Wireless Monitoring and Protection

Topics

- Objectives
- Protocol Analyzers
- WIPS
- Common WIDS/WIPS Features
- Conclusion

Objectives

- Understand how to select and use 802.11 protocol analyzer based on security features.
- Understand the security features of 802.11 WIPS

Wireless Protocol Analyzer

- A Wireless Protocol Analyzer is a tool that can be used to assist with the site survey process, troubleshoot network communication issues and examine wireless frames and their contents.
- Protocol Analyzers do not need to associate to other wireless devices, they are merely “listening” and recording what they “hear”.

Wireless Protocol Analyzer

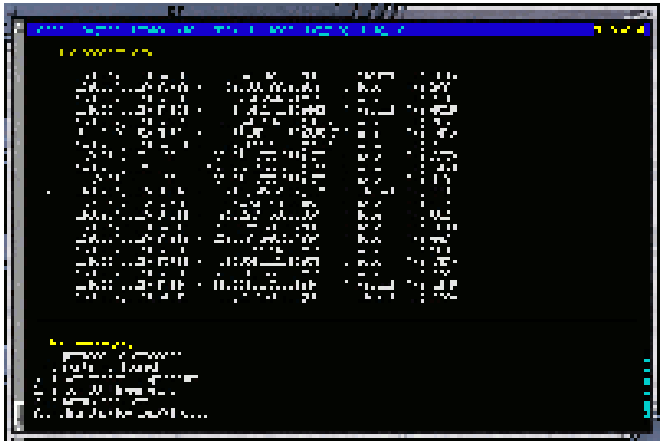
here are some of the free network protocol analyzers available online:

http://sectools.org/tag/sniffers/

1. ettercap
2. Hping
3. Kismet
4. Nemesis
5. Netstumbler/ministumbler
6. ngrep - network grep
7. Tcpdump
8. Windump
9. Wireshark

Wireless Protocol Analyzer

ettercap



Publisher: Alberto Ornaghi and Marco Valleri

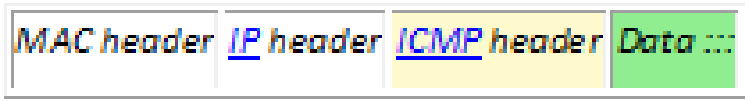
Home Page: http://ettercap.sourceforge.net/index.php

License: GNU General Public License

Platforms: Windows, Linux, Unix

suitable for man in the middle attacks on LAN

ICMP type 8, Echo request message:



ICMP type 8, Echo request message:

0 0	0 1	0 2	0 3	0 4	0 5	0 6	0 7	0 8	0 9	1 0	1 1	1 2	1 3	1 4	1 5	1 6	1 7	1 8	1 9	2 0	2 1	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	3 0	3 1
Type								Code								ICMP header checksum															
Identifier																Sequence number															
Data :::																															

Type. 8 bits. Set to 8.

Passive vs. Active monitoring

- The passive approach: use of devices to watch traffic as it passes by
- The active approach : capability to inject test packets into network

Wireless Protocol Analyzer

hping

Publisher: Salvatore Sanfilippo

Home Page: http://www.hping.org/

License: GNU General Public License

Platforms: Linux, Unix

Wireless Protocol Analyzer

kismet



Publisher: Mike Kershaw

ome Page:http://www.kismetwireless.net/

License: [GNU General Public License](#)

Platforms: Linux, Unix

Wireless Protocol Analyzer

Nemesis

publisher: Jeff Nathan

Home Page:http://nemesis.sourceforge.net/

License: Free

Platforms: Windows, Linux, Unix

Wireless Protocol Analyzer

NetStumbler/MiniStumbler



Publisher: Marius Milner

Home Page:http://www.netstumbler.com/

Wireless Protocol Analyzer

ngrep - network grep

Publisher: Jordan Ritter

Home Page: http://ngrep.sourceforge.net/

License: Free

Platforms: Windows, Linux, Unix

Wireless Protocol Analyzer

tcpdump

Publisher: Lawrence Berkeley National Library

Home Page:http://www.tcpdump.org/

License: Free

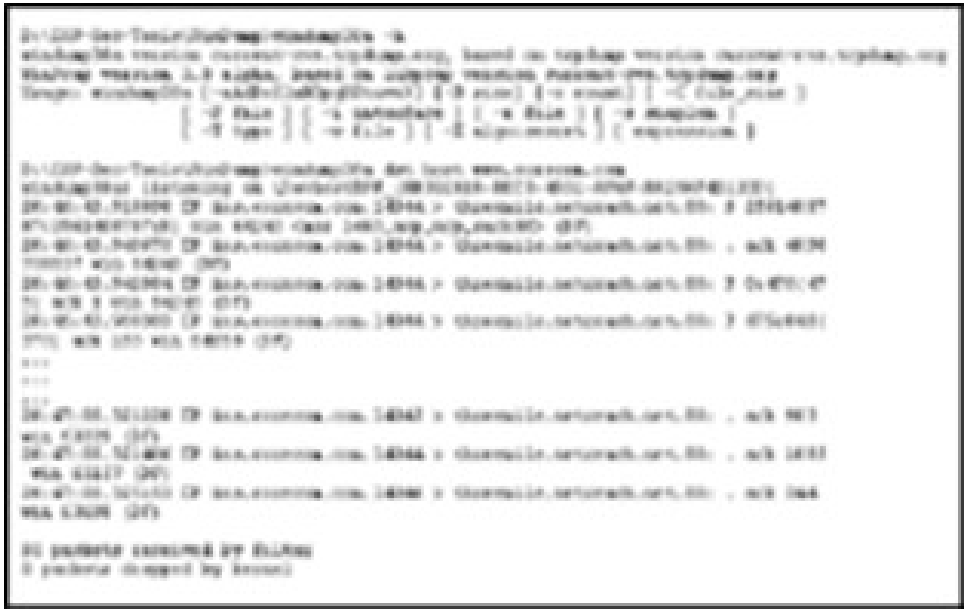
Platforms: iWindows, Linux, Unix

-w flag

-b flag

Wireless Protocol Analyzer

WinDump: tcpdump for Windows



Publisher: Politecnico di Torino

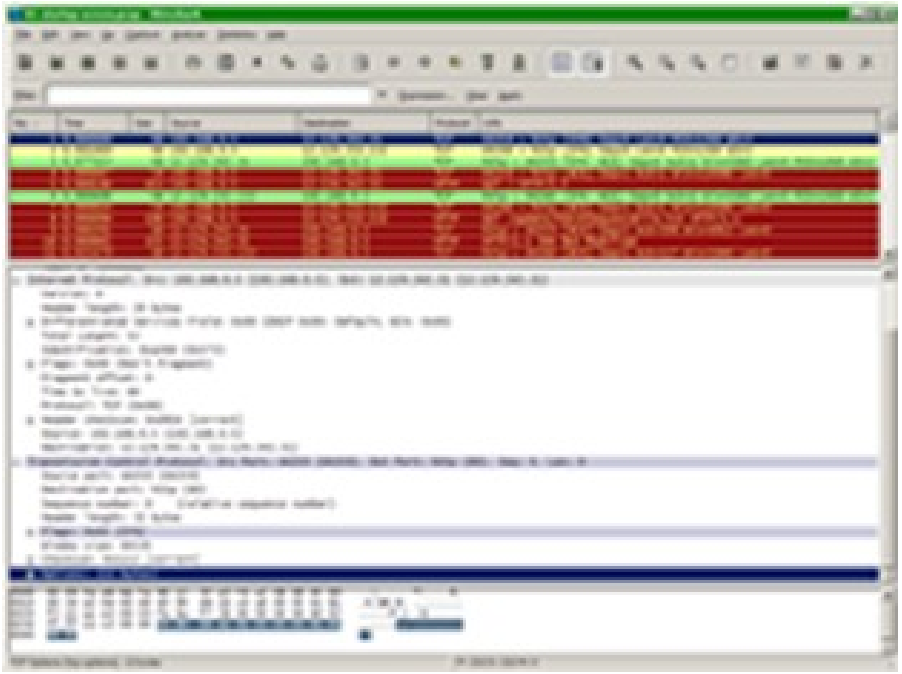
Page:http://www.winpcap.org/windump

License: Free

Platforms: Windows

Wireless Protocol Analyzer

Wireshark



Publisher: Wireshark Development Team

Home Page:http://www.wireshark.org/

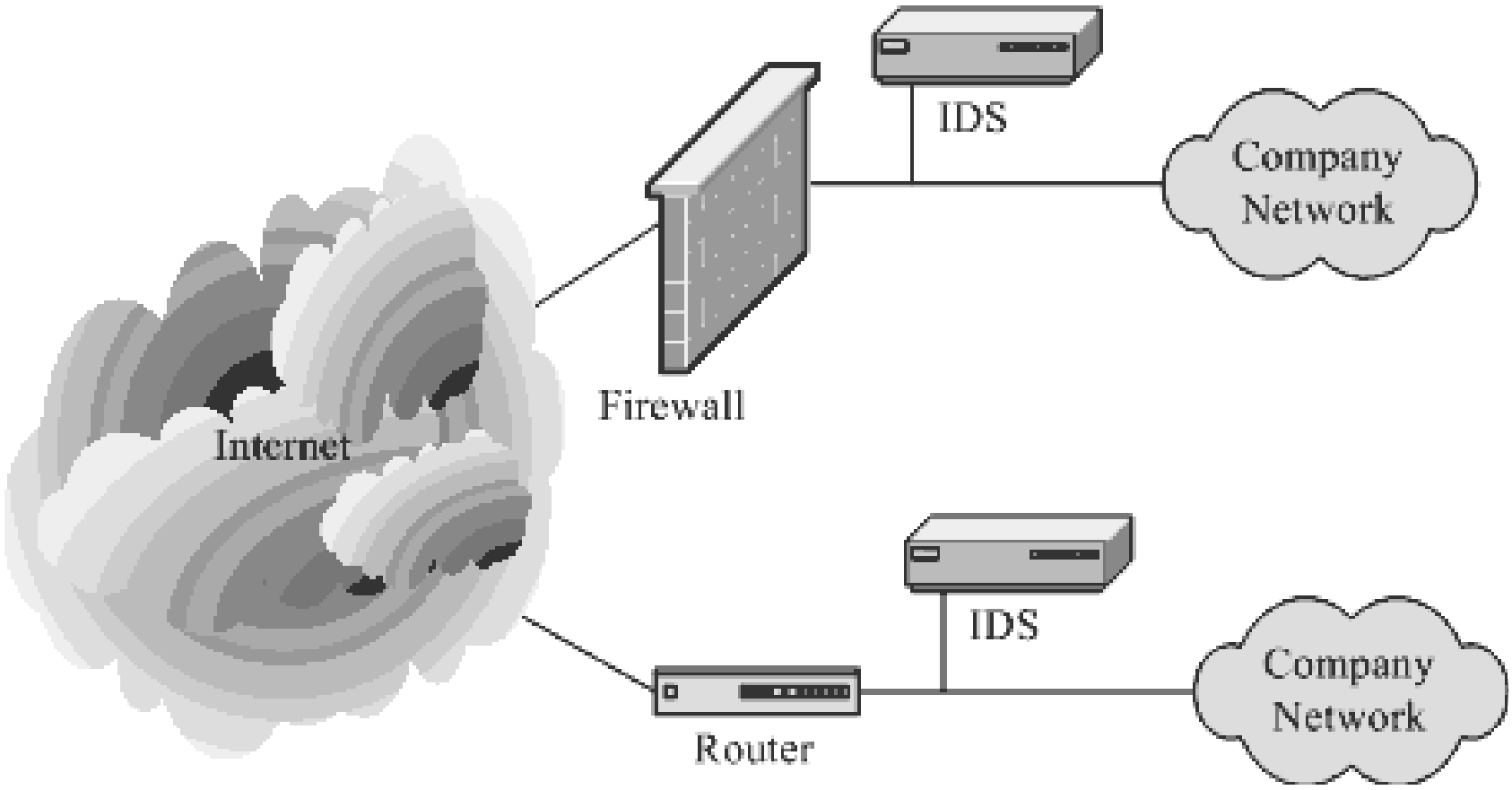
License: GNU General Public License

Platforms: Windows, Linux, Unix

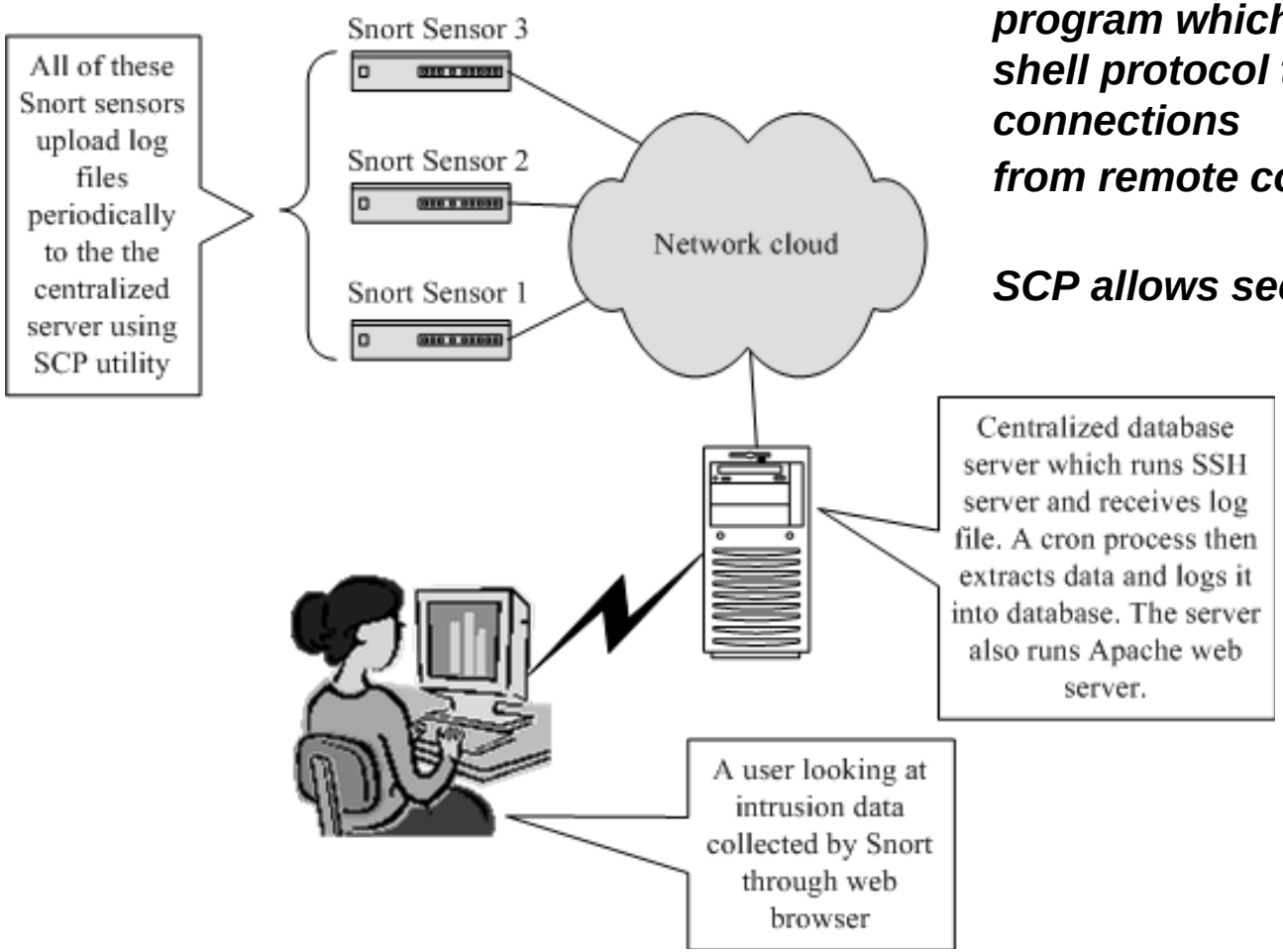
Wireless Intrusion System IDS/IPS/WIDS

- Intrusion detection systems (IDS) are designed to analyze data communications for unauthorized activity and then alert administrators about the situation.
- Intrusion prevention systems (IPS) are designed to not only analyze and alert but also take proactive measures to prevent further access by the unauthorized party.
- A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points.
- WIPS

IDS


IDS
Company Network
Internet
Firewall
IDS
Company Network
Router

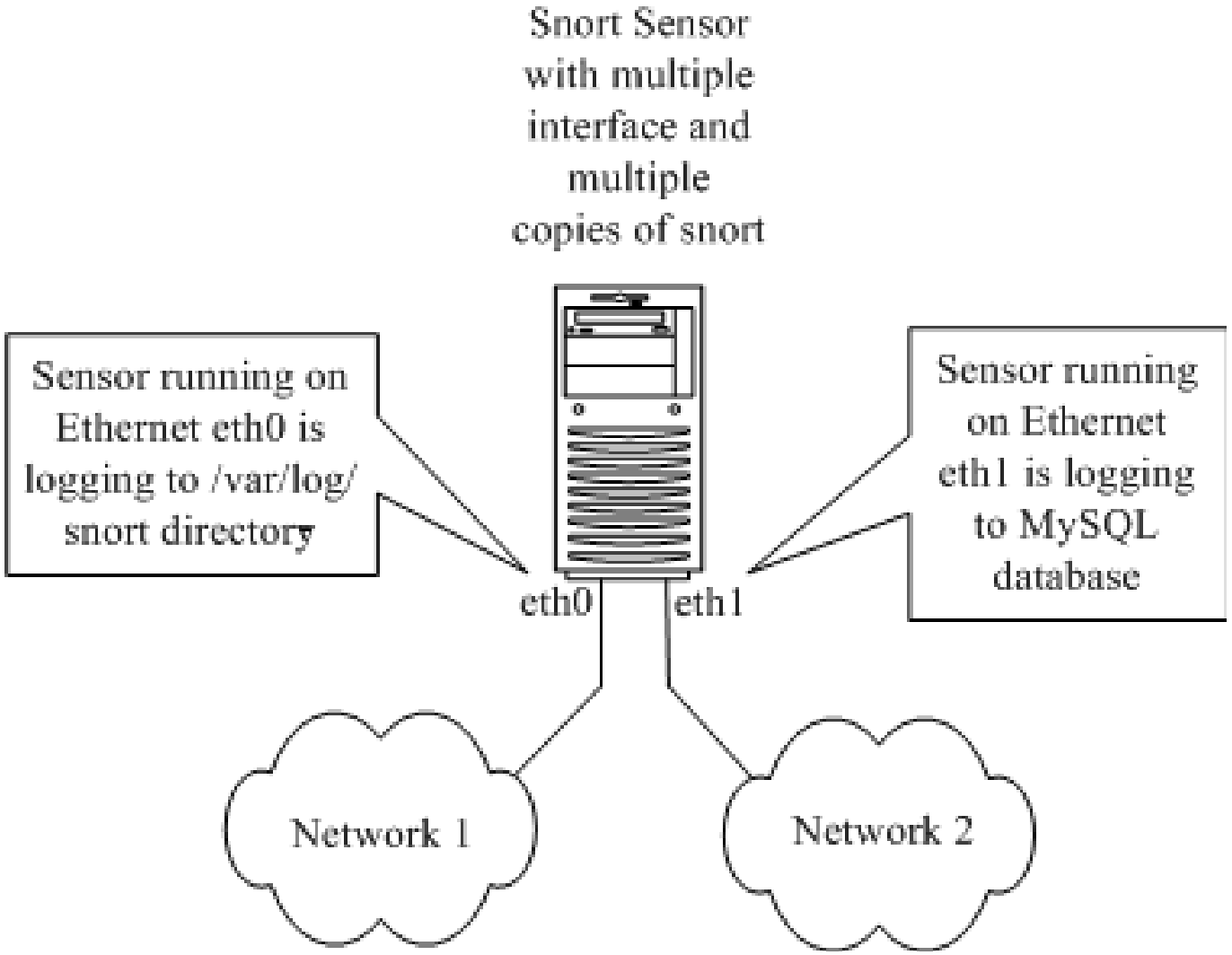
Sensors

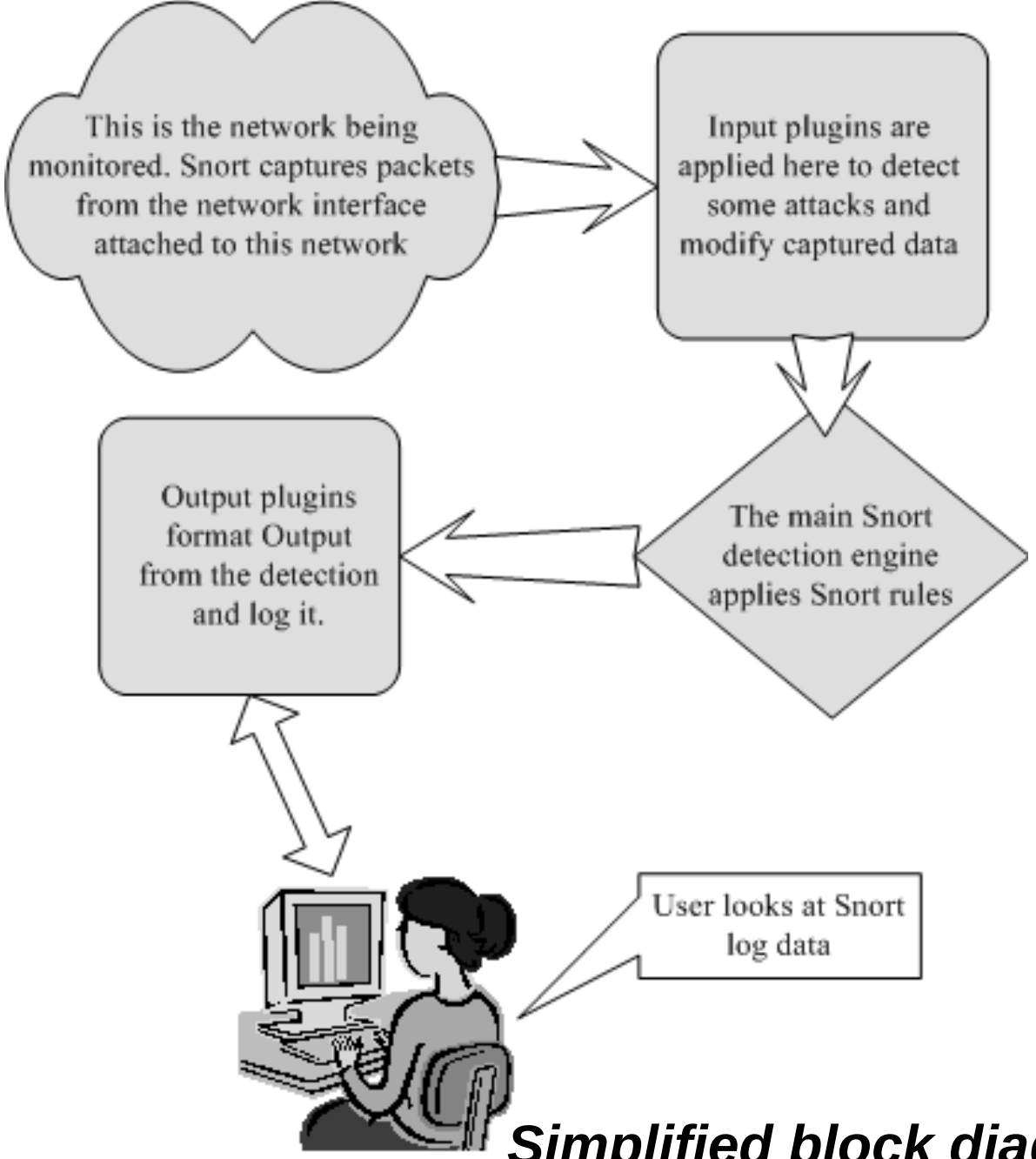


SSH server is a software program which uses the secu shell protocol to accept connections from remote computers

SCP allows secure file transfe

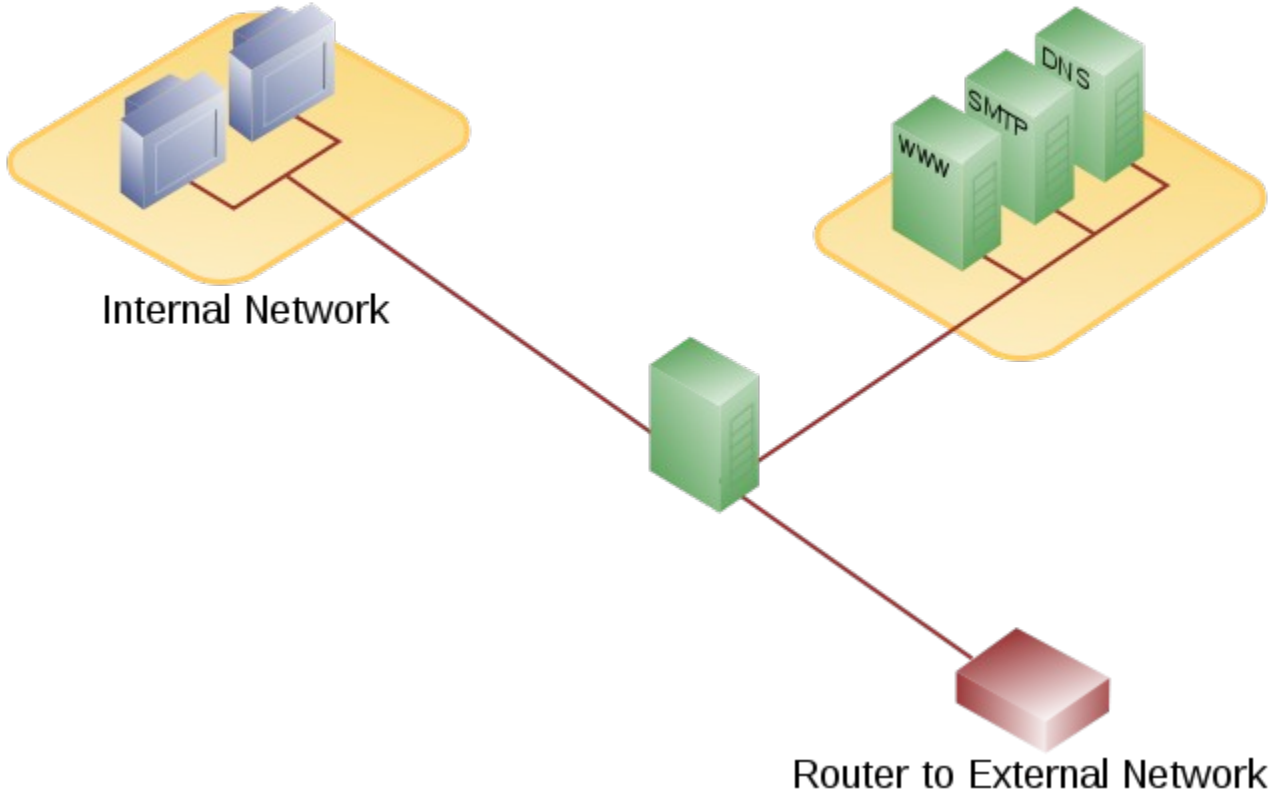
Running Snort on multiple network interfaces and logging to different places





Simplified block diagram for Snort.

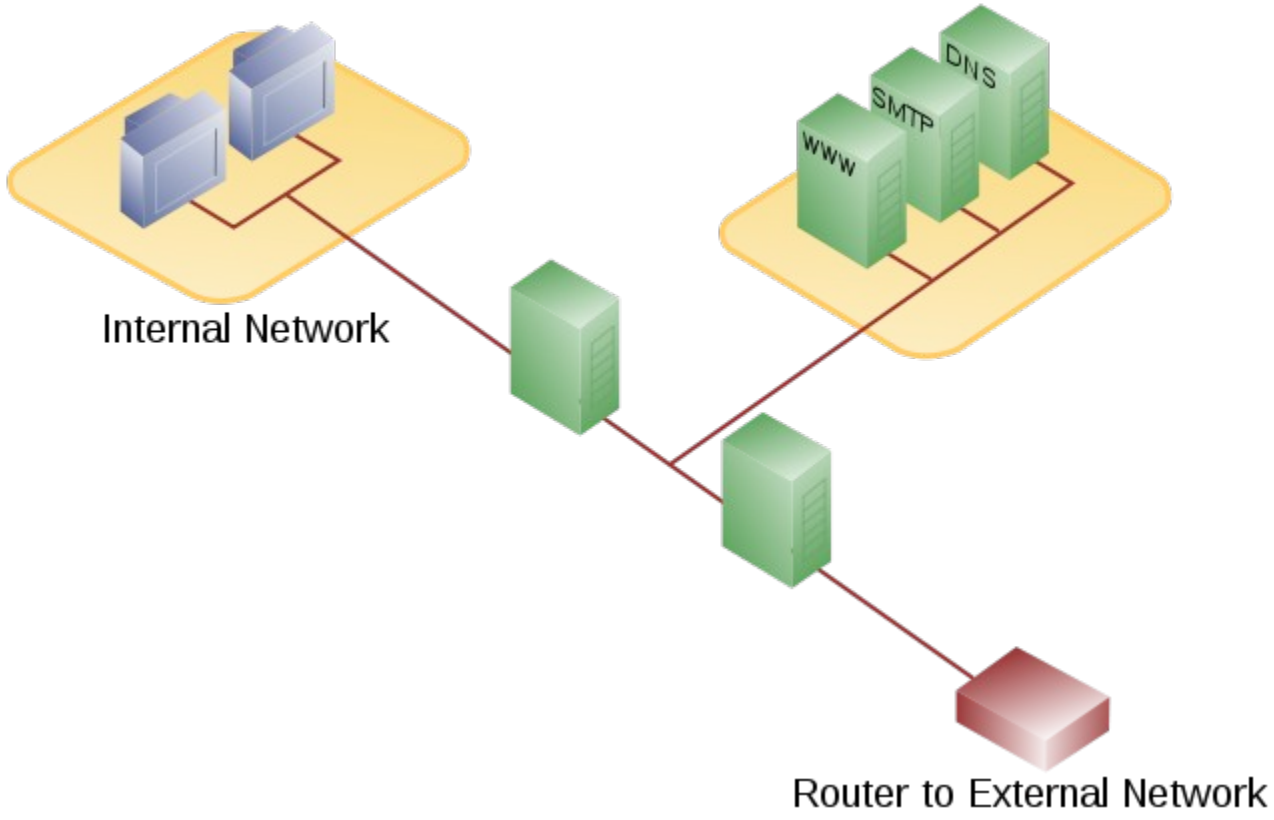
About the DMZ (Demilitarized zone)



DMZ using a three-legged firewall

About the DMZ (Demilitarized zone)

defense in depth

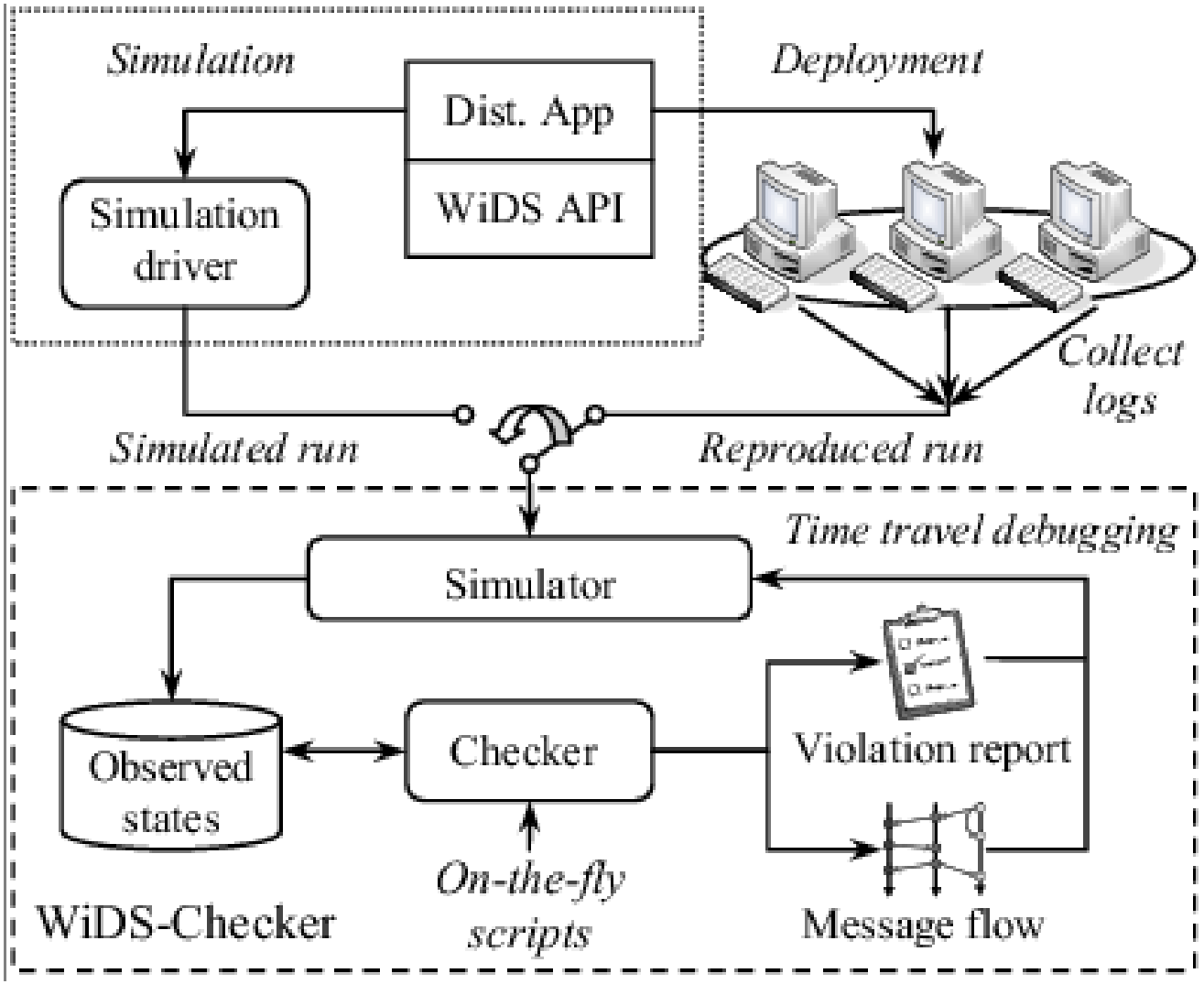


DMZ using dual firewalls

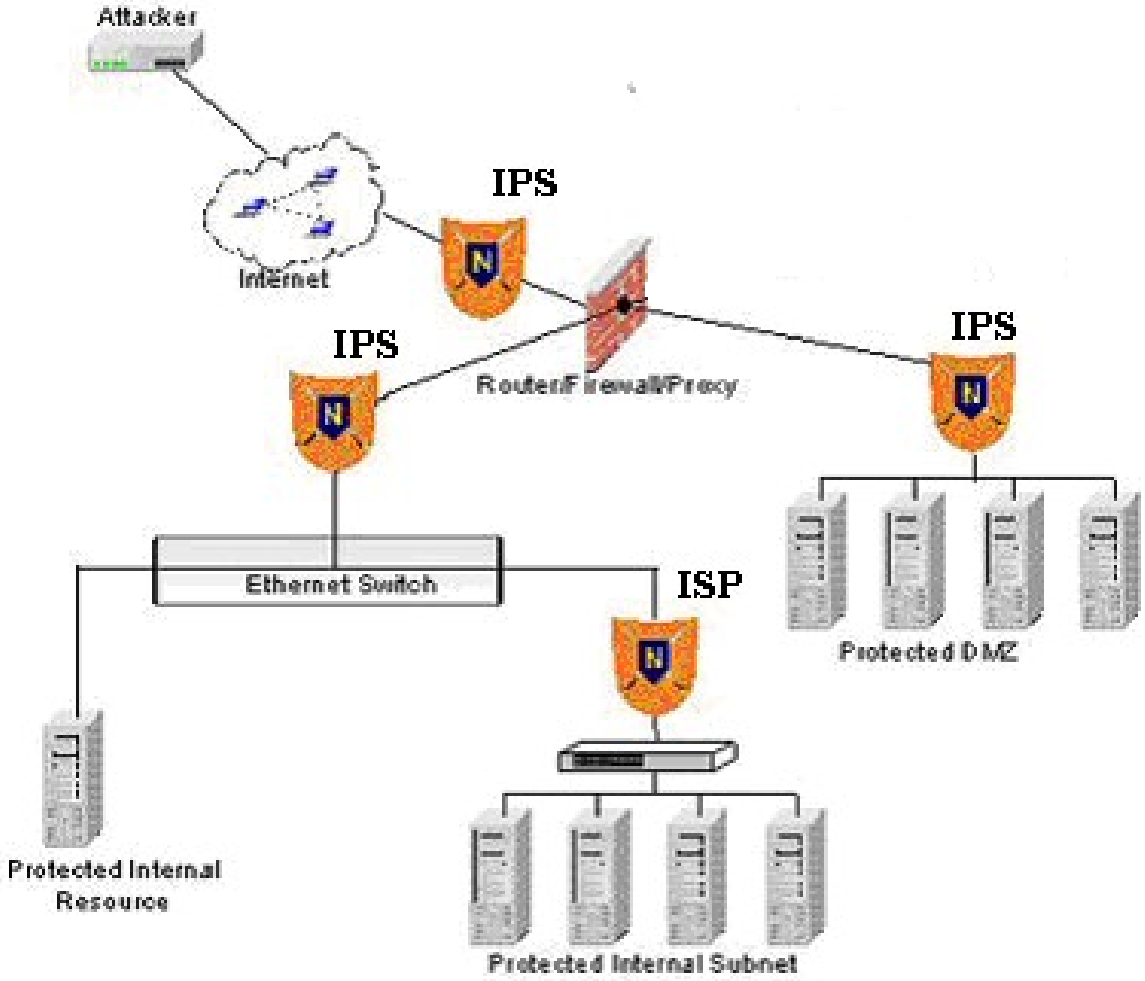
Cont…

- Common WIDS/WIPS features:
  - Device identification and Categorization
  - Event Alerting, Notification and Categorization
  - Rogue Containment (class assignment)
  - Policy enforcement and violation reporting (class assignment)
  - Rogue triangulation and Rogue Fingerprinting (class assignment)

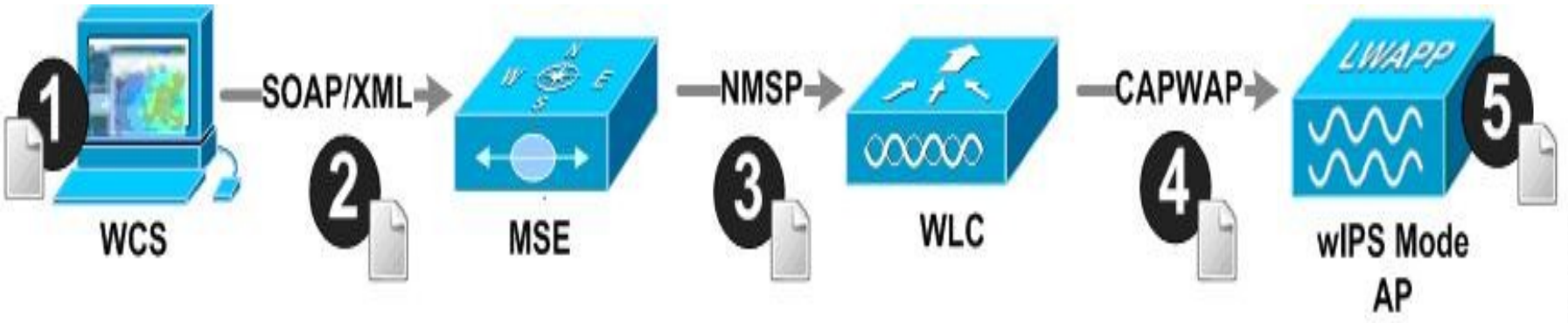
WIDS checking methodology



IPS

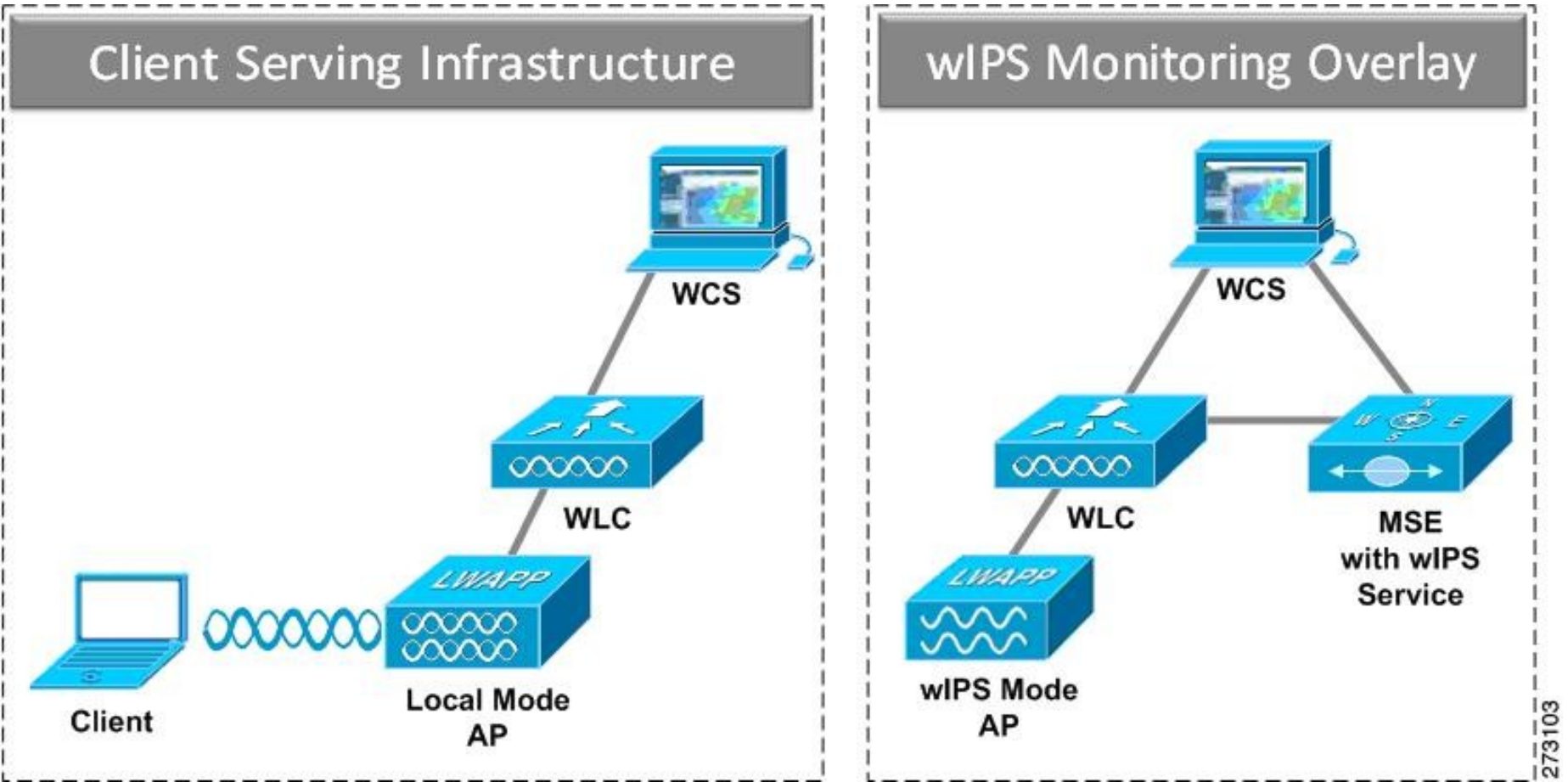

Attacker
Internet
IPS
IPS
IPS
Router/Firewall/Proxy
Ethernet Switch
ISP
Protected DMZ
Protected Internal Resource
Protected Internal Subnet

WCS: Wireless Control System (a management solution)
http://www.cisco.com/en/US/products/ps6305/index.html
WLC: WLAN Controller
http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html
MSE (Mobility Service Engine)



SOAP: **Simple Object Access Protocol**,
is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks

An example of WIPS



Conclusion

- Protocol analyzer is a monitoring tool for examining the contents of wireless frames by decoding the information received by a possible monitoring system.
- Security monitoring is classified to WIDS or WIPS depending whether the system can take proactive steps to protect the network.
- Policy enforcement is an automated way of reacting to wireless conditions deemed critical.
- Rogue triangulation and fingerprinting are ways of physically finding a rogue device.