Fortinet devices as a tool to enhance cybersecurity and meet the requirements of the NIS2 directive by leveraging their services

Michal Janovec[1], Jozef Papán[1], Jerguš Gbur[1], Jan Panuš[2],

Abstract— **The rapid proliferation of Internet of Things (IoT) devices has introduced significant cybersecurity challenges due to the heterogeneity and vulnerability of these systems. This paper investigates the integration of Fortinet's security solutions with IoT systems to enhance threat detection and mitigation capabilities. A hybrid architecture combining conventional networking components with Fortinet technologies, such as FortiGate and FortiAnalyzer, is proposed and implemented. The solution is validated through a series of practical scenarios that simulate real-world network attacks on IoT devices. Results demonstrate improved detection accuracy and response time, emphasizing the effectiveness of Fortinet's centralized logging and anomaly detection mechanisms. The study provides a scalable framework that can be adapted for various IoT environments, contributing to the development of more secure and resilient network infrastructures.**

I. Introduction

Firewalls are key tools for securing computer networks. Due to the continuous rise in cyberattacks, they have become indispensable to network protection for information systems. Nowadays, the market is dominated by next-generation devices, such as Next-Generation Firewalls (NGFWs).

NGFWs represent an advanced type capable of preventing attacks even at the application layer. They allow for in-depth analysis of users, devices, and applications in network traffic. These firewalls provide security functions such as application identification, malware detection, and protection against attacks. Thanks to these features, NGFWs are widely deployed in network infrastructures. [1]

FortiGate is a firewall solution by Fortinet and is classified as a Next-Generation Firewall. FortiGate devices combine security functions with artificial intelligence and machine learning to protect computer networks against cyber threats. These devices offer advanced services and features such as application identification, user and device identification, integrated threat protection (including antivirus, IPS, IDS), and support for encrypted traffic.

FortiGate devices leverage FortiGuard AI-Powered Security Services, enabling them to prevent cyberattacks and mitigate security risks through real-time protection. [2]

The NIS2 directive marks a significant advancement in cybersecurity across EU member states. Its goal is to unify regulations for critical information systems and infrastructures while addressing emerging cyber threats and the increasing reliance of companies on information technologies. NIS2 replaces the original NIS directive and introduces stricter requirements for companies under its scope.

The Directive aims to enhance cooperation between EU states and ensure greater cyberattack resilience.[2] This article explores the NIS2 directive and its impact on the cybersecurity of affected organizations, with particular attention given to implementing NIS2 requirements using various Fortinet devices and services.

II. CHANGES AND OBLIGATIONS INTRODUCED BY DIRECTIVE NIS 2

The NIS2 Directive expands on the original NIS Directive due to the rise of cyber threats and the increasing reliance of companies on information technology. The Directive has stricter requirements, covers a wider range of sectors and areas, and introduces new rules that are key to protecting digital infrastructure in all Member States of the European Union.

A. Key aspects of the NIS2 Directive

The NIS2 Directive is devoted to explaining the purpose and object of the Cybersecurity Directive. The measures aim to achieve a high common level of cybersecurity across the Union. The Directive defines the obligations of Member States - the obligation to establish competent authorities, cyber crisis management authorities, and single points of contact for cyber security and incident response units. It also focuses on cyber risk management and new reporting obligations for critical entities. It defines the rules on cybersecurity information sharing and the obligations of Member States regarding cybersecurity oversight.

B. Scope of the NIS2 Directive

As mentioned above, the Directive covers a wider range of sectors. The scope of the Directive covers all enterprises listed in Table 1 that are considered medium-sized enterprises or exceed the thresholds set for medium-sized enterprises. A medium-sized enterprise is defined as an enterprise with between 50 and 250 employees or an annual turnover of more than 10 million euros but less than 50 million euros. This Directive shall apply to entities identified as critical entities, entities providing domain name registration services, electronic communication services, and services essential for societal or economic activities or services with a potentially significant impact on security, regardless of their size. It does

[1] Authors are with Faculty of Management Science and Informatics, University of Zilina, Univerzitna 8215/1, 010 26 Zilina, Slovakia (corresponding author to provide phone: +421-907-964-016; e-mail: michal.janovec@fri.uniza.sk), (e-mail: jozef.papan@fri.uniza.sk)

[2] Author is with Faculty of Electrical Engineering and Informatics, University of Pardubice, Studentská 95, 532 10 Pardubice 2, Czech Republic (e-mail: jan.panus@upce.cz)

not apply to national security, public safety, defence or law enforcement entities.

C. Member State's responsibilities under the NIS2

Each EU Member State must adopt a national cybersecurity strategy, outlining objectives, resources, and policies to ensure a high level of cybersecurity. This includes risk assessment, incident response, coordination frameworks, and public awareness initiatives. [3]

Member States must enhance supply chain security, cyber resilience, and SME cybersecurity while supporting research institutions. They must notify the Commission of their strategy within three months and review it every five years. [3]

Each State must establish cybersecurity authorities, a single point of contact for cooperation, and a national cyber crisis management framework. [3]

Cybersecurity Incident Response Teams (CSIRTs) must handle incidents, ensure secure communications, and have redundant systems. They monitor threats, assist critical actors, and participate in the European CSIRT network. [3]

A designated CSIRT will act as a coordinator for vulnerability disclosure, assisting whistleblowers, managing vulnerabilities, and ensuring cross-border cooperation [3]

D. New measures and obligations for entities to meet the requirements of the NIS2

The Directive strengthens the responsibilities of key entities in cyber risk management. They must comply with NIS2 measures and are accountable for non-compliance. Member States must ensure governing bodies receive cybersecurity training, encouraging similar training for employees to recognize cyber risks.[3]

Key entities must protect networks and information systems, minimizing incident impact while following EU and international standards. Measures must cover risk analysis, incident handling, business continuity, supply chain security, system maintenance, vulnerability management, cybersecurity policies, encryption, access control, and secure communications. Corrective actions are required for non-compliance.[3]

Organizations must report significant incidents to the national CSIRT. Within 24 hours, they must provide an early warning, a detailed report within 72 hours and a final report within a month. Ongoing incidents require interim updates. [4]

Member States may require key entities to use certified ICT products to enhance security and standardize rules across the EU.[4], [5], [6]

E. Key differences between NIS and NIS2

The main difference concerns the scope of the application. NIS focuses on a limited number of critical infrastructure sectors: energy, transport, health, financial services and essential service providers (OES), whereas NIS 2 extends the scope to a wider range of sectors. [7]

Obligations for OES and Digital Service Providers (DSPs) were less specific, and many countries have implemented them differently. This has caused inconsistency across the EU. Responsibility for the supply chain was left primarily to the OESs themselves, without explicit regulation. Member States had more flexibility in transposing the Directive, leading to different interpretations and implementations. Enforcement of obligations and penalties was inconsistent and depended on national authorities. Incident reporting requirements were less well defined. Incident reporting requirements were less precisely defined.[8]

III. RELATED WORKS

The NIS2 Directive introduces stricter EU-wide cybersecurity rules, requiring Poland to update its legal framework. It broadens the range of regulated entities, enforces stronger risk management, and mandates timely incident reporting. Effective implementation demands coordinated efforts to address resource, supply chain, and enforcement challenges.

The Cybersecurity Resilience Act (CRA), aligned with NIS2, boosts IoT security through risk-based development, security-by-design, and mandatory vulnerability disclosures. Manufacturers must ensure continuous monitoring, though enforcing standards and securing supply chains remain key hurdles.

NIS2 also requires critical sectors to strengthen IT governance, enhance incident response, and align with tighter regulations. It increases accountability and pushes for improved cybersecurity policies and cross-border cooperation, despite integration and resource challenges.

Overall, NIS2 expands regulatory scope, improves risk management and cooperation, and sets a unified cybersecurity standard across the EU to address evolving threats.

IV. CONFIGURATION OF FORTINET DEVICES BY THE REQUIREMENTS OF THE NIS2

A. Principles of risk analysis and information systems security

This requirement aims to protect data and systems' confidentiality, integrity, and availability. Risk analysis begins by identifying potential threats—such as cyber-attacks, natural disasters, human error, or hardware failure—followed by assessing their likelihood and impact. Appropriate measures are then implemented to mitigate risks, and security systems are continuously monitored and audited.

FortiGate offers robust threat detection and prevention, defending against DDoS, malware, and unauthorized access using IPS, web filtering, VPN, and application control. FortiSIEM provides centralized threat and event monitoring, while FortiAnalyzer logs and analyzes events across systems. FortiSandbox detects zero-day threats by analyzing suspicious files and traffic in an isolated environment. [13], [14], [15]

B. Incident handling

Entities must implement systems for effective cyber incident management, covering detection, reporting, response, and recovery.

TABLE I.
CRITICAL AND IMPORTANT SECTORS BY NIS2

High critical sectors	**Other critical sectors**
Energy	Postal and courier services
Transport	Waste management
Banking	Manufacture and distribution of chemicals
Financial markets infrastructure	Food production, processing and distribution
Healthcare	Manufacturing
Drinking water	Digital service providers
Wastewater	Research
Digital infrastructure	
ICT service management	
Public transport	
Universe	

Preparation: Organizations need an incident response plan, trained staff, designated response teams, and monitoring tools. Fortinet's Security Awareness Training supports employee preparedness. [16]

Detection: Early threat detection is critical. FortiGate offers real-time monitoring and intrusion prevention against threats like DDoS and malware. FortiSIEM centralizes event data for real-time analysis.

Response: Rapid action minimizes impact. FortiSOAR automates responses with playbooks, while FortiNAC controls network access and blocks unauthorized devices. [17], [18], [19]

Reporting: Incidents must be reported within 24 hours, with detailed accounts of the timeline, impact, and corrective actions.

To ensure readiness and compliance, organizations should regularly test and audit their response plans through simulations and expert assessments.

C. Continuity of activities such as backup management, disaster recovery and crisis management

Organizations must ensure business continuity during disruptions like cyber-attacks or system failures through data backup, disaster recovery, and crisis management.

Backup Management: Critical data should be encrypted and backed up to secure, diverse locations. FortiManager enables centralized backup and configuration management for Fortinet devices. [20]

Disaster Recovery: Recovery plans should minimize downtime. FortiGate offers high availability and failover, FortiAnalyzer aids in issue detection, and FortiManager supports rapid multi-device recovery. [14], [19], [20]

Crisis Management: Companies need a crisis plan for team coordination, communication, and risk assessment. FortiSIEM provides centralized event monitoring, while FortiSOAR automates incident response to reduce reaction time. [13], [17]

D. Supply chain security, including security aspects relating to the relationship between individual entities and their direct suppliers or service providers

This requirement ensures organizations and their suppliers follow strict cybersecurity standards to protect sensitive data. ISO 27001 provides a framework for secure supplier relationships through risk management, access control, encryption, and auditing. Fortinet, ISO 27001-certified, meets these standards and offers a wide range of integrated security solutions through its Fortinet Security Fabric, enabling centralized control and visibility. [21]

E. Security in the acquisition, development and maintenance of network and information systems, including vulnerability resolution and vulnerability disclosure

Network equipment must be acquired directly from Fortinet or authorized distributors to ensure authenticity and support. Devices must be configured by administrators according to NIS2 standards, using Fortinet's official guidance to minimize vulnerabilities and ensure compliance.

FortiGate firewalls allow for the creation of detailed firewall policies to control device access and behavior within the network. These policies can include intrusion prevention (IPS/IDS), antivirus, application control, and web filtering to block unsafe content. Rules can be tailored for specific users, devices, or VLANs. FortiGate also supports encrypted VPNs for secure remote access and enables network segmentation into VLANs and security zones (e.g., DMZs, internal networks), allowing different security settings for each zone to protect sensitive systems.

FortiGuard enhances device security by providing frequent updates, vulnerability patches, and real-time threat intelligence. Its security advisories notify users of new vulnerabilities and patches, while FortiGate devices can share detected threats with FortiGuard to strengthen protection across the network. Fortinet's dedicated security team ensures timely responses to emerging threats. [19], [22]

F. Principles and procedures for assessing the effectiveness of cyber risk management measures

Assessing the effectiveness of security measures is crucial for an organization to check that the policies implemented are effective and protect the organization from cyber threats. Fortinet Security Fabric enables effective monitoring and improvement of the effectiveness of security measures, thus meeting the requirements of the NIS2 directive. It continuously monitors compliance with security policies across the infrastructure. It checks the configuration of FortiGate, VPN connections and their encryption, firewall policy settings

TABLE II.
FORTINET PRODUCTS

Product	Product feature
FortiEDR	It is used to control access to the network. It manages control and visibility over devices connected to the network.
FortiClient	Endpoint agent that provides visibility, device inventory control and VPN access.
FortiSwitch	Security access switch
FortiAP	WiFi access point
FortiExtender	A bridge between local Ethernet LAN and wireless LTE/5G WAN
FortiGate	Next-Generation Firewall
FortiToken	Device/service for two-factor authentication
FortiAuthenticator	A device for user authentication and authorization in a secure enterprise network.
FortiNAC	A network access control product that provides visibility and protection against unauthorized access.
FortiAnalyzer	Log management, analysis and reporting product.
FortiManager	Centralized control and automation of FortiGate, FortiSwitch and FortiAP device management.
FortiSIEM	An event correlation and risk management platform that integrates logs from different sources and provides real-time analytics.
FortiSOAR	A solution for orchestrating security operations and automating responses to security incidents.
FortiProxy	A proxy server that protects against Internet threats by detecting and blocking malicious activity.
FortiWeb	WAF to protect cloud and DevOps environments from advanced threats.
FortiDeceptor	Technology to detect and eliminate threats using honeypots and lures.
FortiSandbox	AI-powered sandbox to detect and respond to zero-day threats and malware.
FortiSASE	Cloud solutions combine network, security, and WAN technologies to provide secure access to the Internet and cloud applications.
FortiGuard Security Services	Global security services are provided by FortiGuard Labs using AI and machine learning to protect against advanced threats.
FortiCamera	Solution for secure video within the network.
FortiRecorder	A platform for recording and managing video content.

and the status of devices on the network. Security Fabric performs regular security compliance assessments. It ensures that all devices are up-to-date, checks for misconfigured policies, looks for vulnerabilities in the network, and provides recommendations to address any weaknesses found.[19]

Integrating FortiSIEM in the network will allow security measures to be checked against standards such as GDPR or NIS2 and alerts on violations. FortiAnalyzer provides detailed reports on the performance of security measures, identifies trends and provides statistical reports.

G. Principles and procedures for the use of cryptography or encryption. Human resources security, access control policies and asset management

FortiGate offers robust encryption and cryptographic options for secure data transmission. It supports encrypted protocols like HTTPS, SMTPS, IMAPS, POP3S, and LDAPS for secure communications and authentication. FortiGate also supports RADSEC (RADIUS over TLS) for secure authentication channeling. [19]

Remote access is secured through IPSec and SSL VPNs, using TLS 1.2/1.3 and SHA-256 or stronger hashing. Trusted CA-issued certificates are recommended to ensure secure, authenticated communication. [19]

FortiMail enhances email security with S/MIME and TLS encryption, meeting confidentiality requirements. Fortinet systems like FortiAnalyzer, FortiManager, and FortiGuard also use TLS by default. [23]

Access control is enforced through RBAC, limiting permissions by user roles. FortiGate logs user activity, with logs analyzable via FortiAnalyzer to detect suspicious behavior. [16]

FortiAuthenticator manages user access and enables MFA enforcement. FortiNAC authenticates all devices on the network, ensuring only compliant, authorized devices can connect. [18], [24]

H. Using multi-factor authentication to secure communication

A key NIS2 Directive measure is enforcing multi-factor authentication and secure communications. FortiGate supports two-factor authentication via FortiToken, which generates 6- or 8-digit one-time passwords as a second login layer. FortiToken is available as a mobile app or physical token, with encrypted keys stored in the cloud. Each token can only be linked to one FortiGate or FortiAuthenticator device. [19]

FortiGate also secures voice communication using SRTP, preventing eavesdropping and tampering. Additionally, FortiVoice offers encrypted call routing, voicemail, conferencing, and voice account management, ensuring secure, uninterrupted communication during cyber incidents—supporting NIS2 business continuity requirements. [19]

TABLE III.
VENDOR COMPARISON

Feature/Need	Fortinet (FortiGate)	Palo Alto Networks (PA-Series)	Cisco (Firepower)	Check Point (Quantum)
NIS2 Compliance Features	Integrated support via Fortinet Security Fabric	Strong compliance focus, Zero Trust architecture	Modular support via SecureX platform	Good support, complex licensing
AI/ML Integration	FortiGuard Labs real-time AI-based threat intelligence	Advanced inline ML and behavior analytics	Limited inline ML, reliant on Talos Intelligence Group	AI used in ThreatCloud, less automated than competitors
Incident Response	FortiSOAR automation, FortiSIEM event correlation	Cortex XSOAR orchestration, highly customizable	Firepower and SecureX ecosystem, less integrated	Infinity SOC and Smart-1 appliances
Ease of Use / Deployment	High integration and fast deployment	Powerful, but steep learning curve	Can be complex and unintuitive	User-friendly but can be overwhelming in depth
Centralized Management	FortiManager and Fabric Management Center	Panorama centralized system	Cisco Defense Orchestrator	SmartConsole management interface
Cost-Effectiveness	Very cost-effective, ideal for SMBs	High cost, especially for advanced tools	Expensive with complex licensing	High cost for full protection suite
Performance / Threat Detection	Dedicated ASICs, high performance, effective detection	Industry-leading prevention accuracy	Good detection, performance bottlenecks possible	Excellent detection, can struggle with SSL inspection
Remote Work and ZTNA	FortiClient, FortiAuthenticator, built-in ZTNA and VPN	Prisma Access, GlobalProtect for secure remote work	AnyConnect, Duo, and Umbrella integration	Harmony Connect and Quantum VPN

V. Comparison of Cybersecurity Solutions for NIS2 Compliance

As organizations across the European Union prepare to meet the stricter cybersecurity requirements of the NIS2 Directive, choosing the right security solutions is key. The following is a comparison of Frotinet's solutions against leading alternatives from Palo Alto Networks, Cisco and Check Point. The goal is to help decision-makers quickly understand the strengths and weaknesses of each solution in the context of compliance, threat detection and overall cybersecurity resilience. The comparison is illustrated in the table below. The Table III references the NIS2 Directive needs discussed earlier. This comparison is followed by a brief comparison of the pros and cons of each solution (Table IV).

TABLE IV.
PROS AND CONS SUMMARY

Vendor	Pros	Cons
Fortinet	ICost-effective, integrated portfolio, strong NIS2 alignment	Less customizable automation than Palo Alto
Palo Alto	Excellent threat detection, Zero Trust support, advanced ML	High cost, steeper learning curve
Cisco	Broad ecosystem, strong brand, good integrations	Complex licensing, UI inconsistencies
Check Point	Accurate threat prevention, mature management platform	Expensive, slower update agility

VI. Conclusion

With the growing number of IoT devices across various industries, the cybersecurity paradigm is undergoing a fundamental transformation. Traditional protection models are no longer sufficient to address the dynamic, heterogeneous, and inherently vulnerable nature of IoT ecosystems. This paper has demonstrated how Fortinet's architecture—particularly through the integration of FortiGate NGFW, FortiNAC, and the Fortinet Security Fabric—offers a comprehensive and scalable defense against modern threats in IoT environments. A key strength of this approach lies in its ability to implement network-level segmentation, context-aware automated decision-making, and centralized policy management, thereby ensuring a high degree of adaptability and response flexibility.

For organizations facing increasing regulatory pressure from directives such as NIS2 and the Cyber Resilience Act (CRA), such an integrated system represents not only a response to immediate security challenges but also a strategic investment in long-term resilience. A security architecture focused on prevention, visibility, and automated incident response is essential for maintaining the integrity, availability, and confidentiality of data in complex IoT ecosystems. From both scientific and practical perspectives, Fortinet can thus be regarded as one of the technological leaders in proactive protection of Internet of Things devices and infrastructures.

ACKNOWLEDGMENT

This research was funded by the Slovak Grant Agency VEGA project Fast Reroute, No. 1/0316/24.

References

[1] Z. Wang and H. Song, "Research on performance test method for the next generation firewall," 2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications, AEECA 2022, pp. 585–589, 2022, doi: 10.1109/AEECA55500.2022.9919085.

[2] C. C. Almagro, "NIS2 Impact on Electronic Communications Networks Providers," 2023 International Workshop on Fiber Optics on Access Networks, FOAN 2023, p. 16, 2023, doi: 10.1109/FOAN59927.2023.10328082.

[3] A. J. Jara, I. C. Martinez, and J. S. Sanchez, “CyberSecurity Resilience Act (CRA) in Practice for IoT Devices: Getting Ready for the NIS2,” 2024 IEEE Smart Cities Futures Summit, SCFC 2024, pp. 56–60, 2024, doi: 10.1109/SCFC62024.2024.10698057.

[4] “Directive - 2022/2555 - EN - EUR-Lex.” Accessed: Feb. 25, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[5] P. Wanecki, R. Jasek, and I. Drofova, “The Contribution of the European NIS2 Directive to the Design of the Cyber Security Model,” International Conference on Information and Digital Technologies 2023, IDT 2023, pp. 149–154, 2023, doi: 10.1109/IDT59031.2023.10194454.

[6] “EUR-Lex - 32003H0361 - EN - EUR-Lex.” Accessed: Feb. 25, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reco/2003/361/oj/eng

[7] T. Wallis and C. Johnson, “Implementing the NIS Directive, driving cybersecurity improvements for Essential Services,” 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020, Jun. 2020, doi: 10.1109/CYBERSA49311.2020.9139641.

[8] M. Shukla, S. D. Johnson, and P. Jones, “Does the NIS implementation strategy effectively address cyber security risks in the UK?,” 2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019, Jun. 2019, doi: 10.1109/CYBERSECPODS.2019.8884963./

[9] A. Besiekierska, “Legal Assessment of the National Cybersecurity System in Poland in the Light of the New Developments in the NIS2 Directive,” 2023 46th ICT and Electronics Convention, MIPRO 2023 - Proceedings, pp. 1474–1477, 2023, doi: 10.23919/MIPRO57284.2023.10159958.

[10] A. J. Jara, I. C. Martinez, and J. S. Sanchez, “CyberSecurity Resilience Act (CRA) in Practice for IoT Devices: Getting Ready for the NIS2,” 2024 IEEE Smart Cities Futures Summit, SCFC 2024, pp. 56–60, 2024, doi: 10.1109/SCFC62024.2024.10698057.

[11] M. Veigurs, T. Lasmanis, and A. Romanovs, “IT Governance in Critical Sectors: Towards the NIS2 Implementation,” ITMS - International Scientific Conference on Information Technology and Management Science of Riga Technical University, no. 2024, 2024, doi: 10.1109/ITMS64072.2024.10741938.

[12] P. Wanecki, R. Jasek, and I. Drofova, “The Contribution of the European NIS2 Directive to the Design of the Cyber Security Model,” International Conference on Information and Digital Technologies 2023, IDT 2023, pp. 149–154, 2023, doi: 10.1109/IDT59031.2023.10194454.

[13] F. Inc, “FortiSIEM® Unified Event Correlation and Risk Management for Modern Networks”.

[14] Fortinet and Inc, “FortiAnalyzerTM Security Fabric Network Analytics”.

[15] Fortinet and Inc, “FortiSandbox Datasheet”.

[16] “Security Awareness Training — Fortinet.” Accessed: Feb. 25, 2025. [Online]. Available: https://www.fortinet.com/training/security-awareness-training

[17] Fortinet and Inc, “FortiSOAR Data Sheet”.

[18] Fortinet and Inc, “FortiAnalyzerTM Security Fabric Network Analytics”.

[19] “Getting started — FortiGate / FortiOS 7.6.1 — Fortinet Document Library.” Accessed: Feb. 25, 2025. [Online]. Available: https://docs.fortinet.com/document/fortigate/7.6.1/administration-guide/954635/getting-started

[20] Fortinet and Inc, “FortiManager Data Sheet”.

[21] J. D. Christopher, “Enabling NIS2 Directive Compliance with Fortinet for Operational Technology Implementation Guide Enabling NIS2 Directive Compliance with Fortinet for Operational Technology Enabling NIS2 Directive Compliance with Fortinet for Operational Technology”, Accessed: Feb. 25, 2025. [Online]. Available: www.dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/

[22] “FortiGuard AI-Powered Security Services”.

[23] Fortinet and Inc, “FortiMailTM For Email Security”.

[24] F. Inc, “FortiAuthenticatorTM Centralized Identity and Access Management Solution”.