRI0:2, changed state to up
Jan 21 16:09:02.229 est: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 9191234567
vpnjk-2600-20
Jan 21 16:09:03.289 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed
state to up
Jan 21 16:09:03.297 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
192.168.131.30:500       Id: 192.168.131.30
Jan 21 16:09:08.229 est: %ISDN-6-CONNECT: Interface BRI0:2 is now connected to 9191234567
vpnjk-2600-20
vpn-jk2-1712-1#
vpn-jk2-1712-1#show cry ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : VPN3080
Inside interface list: Vlan1,
Outside interface: BRI0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Primary: 172.26.176.10
```

This is an example of the state stuck in SS_OPEN. Manually clearing the EZVPN client will circumvent the problem.

```
vpn-jk2-1712-1#
Jan 21 16:14:25.043 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.4:500       Id: vpn-jk-2691-1.ese.ciscom
Jan 21 16:14:31.424 est: Track: 123 Down change delayed for 60 secs
Jan 21 16:15:31.424 est: Track: 123 Down change delay expired
Jan 21 16:15:31.424 est: Track: 123 Change #52 rtr 233, reachability Up->Down
Jan 21 16:15:32.936 est: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
Jan 21 16:15:33.072 est: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan 21 16:15:33.152 est: %CRYPTO-4-IKMP_NO_SA: IKE message from 192.168.131.30  has no SA
and is not an initialization offer
Jan 21 16:15:33.992 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
state to up
Jan 21 16:15:34.088 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
Jan 21 16:15:36.244 est: %LINK-3-UPDOWN: Interface BRI0:2, changed state to up
Jan 21 16:15:36.248 est: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 9191234567
vpnjk-2600-20
Jan 21 16:15:37.300 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed
state to up
vpn-jk2-1712-1#
Jan 21 16:15:42.248 est: %ISDN-6-CONNECT: Interface BRI0:2 is now connected to 9191234567
vpnjk-2600-20A pre-shared key for address!

vpn-jk2-1712-1#
Jan 21 16:15:45.044 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
192.168.131.30:500       Id: 192.168.131.30
vpn-jk2-1712-1#
vpn-jk2-1712-1#show cry ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : VPN3080
Inside interface list: Vlan1,
Outside interface: BRI0
Current State: SS_OPEN
Last Event: SOCKET_READY
DNS Primary: 172.26.176.10
vpn-jk2-1712-1#
Jan 21 16:16:33.160 est: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down
Jan 21 16:16:33.256 est: %ISDN-6-DISCONNECT: Interface BRI0:1  disconnected from
9191234567 vpnjk-2600-20, call lasted 60 seconds
Jan 21 16:16:33.256 est: %LINK-3-UPDOWN: Interface BRI0:1, changed state to down
Jan 21 16:16:33.332 est: %ISDN-6-DISCONNECT: Interface BRI0:2  disconnected from
9191234567 vpnjk-2600-20, call lasted 57 seconds
Jan 21 16:16:33.332 est: %LINK-3-UPDOWN: Interface BRI0:2, changed state to down
Jan 21 16:16:34.100 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
state to down
Jan 21 16:16:34.100 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed
state to down
Jan 21 16:16:34.160 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to down
vpn-jk2-1712-1#
Jan 21 16:16:37.932 est: %LINK-3-UPDOWN: Interface BRI0:1, changed state to up
Jan 21 16:16:38.064 est: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Jan 21 16:16:38.988 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:1, changed
state to up
Jan 21 16:16:39.080 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
Jan 21 16:16:40.244 est: %LINK-3-UPDOWN: Interface BRI0:2, changed state to up
```

```
Jan 21 16:16:40.248 est: %ISDN-6-CONNECT: Interface BRI0:1 is now connected to 9191234567
vpnjk-2600-20
Jan 21 16:16:41.304 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0:2, changed
state to up
vpn-jk2-1712-1#clear crypto ipsec  client ezvpn VPN3080
vpn-jk2-1712-1#
Jan 21 16:16:46.249 est: %ISDN-6-CONNECT: Interface BRI0:2 is now connected to 9191234567
vpnjk-2600-20
Jan 21 16:16:49.029 est: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
192.168.131.30:500       Id: 192.168.131.30
vpn-jk2-1712-1#show cry ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : VPN3080
Inside interface list: Vlan1,
Outside interface: BRI0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Primary: 172.26.176.10
vpn-jk2-1712-1#



vpn-jk2-1712-1#show cry eng conn act

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
  22 Dialer1         192.168.17.3    alloc  NONE                      0        0
  23 BRI0            10.0.128.1      set    HMAC_MD5+3DES_56_C        0        0
  24 Dialer1         192.168.17.3    alloc  NONE                      0        0
 200 BRI0            10.0.128.1      set    HMAC_MD5+3DES_56_C        0        9
 201 BRI0            10.0.128.1      set    HMAC_MD5+3DES_56_C       16        0
```

RRI Fails to Insert the Appropriate Static Route

In the test topology, without a default route in the routing table of the vpnjk2-2691-1 route (the primary IPSec head-end route), RRI fails to insert the appropriate static route into the routing table. This was using Cisco IOS version 12.3(5). This defect is documented in CSCed69116.

V3PN QoS Service Policy

The V3PN QoS service policy in this configuration is similar to the other chapters in this guide.

Performance Results

Performance results for the Cisco IOS and VPN concentrator head-ends are shown in Table 5-1.

Table 5-1 IPSEC/DPD/RRI Performance

	Spokes	Bi-Directional Traffic (Mbps)	Bi-Directional Traffic (Kpps)	CPU Utilization %	Stopping Point
Cisco 3745 (AIM-II)	120	22.5	14.5	80	CPU
Cisco PIX 535 (VAC+)	500	167	84	89	CPU
Cisco 3080 (SEP/SEP-E)	138	38.8/39.4	19.6/19.6	80/52	CPU
Cisco 7200 NPE-400 (VAM1)	1040	71.7	31.7	88	CPU
Cisco 7200 NPE-G1 (2xVAM1)	1040	106.7	48.1	81	CPU
Cisco 7200 NPE-G1 (2xVAM2)	1040	108.7	48.7	77	CPU
Cisco Catalyst 6500 (VPNSM)	1040	1029.3	488.7	N/A	VPNSM

These test results are from an IPSec/DPD/RRI test bed configuration using a voice and data traffic mix

In a deployment where the VPN 3080 is acting as a backup head end to provide connectivity for point-of-sale terminals or cash machines over an Async interface with no voice traffic, these are very conservative performance numbers.

If the 3080 also supports VPN access by remote users with a VPN software client in addition to functioning as a backup IPSec head end for remote locations, the performance characteristics vary.

Note The Cisco PIX OS earlier than Version 7 does not switch a packet in and out the same interface in the tested release of the code.

Implementation and Configuration

This section describes the implementation and configuration of the Dial Backup to Cisco VPN 3000 Concentrator solution. It includes the following topics:

- Enterprise Intranet Backbone Router(s)
- IPSec Primary and SAA Target Router
- Primary WAN Router
- Remote IPSec (1712) Router
- Cisco VPN 3000 Concentrator Configuration

Enterprise Intranet Backbone Router(s)

The enterprise intranet backbone router is designated as vpnjk-2600-5 in Figure 5-1. A large enterprise customer may have one or more routers that connect their extranet to the intranet. The function of this router is to route packets for the remote subnets to the appropriate IPSec head-end device, either the Cisco IOS head-end or the VPN concentrator. If an active IPSec tunnel is available on the Cisco IOS head end, this is the primary or preferred path. If no IPSec tunnel is available for the remote subnet, route the packets to the VPN concentrator.

This router is an EIGRP neighbor with the Cisco IOS IPSec head-end router, and it learns external routes of the specific remote subnets using EIGRP. In this example, the network prefix is /25. There is a static route to a /18 prefix that represents the address space of all the remote subnets. If the more specific /25 route does not exist, the /18 route is followed, connecting to the VPN 3000 Concentrator.

```
!
hostname vpnjk-2600-5
!
interface FastEthernet0/1
 description dot1q
 no ip address
 ip route-cache flow
!
interface FastEthernet0/1.120
 encapsulation dot1Q 120  This VLAN connects to the IOS IPSec Head-end - 2691
 ip address 10.2.120.5 255.255.255.0
!
interface FastEthernet0/1.128
 encapsulation dot1Q 128  This VLAN connects to the VPN Concentrator - 3080
 ip address 10.2.128.5 255.255.255.0
!
interface FastEthernet0/1.300
 encapsulation dot1Q 300  This VLAN connects to the Enterprise Intranet Backbone
 ip address 10.3.0.5 255.255.255.0
!
router eigrp 100
 network 10.0.0.0
 no auto-summary
 no eigrp log-neighbor-warnings
!
ip route 10.0.64.0 255.255.192.0 10.2.128.30 name VPN3080
!
end

vpnjk-2600-5#sh ip route 10.0.68.0
Routing entry for 10.0.64.0/18                  Primary path down.
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 10.2.128.30
      Route metric is 0, traffic share count is 1

vpnjk-2600-5#sh ip route 10.0.68.0
Routing entry for 10.0.68.0/25                 Primary path available
  Known via "eigrp 100", distance 170, metric 10258432, type external
  Redistributing via eigrp 100
  Last update from 10.2.120.4 on FastEthernet0/1.120, 00:00:35 ago
  Routing Descriptor Blocks:
  * 10.2.120.4, from 10.2.120.4, 00:00:35 ago, via FastEthernet0/1.120
      Route metric is 10258432, traffic share count is 1
      Total delay is 10100 microseconds, minimum bandwidth is 256 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Note: There is a /25 route for each remote subnet active over the primary path. The /18 prefix will always be in the routing table.

```
vpnjk-2600-5#show ip route
…
S       10.0.64.0/18 [1/0] via 10.2.128.30
D EX    10.0.68.0/25
           [170/10258432] via 10.2.120.4, 00:09:36, FastEthernet0/1.120
```

IPSec Primary and SAA Target Router

In other chapters of this guide, the head-end SAA target router and the IPSec head-end routers are separate routers. In this example, both functions are implemented on one router. When there is only one IPSec head-end router, it is practical to use its IP address as the SAA target. If the IPSec tunnel is down, the SAA address is down. When the design has multiple primary peers, it may be advantageous to use a separate SAA target router. A disadvantage to this design is that if the SAA target router is down and the IPSec peers are functional, the backup mechanism is activated when it is not really needed.

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname vpn-jk-2691-1
!
boot system flash c2691-ik9o3s-mz.122-13.T10
logging buffered 4096 debugging
enable secret 5 [removed]
!
memory-size iomem 15
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
no ip cef                              # CEF was disabled, see caveats
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
!
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 crl optional
 auto-enroll 70
crypto ca certificate chain ect-msca
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A
 certificate 5D7B2D4300000000003C
!
!
crypto isakmp policy 1
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
```

```
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
!
crypto dynamic-map DYNO-TEMPLATE 10
 description dynamic crypto map
 set transform-set 3DES_SHA_TRANSPORT 3DES_SHA_TUNNEL
 reverse-route
 qos pre-classify
!
!
crypto map DYNO-MAP local-address FastEthernet0/1.100
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
interface FastEthernet0/1
 description dot1q
 no ip address
 ip route-cache flow
!
interface FastEthernet0/1.100
 description Outside Interface
 encapsulation dot1Q 100
 ip address 192.168.131.4 255.255.255.224      # crypto peer and SAA target address
 crypto map DYNO-MAP
!
interface FastEthernet0/1.120
 description Inside Interface                  # EIGRP neighbor on this interface to
 encapsulation dot1Q 120                       # vpnjk-2600-5 Enterprise Intranet
 ip address 10.2.120.4 255.255.255.0           # Backbone Router
!
router eigrp 100
 redistribute static metric 256 1000 255 1 1500 route-map IPSEC_Subnets
 network 10.0.0.0
 network 192.168.130.0 0.0.1.255
 no auto-summary
!
ip classless
ip http server
!
!
access-list 68 permit 10.0.64.0 0.0.63.255     # Allow redistribution of
access-list 68 deny   any                      # subnets of 10.0.64.0 /18
!
route-map IPSEC_Subnets permit 10
 match ip address 68
!
rtr responder                                  # To respond to SAA requests
!
end
```

Primary WAN Router

This section shows the configuration of the primary enterprise WAN router. There is a issue in the RRI code that presents a problem if there is no default route in the routing table of the IPSec head-end router. To circumvent this issue, this WAN router is configured to advertise a 0/0 route into EIGRP 100 so that the IPSec head-end router learns a default route. In the event this router is down or out-of-service, the secondary WAN router should be similarly configured.

```
version 12.3
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname vpn-jk2-3725-1
!
boot-start-marker
boot system flash c3725-ik9o3s-mz.123-3
boot-end-marker
!
memory-size iomem 15
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
ip cef
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
interface Loopback0
 ip address 192.168.130.1 255.255.255.255
!
!
interface FastEthernet0/1
 description dot1q
 no ip address
!
interface FastEthernet0/1.100
 description vlan 100
 encapsulation dot1Q 100
 ip address 192.168.131.1 255.255.255.224
 no ip proxy-arp
!
interface FastEthernet0/1.102
 description vlan 102
 encapsulation dot1Q 102
 ip address 192.168.131.33 255.255.255.224
 no ip proxy-arp
!
!
interface ATM2/0
description WAN Link to the Internet (AS 65001)
 no ip address
 no atm ilmi-keepalive
!
interface ATM2/0.235 point-to-point
 ip address 192.168.129.6 255.255.255.252
 pvc peer235 2/35
  vbr-nrt 1000 1000
  encapsulation aal5snap
 !
!
router eigrp 100
 redistribute static metric 100 1000 255 1 1500 route-map QuadZero
 redistribute bgp 65030 metric 100 1000 255 1 1500
 network 192.168.130.0 0.0.1.255
 no auto-summary
!
```

```
router bgp 65030
 no synchronization
 bgp log-neighbor-changes
 network 192.168.130.0 mask 255.255.254.0
 network 192.168.230.0 mask 255.255.254.0
 neighbor 192.168.129.5 remote-as 65001
 neighbor 192.168.130.2 remote-as 65030
 neighbor 192.168.130.2 update-source Loopback0
 no auto-summary
!
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Null0 240            # Redistributed into EIGRP 100 for IPSec HE
ip route 192.168.130.0 255.255.254.0 Null0    # Provides 'nailed up' networks for BGP
ip route 192.168.230.0 255.255.254.0 Null0    # Provides 'nailed up' networks for BGP
!
!
access-list 10 permit 0.0.0.0
!
route-map QuadZero permit 10                  # Redistribute the 0/0 route to EIGRP
 match ip address 10
!
ntp source Loopback0
ntp master
ntp server 172.26.176.10 source FastEthernet0/0
!
end
```

Remote IPSec (1712) Router

This is the configuration of the remote Cisco 1712 router.

```
!             System image file is "flash:c1700-k9o3sy7-mz.123-2.XE"
version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone

service password-encryption
!
hostname vpn-jk2-1712-1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable secret 5 [removed]
!
username vpnjk-2600-20 password 7 [removed]
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
ip domain name ese.cisco.com
ip host harry 172.26.176.10
ip host ect-msca 172.26.179.237
ip name-server 172.26.176.10
ip cef
ip audit notify log
```

```
ip audit po max-events 100
!
track 123 rtr 233 reachability
 delay down 60 up 5
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
isdn switch-type basic-5ess
!
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 revocation-check none
!
!
!
crypto ca certificate chain ect-msca
 certificate 5DA1A8EE00000000003D
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A
!
!
crypto isakmp policy 20
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
crypto ipsec transform-set 3DES_SHA_TRANSPORT esp-3des esp-sha-hmac
 mode transport
no crypto ipsec nat-transparency udp-encaps
!
!
!
crypto ipsec client ezvpn VPN3080
 connect auto
 group SOHO key point_of_sale
 mode network-extension
 peer 192.168.131.30
 username site100 password  cisco123
!
!
crypto map IOS_2691 10 ipsec-isakmp
 description used for testing ezvpn for dial backup
 set peer 192.168.131.4
 set transform-set 3DES_SHA_TUNNEL
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
!
class-map match-all VOICE
 match ip dscp ef
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match access-group name IKE
!
!
policy-map V3PN-WAN-EDGE-ISDN
description Note LLQ for PPP/ISDN G.729=56K
 class VOICE
```

```
  priority 48 2400
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class class-default
  fair-queue
  random-detect
policy-map V3PN-teleworker
description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 64
 class class-default
  fair-queue
  random-detect
policy-map Shaper
 class class-default
  shape average 182400 1824
  service-policy V3PN-teleworker
!
interface BRI0
 bandwidth 128
 ip address 10.0.128.1 255.255.255.252
 max-reserved-bandwidth 100
 service-policy output V3PN-WAN-EDGE-ISDN
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 tx-ring-limit 1
 tx-queue-limit 1
 dialer idle-timeout 60
 dialer wait-for-carrier-time 10
 dialer map ip 10.0.128.2 name vpnjk-2600-20 broadcast 9191234567
 dialer map ip 10.0.128.2 name vpnjk-2600-20 broadcast 9194442222
 dialer hold-queue 5
 dialer-group 2
 isdn switch-type basic-5ess
 ppp authentication chap
 ppp multilink
 ppp multilink fragment delay 10
 ppp multilink links minimum 2
 crypto ipsec client ezvpn VPN3080
!
interface FastEthernet0
 description Outside to DSL Modem
 bandwidth 256
 no ip address
 service-policy output Shaper
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface FastEthernet1
 no ip address
 vlan-id dot1q 1
  exit-vlan-config
 !
!
!
interface Vlan1
 description Inside
```

```
 ip address 10.0.68.1 255.255.255.128
 ip route-cache flow
 ip tcp adjust-mss 542
 load-interval 30
 crypto ipsec client ezvpn VPN3080 inside
!
!
interface Dialer1
 description Outside
 bandwidth 256
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 ip tcp adjust-mss 542
 load-interval 30
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication pap callin
 ppp chap refuse
 ppp pap sent-username cisco789@cisco.com password 7 [removed]
 ppp ipcp dns request
 ppp ipcp wins request
 crypto map IOS_2691
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 239 name primary_path track 123
ip route 0.0.0.0 0.0.0.0 10.0.128.2 240 name BRI_peer_20
ip route 10.0.128.2 255.255.255.255 BRI0
!
ip route 192.168.131.4 255.255.255.255 Dialer1 name To2691_head-end
ip route 192.168.131.30 255.255.255.255 10.0.128.2 name To3080_head-end
no ip http server
no ip http secure-server
!
ip access-list extended CRYPTO_MAP_ACL
 permit ip 10.0.68.0 0.0.0.127 any
!
access-list 100 remark DIALER LIST, IKE traffic should not be interesting
access-list 100 deny   icmp any any
access-list 100 deny   udp any eq isakmp any eq isakmp
access-list 100 permit ip any any
dialer-list 2 protocol ip list 100
!
rtr responder
!                     RTR 12 simply generates traffic to simulate background 'noise'
rtr 12
 type echo protocol ipIcmpEcho 10.2.128.5 source-ipaddr 10.0.68.1
 frequency 10
rtr schedule 12 start-time now life forever
!                     RTR 233 is associated with the object tracking
rtr 233
type udpEcho dest-ipaddr 192.168.131.4 dest-port 57005 source-ipaddr 10.0.68.1 source-port
48879
 tos 192
 owner TRACK123
 tag Object Tracking
 frequency 20
 lives-of-history-kept 1
 buckets-of-history-kept 10
 filter-for-history failures
rtr schedule 233 start-time now life forever
!
!                     Aliases to aid in troubleshooting
```

```
alias exec xa crypto ipsec client ezvpn xauth
alias exec ca sh cry eng conn act
alias exec cc crypto ipsec client ezvpn connect VPN3080
alias exec cz clear crypto ipsec  client ezvpn VPN3080
alias exec sz show cry ipsec client ezvpn
!
ntp server 192.168.130.1
!
end
```

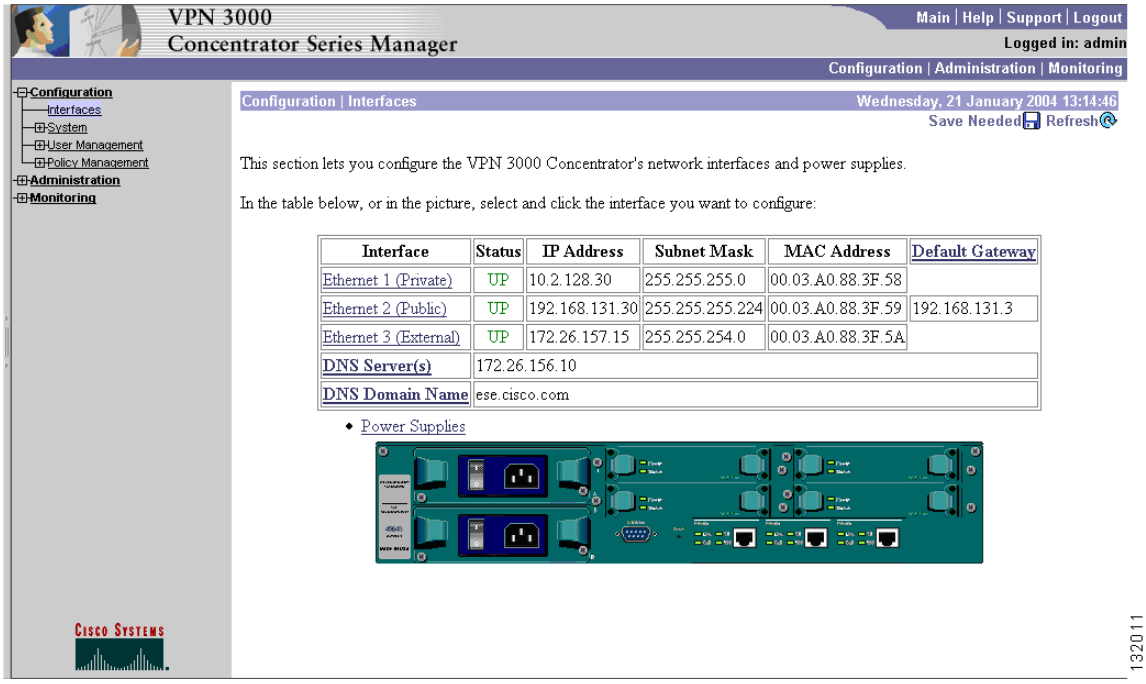
Cisco VPN 3000 Concentrator Configuration

The Cisco VPN 3000 Concentrator is configured with a default route (gateway) of 192.168.131.3, which is the head-end ISDN WAN router. The inside or private address is on the same subnet as the enterprise intranet router. The external address is a lab flashnet address for management.

Interfaces

Figure 5-2 shows the VPN 3000 configuration interface.

Figure 5-2 VPN 3000 Configuration Interface



Groups

This section describes the configuration of the groups.

Identity

The group configuration of the remote router is defined on the window shown in Figure 5-3.

```
crypto ipsec client ezvpn VPN3080
 connect auto
 group SOHO key point_of_sale
 mode network-extension
 peer 192.168.131.30
 username site100 password  cisco123
```

Figure 5-3 VPN 3000 Group Identity

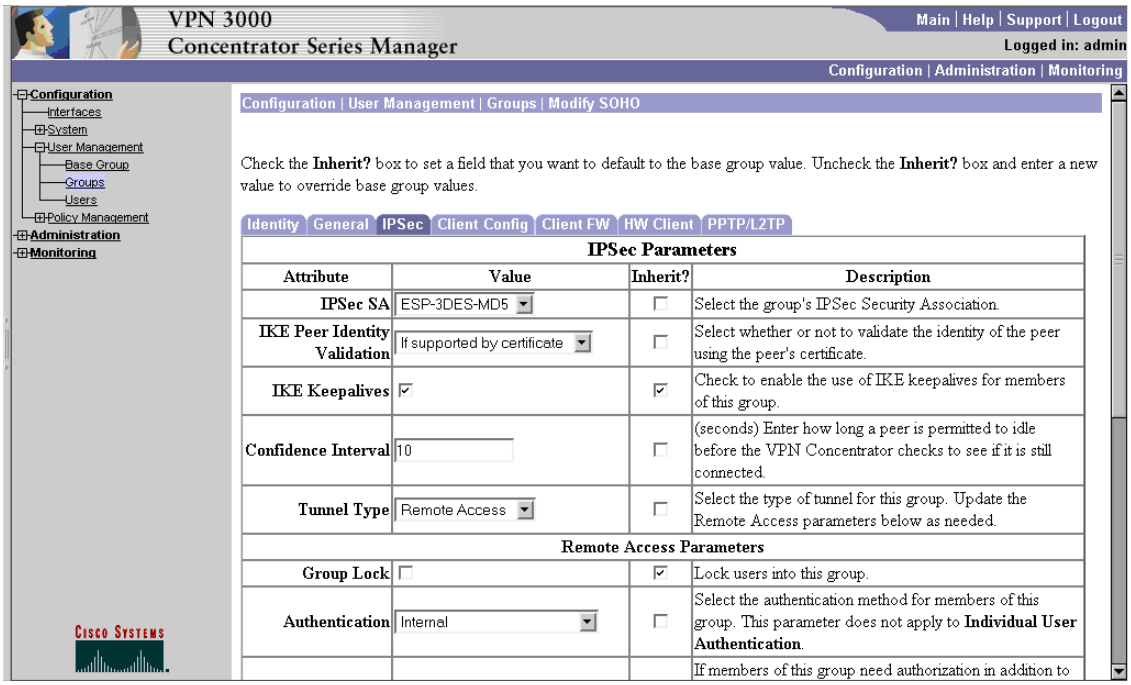
IPSec

IKE keepalives are enabled for this group, and the confidence interval (dead interval) is configured at 10 seconds rather than the default of 5 minutes.

A tunnel type of remote access should be configured.

Figure 5-4 shows the IPSec configuration window.

Figure 5-4 VPN 3000 IPSec



Client Configuration

The IPSec client is permitted to store the password locally. The remote router is disabling NAT-T, so IPSec over UDP is not negotiated because both ends are not configured for NAT-T.

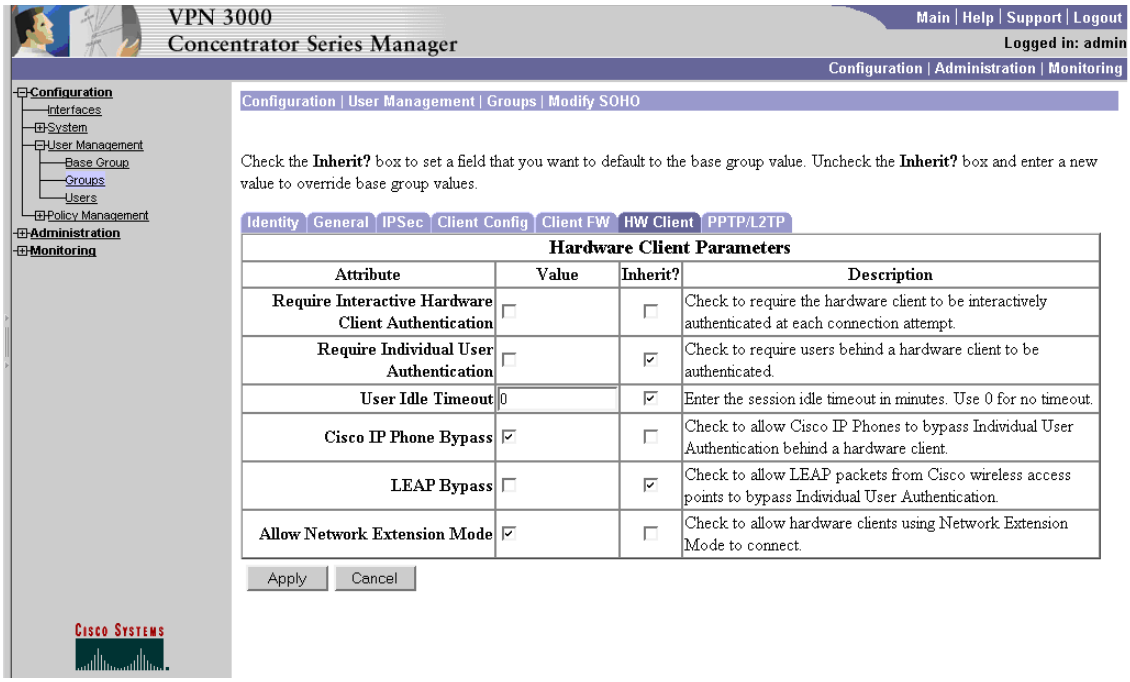
Figure 5-5 shows the VPN 3000 Client Configuration window.

Figure 5-5 VPN 3000 Client Configuration

Hardware Configuration

Network Extension Mode is permitted, as shown in Figure 5-6.

Figure 5-6 VPN 3000 Hardware Configuration



Users

This section describes the configuration of the users.

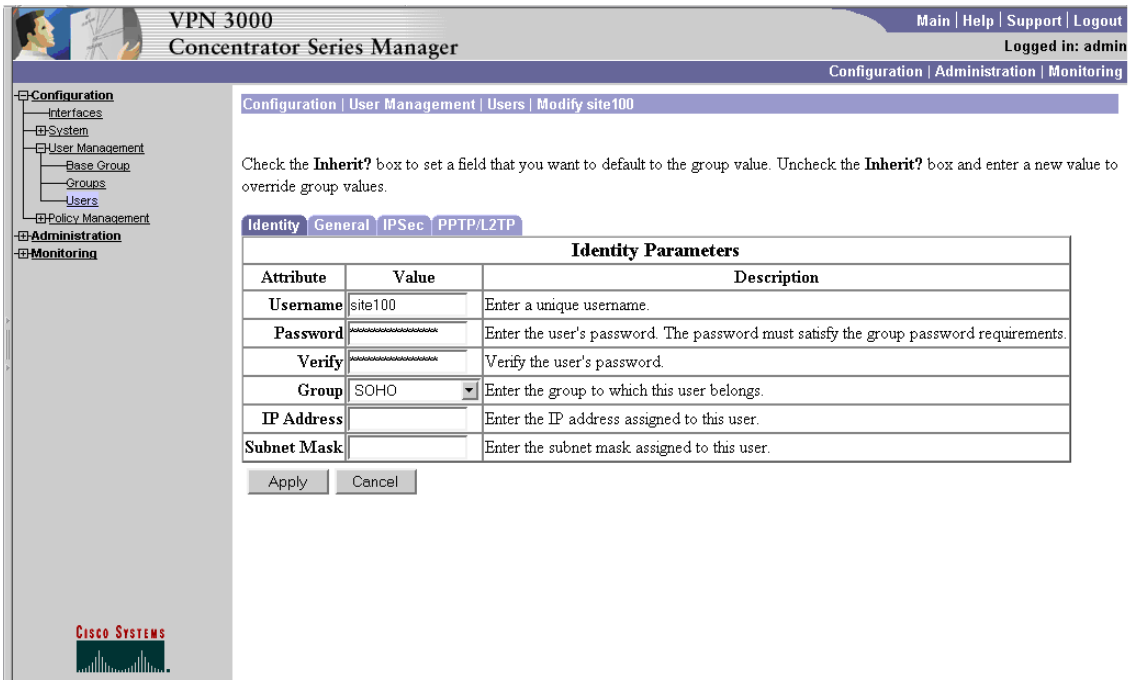
Identity

The username for this location is defined as *site100*. Each location has a unique username.

```
crypto ipsec client ezvpn VPN3080
 connect auto
 group SOHO key point_of_sale
 mode network-extension
 peer 192.168.131.30
 username site100 password  cisco123
```

Figure 5-7 shows the Identity Parameters configuration window.

Figure 5-7 VPN 3000 User Identity

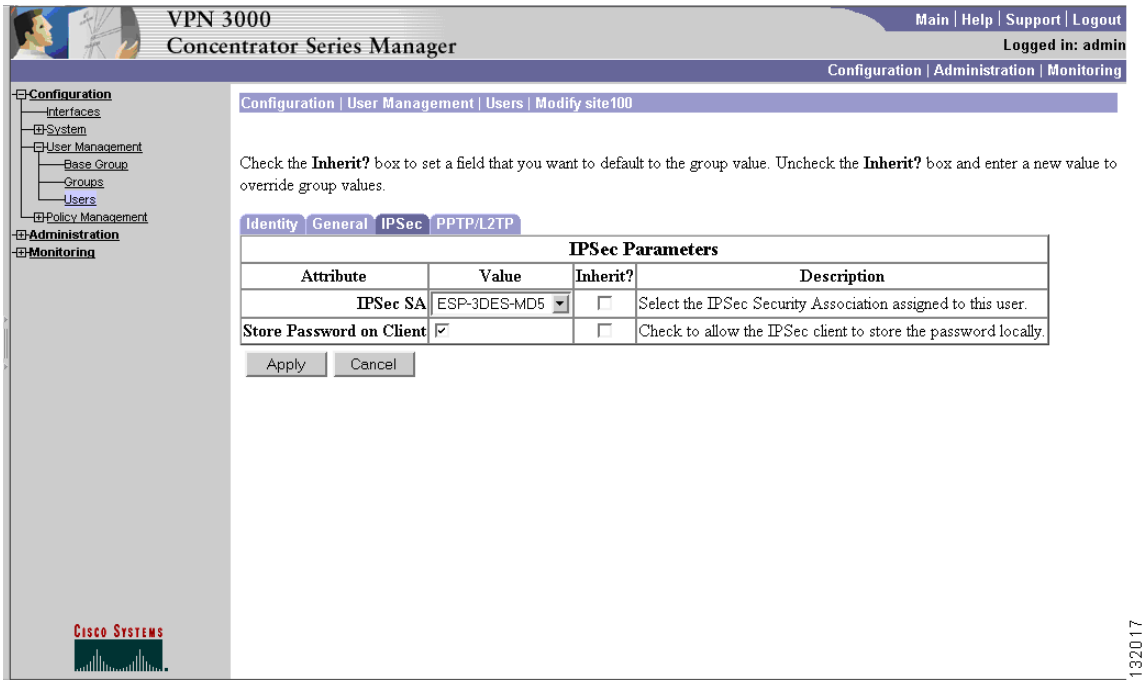


IPSec

The IPSec client is permitted to store the password locally.

Figure 5-8 shows the IPSec Parameters window.

Figure 5-8 VPN 3000 IPSec

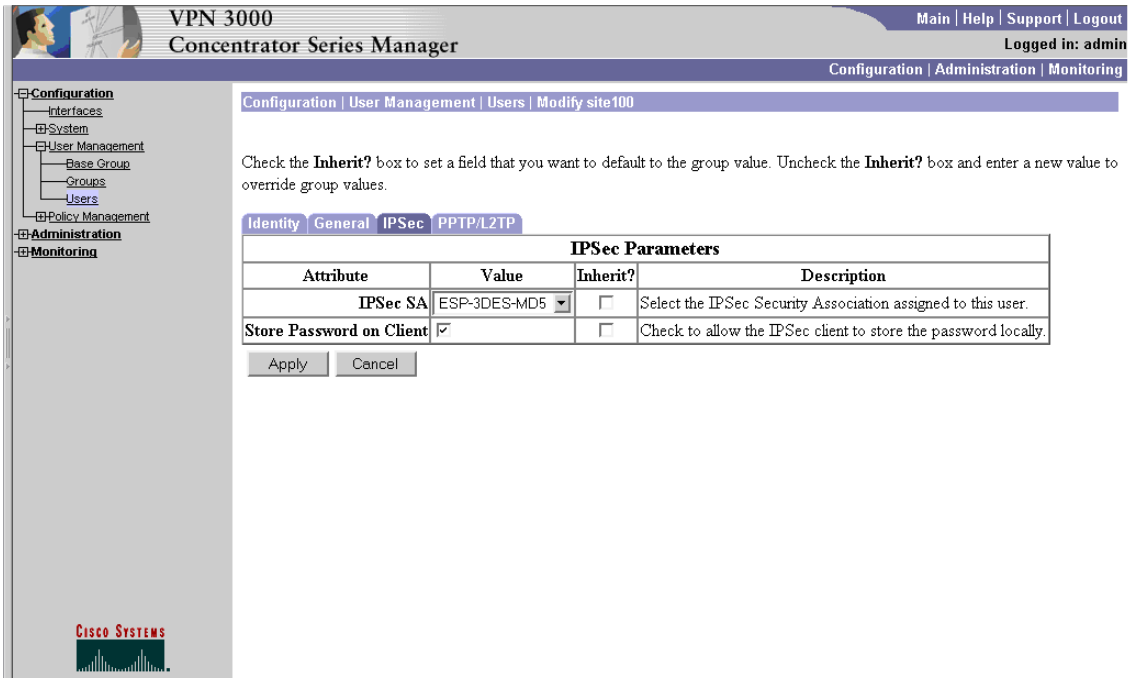


Policy Management/Traffic Management /SAs

The transform set is defined as follows: tunnel mode, 3DES, and MD5 with default lifetimes.

Figure 5-9 shows the Policy Management window.

Figure 5-9 VPN 3000 Policy Management



System/Tunneling Protocols/IPSec/IKE

The IKE proposal is defined. Encryption strength is 3DES, hash is MD5, and Diffie-Hellman value is Group 2. The default lifetimes are also configured.

Figure 5-10 shows the Tunneling Protocols window.

Figure 5-10 VPN 3000 Tunneling Protocols

Cisco IOS Versions Tested

The following code versions were used during testing.

- IPSec head-ends—c2691-ik9o3s-mz.122-13.T10
- Cisco 1712—c1700-k9o3sy7-mz.123-2.XE
- IPSec concentrator—vpn3000-4.0.4.A-k9

The IPSec head-end router was a Cisco 2691 with an AIM hardware VPN module. The Cisco VPN 3000 Concentrator was a Cisco 3080 running Version 4.0.4.A.

This testing was not intended to scale test head-end performance capabilities. In a customer deployment, using IPSec head-ends with suitable performance characteristics aligned with the number of remote routers is advised.

Summary

This design applies to a small-to-medium-sized business with an existing remote access solution using a Cisco VPN 3000 Concentrator that wants to leverage this device to provide backup coverage. This chapter described the head-end routing configuration to demonstrate how you can use a combination of dynamic and static routing to route packets to the appropriate head-end device. The example in this section described the use of Basic Rate ISDN for the dial-backup links, but Async dial-up to an ISP can also be used.