

## 1. IPsec/IKE

Tester IPsec Conformance  
Manual Key IPsec  
Pre-shared Secret IPsec/IKE  
(Pre-shared Secret Authentication(XAUTH, CRACK ) )  
AES, SEED, Blowfish  
IPCOMP  
AH/ESP/IPCOMP  
IKE , (DES, 3DES, MD5, SHA1 )

## 2. IPsec Fragment & PMTU Discovery

IPsec Fragment/Reassembly  
IPsec Path MTU Discovery

## 3. IKE Proposal ID Type

Phase1 Multi-proposal  
Phase1 Proposal  
Phase2 Multi-proposal  
Phase2 Proposal  
ID Type(ID\_IPV4\_ADDR, ID\_FQDN, ID\_DER\_ASN1\_DN )

## 4. PKI IKE ( CA )

X.509  
CA (verification) (Key )  
CDP(CRL Distribution Point) CA CRL  
CRL Revocation

## 5. SA Expire Re-Key

Lifetime Lifetime-in-Bytes Scheme  
Lifetime Expire  
DPD(Dead Peer Detection)  
SA Expire Re-Key 가

## 6. NAT-Traversal

NAT - Traversal

NAT

NAT - Traversal

IPsec

## **7. Hub and Spoke VPN**

VPN

Hub and Spoke VPN