E-DETECTIVE

White Paper for E-Detective System (Wired)

An Introduction

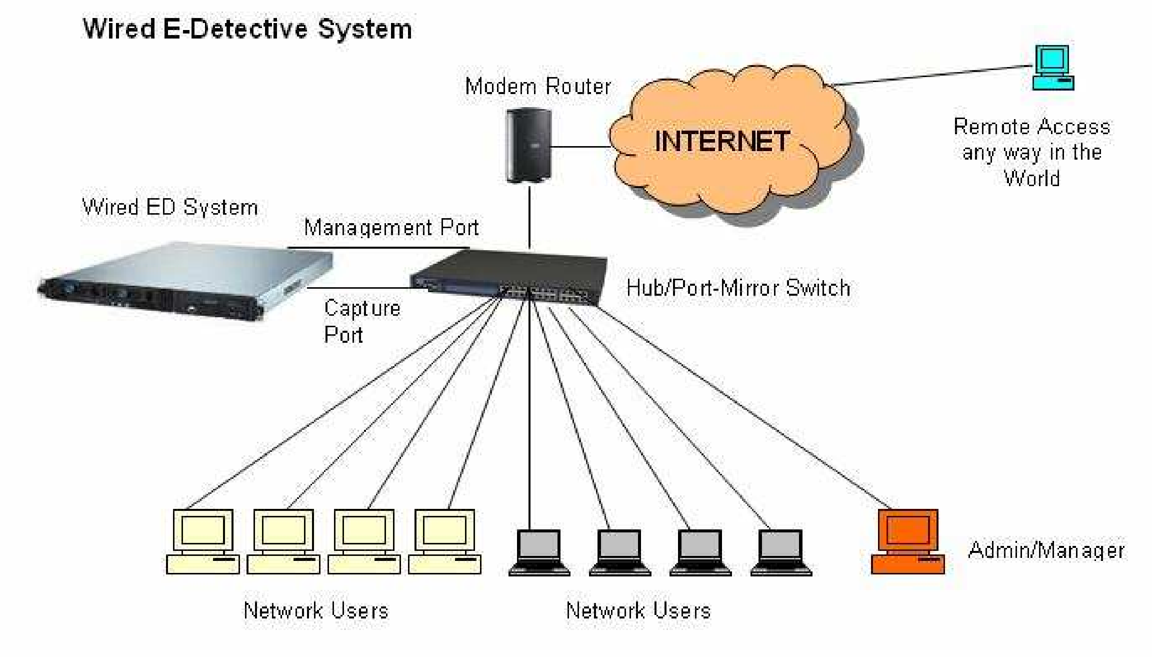
Internetworking becomes the most popular communications nowadays, escalation of frequent communications on internet becomes a challenge of monitoring and management. The most troublesome thing for network manager is confidentiality disclosure and bandwidth abuse. How much confidential information is out flowing without being controlled? How much bandwidth is being wasted on useless activities?

E-Detective is an Internet Surveillance Tool. E-Detective can help you to supervise your employees' activities on network at work, and record the details they did for future reference. It is the best solution to protect your enterprise from the damage of confidential information outflow and loss of productivity. It also provides you with powerful evidence in a lawsuit.

E-Detective captures raw data from the network and decode/reconstruct the content for E-mail (SMTP, POP3, IMAP, Hotmail and Web-mail), MSN, Yahoo Messenger, AOL and ICQ instant message, Web browsing (HTTP Link and HTTP Content), HTTP Download, FTP, P2P, Telnet, Online Game, VoIP and Webcam (for YAHOO and MSN)... and the content and information exchanged via Internet.

Unlike most other sniffer software, E-Detective is dedicated to capture packets containing multiple protocols, reconstruct the sessions, and reassemble the original files transferred by multiple protocols.

E-Detective is optimized and based on Linux OS, It provides user friendly interface powered by Java plug-in, and well-tuned provisioning for easy installation and starting. E-Detective is capable of deep packet interception on high speed IP network, and able to target specific objective by using non-intrusive interception technology. E-Detective is a flexible policy based and non-intrusive network access behavior monitoring solution. Alarm is triggered when violation of rules occurred.



What E-Detective monitors?

1. Email (POP3, SMTP, IMAP, Webmail)

E-Detective reconstructs content of Email (POP3, SMTP, IMAP, Webmail) and display information which include date/time, sender and receiver Email addresses, CC, BCC and email content with attachment files.

Note: Types of Webmail predefined are Hinet, Hotmail Standard, PCHome, Yahoo Standard Mail, URL, Giga, Yam, Sina, Seednet, mail.tom.com, mail.163.com, Sohu.com. User can also defined their own Webmail type in the E-Detective system through a tool known as Webmail Token Analyzer which is provided in the E-Detective system.

2. Instant Messages (IM)

E-Detective reconstructs and displays the content for instant messages such as MSN, Yahoo Messenger, AOL, ICQ and QQ which includes the date/time, IP, user handle, participant, chat content and file transfer through IM.

3. Web Browsing (HTTP LINK and HTTP CONTENT)

E-Detective reconstructs and displays the Internet or webpage browsing details, which include URL Link (HTTP Link), website content (HTTP Content), date/time and IP.

4. HTTP (DOWNLOAD)

E-Detective reconstructs and displays the files downloaded by through HTTP, URL Link, IP and date/time.

4. File Transfer Protocol (FTP)

E-Detective reconstructs and displays the upload and download files, FTP server IP, username and password, user IP and date/time.

6. Peer to Peer Communications (P2P)

E-Detective captures P2P communication logs and displays the details which includes date/time, user IP, user port, peer IP, peer port, upload or download action, file names etc.

7. Telnet

E-Detective reconstructs and displays Telnet session information which include date/time, IP and recorded file. It also provides "playback" function.

8. Online Games

E-Detective captures Online Games logs such as Maplestory, ZT, FairyLand, Kinf of king, Katrider, BnB, Mabinogi, Hotdance, Gatamped, Pangya, Heatproject, DTG, Superrich, O2jam, Seal, COCOCAN, Nage, Gersang, Laghaim, Hot, 3P, SF, Noritel, Elysium, Stoneage, A3, HE, ZU, Cabala, JY1, JY2, Wonderland, SAN, TS, LoveBox, SANGO, Dekaron, Cabal, Rohan, GVO, CG, DOMO, BO, SWDOL, DOMOFREE, RICHOL, RO, Mir3, JX, JX2, TTH, RF Online, SOL, Nobol, FDO, GHOSTSOUL, AL, CPW, 1003b, 9D, EverQuestll,. Silkroad2, Metin, MS, SUN, Hero, HB, WE5, FongShen, FongShen2, Q3baby, SHE and Megaten.

9. VOIP and Webcam (Forensic version)

E-Detective reconstructs and displays VOIP and Webcam sessions. VOIP and Webcam sessions for Yahoo Messenger and MSN Messenger can be playback using specific method.

The Benefits of E-Detective

- Track down work effectiveness and prevent employees' laziness and boredom
- Improve productivity and efficiency
- Prevent spam mails and invitation of virus
- Prevent cookies with “malicious intent” penetrating the network
- Prevent bandwidth wastage
- Prevent confidentiality disclosure
- Prevent company from being hacked
- Protect business right (such as intellectual property right etc)
- Traffic management and utilization monitoring
- Managing network access behavior
- Backup and reconstruction of information
- Help government and law enforcement agencies to neutralize threats from terrorists and criminals

Main Advantages of E-Detective

- E-Detective can be customized based on user requirements
- E-Detective is easy to install and use (web based)
- Passive mode without interfering existing network

Main Features of E-Detective

- Exclusive operating system
- Non-intrusion mode means it is undetectable
- Web-based management interface
- Monitor multiple internet and communications protocols
- Access control ensures only authorized use of resources

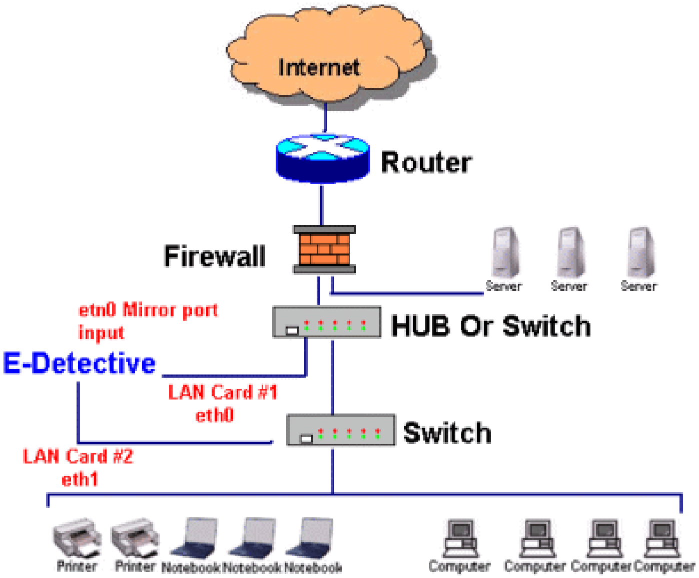
- Easy to define monitoring and alerting rules
- Centralized monitoring of local and remote stations
- Quick search function
- Useful management reports on internet activities statistics
- Data backup and recovery solution

Appliances Deployment

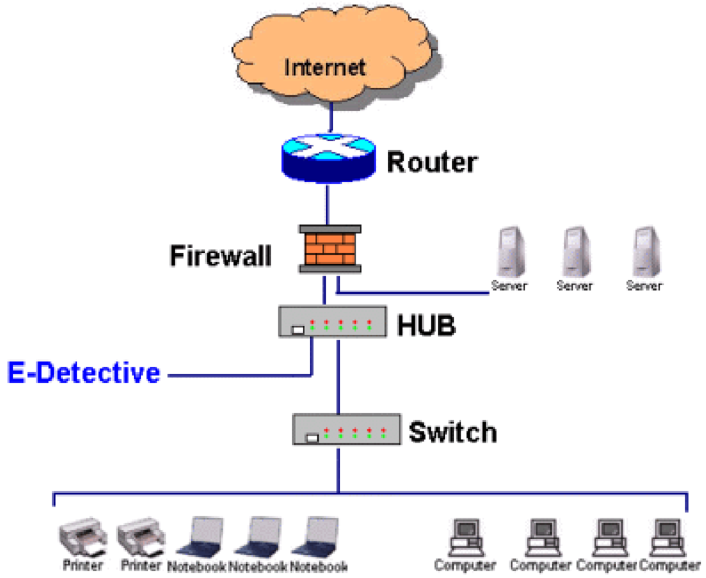
E-Detective System records and reconstructs internet content by monitoring network packet. The best way to get data is to deploy the appliance in Switch, Switch Hub, or Hub between network gateway and servers. If you do it right, E-Detective System will provide you complete information. There are basically four modes of operation for E-Detective: Mirror Mode, Broadcast Mode, Bridge Mode and Double Layer Architecture Mode.

1. Mirror Mode (Medium group of users 10 ~ 1000 users)

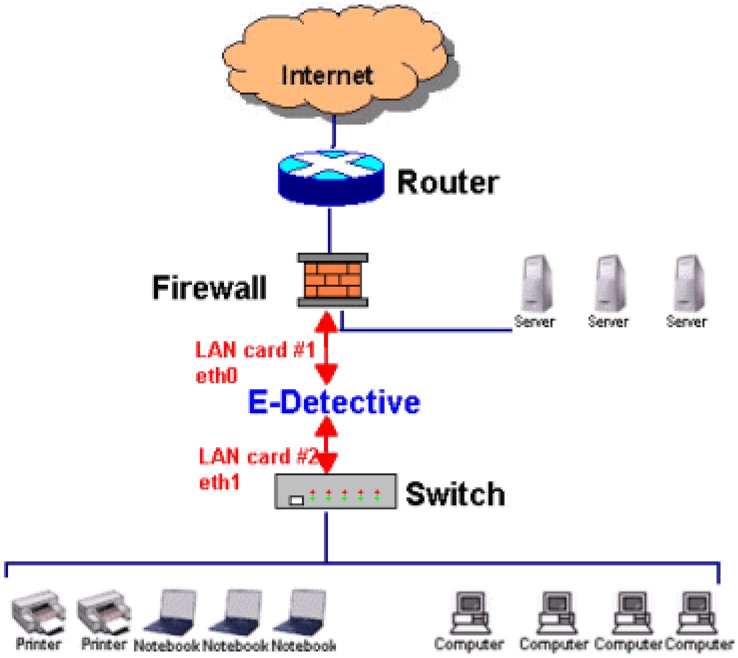
Mirror mode is the most common mode used. Mirror mode means E-Detective collects data by mirror function which is provided by network equipment. You should have two NICs. One adapter is for collecting data, and the other one is for management. You don't need to set IP address for the first adapter. It is used for recording data by mirror port. The other one is used for data management (administration). Default IP address is 192.168.1.60. We suggest you use this mode, if the data flow in customer site is large.



2. Broadcast Mode (Smaller group of users <10 users)
Network equipment provides broadcasting for E-Detective to collect data. You just need one NIC for recording and management. Default IP address is 192.168.1.60. If data flow is small, you can choose this mode.

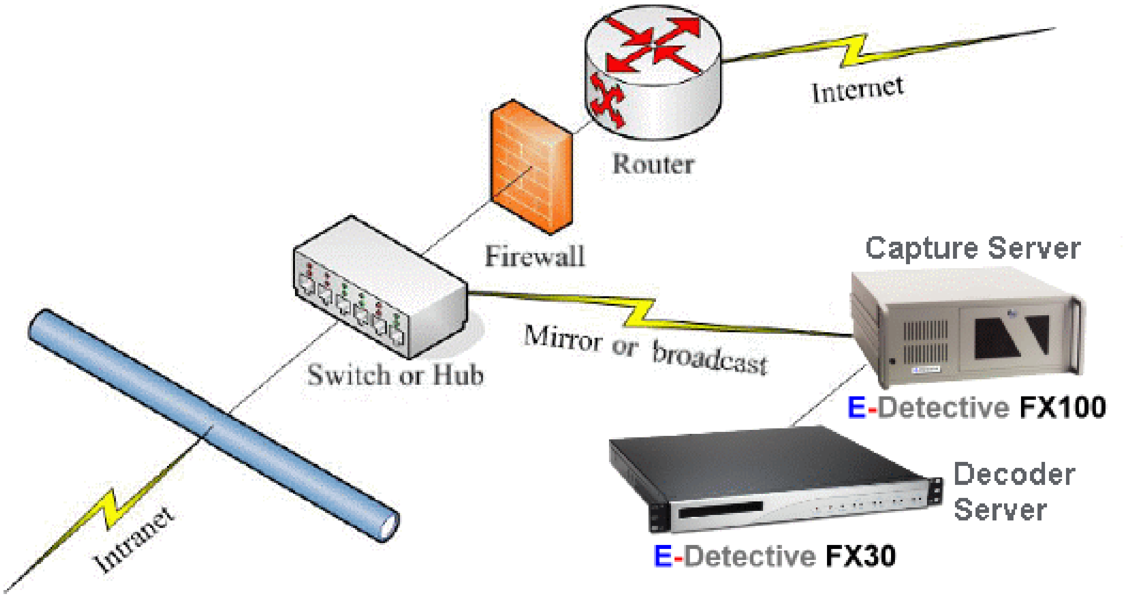


3. Bridge Mode (Medium group of users 10 ~ 200 users)
Bridge mode means Internet data should be transfer through E-Detective. This mode should use two NICs and one IP address. It is used for special customer's environment.



4. Double Layer Architecture Mode (Large group of users >1000 users)

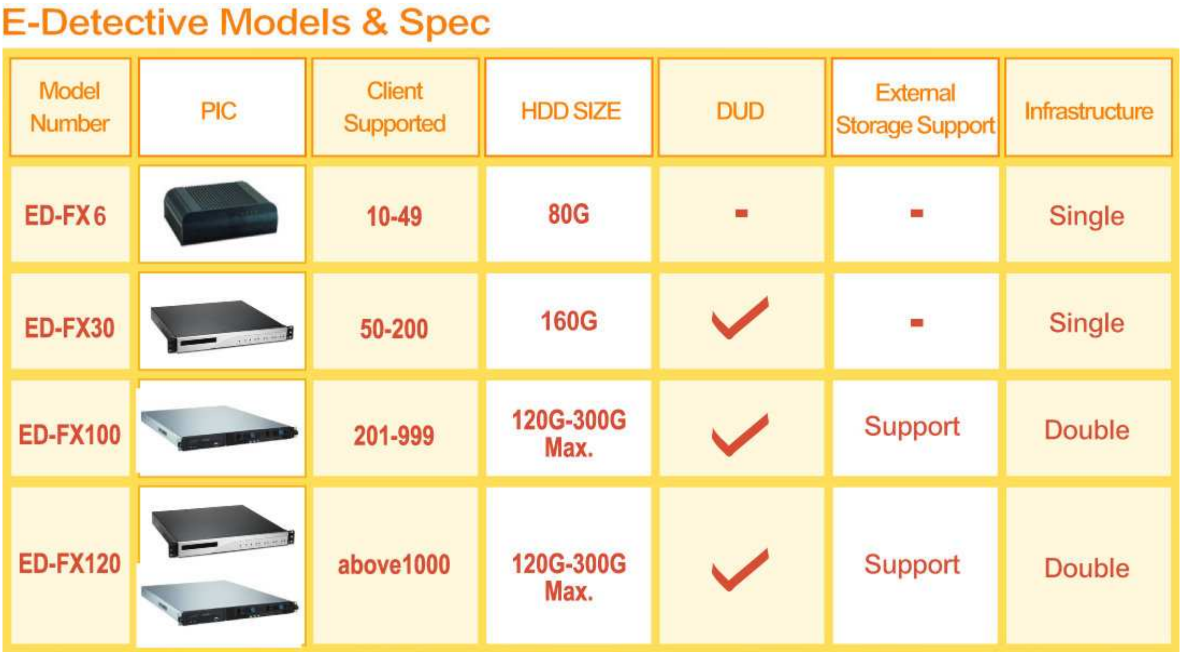
Double layer architecture mode is used for large enterprise network. Its setup consists of two units of E-Detective where one unit is a sender (capture) and another unit as a receiver (decode).



Who needs E-Detective?

- Financial, banking and investment based companies where all company information such as transaction records that need to be monitored.
- Companies such as marketing, design house, high technology, research and development (R&D) that need to prevent important data from leakage.
- Government sectors and ministries that want to protect important information from leaking out.
- Schools, colleges, institutions and universities that want to monitor students and staffs online activities or keep a record for all online applications.
- Any companies who want to monitor, backup and archive daily data.

E-Detective Models



E-Detective Models & Spec

Model Number	PIC	Client Supported	HDD SIZE	DUD	External Storage Support	Infrastructure
ED-FX6		10-49	80G	-	-	Single
ED-FX30		50-200	160G	✓	-	Single
ED-FX100		201-999	120G-300G Max.	✓	Support	Double
ED-FX120		above1000	120G-300G Max.	✓	Support	Double

Note: Wired E-Detective System Functions and Features are subjected to updates and changes by Decision Computer.