COMP 5075 Telecommunications and Device Security

Sample Learning Journal A

Yee Wei Law

March 7, 2025

Learning Journal A addresses Tutorials 1 and 2, while Learning Journal B addresses Tutorials 3 and 4.

Contents

List of acronyms

ASIC	application-specific integrated circuit	5
CPU	central processing unit	5
DLP	data loss prevention	5
DPI	deep packet inspection	3
IoT	Internet of Things	8
IPS	intrusion prevention system	3
IPsec	Internet Protocol Security	3
L2TP	Layer-2 Tunneling Protocol	4
NGFW	next-generation firewall	3
NIST	National Institute of Standards and Technology	3
PPTP	Point-to-Point Tunneling Protocol	4
RAM	random-access memory	7

SD-WAN	software-defined wide area network	4
SIEM	security information and event management	1
SMB	small- or medium-sized business ("small- and medium-sized businesses" in plural)	
SSD	solid-state drive	7
URL	uniform resource locator	8
UTM	unified threat management	1
TLS	transport-layer security	4
VPN	virtual private network	3
WAN	wide area network	4

1 Tutorial 1

1.1 Task 2: UTM

1.1.1 [9 marks] Search strategy and justification

On 23 Feb 2023, searching "unified threat management" on Google Scholar returned 1,940 results. Overall, citation counts were at most double-digit for this search keyword.

- [QYXL07] appeared on the first page with 26 citations, which is the highest on the first page.
- The IEEE conference ICNS '07 seems decent; the quality of the writing is good; and the authors' institution is one of the best universities in China. Therefore, [QYXL07] was selected as the academic reference.

On 23 Feb 2023, searching "unified threat management" on Google returned more than 530,00 results, the first of which was a link to Fortinet [For23b].

- [For23b] linked to [Tit16].
- On the first page of the search results, there was a link to Check Point [Che23b], which in turn linked to [KHL22].
- Gartner's 2022 magic quadrant for network firewalls [KHL22] indicates that Fortinet, Palo Alto Networks and Check Point Software Technologies were the leading vendors. Note Gartner no longer publishes magic quadrant for UTM.
- Considering the significance of Fortinet and Check Point, these references [For23b, Tit16, Che23b, KHL22] were selected.

On 23 Feb 2023, searching "unified threat management" on UniSA library returned more than 1,700 results.

- Among the results that were not patents, the first was the book [TSM+13].
- [Cam16] is an additional book found on Google Books and accessible via UniSA library.

- Both of these books are well written and were produced by reputable publishers, and thus they were selected as references.

Therefore, besides [SH09], [FGCMF21] and [Gar22], the following references were selected: [QYXL07, For23b, Tit16, Che23b, KHL22, TSM$^+$13, Cam16].

1.1.2 [20 marks] UTM: Definition and the state of the art

The term "unified threat management" was first coined in the report entitled "Worldwide Threat Management Security Appliances 2004 – 2008 Forecast and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance" by the market intelligence firm IDC in 2004 [TSM$^+$13, p. 16]. The term refers to a class of security appliances possessing the functionality of 1️⃣ a firewall, 2️⃣ a gateway anti-malware, and 3️⃣ a network-based intrusion prevention system (IPS) [TSM$^+$13, p. 16].

The current definition of UTM has evolved beyond the initial definition. National Institute of Standards and Technology (NIST) has not provided a definition of UTM, but based on the official NIST publication [SH09], Gartner [Gar22] and Fortinet [For23b], UTM is a converged platform of endpoint security products that typically combines the functionality of 1️⃣ a firewall, 2️⃣ an IPS, 3️⃣ a virtual private network (VPN), 4️⃣ a gateway anti-malware that performs web filtering (i.e., filtering of web pages based on their uniform resource locator and content) and email filtering (i.e., filtering of emails for malware and other undesirable content such as spam and phish bait).

UTM is to be differentiated from next-generation firewall (NGFW), a term/concept that Gartner first coined in the same year when IDC first coined UTM [TSM$^+$13, p. 19] (or earlier [Hil15]). While UTM has a broad range of endpoint security features, it does not support all the advanced filtering functionality of NGFWs which typically covers the network layer up to the application layer for deep packet inspection (DPI) [Hal23, Hil15]. In general, NGFWs are recommended for large enterprises, whereas UTM products are more suitable for small- and medium-sized businesses (SMBs) [For23b, Hal23]. This is potentially why Gartner equates UTM to SMB multi-function firewall [KN18].

A state-of-the-art UTM product is expected to support the following features (see Figure 1):

- Deep-packet-inspecting firewall: DPI is a packet filtering method that inspects not only the packet's multiple headers, but also the actual data content [Bar23]. It is possible to use oblivious transfer to perform DPI on encrypted packet [SLPR15], but this technique does not seem to have been commercialised.
- VPN: This creates a private (authenticated and confidential) "tunnel" through a public network (e.g., the Internet), enabling end-to-end security between geographically distributed devices with the right credentials. A VPN can be established via Internet Protocol Security (IPsec) (in conjunction with Internet Key

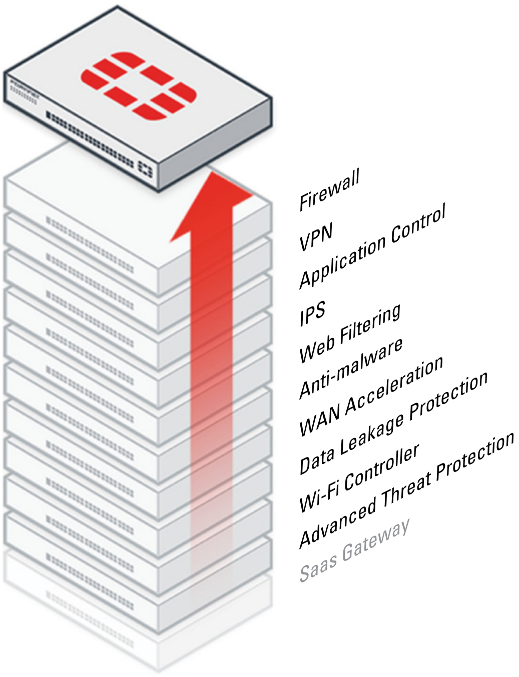


Figure 1: Representative UTM technologies [Tit16, Figure 5-1]. Please ignore the Fortinet logo.

Exchange version 2) [BDF+20] or transport-layer security (TLS) [Tit16]; at least one of these options are supported by a UTM vendor. Despite still being mentioned in some references [Cam16], Point-to-Point Tunneling Protocol (PPTP) and Layer-2 Tunneling Protocol (L2TP) have been found to be insufficiently secure for VPNs [BDF+20, Sec. 8.5].

- Software-defined wide area network (SD-WAN) optimisations: There are scenarios where users of the same organisation are geographically distributed, but for productivity, remote users expect to access their work files as if they are accessing the files in their local office; wide area network (WAN) optimisations are technologies aimed at fulfilling these expectations [Tit16, p. 48]. WAN optimisations include 1️⃣ accelerating the traffic of common protocols, 2️⃣ caching data and files to conserve bandwidth and reduce latency, 3️⃣ offloading the cryptographic operations of TLS to acelerator hardware [Tit16, p. 49]. Figure 2 shows a sample placement of UTM appliances for performing WAN optimisations. The latest trend in WAN optimisations is SD-WAN, where specialised and expensive high-performance routers requiring extensive management efforts are replaced by simple unintelligent boxes that process packets in the *data plane* based on software-defined rules and optimisations dictated by one or more controllers in the *control plane* [MK17].
- Application control: An *application whitelist* is a list of applications and application components (e.g., libraries, configuration files) that are authorised to be present or active on a host according to a well-defined baseline [SSS15]. The technologies used to apply application whitelists, including controlling which applications can be installed or executed on a host, are called *application control* [SSS15].
- Network-based IPS: See the knowledge base entry providing an introduction to

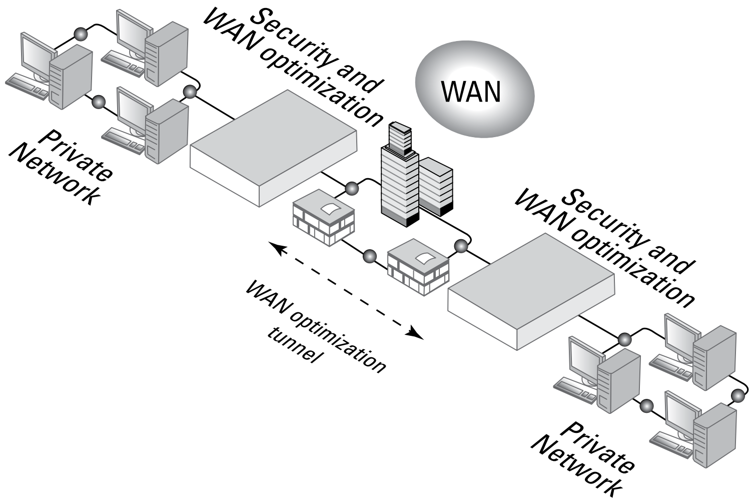


Figure 2: WAN optimisation can be achieved through UTM appliances located on both sides of a WAN, in front of both private organisational networks [Tit16, Figure 5-1].

intrusion detection, and in particular this write-up on different types of IPSs, including network-based IPS.

- Data loss prevention (DLP): There are two types of data loss [LK10]: 1️⃣ leakage, where unauthorised parties make away with data; 2️⃣ disappearance or damage, where data is lost to hardware/software damages or failures. DLP is an enterprise program targeted at preventing both types of data loss [LK10].

  Typical DLP mechanisms implemented by UTM include filtering by scanning inbound and outbound files [Tit16, p. 45]. A document can be fingerprinted by identifying text strings and patterns within the document, as well as the hash of the document. The fingerprints can be stored in a DLP database. Based on fingerprints in the database, a DLP-capable UTM appliance determines whether to allow, archive or block documents from being shared beyond the protected network.

- Sandboxing: A sandbox is a restricted, controlled execution environment that prevents potentially malicious software from accessing any system resources except those for which the software is authorised [CNS22]. Sandboxing is a mainstream dynamic application security testing ("dynamic analysis" for short) paradigm. It has become a common expectation that a UTM appliance tests an executable either in a local sandbox or a cloud-based sandbox [Tit16, p. 26].

For implementing UTM functions, the market leaders are resorting to application-specific integrated circuits (ASICs) to accelerate certain computation (e.g., cryptographic operations, packet processing). For example, in 2023, Fortinet unveiled their 7-nm ASIC called FortiSP5 [For23a], which they claim speeds up firewall performance by 17 times compared to leading standard central processing units (CPUs) at the time of release. For another example, Check Point uses NVIDIA's ASIC-based ConnectX SmartNIC in their Quantum Lightspeed line of UTM appliances [Sch22].

In the academic literature, the term "integrated protocol processing" has been coined [QYXL07] to refer to the combined processing of access control and protocol analysis to reduce the number of memory accesses and hence increase firewall performance. This term has not been picked up by the industry, and it is unclear whether the approach has been widely adopted by the industry.

1.1.3 [9 marks] Description of a commercial UTM product

Representative UTM products can be found on Gartner's 2022 magic quadrant for network firewalls [KHL22]; see Figure 3. We caution that Gartner has published a magic-quadrant report on UTM in 2018 but 1️⃣ the report is behind a paywall [KN18], and 2️⃣ UTM vendors like Check Point [Che23b] and Fortinet [For23b] cite [KHL22] for their UTM products.

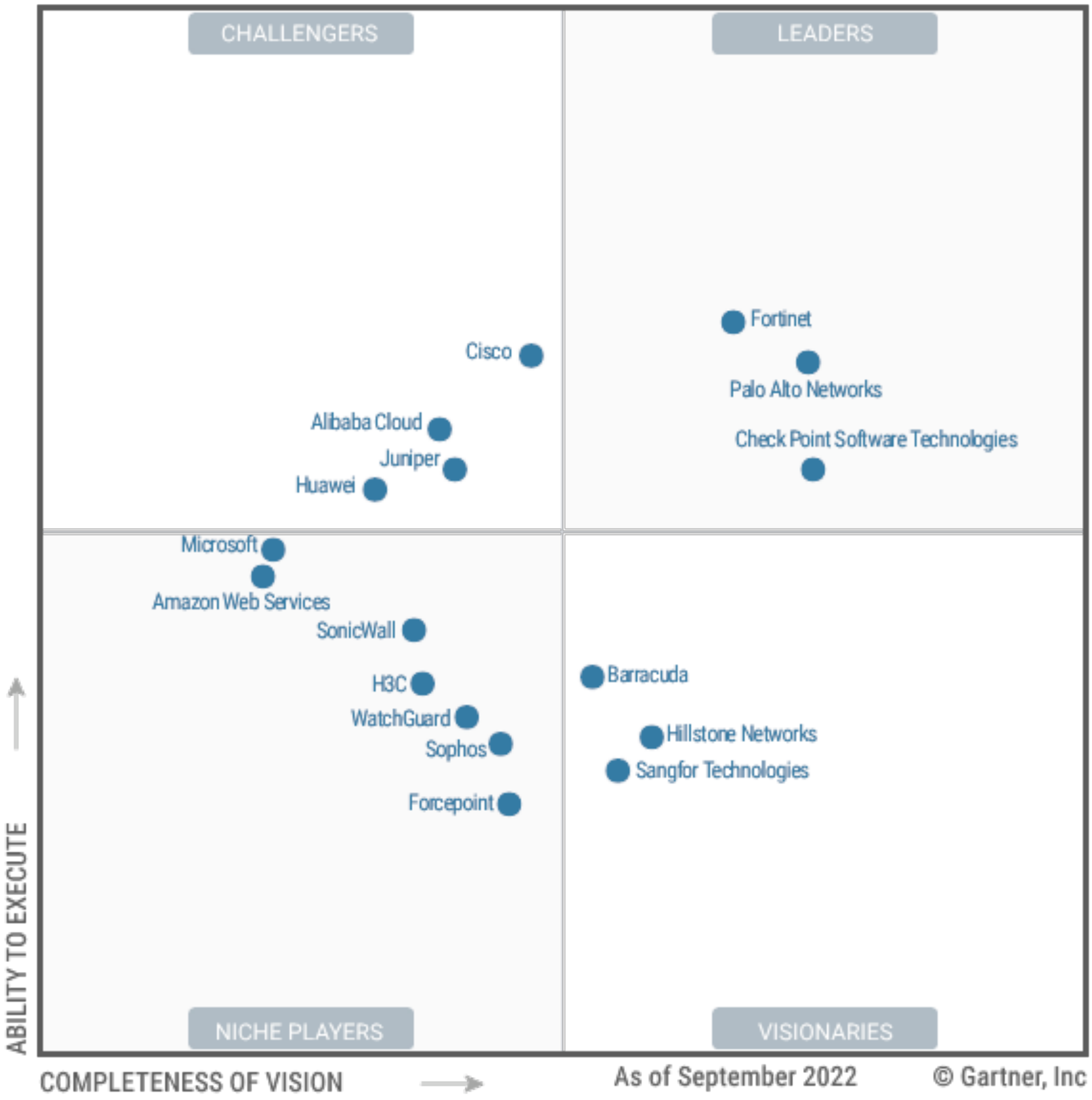


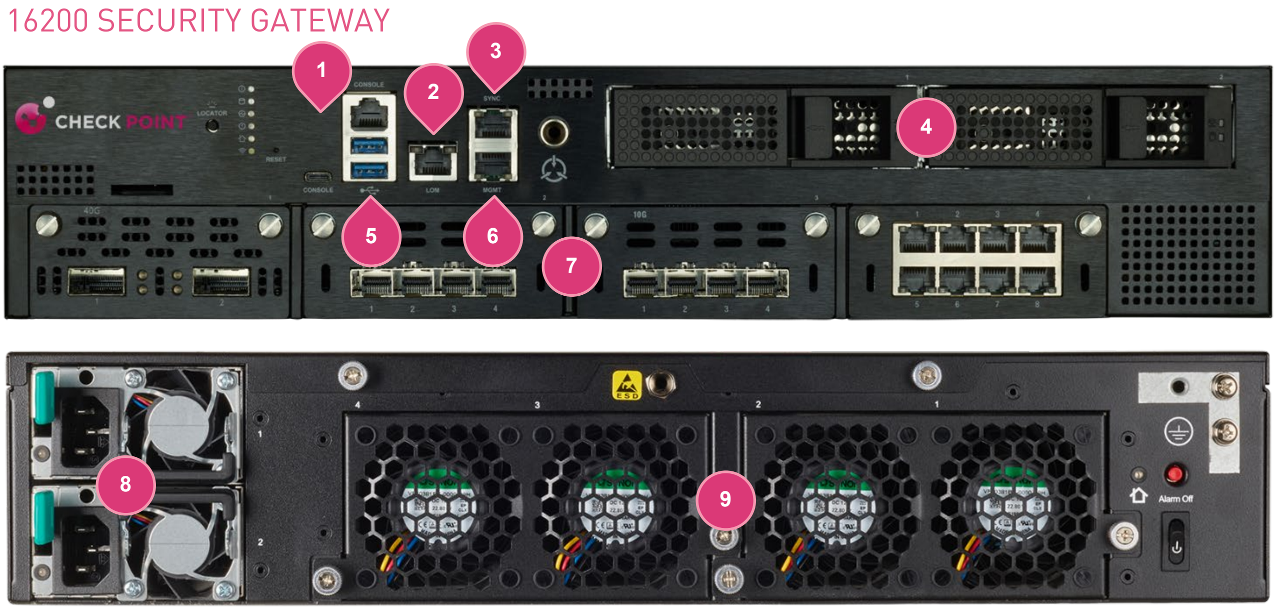
Figure 3: Gartner's 2022 magic quadrant for network firewalls [KHL22, Figure 1].

As shown in Figure 3, Fortinet, Palo Alto Networks and Check Point Software Technologies are among the market leaders. Although Fortinet pioneered UTM [Cam16, p. 171], a product of Check Point is chosen as an example of a commercial UTM product.

Check Point is marketing their NGFWs as UTM appliances [Che23b]. Check Point offers a range of NGFW appliances[1] for 1️⃣ small to large enterprises, 2️⃣ data centres and 3️⃣ rugged environments. In their Quantum range of products [Che22],

- Quantum Spark 1600, Quantum Spark 1800, Quantum 3600, Quantum 3800 are tailored to small enterprises;
- Quantum 6200, Quantum 6600 and Quantum 6900 are designated for SMBs;
- Quantum 7000 and Quantum 16200 are designated for large enterprises;
- Quantum 26000 and Quantum 28000 are high-end appliances for large enterprises.

The discussion here zooms in on the product Quantum 16200 [Che23a] pictured in Figure 4, which in its base configuration provides 10 Gigabit Ethernet ports, 48GB of random-access memory (RAM) and 480 GB of solid-state drive (SSD) storage. The security features of Quantum 16200 [Che23a] include:



1. RJ45 and USB Type-C console ports
2. Lights-out Management port
3. Sync 10/100/1000 Base-T port
4. 2x 480GB SSD RAID1
5. 2x USB 3.0 ports
6. Management 10/100/1000 Base-T port
7. Four network card expansion slots
8. 2x redundant hot-swap power supplies
9. 4x field replaceable fans

Figure 4: The ports of a Quantum 16200 NGFW [Che23a].

- deep-packet-inspecting firewall;
- IPsec-based VPN;
- SD-WAN optimisation;
- application control;
- network-based IPS;

[1] https://www.checkpoint.com/quantum/next-generation-firewall/

- anti-malware;
- Check Point SandBlast Threat Emulation, which attempts to detect threats (including zero-day exploits) in a sandbox;
- Check Point SandBlast Threat Extract, which attempts to remove detected threats from legitimate content (e.g., web pages, emails);
- anti-phishing measures;
- Internet of Things (IoT) security, which is a mix of the preceding defensive measures targeting IoT devices/traffic.

2 Tutorial 2

2.1 Task 1: SIEM

2.1.1 [6 marks] Challenge of spurious correlations

One of the challenges not discussed in the tutorial is *spurious correlations* [BMZ14, p. 40]. In a high-dimensional dataset, many variables can be correlated with events of interest even in the absence of causal relations. In fact, a recently published and highly cited paper [AQP+22] highlights "spurious correlations" as one of ten common pitfalls in applications of machine learning to cybersecurity.

An example of spurious correlations has been demonstrated using the Drebin malware detection scheme [ASH+14]. The uniform resource locator (URL) `play.google.com` turns out to be one of the five most discriminative features for benign apps. The correlation between the URL and the benign class is obviously spurious, and this spurious correlation has misled Drebin to learn to distinguish between "benign" and "malicious" using the origin of the app as a discriminator.

3 References

[ASH+14] D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, and K. Rieck, Drebin: Efficient and explainable detection of Android malware in your pocket, in *NDSS*, 2014. https://doi.org/10.14722/ndss.2014.23247.

[AQP+22] D. Arp, E. Quiring, F. Pendlebury, A. Warnecke, F. Pierazzi, C. Wressnegger, L. Cavallaro, and K. Rieck, Dos and don'ts of machine learning in computer security, in *31st USENIX Security Symposium (USENIX Security 22)*, USENIX Association, Boston, MA, August 2022, pp. 3971–3988. Available at https://www.usenix.org/conference/usenixsecurity22/presentation/arp.

[BDF+20] E. Barker, Q. Dang, S. Frankel, K. Scarfone, and P. Wouters, *Guide to IPsec VPNs*, Special Publication 800-77 Revision 1, NIST, June 2020. https://doi.org/10.6028/NIST.SP.800-77r1.

[Bar23] Barracuda Networks, Deep Packet Inspection (DPI), glossary, 2023, accessed 13 Jun 2023. Available at https://www.barracuda.com/support/glossary/deep-packet-inspection.

[BMZ14] S. Bhatt, P. K. Manadhata, and L. Zomlot, The operational role of security information and event management systems, *IEEE Security & Privacy* **12** no. 5 (2014), 35–41. https://doi.org/10.1109/MSP.2014.103.

[Cam16] T. Campbell, *Practical Information Security Management: A Complete Guide to Planning and Implementation*, Apress, 2016. https://doi.org/10.1007/978-1-4842-1685-9.

[Che22] Check Point, Quantum network security, Quantum security appliance brochure, 2022. Available at https://resources.checkpoint.com/next-generation-firewall/quantum-security-appliance-brochure.

[Che23a] Check Point, Quantum 16200 Security Gateway, datasheet, 2023. Available at https://www.checkpoint.com/downloads/products/16200-security-gateway-datasheet.pdf.

[Che23b] Check Point, What is Unified Threat Management (UTM)?, Cyber Hub, 2023, accessed 21 Feb 2023. Available at https://www.checkpoint.com/cyber-hub/network-security/what-is-unified-threat-management-utm/.

[CNS22] CNSSI, *Committee on National Security Systems (CNSS) Glossary*, Tech. report, March 2022. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

[For23a] Fortinet, Fortinet Unveils New ASIC to Accelerate the Convergence of Networking and Security Across Every Network Edge, press release, February 2023. Available at https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-unveils-new-asic-accelerate-networking-security-conver

[For23b] Fortinet, What Is Unified Threat Management (UTM)?, CyberGlossary, 2023, accessed 23 Feb 2023. Available at https://www.fortinet.com/resources/cyberglossary/unified-threat-management.

[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.

[Gar22] Gartner, Unified Threat Management (UTM), Information Technology Glossary, 2022, accessed 23 Dec 2022. Available at https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm.

[Hal23] D. Hall, NGFW vs UTM: Differences & Use Cases, CIO Insight, February 2023. Available at https://www.cioinsight.com/security/ngfw-vs-utm/.

[Hil15] A. Hills, For 2016, Should We Retire the “Next Generation Firewall”?, Gartner Information Technology Blog, December 2015. Available at https://blogs.gartner.com/adam-hils/for-2016-should-we-retire-the-term-next-generation-firewall/.

[KHL22] R. Kaur, A. Hils, and T. Lintemuth, Magic quadrant for network firewalls, Gartner, December 2022. Available at https://pages.checkpoint.com/gartner-magic-quadrant-for-network-firewall-2022.html.

[KN18] R. Kaur and C. Neiva, Gartner Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls), Gartner Research, 2018, paywalled. Available at https://www.gartner.com/en/documents/3890087.

[LK10] S. Liu and R. Kuhn, Data loss prevention, *IT Professional* **12** no. 2 (2010), 10–13. https://doi.org/10.1109/MITP.2010.52.

[MK17] O. Michel and E. Keller, SDN in wide-area networks: A survey, in *2017 Fourth International Conference on Software Defined Systems (SDS)*, 2017, pp. 37–42. https://doi.org/10.1109/SDS.2017.7939138.

[QYXL07] Y. Qi, B. Yang, B. Xu, and J. Li, Towards system-level optimization for high performance unified threat management, in *International Conference on Networking and Services (ICNS ’07)*, 2007. https://doi.org/10.1109/ICNS.2007.126.

[SH09] K. Scarfone and P. Hoffman, Guidelines on firewalls and firewall policy, NIST Special Publication 800-41 Revision 1, September 2009. Available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf.

[Sch22] R. Schafer, Check Point Software introduces the world’ s fastest firewall delivering 20 times better price performance to the world’ s most demanding datacenters, Security Blog by Check Point Research Team, January 2022. Available at https://blog.checkpoint.com/security/check-point-software-introduces-the-worlds-fastest-firewall-del

[SSS15] A. Sedgewick, M. Souppaya, and K. Scarfone, *Guide to Application Whitelisting*, NIST Special Publication 800-167, October 2015. https://doi.org/10.6028/NIST.SP.800-167.

[SLPR15] J. Sherry, C. Lan, R. A. Popa, and S. Ratnasamy, BlindBox: Deep packet inspection over encrypted traffic, *SIGCOMM ’15*, Association for Computing Machinery, 2015, p. 213 – 226. https://doi.org/10.1145/2785956.2787502.

[TSM+13] K. Tam, M. H. H. Salvador, K. McAlpine, R. Basile, B. Matsugu, and J. More, *UTM Security with Fortinet®: Mastering FortiOS*, Syngress, 2013. https://doi.org/10.1016/C2011-0-05893-3.

[Tit16] E. Tittel, *Unified Threat Management for Dummies*, 2nd Fortinet special ed., Wiley, 2016. Available at https://www.fortinet.com/content/dam/fortinet/assets/white-papers/FTNT_UTM_For_Dummies_r2.pdf.