Aerohive Networks Inc.

Layer3 VPN TestCase

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 0.1 | 07/23/2011 | Chenjie zhong | Initial version |
| 0.2 | 07/29/2011 | Chenjie zhong | Modify cases by review meeting   1. Add capwap info/trap check in 6.1.1 2. Add negtive cases for ike phase 1 failure case 6.2.1.3 3. Add case 6.2.4.3 for multi tunnels rekey 4. Change the priority of some cases 5. Add Case 6.2.6.9, 6.2.6.10 6. Add cli cases 6.8 all |
| 0.3 | 08/01/2011 | Chenjie zhong | Modified cases   1. Remove case 6.2.8.6 2. Remove 6.2.9 3. Remove 6.2.10 4. Remove 6.2.11 5. Add case 6.5.1, 6.5.2 |
| 0.3 | 08/01/2011 | Ligang Zhang | Approved |
| 0.4 | 08/08/2011 | Chenjie zhong | Modified cases by dev review   1. Change TOPO1 and TOPO2 2. Add scenario case 6.1.3 and 6.1.4 to cover TOPO conditions 3. Modify case 6.2.4.1 and 6.2.4.2 to check tunnel status 4. Modify case 6.2.6.7 to check LAN traffic on BR 5. Modify case 6.2.6.10 to check tunnel priority. 6. Modify case 6.2.8.2, 6.2.8.3, 6.2.8.4, 6.2.8.6 to check tunnel status and tunnel routes 7. Modified case 6.5.3 to cover the fragment conditions 8. Modified case 6.6.2 to add add the tunnel recover measure time check 9. Add section 6.2.9 to cover failover |
| 0.5 | 09/05/2011 | Chenjie zhong | 1. Add section 6.2.7 to cover vpn exception list |
| 0.6 | 11/18/2011 | Chenjie zhong | 1. Add case 6.2.9.1 to cover ip fragment over vpn tunnel |
|  |  |  |  |

Table of Contents

[Table of Contents 3](#_Toc316891996)

[1. Introduction 6](#_Toc316891997)

[2. Test Objectives 6](#_Toc316891998)

[3. Test Accept Criterion from Development 6](#_Toc316891999)

[4. Product Pass Criterion 6](#_Toc316892000)

[5. Test Bed/Topo Design 6](#_Toc316892001)

[5.1. Topology 1 6](#_Toc316892002)

[5.2. Topology 2 7](#_Toc316892003)

[6. TestCase 8](#_Toc316892004)

[6.1. Key Scenarios 8](#_Toc316892005)

[6.1.1. CVG side uses wan only, BR side with wan nat, no nat between them 8](#_Toc316892006)

[6.1.2. CVG is wan only, BR is wan nat, the CVG and BR are all behind NAT 16](#_Toc316892007)

[6.1.3. CVG is wan only, BR is wan nat, only BR behind NAT 17](#_Toc316892008)

[6.1.4. CVG is wan only, BR is wan nat, only CVG behind NAT 18](#_Toc316892009)

[6.2. Function Test Case 19](#_Toc316892010)

[6.2.1. ISAKMP (Main Mode) 19](#_Toc316892011)

[6.2.2. ISAKMP Config Mode (included XAuth) 29](#_Toc316892012)

[6.2.3. ISAKMP NAT Traversal 31](#_Toc316892013)

[6.2.4. ISAKMP Rekey Test 33](#_Toc316892014)

[6.2.5. Mgmt-Traffic Tunneling (From BR self to CVG) 35](#_Toc316892015)

[6.2.6. Traffic forwarding strategy on BR 39](#_Toc316892016)

[6.2.7. tunnel-exception list 46](#_Toc316892017)

[6.2.8. Traffic forwarding strategy on CVG 52](#_Toc316892018)

[6.2.9. IP fragment 53](#_Toc316892019)

[6.2.10. Tunnel Flip, Recovery 54](#_Toc316892020)

[6.2.11. Tunnel failover 60](#_Toc316892021)

[6.3. Stress Test 60](#_Toc316892022)

[6.3.1. Tigger the tunnel to up down continuously 60](#_Toc316892023)

[6.3.2. Heavy traffic runs on vpn tunnel 61](#_Toc316892024)

[6.4. Duration Test Case 61](#_Toc316892025)

[6.5. Performance Test Case 62](#_Toc316892026)

[6.5.1. Check the throughput of tcp packet 62](#_Toc316892027)

[6.5.2. Check the throughput when BR with wan nat 62](#_Toc316892028)

[6.5.3. Ip fragment with vpn tunnel 63](#_Toc316892029)

[6.6. Scalability Test Case 63](#_Toc316892030)

[6.6.1. Maximum client-ipsec-tunnel on BR 63](#_Toc316892031)

[6.6.2. 1500 tunnels on CVG 64](#_Toc316892032)

[6.7. Compatibility Test Case 64](#_Toc316892033)

[6.8. CLI (Automation Status: Yes/No) 64](#_Toc316892034)

[6.8.1. Layer 3 vpn cli 65](#_Toc316892035)

[6.8.2. l3-tunnel-action config with user-profile 65](#_Toc316892036)

[6.9. GUI Management-HiveManager 67](#_Toc316892037)

[6.10. GUI Management-HiveUI 67](#_Toc316892038)

[7. Customer Issue or Typical Bug 67](#_Toc316892039)

Glossary and Abbreviations

# Introduction

The route-based VPN requirement is implemented using GRE tunnels over tunnel interfaces. The GRE tunneled packets are further protected with IPsec encryption before sent over the internet. IKE v1 with NAT-Traversal is used for key management of the IPsec security associations.

# Test Objectives

1. The layer 3 vpn tunnel could be setup correctly
2. The layer 3 vpn tunnel is stable enough to carry user data
3. The layer 3 vpn tunnel could be recreated after tunnel down by accident

# Test Accept Criterion from Development

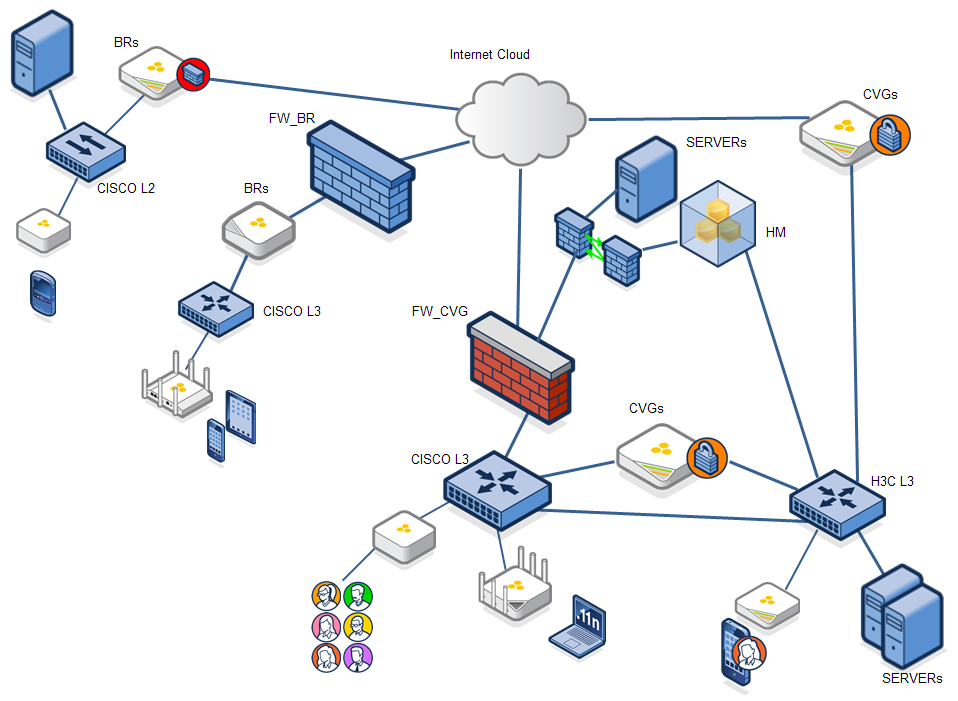
* Approved – Functional Specifications
* <http://saturn.aerohive.com/view.php?fDocumentId=3366>
* Not Approved – Unit Test Plans

# Product Pass Criterion

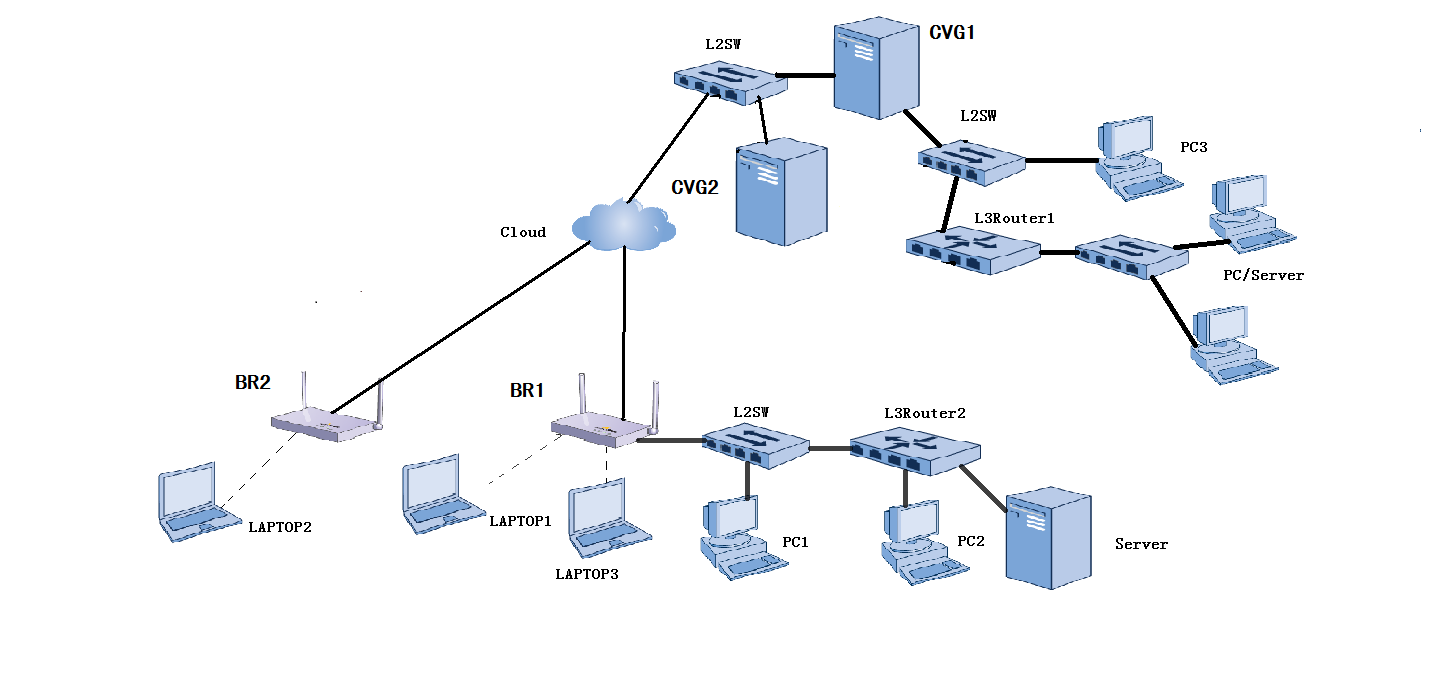
1. Layer 3 vpn could be setup, with various parameters
2. Vpn rekey is success
3. Vpn tunnel could be recover when network or BR/CVG wrong into problems. e.g, wan interface change IP, network unreachable, reboot etc.

# Test Bed/Topo Design

## Topology 1



## Topology 2



# TestCase

## Key Scenarios

### CVG side uses wan only, BR side with wan nat, no nat between them

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_User\_Scenario\_1 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | CVG side uses wan only, BR side with wan nat, no nat between them | | |
| Pre-condition | -config CVG with WAN interface, nat disable  -config CVG eth1 as bridge-access, mac-learning enable  -config CVG act as l3 VPN server  vpn xauth-client-list 000C29A28C96\_clientList local  vpn xauth-client-list 000C29A28C96\_clientList client-name b6rTBhX8aMzUNbLMPn1qECcuAqIIbzcI password \*\*\*  vpn server-ipsec-tunnel 000C29A28C96\_backupServer vpn-mode layer-3  vpn ipsec-tunnel 000C29A28C96\_backupServer client-list 000C29A28C96\_clientList  vpn tunnel-policy vpn\_tunnel\_policy server ipsec-tunnel 000C29A28C96\_backupServer  -one LAN on CVG  -config BR with WAN interface, nat enable  -config BR as l3 VPN client  vpn client-ipsec-tunnel 001977221180\_client\_ipsec\_1 vpn-mode layer-3  vpn ipsec-tunnel 001977221180\_client\_ipsec\_1 gateway 10.155.32.174 client-name 4aTcMqxBcb8qihjL942JGth8cpGLezip password \*\*\*  vpn tunnel-policy vpn\_tunnel\_policy client ipsec-tunnel 001977221180\_client\_ipsec\_1 primary  routing route-request enable  -one LAN on BR  -there is no FW between CVG and BR  -traffic from wan of CVG can reach wan of BR, the LANs are unreachable from each other  -clock time sync with BR/CVG | | |
| Test procedure | -check the status of vpn connection  -check Ike sa and sp is correct on both CVG and BR sides  -check the tunnel interface created after vpn connection success  -check the l3 tunnel created correctly on both sides  -check the ip of mgt0 is added to the peer via tunnel0 in route table  -BR will announce LANs under it, check the route table on CVG  -CVG will push the LANs under it to BR, check the route table on BR  -after vpn connection was setup, check the traffic forward via vpn from BR side based on route table  -STA1 under BR ping a remote server in cloud  -STA1 under BR ping a remote server behind CVG  -BR ping a server in cloud  -BR ping a server behind CVG | | |
| Expect result | 1. Vpn connection can setup between the two nodes successfully 2. Check the status of ike sa, destination IP should be the peer’s wan ip, port(no nat with 500 both, if nat, it’s 4500 on BR, random on CVG side) is correct, and the ST is 9, S is I on BR and R on CVG 3. Check the status of ike sp, the local ip and remote ip is correct, bidirectional, proto is gre(47), esp tunnel mode, and the ip addr is the peer’s wan ip 4. Check the gre tunnel is correct on both BR and cvg, ‘sh vpn layer-3-tunnel’ to check 5. The traffic from clients(wired or wireless, laptop1 and laptop2) forwards correctly as based on route, vpn or wan nat 6. The managerment traffice of BR self forwards correctly based on route table 7. No broadcast traffic should go though tunnel | | |
| Test result | - ‘sh vpn ike sa’ on cvg:  AH-457ec0#sh vpn ike sa  ISAKMP SA Table:  ST=status(value meaning):  --------------------------  1: phase 1 start;  2: msg 1 received;  3: msg 1 sent;  4: msg 2 recived;  5: msg 2 sent;  6: msg 3 received;  7: msg 3 sent;  8: msg 4 received;  9: phase 1 established;  10: phase 1 expired;  S=Side(I=Initiator;R=Responder):V=Version:E=Etype  Created=ISAKMP SA created time;Phase2=Counter of phase 2 rekey  --------------------------------------------------------  Destination Cookies ST S V E Created Phase2 Tunnel-ID  10.155.32.170[2084] fa3a0c01587104ab:8cf8ac079789e4f4 9 R 10 M 2012-02-09 16:49:26 1 94  Total ISAKMP SA Entries: 1  -‘sh vpn ike sp’ on br:  Security Policy Information:  172.32.1.17 [any] 10.3.3.202 [any] 47  tunnel-id: 2  in prio def ipsec  esp/tunnel/10.155.32.170-10.3.3.202/unique:1  created: Feb 9 18:21:13 2012 lastused: Feb 9 19:08:17 2012  lifetime: 3600(s) validtime: 0(s)  spid=352 seq=2 pid=1189  refcnt=3  10.3.3.202 [any] 172.32.1.17 [any] 47  tunnel-id: 2  out prio def ipsec  esp/tunnel/10.3.3.202-10.155.32.170/unique:1  created: Feb 9 18:21:13 2012 lastused: Feb 9 19:08:17 2012  lifetime: 3600(s) validtime: 0(s)  spid=369 seq=1 pid=1189  refcnt=3  172.32.1.17 [any] 10.3.3.202 [any] 47  tunnel-id: 2  fwd prio def ipsec  esp/tunnel/10.155.32.170-10.3.3.202/unique:1  created: Feb 9 18:21:13 2012 lastused:  lifetime: 3600(s) validtime: 0(s)  spid=362 seq=0 pid=1189  refcnt=2  - ‘sh vpn layer-3-tunnel’ on BR  Gateway=remote IPsec gateway address ("anonymous" appears when the local device is a VPN gateway)  Priority=the priority assigned to the interface (the lower the number, the higher the priority)  Remote=remote GRE tunnel endpoint ("any" indicates a point-to-multipoint tunnel endpoint)  Local=local tunnel endpoint  Mode=tunnel encapsulation mode  Iface=tunnel interface name  Iface Mode Remote Local Priority Gateway  ---------- --------- ------------------ ------------------ ---------- ------------------  tunnel0 gre/ipsec 10.3.3.202 172.32.1.17 1 10.155.32.174  - ‘sh vpn layer-3-tunnel’ on CVG  Iface Mode Remote Local Priority Gateway  ---------- --------- ------------------ ------------------ ---------- ------------------  tunnel0 gre/ipsec any 10.3.3.202 0 anonymous  -check route table on cvg:  CVG-czhong#sh ip route  Ref=references; Iface=interface;  U=route is up;H=target is a host; G=use gateway;  Destination Gateway Netmask Flags Metric Ref Use Iface  --------------- --------------- --------------- ----- ------ ------ --- -----  172.32.1.17 172.32.1.17 255.255.255.255 UGH 0 0 0 tunnel0  172.32.1.160 10.3.3.254 255.255.255.240 UG 20 0 0 eth0  172.32.1.64 10.3.3.254 255.255.255.240 UG 20 0 0 eth0  172.32.1.16 172.32.1.17 255.255.255.240 UG 0 0 0 tunnel0  172.16.10.48 10.3.3.254 255.255.255.240 UG 20 0 0 eth0  172.32.1.0 0.0.0.0 255.255.255.240 U 0 0 0 mgt0  172.29.10.80 10.3.3.203 255.255.255.240 UG 20 0 0 eth0  172.17.107.128 10.3.3.254 255.255.255.128 UG 20 0 0 eth0  -pkt through wan nat on br:  2011-12-13 15:21:57 debug kernel: (i) wifi0.1 172.17.107.130->10.155.3.250(466) ttl(128) icmp-echo-req(768/16896) 60 bytes  2011-12-13 15:21:57 debug kernel: [fe]: MAC session (id [3]) found  2011-12-13 15:21:57 debug kernel: [fe]: fflow 0026:b654:b335->0019:7745:7ec0 flag 0x41002, rflow 0019:7745:7ec0->0026:b654:b335 flag 0xe1210  2011-12-13 15:21:57 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0  2011-12-13 15:21:57 debug kernel: [fe]: update from-access counters 74 bytes  2011-12-13 15:21:57 debug kernel: [fe]: QoS: ingress pkt fwd(wifi0.1) profile=5 qos=2  2011-12-13 15:21:57 debug kernel: [fe]: set pkt to self  2011-12-13 15:21:57 debug kernel: [fe]: swap incoming dev wifi0.1 -> mgt0.4  2011-12-13 15:21:57 debug kernel: [fe]: allow to self-pak, dst-ip 10.155.3.250,allow-arp 0 allow-dhcp 0 allow-forwarding 1  2011-12-13 15:21:57 debug kernel: [fe]: ip forward: ip pkt with dst-ip 10.155.3.250 received on wifi0.1  2011-12-13 15:21:57 debug kernel: [fe]: deliver pak to self on mgt0.4 with fw mark 1  2011-12-13 15:21:57 debug kernel: (u) mgt0.4 172.17.107.130->10.155.3.250(466) ttl(128) icmp-echo-req(768/16896) 60 bytes  2011-12-13 15:21:57 debug kernel: [fe]: iptables PRE\_ROUTING pkt 172.17.107.130(mgt0.4)->10.155.3.250(<NULL>) proto(1) 60 bytes: ACCEPT  2011-12-13 15:21:57 debug kernel: [fe]: iptables FORWARD pkt 172.17.107.130(mgt0.4)->10.155.3.250(eth0) proto(1) 60 bytes: ACCEPT  2011-12-13 15:21:57 debug kernel: [fe]: iptables POST\_ROUTING pkt 10.155.32.55(<NULL>)->10.155.3.250(eth0) proto(1) 60 bytes: ACCEPT  2011-12-13 15:21:57 debug kernel: (o) eth0 10.155.32.55->10.155.3.250(466) ttl(127) icmp-echo-req(768/16896) 74 bytes  2011-12-13 15:21:57 debug kernel: [fe]: bypass fe egress procesing and deliver packet to stack on eth0  2011-12-13 15:21:57 debug kernel: (i) eth0 10.155.3.250->10.155.32.55(1014) ttl(127) icmp-echo-reply(768/16896) 60 bytes  2011-12-13 15:21:57 debug kernel: [fe]: bypass fe ingress procesing and deliver packet to stack on eth0  2011-12-13 15:21:57 debug kernel: [fe]: iptables PRE\_ROUTING pkt 10.155.3.250(eth0)->172.17.107.130(<NULL>) proto(1) 60 bytes: ACCEPT  2011-12-13 15:21:57 debug kernel: [fe]: iptables FORWARD pkt 10.155.3.250(eth0)->172.17.107.130(mgt0.4) proto(1) 60 bytes: ACCEPT  2011-12-13 15:21:57 debug kernel: [fe]: iptables POST\_ROUTING pkt 10.155.3.250(<NULL>)->172.17.107.130(mgt0.4) proto(1) 60 bytes: ACCEPT  2011-12-13 15:21:57 debug kernel: [fe]: bypass fe egress procesing and deliver packet to stack on mgt0.4  2011-12-13 15:21:57 debug kernel: [fe]: mark pkt as from self  2011-12-13 15:21:57 debug kernel: [fe]: inject pkt back into flow from mgt0 xmit  2011-12-13 15:21:57 debug kernel: (i) mgt0.4 10.155.3.250->172.17.107.130(1014) ttl(126) icmp-echo-reply(768/16896) 60 bytes  2011-12-13 15:21:57 debug kernel: [fe]: MAC session (id [3]) found  2011-12-13 15:21:57 debug kernel: [fe]: fflow 0019:7745:7ec0->0026:b654:b335 flag 0xe1210, rflow 0026:b654:b335->0019:7745:7ec0 flag 0x41002  2011-12-13 15:21:57 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0  2011-12-13 15:21:57 debug kernel: [fe]: QoS: host pkt fwd(mgt0.4) qos=2 profile=0  2011-12-13 15:21:57 debug kernel: [fe]: wifi0.1 Tx 0019:7745:7ec0 -> 0026:b654:b335 type 0x0800 74 bytes  2011-12-13 15:21:57 debug kernel: (o) wifi0.1 10.155.3.250->172.17.107.130(1014) ttl(126) icmp-echo-reply(768/16896) 74 bytes  2011-12-13 15:21:57 debug kernel: [fe]: update to-access counters 74 bytes  2011-12-13 15:21:57 debug kernel: [fe]: QoS: pkt queued  2011-12-13 15:21:57 debug kernel: [fe]: Tx:wifi0.1:0> 0019:7745:7ec0->0026:b654:b335 profile idx=0 pkt\_len=74 q\_len=0 QoS buf=0  -pkt goes through tunnel on br:  2012-02-10 16:25:20 debug kernel: (i) wifi0.2 172.17.109.3->172.16.130.120(4569) ttl(128) icmp-echo-req(1/28) 60 bytes  2012-02-10 16:25:20 debug kernel: [fe]: MAC session (id [2]) found  2012-02-10 16:25:20 debug kernel: [fe]: fflow 001e:65f2:5628->0019:7722:1180 flag 0x101002, rflow 0019:7722:1180->001e:65f2:5628 flag 0xe1210  2012-02-10 16:25:20 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0  2012-02-10 16:25:20 debug kernel: [fe]: update from-access counters 74 bytes  2012-02-10 16:25:20 debug kernel: [fe]: QoS: ingress pkt fwd(wifi0.2) profile=5 qos=2  2012-02-10 16:25:20 debug kernel: [fe]: set pkt to self  2012-02-10 16:25:20 debug kernel: [fe]: swap incoming dev wifi0.2 -> mgt0.6  2012-02-10 16:25:20 debug kernel: [fe]: allow to self-pak, dst-ip 172.16.130.120,allow-arp 0 allow-dhcp 0 allow-forwarding 1  2012-02-10 16:25:20 debug kernel: [fe]: ip forward: ip pkt with dst-ip 172.16.130.120 received on wifi0.2  2012-02-10 16:25:20 debug kernel: [fe]: deliver pak to self on mgt0.6 with fw mark 1  2012-02-10 16:25:20 debug kernel: (u) mgt0.6 172.17.109.3->172.16.130.120(4569) ttl(128) icmp-echo-req(1/28) 60 bytes  2012-02-10 16:25:20 debug kernel: [fe]: iptables PRE\_ROUTING pkt 172.17.109.3(mgt0.6)->172.16.130.120(<NULL>) proto(1) 60 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: routing done, 172.17.109.3 -> 172.16.130.120 ttl(128) proto(1) mark(1) 60 bytes, found route in table:Main(Split)  2012-02-10 16:25:20 debug kernel: [fe]: create routing cache:172.17.109.3 -> 172.16.130.120 fwmark 1 dev tunnel0  2012-02-10 16:25:20 debug kernel: [fe]: iptables FORWARD pkt 172.17.109.3(mgt0.6)->172.16.130.120(tunnel0) proto(1) 60 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: iptables POST\_ROUTING pkt 172.17.109.3(<NULL>)->172.16.130.120(tunnel0) proto(1) 60 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: (o) tunnel0 172.17.109.3->172.16.130.120(4569) ttl(127) icmp-echo-req(1/28) 60 bytes  2012-02-10 16:25:20 debug kernel: [fe]: QoS: pkt forwarded  2012-02-10 16:25:20 debug kernel: [fe]: GRE-encap packet: 172.17.109.3->172.16.130.120 ttl(127) proto(1) mark(1) 60 bytes  2012-02-10 16:25:20 debug kernel: [fe]: GRE-encap packet done =>172.32.1.17->10.3.3.202 ttl(127) proto(47) mark(1) 84 bytes  2012-02-10 16:25:20 debug kernel: [fe]: iptables LOCAL\_OUT pkt 172.32.1.17(<NULL>)->10.3.3.202(eth0) proto(47) 84 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: iptables POST\_ROUTING pkt 172.32.1.17(<NULL>)->10.3.3.202(eth0) proto(47) 84 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: encap outgoing packet 172.32.1.17->10.3.3.202 ttl(127) proto(47) 84 bytes  2012-02-10 16:25:20 debug kernel: [fe]: encap(ESP, SPI:b6444bf) packet successfully(rc=0) =>10.2.2.14->10.155.32.174 ttl(64) proto(17) mark(1) 160 bytes  2012-02-10 16:25:20 debug kernel: [fe]: iptables LOCAL\_OUT pkt 10.2.2.14(<NULL>)->10.155.32.174(eth0) proto(17) 160 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: iptables POST\_ROUTING pkt 10.2.2.14(<NULL>)->10.155.32.174(eth0) proto(17) 160 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: (o) eth0 10.2.2.14->10.155.32.174(12884) ttl(64) UDP 4500->4500 174 bytes  2012-02-10 16:25:20 debug kernel: [fe]: bypass fe egress procesing and deliver packet to stack on eth0  -receive reply from BR:  2012-02-10 16:25:20 debug kernel: (i) eth0 10.3.3.202->172.32.1.17(0) ttl(61) proto(47) 84 bytes  2012-02-10 16:25:20 debug kernel: [fe]: bypass fe ingress procesing and deliver packet to stack on eth0  2012-02-10 16:25:20 debug kernel: [fe]: iptables PRE\_ROUTING pkt 10.3.3.202(eth0)->172.32.1.17(<NULL>) proto(47) 84 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: iptables LOCAL\_IN pkt 10.3.3.202(eth0)->172.32.1.17(<NULL>) proto(47) 84 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: recv GRE packet 10.3.3.202->172.32.1.17 ttl(61) proto(47) mark(0) 64 bytes  2012-02-10 16:25:20 debug kernel: [fe]: GRE tunnel found 172.32.1.17<->10.3.3.202 GRE iface (tunnel0) proto(47)  2012-02-10 16:25:20 debug kernel: [fe]: GRE-decap packet done => 172.16.130.120->172.17.109.3 ttl(61) proto(1) mark(0) 60 bytes  2012-02-10 16:25:20 debug kernel: (i) tunnel0 172.16.130.120->172.17.109.3(1039) ttl(61) icmp-echo-reply(1/28) 60 bytes  2012-02-10 16:25:20 debug kernel: [fe]: deliver pak to self on tunnel0 with fw mark 0  2012-02-10 16:25:20 debug kernel: (u) tunnel0 172.16.130.120->172.17.109.3(1039) ttl(61) icmp-echo-reply(1/28) 60 bytes  2012-02-10 16:25:20 debug kernel: [fe]: iptables PRE\_ROUTING pkt 172.16.130.120(tunnel0)->172.17.109.3(<NULL>) proto(1) 60 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: routing done, 172.16.130.120 -> 172.17.109.3 ttl(61) proto(1) mark(0) 60 bytes, found route in table:Main(Split)  2012-02-10 16:25:20 debug kernel: [fe]: create routing cache:172.16.130.120 -> 172.17.109.3 fwmark 0 dev mgt0.6  2012-02-10 16:25:20 debug kernel: [fe]: iptables FORWARD pkt 172.16.130.120(tunnel0)->172.17.109.3(mgt0.6) proto(1) 60 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: iptables POST\_ROUTING pkt 172.16.130.120(<NULL>)->172.17.109.3(mgt0.6) proto(1) 60 bytes: ACCEPT  2012-02-10 16:25:20 debug kernel: [fe]: bypass fe egress procesing and deliver packet to stack on mgt0.6  2012-02-10 16:25:20 debug kernel: [fe]: mark pkt as from self  2012-02-10 16:25:20 debug kernel: [fe]: inject pkt back into flow from mgt0 xmit  2012-02-10 16:25:20 debug kernel: (i) mgt0.6 172.16.130.120->172.17.109.3(1039) ttl(60) icmp-echo-reply(1/28) 60 bytes  2012-02-10 16:25:20 debug kernel: [fe]: MAC session (id [2]) found  2012-02-10 16:25:20 debug kernel: [fe]: fflow 0019:7722:1180->001e:65f2:5628 flag 0xe1210, rflow 001e:65f2:5628->0019:7722:1180 flag 0x41002  2012-02-10 16:25:20 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0  2012-02-10 16:25:20 debug kernel: [fe]: QoS: host pkt fwd(mgt0.6) qos=2 profile=0  2012-02-10 16:25:20 debug kernel: [fe]: wifi0.2 Tx 0019:7722:1180 -> 001e:65f2:5628 type 0x0800 74 bytes  2012-02-10 16:25:20 debug kernel: (o) wifi0.2 172.16.130.120->172.17.109.3(1039) ttl(60) icmp-echo-reply(1/28) 74 bytes  2012-02-10 16:25:20 debug kernel: [fe]: update to-access counters 74 bytes  2012-02-10 16:25:20 debug kernel: [fe]: QoS: pkt queued  2012-02-10 16:25:20 debug kernel: [fe]: Tx:wifi0.2:0> 0019:7722:1180->001e:65f2:5628 profile idx=0 pkt\_len=74 q\_len=0 QoS buf=0 | | |
| Comment | -IPs in examples:  -cvg.wan=10.3.3.202  -cvg.fw=10.155.32.174  -cvg.mgt0=172.32.1.1  -br.wan=10.2.2.14  -br.mgt0=172.32.1.17  -br.fw= 10.155.32.170  -br.client=172.17.109.3  -cvg.pc=172.16.130.120  -debug and filters:  -‘\_ff id 1 src-ip 172.17.109.3 protocol 1 bid’  -‘\_ff id 2 protocol 47 bidirectional’  -‘\_ff id 3 protocol 50 bidirectional’  -‘\_kde fe detail’  -‘\_kde fe basic’  -add static ip route under shell for test purpose:  “ip route add BR\_SUBNET via BR\_WAN\_IP dev tunnel0 onlink”, on CVG side  “ip route add CVG\_SUBNET dev tunnel0”, on BR side  -we don’t contain any case of wan nat enable on CVG since HM does not support this way now | | |

### CVG is wan only, BR is wan nat, the CVG and BR are all behind NAT

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_User\_Scenario\_2 | | |
| Priority | Accept | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | CVG is wan only, BR is wan nat, the CVG and BR are all behind NAT | | |
| Pre-condition | -config CVG with WAN interface, nat disable  no interface ethx mode wan nat  -config CVG act as l3 VPN server  -one LAN on CVG  -config BR with WAN interface, nat enable  -config BR as l3 VPN client  -one LAN on BR  -both BR and CVG are behind a FW  -traffic from wan of CVG can reach wan of BR, the LANs are unreachable from each other  -clock time sync with BR/CVG | | |
| Test procedure | **-check the status of vpn connection**  **-check Ike sa and sp is correct on both CVG and BR sides**  **-check the tunnel interface created after vpn connection success**  **-check the l3 tunnel created correctly on both sides**  **-check the ip of mgt0 is added to the peer via tunnel0 in route table**  **-BR will announce LANs under it, check the route table on CVG**  **-CVG will push the LANs under it to BR, check the route table on BR**  **-after vpn connection was setup, check the traffic forward via vpn from BR side based on route table**  **-STA1 under BR ping a remote server in cloud**  **-STA1 under BR ping a remote server behind CVG**  **-BR ping a server in cloud**  **-BR ping a server behind CVG** | | |
| Expect result | 1. Vpn connection can setup between the two nodes successfully 2. Check the status of ike sa, destination IP should be the peer’s wan ip, port(no nat with 500 both, if nat, it’s 4500 on BR, random on CVG side) is correct, and the ST is 9, S is I on BR and R on CVG 3. Check the status of ike sp, the local ip and remote ip is correct, bidirectional, proto is gre(47), esp tunnel mode, and the ip addr is the peer’s wan ip 4. Check the gre tunnel is correct on both BR and cvg, ‘sh vpn layer-3-tunnel’ to check 5. The traffic from clients(wired or wireless, laptop1 and laptop2) forwards correctly as based on route, vpn or wan nat 6. The managerment traffice of BR self forwards correctly based on route table 7. No broadcast traffic should go though tunnel | | |
| Comment | -overall process:  2011-07-22 03:30:01:Phase 1 established(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Xauth exchange start(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Xauth exchange passed(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Add security policy into kernel stack done(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:ISAKMP mode config done(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Phase 2 started(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Phase 2 established(10.155.32.6[4500]->10.155.32.172[4500]) | | |

### CVG is wan only, BR is wan nat, only BR behind NAT

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_User\_Scenario\_3 | | |
| Priority | Accept | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | CVG is wan only, BR is wan nat, only BR behind NAT | | |
| Pre-condition | -config CVG with WAN interface,no nat enable  -config eth0 port as bridge-access, mac-learning enable  -config CVG act as l3 VPN server  -one LAN on CVG  -config BR with WAN interface, nat enable  -config BR as l3 VPN client  -one LAN on BR  -BR is behind a NAT firewall(NAPT)  -traffic from wan of CVG can reach wan of BR, the LANs are unreachable from each other | | |
| Test procedure | **-check the status of vpn connection**  **-check Ike sa and sp is correct on both CVG and BR sides**  **-check the l3 tunnel created correctly on both sides**  **-check the ip of mgt0 is added to the peer via tunnel0 in route table**  **-BR will announce LANs under it, check the route table on CVG**  **-CVG will push the LANs under it to BR, check the route table on BR**  **-after vpn connection was setup, check the traffic forward via vpn from BR side based on route table**  **-STA1 under BR ping a remote server in cloud**  **-STA1 under BR ping a remote server behind CVG**  **-BR ping a server in cloud**  **-BR ping a server behind CVG** | | |
| Expect result | 1. Vpn connection can setup between the to nodes successfully 2. The status of ike sa and sp are correct 3. The traffic from clients(wired or wireless) forwards correctly as pre-defined based on route, vpn or wan nat 4. The managerment traffice of BR self forwards correctly based on route table 5. The traffic from clients under BR can be forwarded correctly based on the route table 6. The traffic from client under CVG can be forwarded correctly | | |
| Comment | -overall process:  2011-07-22 03:30:01:Phase 1 established(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Xauth exchange start(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Xauth exchange passed(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Add security policy into kernel stack done(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:ISAKMP mode config done(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Phase 2 started(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Phase 2 established(10.155.32.6[4500]->10.155.32.172[4500]) | | |

### CVG is wan only, BR is wan nat, only CVG behind NAT

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_User\_Scenario\_4 | | |
| Priority | Accept | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | CVG is wan only, BR is wan nat, only CVG behind NAT | | |
| Pre-condition | -config CVG with WAN interface,no nat enable  -config eth0 port as bridge-access, mac-learning enable  -config CVG act as l3 VPN server  -one LAN on CVG  -config BR with WAN interface, nat enable  -config BR as l3 VPN client  -one LAN on BR  -CVG is behind a NAT firewall(MIPS)  -traffic from wan of CVG can reach wan of BR, the LANs are unreachable from each other | | |
| Test procedure | **-check the status of vpn connection**  **-check Ike sa and sp is correct on both CVG and BR sides**  **-check the l3 tunnel created correctly on both sides**  **-check the ip of mgt0 is added to the peer via tunnel0 in route table**  **-BR will announce LANs under it, check the route table on CVG**  **-CVG will push the LANs under it to BR, check the route table on BR**  **-after vpn connection was setup, check the traffic forward via vpn from BR side based on route table**  **-check the traffic forward via nat from BR side based on route table**  **-check the traffic forward via vpn from CVG side based on route table**  **-check the traffic forward between LAN and wan on CVG side**  **-the traffic contans both client and CVG/BR self management** | | |
| Expect result | 1. Vpn connection can setup between the to nodes successfully 2. The status of ike sa and sp are correct 3. The traffic from clients(wired or wireless) forwards correctly as pre-defined based on route, vpn or wan nat 4. The managerment traffice of BR self forwards correctly based on route table 5. The traffic from clients under BR can be forwarded correctly based on the route table 6. The traffic from client under CVG can be forwarded correctly | | |
| Comment | -overall process:  2011-07-22 03:30:01:Phase 1 established(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Xauth exchange start(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Xauth exchange passed(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Add security policy into kernel stack done(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:ISAKMP mode config done(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Phase 2 started(10.155.32.6[4500]->10.155.32.172[4500])  2011-07-22 03:30:01:Phase 2 established(10.155.32.6[4500]->10.155.32.172[4500]) | | |

## Function Test Case

### ISAKMP (Main Mode)

#### A minimal configuration for layer 3 vpn

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_1 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | A minimium configuration for layer 3 vpn | | |
| Pre-condition |  | | |
| Test procedure | -CVG side:  -configure a xauth-client-list  -enable server-ipsec-tunnel layer-3 mode  -bind the client-list to ipsec-tunnel  -bind the ipsec-tunnel to tunnel-policy  -BR side:  -configure client-ipsec-tunnel layer-3 mode enable  -configure ipsec-tunnel gateway  -bind the ipsec-tunnel to tunnel-policy  -leave all other parameters default  -check ike sa/sp, ipsec sa BR/CVG  -check layer-3-tunnel on BR/CVG  -check ipsec-tunnel | | |
| Expect result | 1. the vpn tunnel could be created successfully 2. Traffic can pass through vpn tunnel success | | |
| Test result | -debug info:  2011-08-12 17:12:24 debug kernel: (i) wifi0.2 172.17.106.222->61.135.169.125(32565) ttl(128) icmp-echo-req(768/50176) 60 bytes  2011-08-12 17:12:24 debug kernel: [fe]: MAC session (id [3]) found  2011-08-12 17:12:24 debug kernel: [fe]: fflow 0026:b654:b335->0019:7745:97c0 flag 0x41202, rflow 0019:7745:97c0->0026:b654:b335 flag 0xe1010  2011-08-12 17:12:24 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0  2011-08-12 17:12:24 debug kernel: [fe]: QoS: ingress pkt fwd(wifi0.2) profile=2000 qos=2  2011-08-12 17:12:24 debug kernel: [fe]: set pkt to self  2011-08-12 17:12:24 debug kernel: [fe]: swap incoming dev wifi0.2 -> mgt0  2011-08-12 17:12:24 debug kernel: [fe]: allow to self-pak, dst-ip 61.135.169.125,allow-arp 0 allow-dhcp 0 allow-forwarding 1  2011-08-12 17:12:24 debug kernel: [fe]: deliver pak to self on mgt0 with fw mark 4  2011-08-12 17:12:24 debug kernel: (u) mgt0 172.17.106.222->61.135.169.125(32565) ttl(128) icmp-echo-req(768/50176) 60 bytes  2011-08-12 17:12:24 debug kernel: [fe]: routing done, 172.17.106.222 -> 61.135.169.125 ttl(128) proto(1) mark(4) 60 bytes, found route in table:Tunnel-All  2011-08-12 17:12:24 debug kernel: [fe]: create routing cache:172.17.106.222 -> 61.135.169.125 fwmark 4 dev tunnel0  2011-08-12 17:12:24 debug kernel: (o) tunnel0 0000:7f01:be97->4500:003c:7f35(0xac11) 60 bytes  2011-08-12 17:12:24 debug kernel: [fe]: QoS: pkt forwarded  2011-08-12 17:12:24 debug kernel: [fe]: GRE-encap packet: 172.17.106.222->61.135.169.125 ttl(127) proto(1) mark(4) 60 bytes  2011-08-12 17:12:24 debug kernel: [fe]: GRE-encap packet done =>10.155.32.6->10.3.3.202 ttl(127) proto(47) mark(4) 84 bytes  2011-08-12 17:12:24 debug kernel: [fe]: encap outgoing packet 10.155.32.6->10.3.3.202 ttl(127) proto(47) 84 bytes  2011-08-12 17:12:24 debug kernel: [fe]: encap(ESP, SPI:11afdfb) packet successfully(rc=-115) =>10.155.32.6->10.155.32.174 ttl(64) proto(17) mark(4) 160 bytes  2011-08-12 17:12:24 debug kernel: [fe]: recv GRE packet 10.3.3.202->10.155.32.6 ttl(46) proto(47) mark(0) 64 bytes  2011-08-12 17:12:24 debug kernel: [fe]: GRE tunnel found 10.155.32.6<->10.3.3.202 GRE iface (tunnel0) proto(47)  2011-08-12 17:12:24 debug kernel: [fe]: GRE-decap packet done => 61.135.169.125->172.17.106.222 ttl(46) proto(1) mark(0) 60 bytes  2011-08-12 17:12:24 debug kernel: (i) tunnel0 4000:2e2f:140e->4500:0054:0000(0x0a03) 60 bytes  2011-08-12 17:12:24 debug kernel: [fe]: deliver pak to self on tunnel0 with fw mark 0  2011-08-12 17:12:24 debug kernel: (u) tunnel0 4000:2e2f:140e->4500:0054:0000(0x0a03) 60 bytes  2011-08-12 17:12:24 debug kernel: [fe]: routing done, 61.135.169.125 -> 172.17.106.222 ttl(46) proto(1) mark(0) 60 bytes, found route in table:Main(Split)  2011-08-12 17:12:24 debug kernel: [fe]: create routing cache:61.135.169.125 -> 172.17.106.222 fwmark 0 dev mgt0  2011-08-12 17:12:24 debug kernel: [fe]: mark pkt as from self  2011-08-12 17:12:24 debug kernel: [fe]: inject pkt back into flow from mgt0 xmit  2011-08-12 17:12:24 debug kernel: (i) mgt0 61.135.169.125->172.17.106.222(32565) ttl(45) icmp-echo-reply(768/50176) 60 bytes  2011-08-12 17:12:24 debug kernel: [fe]: MAC session (id [3]) found  2011-08-12 17:12:24 debug kernel: [fe]: fflow 0019:7745:97c0->0026:b654:b335 flag 0xe1010, rflow 0026:b654:b335->0019:7745:97c0 flag 0x41202  2011-08-12 17:12:24 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0  2011-08-12 17:12:24 debug kernel: [fe]: QoS: host pkt fwd(mgt0) qos=2 profile=0  2011-08-12 17:12:24 debug kernel: [fe]: wifi0.2 Tx 0019:7745:97c0 -> 0026:b654:b335 type 0x0800 74 bytes  2011-08-12 17:12:24 debug kernel: (o) wifi0.2 61.135.169.125->172.17.106.222(32565) ttl(45) icmp-echo-reply(768/50176) 74 bytes | | |
| Comment | -filter gre, esp and icmp packets  -\_ff id 1 protocol 47, \_ff id 2 protocol 47, \_ff id 1 protocol 1 | | |

#### All types of auth-method should work

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_2 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | All types of auth-method should work | | |
| Pre-condition | -both CVG and BR use the same auth method | | |
| Test procedure | -as the minimal configuration of l3 vpn, change the auth-method  -check the status of vpn tunnel | | |
| Expect result | 1. Auth method hybrid is most important, rsa-sig is not commonly used, psk is deprecated 2. Tunnel should be created successful when all cert and password are matched 3. Traffic can pass through vpn tunnel success(ping success is ok) | | |
| Test result |  | | |
| Comment |  | | |

#### All types of encryption algorithm should work, both phase 1 and 2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_3 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | All types of encryption algorithm should work, both phase 1 and 2 | | |
| Pre-condition | -a minimal l3 vpn configuration is done, both CVG and BR | | |
| Test procedure | -change the various encryption method  -check the vpn tuunel  -check the traffic pass through tunnel | | |
| Expect result | 1. Vpn tunnel could setup successfully 2. Traffic can pass through vpn tunnel success | | |
| Test result |  | | |
| Comment | -so far, we support 3des,aes128,aes192,aes256, default is aes128 | | |

#### All types of dh-group should work in phase 1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_4 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | All types of dh-group should work in phase 1 | | |
| Pre-condition |  | | |
| Test procedure | 1. Verify that default dh-group is group2 2. Check that the proposal contains group2 in first exchanged. 3. Check that the nonce payload is according to in the second exchanged and the length of nonce payload MUST be between 8 and 256 bytes inclusive. 4. Check that the Diffie-Hellman public value passed in a KE payload, in either a phase 1 or phase 2 exchange, MUST be the length of the negotiated Diffie-Hellman group enforced, if necessary, by pre-pending the value with zeros 5. Check that the content of “show vpn ike configuration”is according to 6. Repeated the upper steps when change the dh-group to group1 7. Repeated the upper steps when change the dh-group to group5 8. Verify that the default value is group5 when no command is excuted. 9. Repeated the upper steps in abg boxes. | | |
| Expect result | 1. Vpn tunnel could setup successfully 2. Traffic can pass through vpn tunnel success | | |
| Test result |  | | |
| Comment | -now we support group1, 2, 5 in phase 1 | | |

#### All types of hash(HMAC) method should work, both phase 1 and 2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_5 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | All types of hash(HMAC) method should work, both phase 1 and 2 | | |
| Pre-condition |  | | |
| Test procedure | 1. Verify that default Hash algorithm is SHA1 2. Check that the proposal contains hybrid in first exchanged 3. Verify that the content of “show vpn ike configuration”is according to 4. Verify that the config mode and phass II is hased by SHA1. 5. Repeated the upper step for MD5 6. Repeated the upper step for abg box | | |
| Expect result | 1. Vpn tunnel could setup successfully 2. Traffic can pass through vpn tunnel success | | |
| Test result |  | | |
| Comment | -now we support md5, sha1 in both phase 1 and phase 2 | | |

#### Check the retransmission in ISAKMP processs

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_6 | | |
| Priority | Low | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | When transmitting an ISAKMP message, the Timer and Counter must do the following.(from RFC2408) | | |
| Pre-condition |  | | |
| Test procedure | 1. Set a timer and initialize a retry counter. NOTE: Implementations MUST NOT use a fixed timer. Instead, transmission timer values should be adjusted dynamically based on measured round trip times. In addition, successive retransmissions of the same packet should be separated by increasingly longer time intervals (e.g., exponential backoff).  2. If the timer expires, the ISAKMP message is resent and the retry counter is decremented.  3. If the retry counter reaches zero (0), the event, RETRY LIMIT REACHED, MAY be logged in the appropriate system audit file.  4. The ISAKMP protocol machine clears all states and returns to  IDLE.  5. verify that our device following the advice for the main mode packet.(counter == 3 && timer == 10s now) | | |
| Expect result |  | | |
| Test result |  | | |
| Comment |  | | |

#### using IPV4\_ADDR as the ID in Identity Payload works

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_7 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | using IPV4\_ADDR as the ID in Identity Payload works | | |
| Pre-condition | -a minimal configuration of vpn CVG/BR is done | | |
| Test procedure | 1. configure the local-ike-id and peer-ike-id are set as ip 2. Implementations MUST be capable of verifying that the IP address presented in ID matches via bitwise comparison the IP address present in the certificate’s iPAddress field of the SubjectAltName extension. 3. Certificates may contain multiple address identity types -- in which case, at least one must match the source IP. 4. Implementation MUST be capable of verifying that the address contained in the ID is the same as the address contained in the IP header. Implementations SHOULD be able to check the address in either the outermost or innermost IP header and MAY provide a configuration option provided, an implementation SHOULD check the peer source address contained in the outermost header. If ID is one of the IP address types, then implementations MUST perform this verification by default. 5. A mismatch between the two address MUST be treated as an error, and security association setup MUST be aborted. This event SHOULD be auditable(notice information) 6. When the ID mismatch with the local-ike-id authentication does not care about. If the local-ike-id is not set check is not done. 7. When the peer-ike-id is not set but the local-ike-id is set verify the result. 8. When the hybrid is set the check is always not done for initiator. 9. When rsa-sig is set the upper steps need be verified in both sides. | | |
| Expect result |  | | |
| Test result | -log info:  2011-08-11 16:17:20:Compare IKE ID and certificate name failed(10.155.32.6[4500]->10.155.32.174[4500]) | | |
| Comment | RFC4945  Deployments may only want to consider using the IP address as ID if  all of the following are true:  o the peer’s IP address is static, not dynamically changing  o the peer is NOT behind a NAT’ing device  o the administrator intends the implementation to verify that the  peer source address matches the IP address in the ID received, and  that in the iPAddress field in the peer certificate’s  SubjectAltName extension. | | |

#### using FQDN as the ID in Identity Payload works

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_8 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | using FQDN as the ID in Identity Payload works | | |
| Pre-condition | -a minimal configuration of vpn CVG/BR is done | | |
| Test procedure | 1. configure local-ike-id and peer-ike-id are set as FQDN 2. If ID contains an ID\_FQDN, implementations MUST be capable of verifying that the identity contained in the ID payload matches identity information contained in the peer end-entity certificate, in the dNSName field in the SubjectAltName extension. Implementations MUST perform this verification by default. 3. When comparing the contents of ID with the dNSName field in the SubjectAltName extension for equality, case-insensitive string comparison MUST be performed. 4. If this default is enabled, then a mismatch MUST be treated as an error, and security associate setup MUST be aborted. 5. When the ID mismatch with the local-ike-id authentication does not care about. If the local-ike-id is not set check is not done. 6. When the peer-ike-id is not set but the local-ike-id is set verify the result. 7. When the hybrid is set the check is always not done for initiator. 8. When rsa-sig is set the upper steps need be verified in both sides. | | |
| Expect result |  | | |
| Comment |  | | |

#### using USER\_FQDN as the ID in Identity Payload work

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_9 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | using USER\_FQDN as the ID in Identity Payload work | | |
| Pre-condition | -a minimal configuration of vpn CVG/BR is done | | |
| Test procedure | 1. configure local-ike-id and peer-ike-id are set as USER\_FQDN 2. Implementations MUST be capable of verifying that identity contained in the ID payload matches identity information contained in the peer end-entity certificate, in the rfc822Name field in the SubjectAltName extension. Implementations MUST perform this by default. 3. When comparing the contents of ID with the rfc822Name field in the SubjectAltName extension for equality, case-insensitive string comparison MUST be performed. 4. If this default is enabled, then a mismatch MUST be treated as an error, and security associate setup MUST be aborted. 5. When the ID mismatch with the local-ike-id authentication does not care about. If the local-ike-id is not set check is not done. 6. When the peer-ike-id is not set but the local-ike-id is set verify the result. 7. When the hybrid is set the check is always not done for initiator. 8. When rsa-sig is set the upper steps need be verified in both sides. | | |
| Expect result |  | | |
| Comment | Log must have | | |

#### using DER\_ASN1\_DN as the ID in Identity Payload work

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_10 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | Using DER\_ASN1\_DN as the ID in Identity Payload work | | |
| Pre-condition | - a minimal configuration of vpn CVG/BR is done | | |
| Test procedure | 1. configure local-ike-id and peer-ike-id are set as asn1dn 2. When generating this type, implementations MUST popular the contents of ID with the Subject field from the end-entity certificate, and MUST do so such that a binary comparison of the two will succeed. 3. Implementation MUST NOT populate ID with the Subject from the end-entity certificate if it is empty, even though an empty certificate Subject is explicitly allowed in the ‘Subject’ section of the PKIX certificate profile. 4. MUST support lookup on any combination of C, CN, O, or OU. 5. If there is not a match, this MUST be treated as an error, and security associate setup MUST be aborted. This event SHOULD be auditable. 6. When the ID mismatch with the local-ike-id authentication does not care about. If the local-ike-id is not set check is not done. 7. When the peer-ike-id is not set but the local-ike-id is set verify the result. 8. When the hybrid is set the check is always not done for initiator. 9. When rsa-sig is set the upper steps need be verified in both sides. | | |
| Expect result |  | | |
| Comment | Log must have | | |

#### Verify that the certificate availability include CA and Service certificate etc

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_11 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | Verify the certificate availability include CA and Service certificate etc | | |
| Pre-condition |  | | |
| Test procedure | 1. Implementations MUST support certificates that contain more than a single identity, such as when the Subject field and the SubjectAltName extension are both populated, or the SubjectAltName extension contains multiple identities irrespective of whether or not the Subject is empty. In many cases, a certificate will contain an identity, such as an IP address, in the SubjectAltName extension in addition to a non-empty Subject 2. Verify that the valid date of the server certification is out of the current date then authentication fails 3. Verify that the valid date of the CA is out of the current date then the authentication fails. 4. Verify that authentication fails when the CA mismatch with service certification. 5. Verify that authentication fails when the service certification mismatch with private key. 6. Verify that packet can be deal with correctly when service certification is large(such as more than 1500 bytes total) 7. Verify that authentication fail when CA or server certification or private key are not stored. 8. The upper step need be performed in both side when auth-mode is rsa-sig | | |
| Expect result |  | | |
| Comment | Comment: log info. | | |

#### disable nat-traversal function

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_12 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | disable nat-traversal function | | |
| Pre-condition |  | | |
| Test procedure | 1. The Vendor ID - RFC3947 is not contained in first exchange. 2. The NAT-D payload is not contained in the second exchange. 3. The port is not changed to 4500 and Non-ESP Marker does not appear in the third exchange. 4. If there is NAT in the middle. There is log recorded. | | |
| Expect result |  | | |
| Comment | -Nat-traversal is enable by default | | |

#### Various reasons cause IKE Phase 1 fail

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_13 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | Various reasons cause IKE Phase 1 fail | | |
| Pre-condition | -a minimal configuration of vpn tunnel is setup | | |
| Test procedure | -upload certs on CVG and BR, the CA and vpn CVG certs mismatch  -clock time on BR/CVG is overtake the cert deadline  -the client-name and password mismatch with CVG/BR | | |
| Expect result |  | | |
| Test result | -parameter mismatch:  2011-08-03 10:09:54 err ah\_vpn: <IKE> receive notify message:NO-PROPOSAL-CHOSEN  2011-08-04 11:15:32 info ah\_vpn: <IKE 10.155.32.8[500]> ERROR: Phase 1 proposal mismatch with peer  2011-08-04 11:15:32 info ah\_vpn: <IKE 10.155.32.8[500]> ERROR: Phase 1 proposal mismatch, failed to get valid proposal.  2011-08-04 11:15:32 info ah\_vpn: <IKE 10.155.32.8[500]> ERROR: no suitable proposal found.  2011-08-04 11:15:32 info ah\_vpn: <IKE> ERROR: rejected authmethod: DB(prop#1:trns#1):Peer(prop#1:trns#1) = Hybrid RSA server:Hybr id RSA client | | |
| Comment | -‘sh vpn ike event’ or ‘sh log bu’ to check | | |

### ISAKMP Config Mode (included XAuth)

#### FT\_RemoteVPN\_Config\_Mode\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_CONFIG\_1 | | |
| Priority | Low | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | Xauth authentication procession is valid in the phass of Config Mode | | |
| Pre-condition | Hybrid auth mode is set. | | |
| Test procedure | 1. The Phase 1 Exchange MUST be immediately followed by a Transaction Exchange whose initiator is the Edge Device 2. The Transaction Exchange MUST be protected by the IKE SA negotiated in the preceding Phase 1 Exchange 3. This IKE SA MUST NOT be used for any other exchange before the Transaction Exchange terminates successfully and the User is authenticated 4. ISAKMP\_CFG\_REQUEST - This message is sent from an edge device to an IPSec host trying to request extended authentication. Attributes that it requires sent back in the reply MUST be included with a length of zero (0). Attributes required for the authentication reply, such as a challenge string MUST be included with the proper values filled in. 5. ISAKMP\_CFG\_REPLY - This message MUST contain the filled in authentication attributes that were requested by the edge device or if the proper authentication attributes can not be retrieved, then this message MUST contain the XAUTH\_STATUS attribute with a value of FAIL. 6. ISAKMP\_CFG\_SET - This message is sent from an edge device and is only used, within the scope of this document, to state the success of the authentication. This message MUST only include the success or failure of the authentication and MAY contain some clarification text. 7. ISAKMP\_CFG\_ACK - This message is sent from the IPSec host acknowledging receipt of the authentication result. Its attributes are not relevant and MAY be skipped entirely, thus no attributes SHOULD be included. This last message in the authentication transaction is used solely as an acknowledgement of the previous message and to eliminate problems with unacknowledged messages over UDP. | | |
| Expect result |  | | |
| Comment | 4.2 Attributes  Attribute Value Type  --------------------- ------ ---------------------  XAUTH\_TYPE 16520 Basic  XAUTH\_USER\_NAME 16521 Variable ASCII string  XAUTH\_USER\_PASSWORD 16522 Variable ASCII string  XAUTH\_PASSCODE 16523 Variable ASCII string  XAUTH\_MESSAGE 16524 Variable ASCII string  XAUTH\_CHALLENGE 16525 Variable ASCII string  XAUTH\_DOMAIN 16526 Variable ASCII string  XAUTH\_STATUS 16527 Basic | | |

#### FT\_RemoteVPN\_Config\_Mode\_2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_CONFIG\_2 | | |
| Priority | Low | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | Xauth authentication procession is valid in the phass of Config Mode | | |
| Pre-condition | Hybrid auth mode is set. | | |
| Test procedure | 1. Verify that the max and min length or especial characters can be set for local name and password. 2. When the client name and password in remote side match the client name and password in server side notice that the maximal length, minimum length, especial characters, case-sensitive. 3. The Server can search the correct the user-name and password when multi user-name and password are set. 4. Verify the client action when multi user-name and password are set in local. 5. Verify when user-name or password mismatch then authentication failed. 6. Verify that the user-name or password is changed in remote side or server side after phase II what happen. 7. If the extended authentication fails, then the phase 1 SA MUST be immediately deleted. The edge device MAY choose to retry an extended authentication request if the user failed to retry an be authenticated, but must do so in the same ISAKMP-Config transaction, and MUST NOT send the SET message until the user is authenticated, or until the edge device wishes to stop retrying and fail the user. 8. Extended Authentication MAY be initiated by the edge device at any time after the initial authentication exchange. For example, RADIUS servers may specify that a user only be authenticated for a certain time period. Once that time period has elapsed (minus a possible jitter), the edge device may request a new Extended Authentication exchange. If the Extended Authentication exchange fails, the edge device MUST tear down all phase 1 and phase 2 SAs associated with the user.(it is tested when Remote AP - Advanced functions (Failover, tunnel option of mgmt traffic, restartability) is utilized) | | |

### ISAKMP NAT Traversal

#### FT\_RemoteVPN\_NAT\_Traversal\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_NAT\_TRAVERSAL\_1 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | Capability and Negotiation of Nat-Traversal in Phass I | | |
| Pre-condition |  | | |
| Test procedure | 1. The Vendor ID of NAT-Traversal is contained in the first exchange. 2. The NAT-D payload is contained in the second exchange. 3. Ports are not be changed to 4500 and Non-ESP Marker is not attached to the packets in the third exchange when there is not NAT in the middle. 4. Both Ports is changed to 4500 in initiator. In addition, the IKE data MUST be prepended with a non-ESP marker allowing for demultiplexing of trffic. 5. When NAT-Traversal is supported in box but NAT exist between remote and gateway. Ipsec SA can be created but Data traffic broken. 6. “The NAT-D payload not only detects the presence of NAT between the two IKE peers, but also detects where the NAT is. The location of the NAT device is important, as the keepalives have to initiate from the peer "behind" the NAT“ so place NAT device in different place to verify the initiator of the keepalive. | | |
| Expect result |  | | |
| Comment | The first NAT-D payload contains the remote end’s IP address and port (i.e., the destination address of the UDP packet). The remaining NAT-D payloads contain possible local-end IP addresses and ports (i.e., all possible source addresses of the UDP packet) | | |

#### FT\_RemoteVPN\_NAT\_Traversal\_2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_NAT\_TRAVERSAL\_2 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | Rekey happen in phass I and phass II when NAT is supported. | | |
| Pre-condition |  | | |
| Test procedure | 1. If the responder has to rekey the Phase 1 SA, then the rekey negotiation MUST be started by using UDP(4500,Y). Any implementation that supports NAT traversal MUST support negotiations that begin on port 4500. If a negotiation starts on port 4500, then it doesn’t need to change anywhere else in the exchange. 2. Verify the result rekey happen in phase II and NAT is supported. | | |
| Expect result |  | | |
| Comment |  | | |

#### FT\_RemoteVPN\_NAT\_Traversal\_3

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_NAT\_TRAVERSAL\_3 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | Nat Keepalive is carried out in box. | | |
| Pre-condition |  | | |
| Test procedure | 1. Nat Keepalive is send from the device behind NAT. 2. The sender MUST use a one-octet-long payload with the value 0xFF. 3. The receiver SHOULD ignore a received NAT-keepalive packet. | | |
| Expect result |  | | |
| Comment |  | | |

### ISAKMP Rekey Test

#### IKE phase 2 rekey

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_REKEY\_1 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | IKE phase 2 rekey work | | |
| Pre-condition | -a minimal BR/GW environment setup | | |
| Test procedure | -check the phase to lifetime  -wait for the phase to lifetime out  -the ike phase two will renegotiate, new sa will be generated  -after phase 2 rekey, check the tunnel status  -check route table, pay attention to the tunnel routes  -check the traffic on tunnel after phase2 rekey | | |
| Expect result | 1. after phase 2 lifetime is out, phase 2 will renegotiate the sa 2. layer-3-tunnel status should be correct 3. after tunnel is down, the tunnel routes should be removed 4. after tunnel is up, the tunnel routes should be added correctly 5. traffic can pass through tunnel after rekey | | |
| Comment | -default lifetime of phase2 is 3600  -parameter mismatch will cause ike negotiation fail | | |

#### IKE phase 1 rekey

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_REKEY\_2 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | IKE phase 1 rekey | | |
| Pre-condition | -a minimal BR/GW environment setup | | |
| Test procedure | -Configure IKE Phase 1 lifetime to be the minimum value (180 sec)  -Configure IKE Phase 2 lifetime to be 230 sec, so that IKE Phase 1 SA would expire before IKE Phase 2 SA rekeys  -Verify IKE Phase 2 SA is rekeyed before its lifetime expires.  -Verify Only IKE Phase 2 rekey when it’s lifte time is longer than phase 1 life time.  -Verify system clock is changed in remote or gateway side.  -repeated with no NAT devices between the VPN client and VPN server  -after phase1 rekey is done, check the tunnel status  -check the tunnel routes | | |
| Expect result | -tunnel status should be correct, “sh vpn layer-3-tunnel” to check  -tunnel routes should be added correct to route table | | |
| Comment | -default lifetime of phase1 is 86400 | | |

#### rekey of multi tunnels on BR

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_REKEY\_3 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | rekey of multi tunnels on BR | | |
| Pre-condition | -there are two vpn tunnels on BR  -the life time of the two tunnels are different | | |
| Test procedure | -check the rekey on two tunnels is correct  -check the tunnel status  -check the tunnel routes, both on BR and CVG  -check traffic pass through the two tunnels | | |
| Expect result | 1. after rekey, the vpn tunnel would recreate successfully 2. traffic could pass through tunnel success | | |
| Comment |  | | |

#### rekey of multi tunnels on CVG

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_ISAKMP\_REKEY\_4 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 2 | | |
| Description | rekey of multi tunnels on CVG | | |
| Pre-condition | -there are several vpn tunnels on CVG  -the life time of the two tunnels are different | | |
| Test procedure | -check the rekey on two tunnels is correct  -check the tunnel status  -check the tunnel routes, both on BR and CVG  -check traffic pass through the two tunnels | | |
| Expect result | 1. after rekey, the vpn tunnel would recreate successfully 2. traffic could pass through tunnel success | | |
| Comment |  | | |

### Mgmt-Traffic Tunneling (From BR self to CVG)

#### traffic from BR to dest which is behind the remote CVG should passed successfully through VPN tunnel

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_MGMT\_TRAFFIC\_1 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | traffic from BR to dest which is behind the remote CVG should passed successfully through VPN tunnel | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG | | |
| Test procedure | -BR trigger icmp traffic to the LAN behind remote CVG  -BR trigger udp traffic to the LAN behind remote CVG  -BR trigger tcp traffic to the LAN behind remote CVG | | |
| Expect result | 1. BR should receive correct icmp response 2. BR should receive correct udp response 3. BR should receive correct tcp response | | |
| Test result | -debug info for gre and esp encap  2011-08-12 16:27:54 debug kernel: (o) tunnel0 0000:7f01:8f89->4500:003c:66bf(0xac11) 60 bytes  2011-08-12 16:27:54 debug kernel: [fe]: GRE-encap packet: 172.17.106.222->172.16.130.120 ttl(127) proto(1) mark(4) 60 bytes  2011-08-12 16:27:54 debug kernel: [fe]: GRE-encap packet done =>10.155.32.6->10.3.3.202 ttl(127) proto(47) mark(4) 84 bytes  2011-08-12 16:27:54 debug kernel: [fe]: encap outgoing packet 10.155.32.6->10.3.3.202 ttl(127) proto(47) 84 bytes  2011-08-12 16:27:54 debug kernel: [fe]: encap(ESP, SPI:40d8b21) packet successfully(rc=-115) =>10.155.32.6->10.155.32.174 ttl(64) | | |
| Comment |  | | |

#### traffic from CVG to dest which is behind the BR should passed successfully through VPN tunnel

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_MGMT\_TRAFFIC\_2 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | traffic from CVG to dest which is behind the BR should passed successfully through VPN tunnel | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG | | |
| Test procedure | -CVG trigger icmp traffic to the LAN behind remote CVG  -CVG trigger udp traffic to the LAN behind remote CVG  -CVG trigger tcp traffic to the LAN behind remote CVG | | |
| Expect result | 1. CVG should receive correct icmp response 2. CVG should receive correct udp response 3. CVG should receive correct tcp response | | |
| Comment |  | | |

#### Verify the SNMP traffic can be routed via VPN tunnel successfully

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_MGMT\_TRAFFIC\_3 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Verify the SNMP traffic can routing via VPN tunnel successfully | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -BR enable SNMP, the trap-host is behind CVG | | |
| Test procedure | -check the snmp trap msg by fe debug, should go through vpn tunnel  -check the server side, msg should be received by trap-host correctly | | |
| Expect result | 1. check the snmp packets will be sent via vpn tunnel successfully 2. BR gets response correctly from remote | | |
| Comment | -udp port 162 for snmp | | |

#### Verify the syslog traffic can be routed via VPN tunnel successfully

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_MGMT\_TRAFFIC\_4 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Verify the syslog traffic can be routed via VPN tunnel successfully | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -BR enable syslog, logging server is behind CVG | | |
| Test procedure | -check the syslog msg by fe debug, should go through vpn tunnel  -check the server side, msg should be received by syslog server correctly | | |
| Expect result | 1. check the syslog packets will be sent via vpn tunnel successfully 2. BR gets response correctly from remote | | |
| Comment | - | | |

#### Verify the radius traffic can be routed via VPN tunnel successfully

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_MGMT\_TRAFFIC\_5 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Verify the radius traffic can be routed via VPN tunnel successfully | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -BR acts as a radius client(NAS), the radius server is behind CVG  -setup a ssid using this radius client | | |
| Test procedure | -STA connects to ssid, trigger the 802.1x auth  -check the radius msg by fe debug, should go through vpn tunnel  -check the server side, msg should be received by syslog server cor | | |
| Expect result | 1. check the radius packets will be sent via vpn tunnel successfully, both auth and acct traffic 2. STA connects to this ssid using radius client can pass auth successfully | | |
| Comment | -udp 1812, 1813 for radius | | |

#### Verify the capwap traffic can be routed via VPN tunnel successfully

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_MGMT\_TRAFFIC\_6 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Verify the capwap traffic can be routed via VPN tunnel successfully | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG | | |
| Test procedure | -BR enable capwap, HM server is behind CVG | | |
| Expect result | 1. BR can connected to HM successfully | | |
| Comment | -http 80 or udp 12222 for capwap | | |

#### Verify the AD traffic can be routed via VPN tunnel successfully

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_MGMT\_TRAFFIC\_7 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Verify the AD traffic can be routed via VPN tunnel successfully | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG | | |
| Test procedure | -BR enables local radius server, db-type is AD  -BR join the domain  -check ntlm-auth on BR | | |
| Expect result | 1. BR can join domain successfully 2. Ntml-auth can success when using correct username and passwd | | |
| Comment | -mostly samba traffic, udp 88 for krbv5, tcp 139, 445 for ntlm | | |

#### Verify the LDAP traffic can be routed via VPN tunnel successfully

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_MGMT\_TRAFFIC\_8 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Verify the LDAP traffic can be routed via VPN tunnel successfully | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG | | |
| Test procedure | -BR enables local radius server, db-type is LDAP  -check ldap-search on BR | | |
| Expect result | 1. Ldap search return success | | |
| Comment | -tcp 389 for ldap, 636 for ldaps | | |

#### Verify the radius proxy traffic can be routed via VPN tunnel successfully

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_MGMT\_TRAFFIC\_9 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Verify the radius proxy traffic can be routed via VPN tunnel successfully | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG | | |
| Test procedure | -BR enables radius proxy, the remote radius server is behind CVG  -STA connects to ssid, via radius auth | | |
| Expect result | 1. Check both the radius auth and acct packets can proxy correctly | | |
| Comment | -udp1814 for radius proxy | | |

### Traffic forwarding strategy on BR

#### Forward packet based on the default routing table

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_1 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Forward packet based on the default routing table | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -setup all wifi radio and eth interface as access mode  -connect STA1 under wifi, connect a STA2 under eth1 | | |
| Test procedure | -ping from STA1 to a dst behind CVG  -ping from STA2 to a destination behind CVG  -ping from STA1 to a dst via default gateway on BR  -ping from STA2 to a dst via default gateway on BR | | |
| Expect result | 1. Check the default routing table, make sure the items in table are correct 2. STA1 can get reply successfully from the peer behind remote CVG 3. STA2 can get reply successfully from the peer behind remote CVG 4. STA1 can get reply via default gateway on BR 5. STA2 can get reply via default gateway on BR | | |
| Test result |  | | |
| Comment | -jus check unicast packet forward here  -this is the default splite tunnel mode | | |

#### Forward multicast packet via tunnel

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_2 | | |
| Priority | Low | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Forward multicast packet via tunnel | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -setup a multicast server in CVG’s LAN  -BR setup VPN connection with the CVG  -setup all wifi radio and eth interface as access mode  -connect STA1 under wifi, connect a STA2 under eth1 | | |
| Test procedure | -check the routing table  -STA1 trigger a multicast stream to the remote server  -STA2 trigger a multicast stream to the remote server | | |
| Expect result | 1. Check the default routing table, make sure the multicast addr is added to tunnel 2. The multicast packet could pass through vpn tunnel successfully 3. STA1 and STA2 can receive the multicast packet successfully | | |
| Test result |  | | |
| Comment | -not supported yet  -try tunnel all | | |

#### Forward all traffic through tunnel by default

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_3 | | |
| Priority | Accept | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Forward all traffic via tunnel by default | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -setup all wifi radios and eth interfaces as access mode  -bind user-profile with l3-tunnel-action all on both wifi radio and wired eth interfaces | | |
| Test procedure | -check the ip policy-route l3-tunnel-all  -STA1 ping web server on internet  -STA1 ping servers behind remote CVG  -STA1 ping local LANs | | |
| Expect result | 1. the traffic will go through tunnel first, then the CVG will forward them to the right places 2. when STA1 ping local LANs, BR should not forward them to remote CVG via tunnel 3. default traffic is via tunnel | | |
| Test result | -debug info:  2011-08-12 16:27:54 debug kernel: [fe]: create routing cache:172.17.106.222 -> 172.16.130.120 fwmark 4 dev tunnel0 | | |
| Comment |  | | |

#### Forward all packet through tunnel by default, with exception

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_4 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Forward all packet through tunnel by default, with exception | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -setup all wifi radios and eth interfaces as access mode  -bind user-profile with l3-tunnel-action with-exception on both wifi radio and wired eth interfaces | | |
| Test procedure | - check the ip policy-route l3-tunnel-exception  -STA1 ping web server on internet  -STA1 ping servers behind remote CVG  -STA1 ping local LANs  -STA1 ping ip in exception list | | |
| Expect result | 1. the traffic will go through tunnel first, then the CVG will forward them to the right places 2. when STA1 ping local LANs, BR should not forward them to remote CVG via tunnel 3. default traffic is via tunnel 4. STA1ping ip in exception list should not via tunnel | | |
| Comment |  | | |

#### Forward packet with split tunnel

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_5 | | |
| Priority | High | Automation Flag |  |
| Topology to use | Topo 1 | | |
| Description | Forward packet with split tunnel | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -setup all wifi radios and eth interfaces as access mode  -bind user-profile with l3-tunnel-action split on both wifi radio and wired eth interfaces | | |
| Test procedure | - check the ip policy-route l3-tunnel-split, it should be the same as default route table  -STA1 ping web server on internet  -STA1 ping servers behind remote CVG  -STA1 ping local LANs | | |
| Expect result | 1. Traffic from STA1 will forward base on the default route table, it’s the default l3-tunnel-action | | |
| Comment |  | | |

#### Drop all packet through tunnel

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_6 | | |
| Priority | High | Automation Flag |  |
| Topology to use | Topo 1 | | |
| Description | Drop all packet through tunnel | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -setup all wifi radios and eth interfaces as access mode  -bind user-profile with l3-tunnel-action drop-tunnel-traffic on both wifi radio and wired eth interfaces | | |
| Test procedure | - check the ip policy-route l3-tunnel- drop  -STA1 ping web server on internet  -STA1 ping servers behind remote CVG  -STA1 ping local LANs  -STA1 ping ip in exception list | | |
| Expect result | 1. All traffic which go through tunnel will be droped | | |
| Test resule | -debug info:  2011-08-15 14:40:50 debug kernel: (u) mgt0 172.17.106.222->172.16.130.120(24629) ttl(128) icmp-echo-req(768/1537) 60 bytes  2011-08-15 14:40:50 debug kernel: [fe]: routing done, 172.17.106.222 -> 172.16.130.120 ttl(128) proto(1) mark(4) 60 bytes, no available route!!! | | |
| Comment |  | | |

#### Use different forwarding policy on different interface

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_7 | | |
| Priority | High | Automation Flag |  |
| Topology to use | Topo 1 | | |
| Description | Use different forwarding policy on different interface | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -setup all wifi radios and eth interfaces as access mode  -bind different interface with different l3-tunnel-action  -e.g ssid1 uses l3-tunnel-action all  - ssid2 with l3-tunnel-action drop-tunnel-traffic  -ssid3 with split  -ssid4 with no l3-tunnel-action  -eth1 with exception | | |
| Test procedure | -STA1 connected to each interfaces one by one  -STA1 trigger traffic via different dest | | |
| Expect result | 1. On ssid1, all traffic should go through tunnel, how about traffic in local LANs ? 2. On ssid2, all traffic want to go through tunnel will be dropped 3. On ssid3, all traffic will be forwarded based on the default route table 4. On ssid4, the same action as ssid3 5. On eth1, all traffic should go through tunnel except those in exception list 6. Check the traffic in local LAN do not go thru tunnels | | |
| Comment |  | | |

#### Change the l3-tunnel-action of the user-profile

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_8 | | |
| Priority | High | Automation Flag |  |
| Topology to use | Topo 1 | | |
| Description | Change the l3-tunnel-action of the user-profile | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -setup all wifi radios and eth interfaces as access mode  -bind different interface with different l3-tunnel-action  -e.g ssid1 uses l3-tunnel-action all  - ssid2 with l3-tunnel-action drop-tunnel-traffic  -ssid3 with split  -ssid4 with no l3-tunnel-action  -eth1 with exception | | |
| Test procedure | -STA1 connected to each interfaces one by one  -STA1 trigger traffic via different dest | | |
| Expect result | 1. On ssid1, all traffic should go through tunnel, how about traffic in local LANs ? 2. On ssid2, all traffic want to go through tunnel will be dropped 3. On ssid3, all traffic will be forwarded based on the default route table 4. On ssid4, the same action as ssid3 5. On eth1, all traffic should go through tunnel except those in exception list | | |
| Comment |  | | |

#### User-profile with several aids

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_9 | | |
| Priority | High | Automation Flag |  |
| Topology to use |  | | |
| Description | User-profile with several aids | | |
| Pre-condition | -config a remote CVG, there is several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVG  -setup all wifi radios and eth interfaces as access mode  -bind the user-profile with several aid  -bind two ssid with this user-profile, but uses different aid | | |
| Test procedure | -STA connects to this two ssid  -check the ip forward policy | | |
| Expect result | 1. The different aid point to the same user-profile, so it will map to the same user-profile index, the same ip-policy used, forward should be the same | | |
| Test result |  | | |
| Comment |  | | |

#### There are two vpn tunnels on BR, use l3-tunnel-action tunnel all

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_10 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use |  | | |
| Description | There are two vpn tunnels on BR, use l3-tunnel-action tunnel all | | |
| Pre-condition | -config two remote CVGs, there are several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with the CVGs, both two tunnels are created  -set CVG1 as primary  -setup all wifi radio and eth interfaces as access mode  -bind a user-profile with l3-tunnel action tunnel all  -bind the user-profile to ssid  -STA connects to ssid | | |
| Test procedure | -check the route table, tunnel routes added correctly  -trigger traffic to LAN behind CVG1 from STA  -trigger traffic to LAN behind CVG2 from STA  -trigger traffic to BR outside from STA | | |
| Expect result | 1. All tunneled routes should be acted as before 2. Default tunnel is the one with higher priority, which should be set as primary | | |
| Comment | -the first configured tunnel will be primary by default | | |

#### l3-tunnel-action split with two tunnels

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_TRAFFIC\_BR\_11 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | l3-tunnel-action split with two tunnels | | |
| Pre-condition | -config two remote CVGs, there are several LANs behind them  -there are some services in CVG’s LANs  -BR setup VPN connection with the both CVG  -setup all wifi radios and eth interfaces as access mode  -bind user-profile with l3-tunnel-action split on both wifi radio and wired eth interfaces | | |
| Test procedure | - check the ip policy-route l3-tunnel-split,tunnel routes should be correct  -STA1 ping web server on internet  -STA1 ping servers behind remote CVG1  -STA1 ping servers behind remote CVG2  -STA1 ping local LANs | | |
| Expect result | 1. Traffic from STA1 will forward base on the default route table, it’s the default l3-tunnel-action 2. Traffic forward to two tunnels correctly based on the ip route | | |
| Test result |  | | |
| Comment |  | | |

### tunnel-exception list

#### Add an ip addr to exception list

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_EXCEPTION\_1 | | |
| Priority | High | Automation Flag |  |
| Topology to use | Topo 1 | | |
| Description | Add an ip addr to exception list | | |
| Pre-condition | -l3 vpn tunnel is created between BR and CVG  -setup a ssid on BR, bind a user-profile with l3-tunnel-action with-exception  -setup a eth interface to bind a user-profile with l3-tunnel-action with-exception  -STA connects to ssid or ethx | | |
| Test procedure | -add an ip addr(host) to the exception list,  ‘vpn l3-tunnel-exception 1.1.1.1’  -check the tunnel exception list,  ‘sh vpn l3-tunnel-exception’  -check the Tunnel All With Exception Routing Table,  ‘sh ip policy-route l3-tunnel-exception’  -STA ping the above host | | |
| Expect result | 1. Make sure exception list contains correct host ip 2. Make sure Tunnel All With Exception Routing Table add an addition item to route the above host via wan interface 3. Make sure packet to this host is not tunneled | | |
| Test result |  | | |
| Comment | -these ip addr should be added to Tunnel All With Exception Routing Table after BR boot up | | |

#### Add an ip subnet to exception list

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_EXCEPTION\_2 | | |
| Priority | High | Automation Flag |  |
| Topology to use | Topo 1 | | |
| Description | Add an ip subnet to exception list | | |
| Pre-condition | -l3 vpn tunnel is created between BR and CVG  -setup a ssid on BR, bind a user-profile with l3-tunnel-action with-exception  -setup a eth interface to bind a user-profile with l3-tunnel-action with-exception  -STA connects to ssid or ethx | | |
| Test procedure | -add an ip subnet to the exception list,  ‘vpn l3-tunnel-exception 172.16.106.0/24’  -check the tunnel exception list,  ‘sh vpn l3-tunnel-exception’  -check the Tunnel All With Exception Routing Table,  ‘sh ip policy-route l3-tunnel-exception’  -STA ping a host in above subnet | | |
| Expect result | 1. Make sure exception list contains correct ip subnet 2. Make sure Tunnel All With Exception Routing Table add an addition item to route the above subnet via wan interface 3. Make sure packet to hosts in this subnet is not tunneled | | |
| Test result |  | | |
| Comment |  | | |

#### Add an domain name to exception list resolved by ext-resolve

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_EXCEPTION\_3 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Add an domain name to exception list resolved by ext-resolve | | |
| Pre-condition | -l3 vpn tunnel is created between BR and CVG  -setup a ssid on BR, bind a user-profile with l3-tunnel-action with-exception  -create a ethx.y, use it as dns server  -config a ext-resolve dns server  -setup a ethx.y interface to bind a user-profile with l3-tunnel-action with-exception  -STA connects to ssid or ethx.y | | |
| Test procedure | -add an domain to the exception list,  ‘vpn l3-tunnel-exception www.google.com’  -check the tunnel exception list,  ‘sh vpn l3-tunnel-exception’  -check the Tunnel All With Exception Routing Table,  ‘sh ip policy-route l3-tunnel-exception’  -STA ping domain www.google.com  - check the Tunnel All With Exception Routing Table again | | |
| Expect result | 1. Make sure exception list contains correct domain name 2. Make sure Tunnel All With Exception Routing Table does not add route before a success dns resolve is performed 3. Every time when BR perform a success dns resolve to the domain in whitelist, it will notify vpn process, then add extra route to Exception Routing Table with all resolved ip, check it 4. Make sure packet to this domain is not tunneled | | |
| Test result | -add domain check to dnsmasq:  info dnsmasq[2036]: whitelist pattern added: test1.test.com  info dnsmasq[2036]: whitelist pattern added: virus.aerohive-hz.cn  -if dns resolve success with a whitelist domain, notify ah\_vpn:  info dnsmasq[2244]: End of successful whitelisted\_ips\_change  info ah\_vpn: <IKE> VPN receive DNS proxy event(name:www.baidu.com, add-ip:2, del-ip:0)  info dnsmasq[2244]: DNS Server: 172.16.130.120  info dnsmasq[2244]: DNS pattern: www.baidu.com  info dnsmasq[2244]: DNS name: www.baidu.com  info dnsmasq[2244]: Del IPS:  info dnsmasq[2244]: Add IPs: 119.75.217.56,119.75.218.45  info dnsmasq[2244]: whitelisted\_ips\_changed  info dnsmasq[2244]: 0: 10.155.3.250  info dnsmasq[2244]: Start of whitelisted\_ips\_change  info dnsmasq[2244]: 0: 10.155.3.250  -add route to exception route table:  info ah\_vpn: <IKE> add exception route: ip route add 119.75.217.56/32 via 10.2.2.1 dev eth0 table t\_exception onlink | | |
| Comment | -no wildmask supported here | | |

#### Add an domain name to exception list resolved by int-resolve

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_EXCEPTION\_4 | | |
| Priority | Middle | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Add an domain name to exception list | | |
| Pre-condition | -l3 vpn tunnel is created between BR and CVG  -setup a ssid on BR, bind a user-profile with l3-tunnel-action with-exception  -create a ethx.y, use it as dns server  -config a ext-resolve dns server  -setup a ethx.y interface to bind a user-profile with l3-tunnel-action with-exception  -STA connects to ssid or ethx.y | | |
| Test procedure | -add an domain to the exception list,  ‘vpn l3-tunnel-exception www.google.com’  -check the tunnel exception list,  ‘sh vpn l3-tunnel-exception’  -check the Tunnel All With Exception Routing Table,  ‘sh ip policy-route l3-tunnel-exception’  -STA ping domain www.google.com  - check the Tunnel All With Exception Routing Table again | | |
| Expect result | 1. Make sure exception list contains correct domain name 2. Make sure Tunnel All With Exception Routing Table does not add route before a success dns resolve is performed 3. Every time when BR perform a success dns resolve to the domain in whitelist, it will notify vpn process, then add extra route to Exception Routing Table with all resolved ip, check it 4. Make sure packet to this domain is not tunneled | | |
| Test result | -add domain check to dnsmasq:  info dnsmasq[2036]: whitelist pattern added: test1.test.com  info dnsmasq[2036]: whitelist pattern added: virus.aerohive-hz.cn  -if dns resolve success with a whitelist domain, notify ah\_vpn:  info dnsmasq[2244]: End of successful whitelisted\_ips\_change  info ah\_vpn: <IKE> VPN receive DNS proxy event(name:www.baidu.com, add-ip:2, del-ip:0)  info dnsmasq[2244]: DNS Server: 172.16.130.120  info dnsmasq[2244]: DNS pattern: www.baidu.com  info dnsmasq[2244]: DNS name: www.baidu.com  info dnsmasq[2244]: Del IPS:  info dnsmasq[2244]: Add IPs: 119.75.217.56,119.75.218.45  info dnsmasq[2244]: whitelisted\_ips\_changed  info dnsmasq[2244]: 0: 10.155.3.250  info dnsmasq[2244]: Start of whitelisted\_ips\_change  info dnsmasq[2244]: 0: 10.155.3.250  -add route to exception route table:  info ah\_vpn: <IKE> add exception route: ip route add 119.75.217.56/32 via 10.2.2.1 dev eth0 table t\_exception onlink | | |
| Comment | -no wildmask supported here | | |

#### Remove a exception ip

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_EXCEPTION\_5 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Remove a exception ip | | |
| Pre-condition | -l3 vpn tunnel is created between BR and CVG  -setup a ssid on BR, bind a user-profile with l3-tunnel-action with-exception  -connect a ssid to the above ssid | | |
| Test procedure | - check the ip policy-route l3-tunnel-split,tunnel routes should be correct  -STA1 ping web server on internet  -STA1 ping servers behind remote CVG1  -STA1 ping servers behind remote CVG2  -STA1 ping local LANs | | |
| Expect result | 1. Traffic from STA1 will forward base on the default route table, it’s the default l3-tunnel-action 2. Traffic forward to two tunnels correctly based on the ip route | | |
| Test result | - | | |
| Comment |  | | |

#### Remove a exception sub network

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_EXCEPTION\_6 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Remove a exception sub network | | |
| Pre-condition | -l3 vpn tunnel is created between BR and CVG  -setup a ssid on BR, bind a user-profile with l3-tunnel-action with-exception  -connect a ssid to the above ssid | | |
| Test procedure | - check the ip policy-route l3-tunnel-split,tunnel routes should be correct  -STA1 ping web server on internet  -STA1 ping servers behind remote CVG1  -STA1 ping servers behind remote CVG2  -STA1 ping local LANs | | |
| Expect result | 1. Traffic from STA1 will forward base on the default route table, it’s the default l3-tunnel-action 2. Traffic forward to two tunnels correctly based on the ip route | | |
| Test result | - | | |
| Comment |  | | |

#### Remove a exception url

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_EXCEPTION\_7 | | |
| Priority | High | Automation Flag | N/A |
| Topology to use | Topo 1 | | |
| Description | Remove a exception url | | |
| Pre-condition | -l3 vpn tunnel is created between BR and CVG  -setup a ssid on BR, bind a user-profile with l3-tunnel-action with-exception  -connect a ssid to the above ssid | | |
| Test procedure | - check the ip policy-route l3-tunnel-split,tunnel routes should be correct  -STA1 ping web server on internet  -STA1 ping servers behind remote CVG1  -STA1 ping servers behind remote CVG2  -STA1 ping local LANs | | |
| Expect result | 1. Traffic from STA1 will forward base on the default route table, it’s the default l3-tunnel-action 2. Traffic forward to two tunnels correctly based on the ip route | | |
| Test result | - | | |
| Comment |  | | |

### Traffic forwarding strategy on CVG

#### Forward packet from a BR to LANs behind CVG

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_POLICY\_CVG\_1 | | |
| Priority | High | Automation Flag |  |
| Topology to use |  | | |
| Description | Forward packet from a BR to LANs | | |
| Pre-condition | -config a remote CVG, there are several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with CVG  -setup all wifi radio and eth interfaces as access mode  -BR have several LANs behind it | | |
| Test procedure | -STA1 and STA2 are in different LANs under BR  -ping from STA1 to STA2  -ping from STA2 to STA1 | | |
| Expect result | 1. Ping success in both direction 2. Make sure the traffic doesn’t forward to tunnel | | |
| Comment |  | | |

#### Forward packet between BRs

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FORWARDING\_POLICY\_CVG\_2 | | |
| Priority | High | Automation Flag |  |
| Topology to use |  | | |
| Description | Forward packet between BRs | | |
| Pre-condition | -config a remote CVG, there are several LANs behind it  -there are some services in CVG’s LANs  -BR1 setup VPN connection with CVG  -BR2 setup VPN connection with CVG  -setup all wifi radio and eth interfaces as access mode  -BR1 have several LANs behind it  -BR2 have several LANs behind it  -STA1 in BR1’s LANs, STA2 in BR2’s LANs | | |
| Test procedure | -STA1 ping STA2  -STA2 ping STA2 | | |
| Expect result | 1. All the traffic should be forwarded to CVG first, then CVG will forward it to the right BR | | |
| Comment |  | | |

### IP fragment

#### BR/CVG receives over length packet from LAN to WAN

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_IP\_FRAGMENT\_1 | | |
| Priority | High | Automation Flag |  |
| Topology to use | PC1---BR(WAN)-----SW----CVG----PC2 | | |
| Description | BR receives over length packet from LAN to vpn tunnel | | |
| Pre-condition | PC1 and PC2 can talk via vpn tunnel | | |
| Test procedure | -check the mtu on eth0(WAN) and tunnel  -PC1 send an over length packet to PC2, result 4  - PC1 send an over length packet to PC2 with DF set, result 5  -PC2 send an over length packet to PC1, result 6  -PC2 send an over length packet to PC1 with DF set, result 7 | | |
| Expect result | 1. Default mtu on eth0 is 1500 2. Default mtu on tunnel interface is 1476 3. Default mtu after ESP encapsulation is 1396 4. PC1 got ping reply from PC2 when packet size over 1500 and 1476, no DF set 5. PC1 could get ping reply from PC1 only when packet size is smaller then 1396, DF set 6. PC2 got ping reply from PC1 when packet size is over 1500 and 1476, no DF set 7. PC2 could get ping reply from PC1 only when packet size smaller then 1396, DF set | | |
| Test result | -CVG receive over length packet, operate on linux PC  [qatest@water ~]$ ping 172.17.107.130 -s 1471 -M do -c 2  PING 172.17.107.130 (172.17.107.130) 1471(1499) bytes of data.  From 172.16.130.120 icmp\_seq=1 Frag needed and DF set (mtu = 1476)  From 172.16.130.120 icmp\_seq=1 Frag needed and DF set (mtu = 1476)  --- 172.17.107.130 ping statistics ---  0 packets transmitted, 0 received, +2 errors  [qatest@water ~]$ ping 172.17.107.130 -s 1448 -M do -c 2  PING 172.17.107.130 (172.17.107.130) 1448(1476) bytes of data.  From 10.3.3.202 icmp\_seq=1 Frag needed and DF set (mtu = 1396)  From 172.16.130.120 icmp\_seq=2 Frag needed and DF set (mtu = 1396)  [qatest@water ~]$ ping 172.17.107.130 -s 1368 -M do -c 2  PING 172.17.107.130 (172.17.107.130) 1368(1396) bytes of data.  1376 bytes from 172.17.107.130: icmp\_seq=1 ttl=124 time=1046 ms  1376 bytes from 172.17.107.130: icmp\_seq=2 ttl=124 time=60.7 ms  --- 172.17.107.130 ping statistics ---  2 packets transmitted, 2 received, 0% packet loss, time 1009ms  rtt min/avg/max/mdev = 60.726/553.725/1046.725/493.000 ms, pipe 2 | | |
| Comment |  | | |

### Tunnel Flip, Recovery

#### Check the DPD keepalive interval

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_FLIP\_1 | | |
| Priority | High | Automation Flag |  |
| Topology to use |  | | |
| Description | Check the DPD(Dead Peer Detection) keepalive interval | | |
| Pre-condition | -config a remote CVG, there are several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with CVG  -setup all wifi radio and eth interfaces as access mode  -BR have several LANs behind it  -STA1 connected to BR’s LAN | | |
| Test procedure | -after tunnel creation success, check the keepalive message interval by default  -change the value of idle-interval, check the keepalive message sending interval  -change the value of idle-interval to 0, check the keepalive message sending interval | | |
| Expect result | 1. Keepalive message is enable by default, should be 10 sec, sending from BR to CVG, the peer is responsed correctly 2. After changing the idle-interval, it should be take effect at once, check it 3. Set idle-interval to 0 is disable keepalive message, no keepalive message send to peer | | |
| Test result | -DPD send by BR every 10 sec by default:  2011-08-02 12:23:52 debug ah\_vpn: [vpn\_info]: <IKE 10.155.32.169[500]> DPD R-U-There(2070) sent (to:10.155.32.169[500]), failed co unter: 0  2011-08-02 12:23:42 debug ah\_vpn: [vpn\_info]: <IKE 10.155.32.169[500]> DPD R-U-There(2069) sent (to:10.155.32.169[500]), failed co unter: 0  2011-08-02 12:23:32 debug ah\_vpn: [vpn\_info]: <IKE 10.155.32.169[500]> DPD R-U-There(2068) sent (to:10.155.32.169[500]), failed co unter: 0  2011-08-02 12:23:22 debug ah\_vpn: [vpn\_info]: <IKE 10.155.32.169[500]> DPD R-U-There(2067) sent (to:10.155.32.169[500]), failed co unter: 0  -DPD recv from GW:  2011-08-02 12:40:23 debug ah\_vpn: [vpn\_info]: <IKE 10.155.32.172[4500]> DPD R-U-There-Ack(2169) received (from:10.155.32.172[4500] )  2011-08-02 12:40:13 debug ah\_vpn: [vpn\_info]: <IKE 10.155.32.172[4500]> DPD R-U-There-Ack(2168) received (from:10.155.32.172[4500] )  2011-08-02 12:40:03 debug ah\_vpn: [vpn\_info]: <IKE 10.155.32.172[4500]> DPD R-U-There-Ack(2167) received (from:10.155.32.172[4500] ) | | |
| Comment | -max value is 65535 | | |

#### Check the DPD keepalive retry interval

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_FLIP\_2 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | Check the DPD keepalive retry and retry interval on BR | | |
| Pre-condition | -config a remote CVG, there are several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with CVG  -setup all wifi radio and eth interfaces as access mode  -BR have several LANs behind it  -STA1 connected to BR’s LAN  -vpn tunnel setup success | | |
| Test procedure | -shutdown the wan interface on CVG  -check the keepalive packet sending from BR  -recover the wan interface of CVG  -change the retry and retry interval on BR  -shutdown the wlan interface on CVG  -check the keepalive packet sending from BR | | |
| Expect result | 1. After wan interface shutdown on CVG, BR can’t receive response now, BR will resend keepalive message, check the default retry interval is 3 sec 2. The BR will keep retrying several times, which is 5 times by default 3. After retry times run out, the tunnel will down on BR, check the tunnel status is correct 4. After tunnel is down, BR will try to trigger ISAKMP phase1 5. After retry and retry interval changed, it should take effect right now 6. The tunnel will recover after network resume 7. After vpn tunnel recover check the tunnel status and tunnel routes are correct 8. After vpn tunnel recover, check the traffic pass through vpn tunnel success | | |
| Comment |  | | |

#### Check the DPD keepalive retry and retry interval on CVG

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_FLIP\_3 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | Check the DPD keepalive retry and retry interval on CVG | | |
| Pre-condition | -config a remote CVG, there are several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with CVG  -setup all wifi radio and eth interfaces as access mode  -BR have several LANs behind it  -STA1 connected to BR’s LAN  -vpn tunnel setup success | | |
| Test procedure | -shutdown the wan interface on BR  -recover the wan interface on BR  -change the value of retry and retry interval  -shutdown the wan interface on BR | | |
| Expect result | 1. After wan interface shutdown on BR, CVG can’t receive keepalive packet now 2. Check the tunnel status and tunnel routes when tunnel is down 3. After retry x retry interval time, the tunnel will down on CVG, check the ike sa, sp and ipsec sa should be cleared 4. Check the tunnel status and tunnel routes after tunnel recover 5. After retry and retry interval changed, it should take effect right now | | |
| Comment |  | | |

#### Clear ike/ipsec sa

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_FLIP\_4 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | Clear ike/ipsec SA | | |
| Pre-condition | -config a remote CVG, there are several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with CVG  -setup all wifi radio and eth interfaces as access mode  -BR have several LANs behind it  -STA1 connected to BR’s LAN  -vpn tunnel setup success | | |
| Test procedure | -clear ipsec sa on BR  -clear ike sa on BR  -clear ipsec sa on CVG  -clear ike sa on CVG | | |
| Expect result | 1. Clear ipsec sa on BR will trigger BR to do ISAKMP phase 2 2. Clear ike sa on BR will trigger BR to do ISAKMP phase 1 3. Clear ipsec sa on CVG will trigger BR to do ISAKMP phase 2 4. Clear ike sa on CVG will trigger BR to do ISAKMP phase 1 5. Every time after vpn tunnel is recover, check the traffic could pass through vpn tunnel successfully 6. Check the tunnel status and tunnel routes when tunnel is down | | |
| Comment |  | | |

#### Verify that Tunnel can be recreated after reboot.

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_FLIP\_5 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | Verify that Tunnel can be recreated after reboot | | |
| Pre-condition | -config a remote CVG, there are several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with CVG  -setup all wifi radio and eth interfaces as access mode  -BR have several LANs behind it  -STA1 connected to BR’s LAN  -vpn tunnel setup success | | |
| Test procedure | -reboot BR  -reboot CVG | | |
| Expect result | 1. After BR or CVG reboot, the vpn tunnel could be recreated successfully | | |
| Comment |  | | |

#### Vpn tunnel should be recreated after mgt0 ip changed on CVG

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_FLIP\_6 | | |
| Priority | High | Automation Flag |  |
| Topology to use |  | | |
| Description | Vpn tunnel should be recreated after mgt0 ip changed on CVG | | |
| Pre-condition | -config a remote CVG, there are several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with CVG  -setup all wifi radio and eth interfaces as access mode  -BR have several LANs behind it  -STA1 connected to BR’s LAN  -vpn tunnel setup success | | |
| Test procedure | -change the ip of mgt0 on CVG | | |
| Expect result | 1. CVG will break all tunnel on it, trigger the BR to recreate vpn tunnel 2. Check tunnel status 3. After tunnel refresh, check the ip route table on BR, the route for mgt0 of CVG should be updated | | |
| Comment |  | | |

#### Vpn tunnel should be recreated after wan ip changed, both on BR and CVG

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_FLIP\_7 | | |
| Priority | High | Automation Flag |  |
| Topology to use |  | | |
| Description | Vpn tunnel should be recreated after wan ip changed | | |
| Pre-condition | -config a remote CVG, there are several LANs behind it  -there are some services in CVG’s LANs  -BR setup VPN connection with CVG  -setup all wifi radio and eth interfaces as access mode  -BR have several LANs behind it  -STA1 connected to BR’s LAN  -vpn tunnel setup success | | |
| Test procedure | -change the ip of mgt0 on CVG | | |
| Expect result | 1. CVG will break all tunnel on it, trigger the BR to recreate vpn tunnel 2. After tunnel refresh, check the ip route table on BR, the route for mgt0 of CVG should be updated | | |
| Comment |  | | |

#### Tunnel recreate after parameters change

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_FLIP\_8 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | Tunnel recreate after parameters change | | |
| Pre-condition |  | | |
| Test procedure | 1. The Phase I restart when change any parameters such as auth-method, dh-group, encryption-algorithm, hash, lifetime, nat-traversal disable, gre-gateway, ipsec gateway, local-id, peer-id etc. Tunnel down. 2. The Phase I restart when lifetime expired. Tunnel up 3. The Phase I restart when counter reach 0 or error information be received(be tested separated in every part). 4. The Phase I restart when receive one delete information (be tested in pass II). 5. The Phase I restart when change the parameter of Phase II? 6. Verify the Result when these changes happen in Responder. | | |
| Expect result |  | | |
| Comment |  | | |

#### The vpn process/daemon brings up by process monitor after abnormal killed

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_TUNNEL\_FLIP\_9 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | The vpn process/daemon brings up by process monitor after abnormal killed | | |
| Pre-condition | Vpn tunnel created between BR and CVG | | |
| Test procedure | -kill vpn process under shell on BR side, check pm action  -kill vpn process under shell on CVG side, check the pm action | | |
| Expect result | 1. PM could detect the abnormal process, bring it up 2. The vpn tunnel could be recreated after process up 3. Traffic could pass through vpn tunnel success | | |
| Comment | -ah\_vpn | | |

### Tunnel failover

#### when primary tunnel is down, failover to back

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_FAILOVER\_1 | | |
| Priority | High | Automation Flag |  |
| Topology to use |  | | |
| Description | when primary tunnel is down, failover to back | | |
| Pre-condition | -setup two CVGs in the same subnet | | |
| Test procedure | -one BR connected to both CVGs, set CVG1 as primary  -check the tunnel routes on BR  -STA1 is behind BR  -STA2 is behind CVG  -STA1 ping STA2 in CVG LAN  -shut down the wan interface of CVG1  -check the tunnel status and tunnel routes on BR  -STA1 ping CVG1, unreachable  -STA1 ping STA2  -recover the wan interface on CVG1  -STA1 ping CVG1  -STA1 ping STA2 | | |
| Expect result | 1. when two tunnels are all up, the traffic should pass through the primary tunnel 2. if primary tunnel is down, all route records of this tunnel should be removed, and the traffic go through the backup tunnel 3. after primary tunnel recover, traffic will go through primary tunnel | | |
| Comment | Current doesn’t support by device | | |

## Stress Test

### Tigger the tunnel to up down continuously

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_stress\_1 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | Tigger the tunnel to up down continuously | | |
| Pre-condition | -setup two CVGs, several BRs setup vpn tunnel to them | | |
| Test procedure | -clear ike/ipsec sa on CVG continuously to trigger tunnel to recreate  -clear ike/ipsec sa on BRs continuously to trigger tunnel to recreate  -after tunnel recreation success, check the traffic passing through the tunnel  -monitor the cpu and memory usage on BR/CVG | | |
| Expect result | 1. The tunnel could be recreate after clear sa 2. Tfaffic could pass through tunnel successfully after tunnel recreation 3. The cpu and memory usage is reasonable | | |
| Comment | -other ways for tunnel up/down:  -up down wan interface on BR/CVG  -change mgt0/wan ip | | |

### Heavy traffic runs on vpn tunnel

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_stress\_2 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | Heavy traffic runs on vpn tunnel | | |
| Pre-condition | -One BR setup two vpn tunnel to CVGs  -one CVG create several tunnels to BRs  -some tunnels are behind nat firewall, others are not  -make sure the packets do not fragment | | |
| Test procedure | -run heavy traffic on tunnels  -check the throughput on tunnel  -check the cpu and memory usage on BR and CVG | | |
| Expect result | 1. Through put is reasonable 2. Cpu and memory usage are reasonable | | |
| Comment |  | | |

## Duration Test Case

#### Phase 1 and phase 2 long-time rekey

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_DURATION\_1 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | Phase 1 and phase 2 long-time rekey | | |
| Pre-condition | -one BR setup tunnels with two CVG  -one CVG setup tunnels with several BR | | |
| Test procedure | -run some background traffic  -check the rekey logs | | |
| Expect result | 1. Check the rekey periods are correct everytime 2. Rekey will success every time, traffic should not be brocken by phase 2 rekey | | |
| Comment |  | | |

## Performance Test Case

### Check the throughput of tcp packet

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_VPN\_NAT\_Performance\_1 | | |
| Priority | High | Automation Flag |  |
| Topology to use | TOPO 2 | | |
| Description | Check the throughput of tcp packet | | |
| Pre-condition | -a minial BR/CVG environment is setup, wan interface isn’t enable nat  -two clients, one is behind BR, another is behind CVG | | |
| Test procedure | -send packets through the tunnel from one client to another | | |
| Expect result | 1. Check the throughput | | |
| Test result |  | | |
| Comment | - chariot high throughput | | |

### Check the throughput when BR with wan nat

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_VPN\_NAT\_Performance\_2 | | |
| Priority | High | Automation Flag |  |
| Topology to use | TOPO 2 | | |
| Description | Check the throughput when BR with wan nat | | |
| Pre-condition | -a minial BR/CVG environment is setup, wan interface enable nat  -two clients, one is behind BR, another is behind CVG | | |
| Test procedure | -send packets through the tunnel from one client to another | | |
| Expect result | 1. Check the throughput, compare to the no wan nat result, should not be loss much | | |
| Test result |  | | |
| Comment |  | | |

### Ip fragment with vpn tunnel

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_VPN\_NAT\_Performance\_3 | | |
| Priority | Low | Automation Flag |  |
| Topology to use | TOPO 2 | | |
| Description | Ip fragment with vpn tunnel | | |
| Pre-condition | -a minial BR/GW environment is setup  -STA1 connects to BR LAN  -STA2 connects to CVG LAN | | |
| Test procedure | -STA1 ping STA2 with fragmented ip packet  -STA1 ping STA2, fragment packet after gre/esp encapsulation  -check the through put | | |
| Expect result | 1. Fragment packets should pass vpn tunnel success in all above conditions 2. The performance should not be affected much | | |
| Test result |  | | |
| Comment |  | | |

## Scalability Test Case

### Maximum client-ipsec-tunnel on BR

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_CAPACITY\_1 | | |
| Priority | Middle | Automation Flag |  |
| Topology to use |  | | |
| Description | Maximum client-ipsec-tunnel on BR | | |
| Pre-condition |  | | |
| Test procedure | -create client-ipsec-tunnel as many as you can | | |
| Expect result | Maximium client-ipsec-tunnel is 2 | | |
| Test result | AH-4597c0#vpn client-ipsec-tunnel fake vpn-mode layer-3  Unable to create the IPsec tunnel profile. Either the maximum number of VPN client tunnels has been reached (2), or a VPN server tunnel has already been configured. | | |
| Comment |  | | |

### 1500 tunnels on CVG

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_CAPACITY\_2 | | |
| Priority | Low | Automation Flag |  |
| Topology to use |  | | |
| Description |  | | |
| Pre-condition | 1500 tunnels on CVG | | |
| Test procedure | -setup vpn tunnels on this CVG  -check the tunnel status and tunnel routes are correct  -reboot CVG  - measure time for all tunnel to come up | | |
| Expect result |  | | |
| Comment | -test 20 tunnels by now | | |

## Compatibility Test Case

Does it support private MIBs? If so defines all SNMP MIBs here or linked it to a MIB file.

## CLI (Automation Status: Yes/No)

### Layer 3 vpn cli

#### Enable layer 3 vpn, both CVG and BR side

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_CLI\_1 | | |
| Priority | Low | Automation Flag |  |
| Topology to use |  | | |
| Description | Enable layer 3 vpn, both CVG and BR side | | |
| Pre-condition |  | | |
| Test procedure | -enable layer 3 vpn on CVG side  -enable layer 3 vpn on BR sid | | |
| Expect result | 1. vpn server-ipsec-tunnel xxx vpn-mode layer-3 2. vpn client-ipsec-tunnel xxx vpn-mode layer-3 3. layer 3 vpn tunnel could be setup after cli send | | |
| Comment |  | | |

#### Change layer 3 vpn to layer 2, both CVG and BR side

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_CLI\_2 | | |
| Priority | Low | Automation Flag |  |
| Topology to use |  | | |
| Description | Change layer 3 vpn to layer 2, both CVG and BR side | | |
| Pre-condition |  | | |
| Test procedure | -change vpn from layer 3 to layer 2on CVG side  - change vpn from layer 3 to layer 2on BR side | | |
| Expect result | 1. layer 2 vpn tunnel could be setup after cli send 2. sh run to check the cli is correct | | |
| Comment |  | | |

### l3-tunnel-action config with user-profile

#### Config l3-tunnel-action with user-profile

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_CLI\_3 | | |
| Priority | Low | Automation Flag |  |
| Topology to use |  | | |
| Description | Config l3-tunnel-action with user-profile | | |
| Pre-condition |  | | |
| Test procedure | -user-profile xxx l3-tunnel-action {all|with-exception|split|drop-tunnel-traffic} | | |
| Expect result | 1. cli could be configured success 2. sh run to check cli is correct | | |
| Comment |  | | |

#### no l3-tunnel-action with user-profile

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_CLI\_4 | | |
| Priority | Low | Automation Flag |  |
| Topology to use |  | | |
| Description | no l3-tunnel-action with user-profile | | |
| Pre-condition |  | | |
| Test procedure | - no user-profile xxx l3-tunnel-action | | |
| Expect result | 1. cli could be configured success 2. sh run to check cli is correct 3. sh user-profile xxxx to check l3-tunnel-action changed to default | | |
| Comment |  | | |

#### check the ip-policy of each user-profile

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_CLI\_5 | | |
| Priority | Low | Automation Flag |  |
| Topology to use |  | | |
| Description | check the ip-policy of each user-profile | | |
| Pre-condition |  | | |
| Test procedure | - sh ip-policy user-profile  <number> Enter the user profile name or ID  <string> Enter the user profile name or ID  - show ip policy-route [ {l3-tunnel-all|l3-tunnel-exception|l3-tunnel-split|l3-tunnel-drop} | | |
| Expect result | 1. check the ip-policy of each user-profile | | |
| Comment |  | | |

#### add or remove l3-tunnel-exception

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FT\_L3\_VPN\_CLI\_6 | | |
| Priority | Low | Automation Flag |  |
| Topology to use |  | | |
| Description | add or remove l3-tunnel-exception | | |
| Pre-condition |  | | |
| Test procedure | - vpn l3-tunnel-exception <ip\_addr|string> | | |
| Expect result | 1. show vpn l3-tunnel-exception to check the exception table | | |
| Comment |  | | |

## GUI Management-HiveManager

## GUI Management-HiveUI

# Customer Issue or Typical Bug