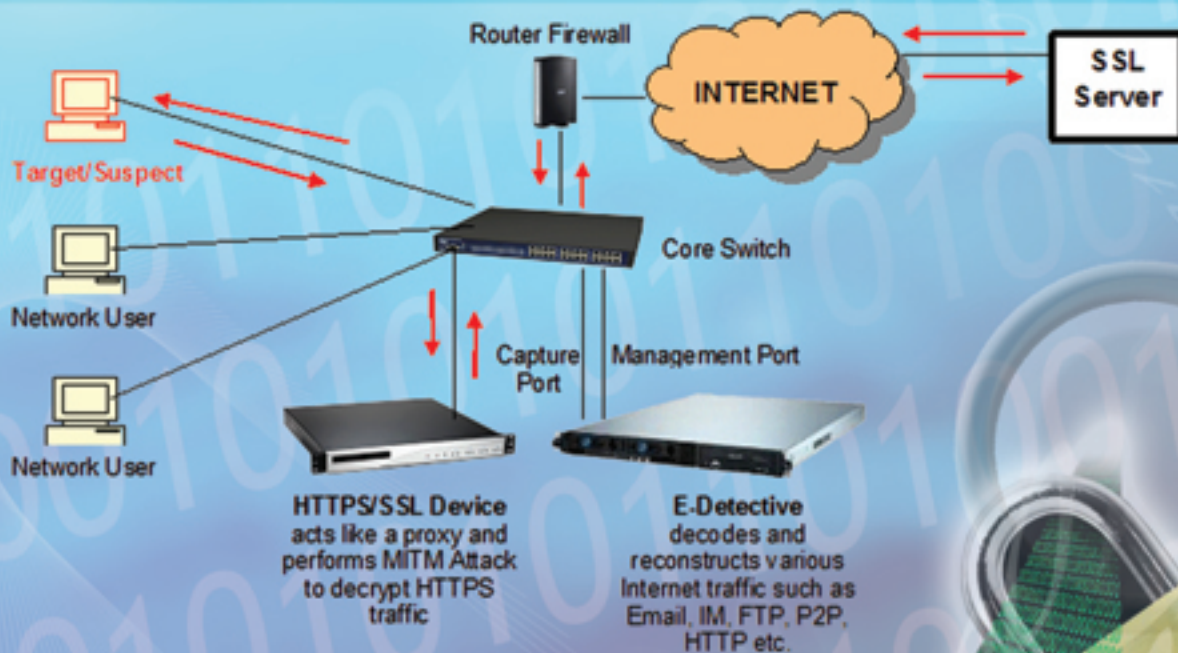




HTTPS / SSL Network Packet Forensics Device



Application Features:

- Decrypt and decode HTTPS network packets within the same network domain.
- Two application modes: 1. Online – Man-in-the-Middle (MITM) Attack; and 2. Offline Decryption (Decrypt HTTPS raw data packets with Private/Secret key known).
- In MITM Attack Method, it acts as proxy to the targeted user/PC (using ARP and DNS positioning). The HTTP and HTTPS traffic between the targeted user/PC and SSL server can therefore be redirected to the HTTPS/SSL Network Packet Forensics Device. This will allow the HTTPS/SSL Device to decrypt the HTTPS traffic with genuine SSL certificate obtained.
- Login Username and password for HTTP and HTTPS websites such as Gmail, Yahoo Mail, E-Bay etc. can be extracted and obtained.

! ? * # @ ,
? ! * ? \$ & # # # @ ,
* ? ! & ? \$ & ? ! &
HTTPS/SSL
Encrypted Raw Data



HTTPS/SSL Network
Forensic Device

Decrypted Content
No More Secret



DECISION GROUP

Address : 4/F No.31, Alley 4, Lane 36, Sec. 5, Ming-Sheng East Rd, Taipei Taiwan ROC

Phone : +886 2 27665753 Fax : +886 2 27665702

Email : decision@decision.com.tw ; decision@ms1.hinet.net

URL : www.decision.com.tw ; www.edecision4u.com

Distributor / Partner :