COMP 5075 Telecommunications and Device Security

Sample Learning Journal A

Yee Wei Law

June 14, 2023

This document serves as the template for the Learning Journal assessment in COMP 5075 Telecommunications and Device Security.

Contents

List of acronyms

DMZ	demilitarised zone	4
IDS	intrusion detection system	1
IDPS	intrusion detection and prevention system (synonymous with "intrusion prevention system")	4
SIEM	security information and event management	4
SPAN	switched port analyser	4
TAP	test access point	4

1 Tutorial 1

1.1 Task 1: Classification of intrusion detection systems

An intrusion detection system (IDS) (defined in Tutorial 1) can be classified as:

- **Host-based**: A host-based IDS is an IDS that monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activities [SM07, Appendix A].

  Figure 1 shows an example of how a host-based IDS can be deployed.

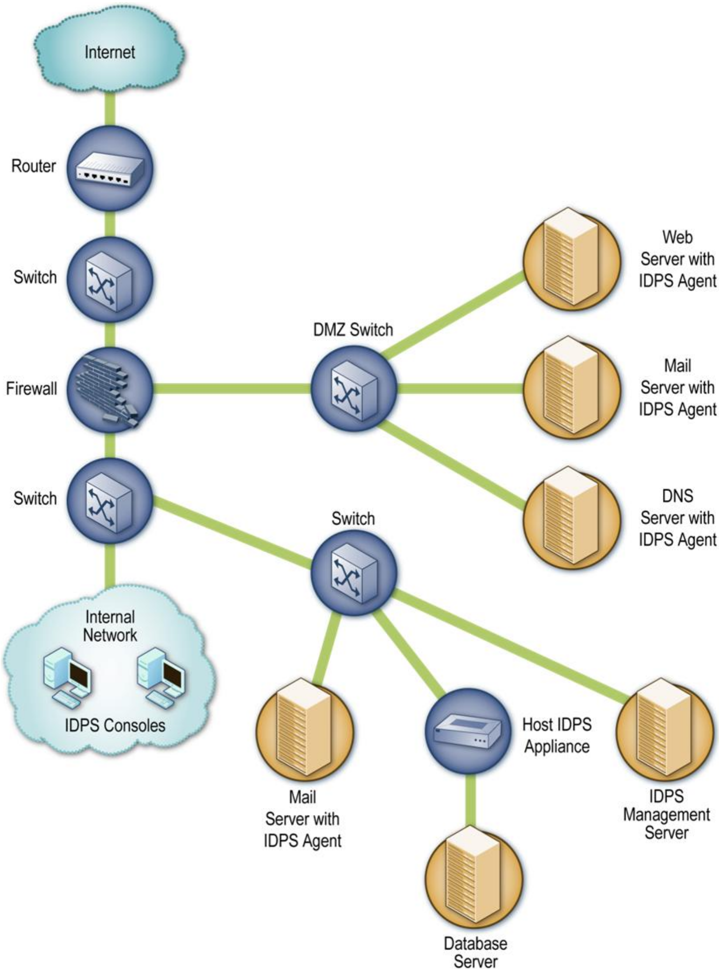


Figure 1: An example of how a host-based IDS can be deployed [SM07, Figure 7-1]. Note 1️⃣ the IDS sensors/agents monitoring the web server, mail servers, Domain Name System server and database server; 2️⃣ a host-based IDS can exist in the form of software or hardware.

  Examples of characteristics a host-based IDS monitors include wired and wireless network traffic (only for that host), firewall logs, system logs, database logs, running processes, file access and modification traces, as well as system and application configuration changes [SM07, KGVK19].

- **Network-based**: A network-based IDS is an IDS that monitors network traffic for particular network segments or devices and analyses the network and application protocol activities to identify and stop suspicious activities [SM07, Appendix A].

  Figure 2 shows an example of how a network-based IDS can be deployed.

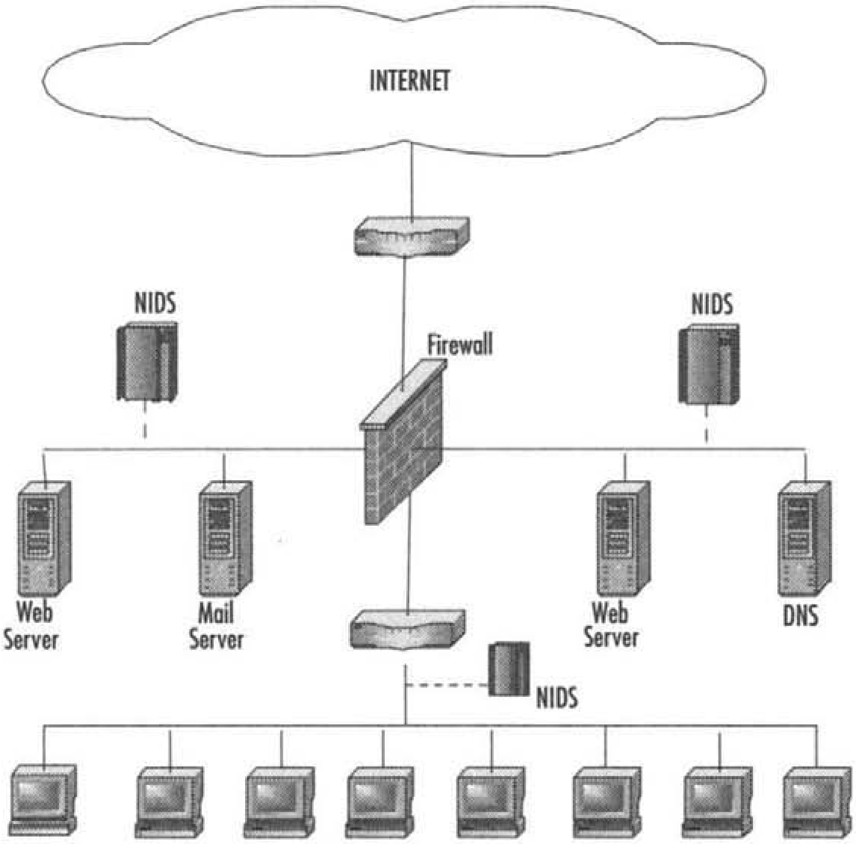


Figure 2: An example of how a network-based IDS can be deployed: two IDS sensors monitoring two public-facing subnets and one IDS sensor monitoring a subnet of internal terminals [BE07, Figure 1.1].

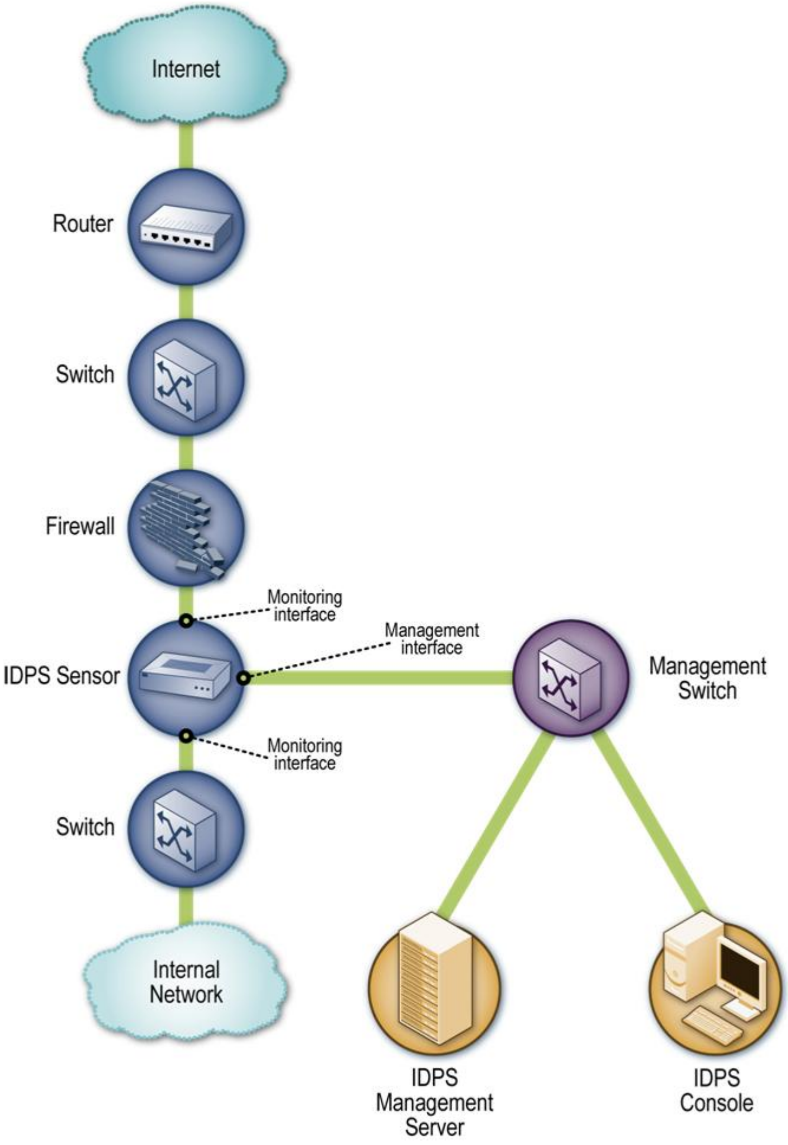


Figure 3: An example of an inline network-based IDS [SM07, Figure 4-2]. Note how the IDS sensor is placed right after the firewall, on the more secure side of the network boundary. The IDS sensor can also be placed on the less secure side of the network boundary to reduce load on the firewall [SM07, Sec. 4.2.2].

Network-based IDS products typically provide a wide variety of security capabilities, e.g., security information and event management (SIEM) capabilities (see Tutorial 2).

A network-based IDS can work in either of these two modes:

- **Inline mode**: An inline sensor is deployed so that all network traffic to be monitored is channelled through it, e.g., at the boundary between an external network and an internal network (see Figure 3), or the boundary between internal networks that should be segregated [SM07, Sec. 4.2.2].

  An IDS with preventive capabilities, i.e., an intrusion detection and prevention system (IDPS), is usually deployed in the inline mode.

- **Passive mode**: A passive sensor is deployed so that it gets a *copy* of the actual network traffic (see Figure 4).

  Passive sensors are typically deployed so that they can monitor the traffic at key network locations, e.g., network boundaries, demilitarised zone (DMZ) subnets.

  Passive sensors can monitor traffic through [SM07, Sec. 4.2.2]:

  - The *switched port analyser* (SPAN) ports (also called mirror or mirroring ports) of a switch: A SPAN is a software function of a switch or router that duplicates traffic from incoming or outgoing ports and forwards the copied traffic to a specialised port called a SPAN port [Gig20].

  - A network *test access point* (TAP): This is a hardware component that can be connected to a cabling infrastructure to copy packets for monitoring purposes [Gig20].

    A TAP is preferred to a SPAN because 1️⃣ SPAN ports are easily oversubscribed resulting in packet drops; 2️⃣ packets are duplicated when a SPAN port is configured to capture both ingress and egress traffic flows; 3️⃣ the time stamps of packets collected through SPAN may be changed; 4️⃣ SPAN operations are processor-intensive and can negatively impact the performance of the switch; 5️⃣ SPAN ports are programmable/reconfigurable and subject to cyber attacks [Lac17, Gig20, Gar21].

    Nevertheless, SPAN ports remain useful for links with power budget limitations and low-utilisation or low-throughput links at remote sites [Lac17, Gig20].

    Figure 4(b) depicts the data flows between a switch and a router when either a SPAN port or a network TAP is used.

  - An IDS *load balancer*: This is a device that aggregates and directs network traffic to IDS sensors.

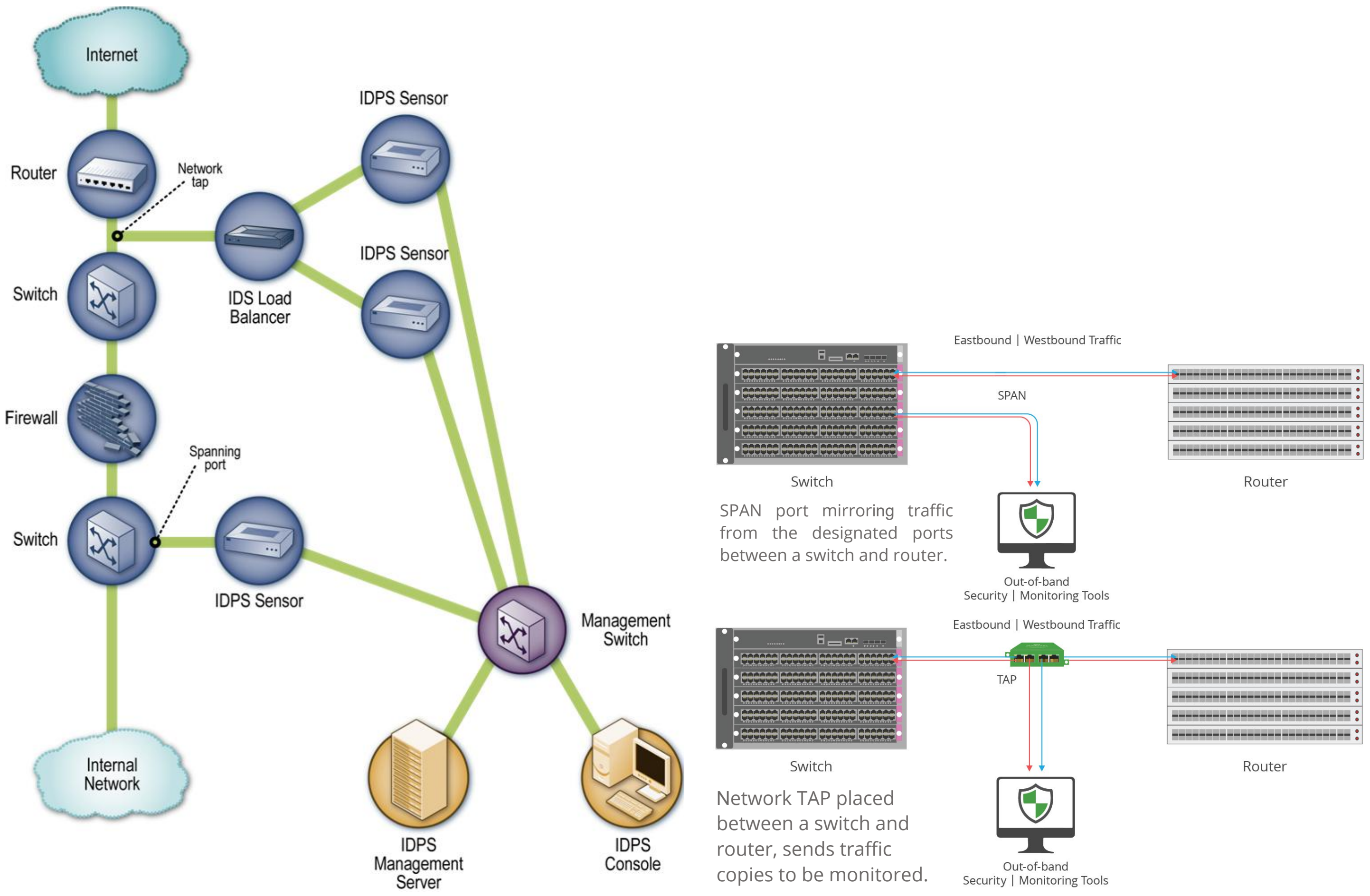
    An IDS load balancer works according a set of rules configured by an administrator.

    These rules may direct all traffic to multiple IDS sensors, or split the traffic among multiple sensors by volume, IP address, protocol or some other characteristics.

Traffic splitting may however cause signs of malicious events to be missed.

- **Distributed**: When 1️⃣ a mix of host-based and network-based sensors are employed, and 2️⃣ IDS management is centralised (e.g., in Figure 1, Figure 3 and Figure 4), some authors [BE07, pp. 7-8] refer to the resultant architecture as *distributed* IDS.

  Distributed IDSs combine host-based and network-based analytics, and this is especially helpful for detecting insider attacks [LDVH+18].



SPAN port mirroring traffic from the designated ports between a switch and router.

Network TAP placed between a switch and router, sends traffic copies to be monitored.

(a)

(b)

Figure 4: (a) An example of a passive network-based IDS [SM07, Figure 4-3]. (b) SPAN vs TAP for monitoring [Gar21].

Table 1 compares the advantages and disadvantages of host-based and network-based IDSs.

Network-based IDSs can be further differentiated as:

- **Wired vs wireless**: A network-based IDS typically works in a wired infrastructure but a *wireless* IDS is a special type of network-based IDS tailored to monitoring wireless network traffic and analysing wireless networking protocols (e.g., Wi-Fi, cellular, Bluetooth, LoRa) for the purpose of identifying suspicious activities involving these protocols; see [SM07, Sec. 5] and [Led22].

  Wireless IDS vendors include Bastille and SonicWall.

- **Protocol-based vs application protocol-based**: In a *protocol-based* IDS, sensors are placed at the front of a server to monitor traffic between the server and its clients [Led22].

  In an *application protocol-based* IDS, the traffic across a group of servers is monitored [Led22]. Furthermore, specialised application protocols are usually leveraged for monitoring, to help network administrators segment and classify their network monitoring activities [Led22].

Table 1: Comparing host-based and network-based IDSs, based on [KGVK19, Table 4], [BE07, p. 6] and [FGCMF21].

	Host-based	Network-based
Pros	Can check end-to-end encrypted traffic Can reassemble fragmented packets Ruleset can be tailored to individual hosts	Runs on its own resources Monitor traffic of multiple hosts at the same time Aware of a broad range of network protocols
Cons	Relies on the host's resources Only detects attacks targeted at the host	Cannot check end-to-end encrypted traffic Might struggle with packet reassembly and not cope with peak traffic Insufficient for detecting insider attacks
Examples	OSSEC, Sagan, Spartan RDP Guard, AIDE, Tripwire, Security Onion	Snort, Suricata, Zeek, Sguil, Security Onion

1.2 Task 2

2 Tutorial 2

2.1 Task 1

2.2 Task 2

3 References

[BE07] A. R. Baker and J. Esler (eds.), *Snort IDS and IPS Toolkit*, Syngress, 2007. https://doi.org/10.1016/B978-1-59749-099-3.X5000-9.

[FGCMF21] M. Fuentes-García, J. Camacho, and G. Maciá-Fernández, Present and future of network security monitoring, *IEEE Access* **9** (2021), 112744–112760. https://doi.org/10.1109/ACCESS.2021.3067106.

[Gar21] Garland Technology, TAP vs SPAN: Best Practice Guide to Improving Network Visibility, white paper, 2021. Available at https://www.garlandtechnology.com/hubfs/Current/Documents/Whitepaper/GTWP-TAP-vs-SPAN21.pdf.

[Gig20] Gigamon, Understanding Network TAPs: The First Step to Visibility, white paper, 2020. Available at https://www.gigamon.com/content/dam/resource-library/english/white-paper/wp-network-taps-first-step-to-visibility.pdf.

[KGVK19] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, Survey of intrusion detection systems: techniques, datasets and challenges, *Cybersecurity* **2** no. 1 (2019), 20. https://doi.org/10.1186/s42400-019-0038-7.

[Lac17] J. Lackey, SPAN Port: The ABCs of Network Visibility, Keysight Blogs, August 2017. Available at https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2017/08/10/span_port_the_abcs-MMVt.html.

[Led22] J. Ledesma, IDS vs. IPS: What Organizations Need to Know, Varonis Inside Out Security Blog, June 2022. Available at https://www.varonis.com/blog/ids-vs-ips.

[LDVH+18] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, Detecting and preventing cyber insider threats: A survey, *IEEE Communications Surveys & Tutorials* **20** no. 2 (2018), 1397–1417. https://doi.org/10.1109/COMST.2018.2800740.

[SM07] K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94, 2007. Available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf.