Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

Multi-Vendor Firewall Strategy: IT, OT, and Edge Networks

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract - The perennial belief that one firewall product is enough to safeguard all sections of a modern enterprise is not merely a fallacy that is based on budget constraint. It is an architectural disaster that has quantifiable effects. This paper has brought forward a domain specific model to comprehend why information technology (IT) networks, operational technology (OT) space, as well as internet-facing web edge infrastructure all need purpose-built, and often vendor-differentiated, firewall solutions. The article utilizes the Purdue Enterprise Reference Architecture, the principles of Zero Trust, the OWASP security standards, and the IEC 62443 compliance requirements and focuses on the specific threat landscapes, traffic characteristics, protocol constraints and availability requirements unique to each domain. It compares the categories of firewalls, such as next-generation firewalls (NGFWs), industrial security gateways, web application firewalls (WAFs), and Firewall-as-a-Service (FWaaS) against domain-specific selection criteria. The architectural arguments are based on real-world examples such as the Colonial Pipeline attack and Triton/TRISIS malware campaign and reported OWASP Top 10 exploitation patterns to base the architectural arguments on operational reality. Guidance on deployment sequencing, policy design, change management and continuous validation is given throughout. The article concludes that the choice of product is not the only factor that can lead to the creation of true security resilience or false confidence at high cost by enterprise firewall investments but rather architecture and disciplined management practice.

Keywords: Next-Generation Firewall, Operational Technology Security, Web Application Firewall, ICS/SCADA, Network Segmentation, Zero Trust Architecture, IEC 62443, SASE, Multi-Vendor Security Architecture, Industrial DMZ.

1. INTRODUCTION

1.1 The Question That Reveals the Gap

This is a question that comes out in almost every security discussion about enterprises. The most common response is in the following format "We have a firewall already. What difference would we have with another one. The inquiry is decent at face value and it is usually budget conscious and not careless. However, it represents a basic misconception as to what a firewall is and what the firewall domain it is meant to operate in and what threat it can actually cope with.

The modern organization does not have one network. It has multiple, and usually concurrent, operations, with various purposes, various assets, various risk tolerance, and varying regulatory requirements. An example of a large hospital is one that operates an IT network that serves electronic health records, administrative operations, and communication between staff members. It also operates an OT network that manages infusion pumps, ventilators, building access and HVAC systems. And it has a consumer-facing web platform producing patient portals, appointment booking, and billing interfaces. Both of these environments are threatened by various enemies with varying ways and effects that can be both financial

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

loss and data disclosure to physical damages and even business closure. It is not only inefficient to treat them as a unit security issue. It is a wrong strategic move.

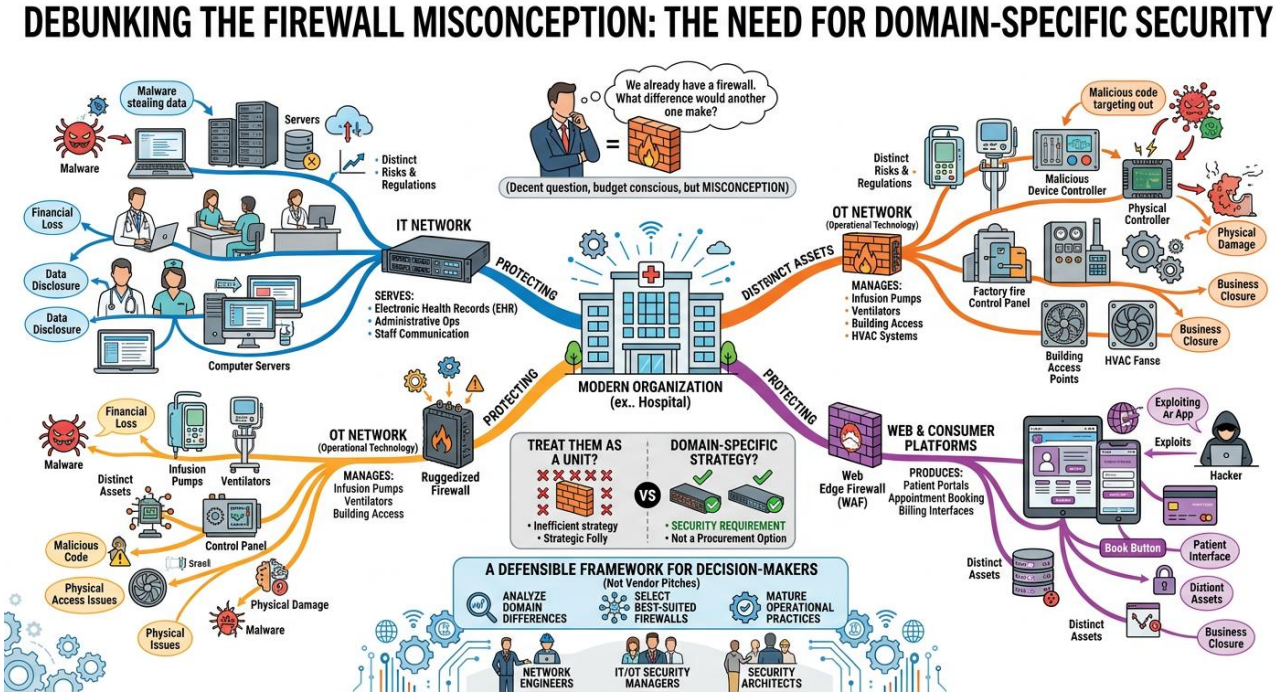

Fig -1: Debunking the Firewall Misconception

This paper has given an answer to the question of why using multi-vendor, domain-specific firewall strategies is a security requirement, and not a procurement option. It discusses the differences between IT, OT, and web edge environments and what types of firewall solutions work best in each area, how decision-making structures reflect architectural designs, why organizations need to determine and contrast solutions across areas and what mature operational practices are like in each setting. It is targeted at network engineers, IT/OT security managers, and security architects who require defensible and well-grounded frameworks to make actual decisions, not vendor pitches disguised as technical advice.

2. OBJECTIVES

The major aims of this article are the following. First, to define the clear taxonomy of three main network domains in modern enterprise settings, IT, OT, and web edge, and establish the peculiarities of the threats that can be identified on each. Second, to demonstrate, technically, why functional specialization in the categories of firewall products is an automatic result of domain specifications and not a taste towards complexity. Third, to offer domain sensitive vendor evaluation framework that can be used by practitioners to organize selection decisions with justifiable criteria. Fourth, to characterize deployment patterns, design principles of policies and change management disciplines that dictate whether properly selected firewalls generate actual security value or turn out to be costly underachievers. Fifth, to analyze the existing trends in firewall architecture, such as the adoption of Zero Trust, the development of FWaaS, and the adoption of IEC 62443 compliance requirements and to evaluate the impact of each on the future security strategy.

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

The article is intended to help practitioners to have the conceptual clarity and practical detail required to construct resilient, audit-Ready, multi-domain security architectures.

3. HISTORICAL CONTEXT HOW FIREWALL ARCHITECTURE REACHED THIS POINT

To explain the need of domain-specific firewalls in the current times, it is better to take a quick glance at how network security architecture has developed during the last 30 years. Early 1990s packet filters The packet filters of the first generation were firewalls: they looked at source IP, destination IP and port numbers and either allowed or denied access according to rules set by the administrator. They suited their era as the enterprise networks were relatively easy, the internet connectivity was not as widespread, and the threat spectrum was also constitute a comparatively narrow threat scope.

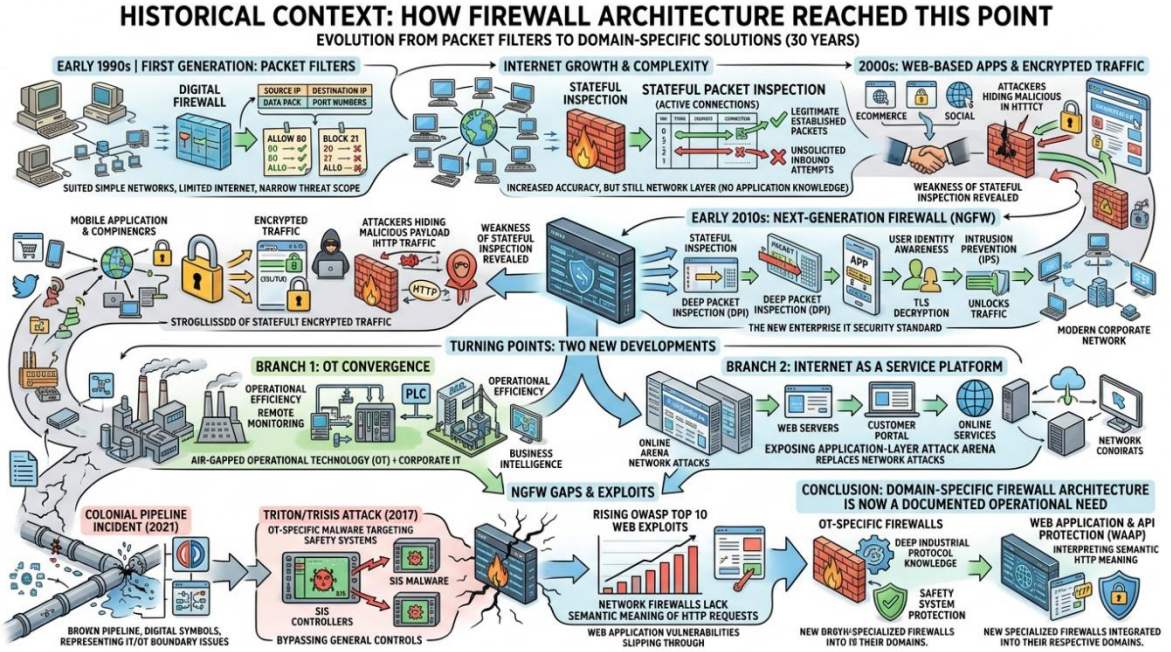

Fig -2: How Firewall Architecture reached this Point

With the growth of the internet and the complexity of the organizational networks, the stateful packet inspection became the norm. Stateful firewalls monitored the state of active connections and were able to differentiate between packets that were part of an established connection that were legitimate and unsolicited inbound packets that tried to complete a connection. This was a significant increase in accuracy but it all was at the network layer with no knowledge of application-layer behavior.

In the 2000s, the growth of web-based applications and the emergence of encrypted traffic had revealed the weakness of stateful inspection. The attackers started to inject malicious payloads into the HTTP traffic which stateful firewalls lacked a system to detect. The next-generation firewall was the next answer and it integrated stateful inspection together with deep packet inspection, application recognition, awareness of user identity, intrusion prevention, and later TLS decryption. As of the early 2010s, NGFWs were the new standard of enterprise IT security.

The same decade in which NGFW was adopted was however the same period in which two developments occurred that changed the security issue in essence. OT environments that were air-gapped or physically

isolated on corporate IT networks started to integrate with enterprise systems in order to be operationally efficient, provide remote monitoring and business intelligence. And the general internet turned out to be the main platform on which organizations were providing services to their customers which exposed a whole new arena of attack, which is exploitation of applications-layers instead of network-layer attack. The NGFW did not accommodate either of these environments, and deployment in either without modification or supplementation had left security gaps that were rapidly acquired by even more advanced adversaries to exploit.

The issue of the IT/OT boundary within the national level was represented by the Colonial Pipeline incident in 2021. The Triton/TRISIS attack of 2017 showed that OT-specific malware could be created to bypass the general controls of the network and directly attack the safety systems. And the fact that the number of OWASP Top 10 incidents of web-facing application exploits has increased annually validated that network firewalls, though possibly able to inspect the transport layer, do not have any insight into the semantic meaning of the HTTP requests. Such developments render the argument of domain-specific firewall architecture more than a theoretical preference but a documented operation need.

4. THREE NETWORKS, THREE FUNDAMENTALLY DIFFERENT PROBLEMS

4.1 The IT Network Dynamic Threats Against Familiar Infrastructure

The first environment that a security professional is exposed to is the IT network. It includes servers, workstations, laptops, identity systems, email services, databases and cloud-linked services. Traffic on this is mostly TCP/IP based on familiar application-layer protocols such as HTTP/S, DNS, SMTP, SMB, and RDP. IT security is directed by the CIA triad, which includes confidentiality, integrity, and availability, with the former two being mostly prioritized. In practice, this implies that IT systems will be able to endure scheduled maintenance periods and patching more than other environments can.

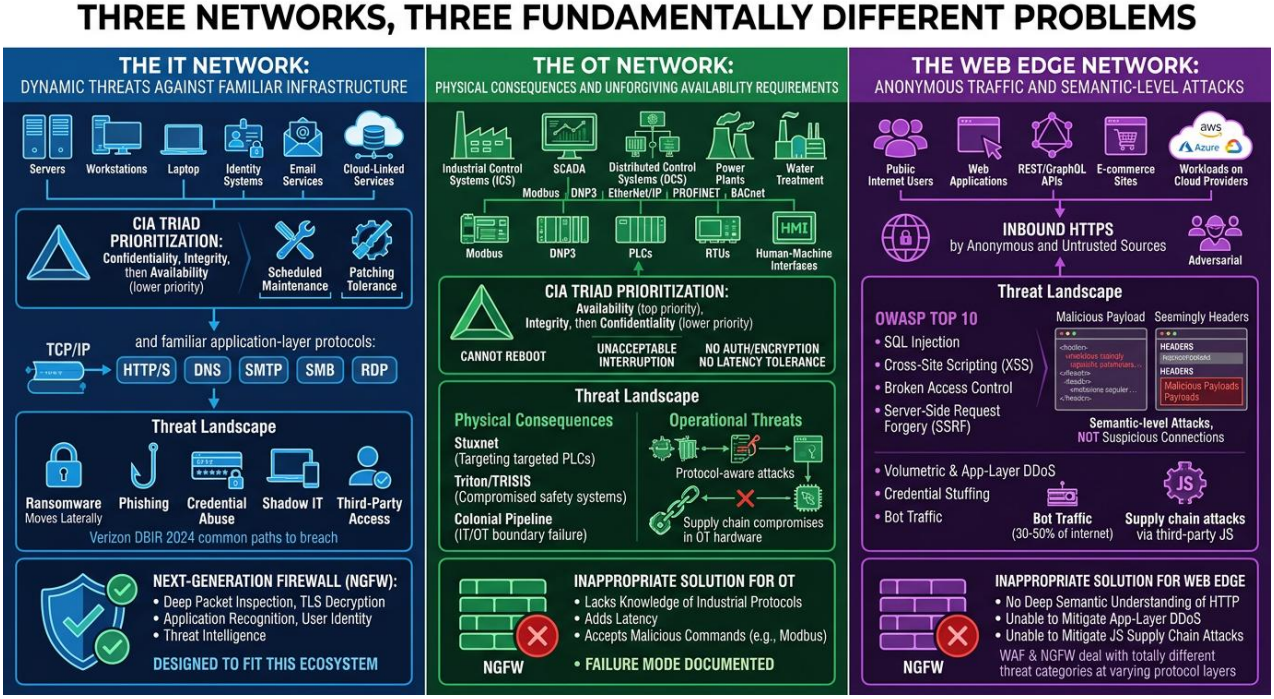

Fig -3: Three Networks, Three Fundamentally Different Problems

IT network threat is extensive, flexible, and documented. Ransomware is the most prevalent operational risk, which normally finds its way into the system via phishing emails, open and unprotected RDP portals, or hacked VPN logins and then moves laterally through the system to cause as much damage as possible before it detonates. The data breach investigations report 2024 by Verizon lists credential abuse, phishing, and use of public-facing applications as the three most common paths to breach in an enterprise setup, which has remained largely similar in each of the annual reports. The intellectual property, customer data, and credentials are targeted by nation-state and financially motivated actors. The insider threats, the spread of shadow IT, and the uncontrolled access points of third parties make the situation more complex.

The NGFW has been designed to fit this ecosystem. The fact that it can inspect all protocol layers, decrypt and inspect traffic encrypted with TLS, identify applications without particular attention to ports, associate sessions with user identities and use real-time threats intelligence make it the right tool in this task. It is also, exactly because it was created to fit in this environment, the inappropriate tool to the situations outlined below.

4.2 The OT Network Physical Consequences and Unforgiving Availability Requirements

Operational technology includes the hardware and computer programs which oversee and regulate the physical industrial processes. These are industrial control systems (ICS), SCADA platforms, distributed control systems (DCS), programmable logic controllers (PLCs), remote terminal units (RTUs), human-machine interfaces (HMIs) and the specialized protocols that link them: Modbus, DNP3, EtherNet/IP, PROFINET, IEC 61850, BACnet, and OPC-UA.

OT settings can be found in factories, power plants, water treatment plants, oil and gas companies, highway infrastructure and building automation. Security prioritization is the opposite of IT, availability, integrity, and then confidentiality. It is impossible to reboot a power generator in order to patch it. The interruption that would be caused by a typical IT network vulnerability scan would be unacceptable to a water treatment plant. More importantly, much of the OT devices are operating firmware that was developed prior to networked security being thought about at all. They lack authentication, no support of encryption and are not able to support the latency that could be created by a standard firewall.

The OT threat environment has shifted significantly to an operational threat. In 2010, Stuxnet proved that nation-state actors would develop malware that was highly targeted at PLCs. In 2017, Triton/TRISIS also compromised safety instrumented systems, which is a final barrier between an industrial process and the devastating physical damage (Lee, Assante, and Conway, 2017). The case of the Colonial Pipeline in 2021 demonstrated that IT ransomware, without necessarily attacking the OT systems, can cause a pipeline to shut down when the IT/OT boundary is not adequately defined . The modern threats encompass protocol-aware attacks releasing malformed or malicious commands via the Modbus or EtherNet/IP protocols, the compromises of the supply chain in OT hardware, and the persistent threats that IT/OT convergence pose to OT systems due to their exposure to IT-borne malware vectors.

A NGFW installed in an OT environment that lacks knowledge of industrial protocols is not a solution of any sort. It may add milliseconds of extra latency that will interfere with timing of control system operation, and it will accept malicious Modbus write commands since it is unable to decode the function codes contained in the protocol frame. This is not just a theoretical risk. It is a failure mode documented.

4.3 The Web Edge Network Anonymous Traffic and Semantic-Level Attacks

The web edge refers to the edge where an organization offers services to the common internet. This includes web applications, REST and GraphQL APIs, authentication portals, e-commerce sites and

workloads that are based on cloud-native and running on AWS, Azure, or Google Cloud. Web edge traffic is defined by its inbound HTTPS by anonymous and untrusted sources with often adversarial sources.

The OWASP Top 10 that lists the most severe vulnerabilities to application security, SQL injection, cross-site scripting, broken access control, cryptographic failures, server-side request forgery, and others characterizes the threat landscape here. These threats are not manifested in the form of suspicious network connections. They appear as syntactically sound HTTP requests with malicious payloads in the parameters, the headers, or the request bodies that appear to be just regular traffic at the network layer. None of the NGFWs examine the semantics of the HTTP at the depth that they are needed.

In addition to application-layer attacks, volumetric DDoS, application-layer DDoS attacks, credential stuffing, API abuse, and automated bot traffic are operations that will be constantly challenged. A study conducted by Imperva has shown that bot traffic represents between 30 and 50 percent of the total internet traffic according to industry with large percentage of that traffic being malicious or potentially harmful automated traffic. JavaScript libraries, payment processors, and chatbot integrations are third-party code that injects supply chain attack vectors at the application layer that network firewalls are unable to mitigate no matter how deeply they inspect it. The cognizant realization that a WAF and an NGFW is dealing with totally different category of threats at varying protocol layers is the conceptual antecedent to developing an efficient web edge security architecture.

5. THE CORE ARGUMENT WHY VENDOR DIFFERENTIATION ACROSS DOMAINS IS A SECURITY DECISION, NOT A PROCUREMENT PREFERENCE

The issue of why the various vendor firewall products is recommendable in the various domains should have a straight forward unambiguous response. This is because of functional specialization. No one vendor has designed one line of products that best fits the limitations in all three domains at the same time, as these limitations are in direct opposition to each other on the hardware and software design level.

Take into consideration the engineering conflict between OT and IT requirements. Stateful inspection of high bandwidth, dynamic TCP/IP traffic with TLS decryption, application identification and cloud-based threat intelligence are main features that are optimized with an IT NGFW. It operates on commercial grade server hardware under temperature controlled data centers. A OT industrial firewall has to provide sub-milliseconds deterministic latency, decode industrial protocol function codes, run on fanless hardened casing down to minus 40 degrees Celsius, mountable on the DIN-rail to control panel, and fail in a predictable and configurable manner that does not interfere with the physical process it is protecting. These are not sets of overlapping features. They are various product engineering fields that cater to the various operational realities. A gadget that is good in one of the requirements will inevitably be substandard in the other.

Dual-firewall DMZ is the specifically suggested diversity pattern of vendors that formalizes the concept of diversity as a premeditated security measure, and not a byproduct of buying the products of a variety of vendors as suggested by NIST, IEC 62443, and PCI-DSS. In the event that two firewall products of different vendors have the same network boundary in series, a zero-day vulnerability in the implementation of one vendor will not be able to be used to compromise both layers at the same time. A malicious attacker who discovers a vulnerability in TLS inspection engine by Vendor A is not able to use that vulnerability to exploit the inner perimeter firewall of Vendor B. Diversity in vendors is transformed into a structural element of defense-in-depth.

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

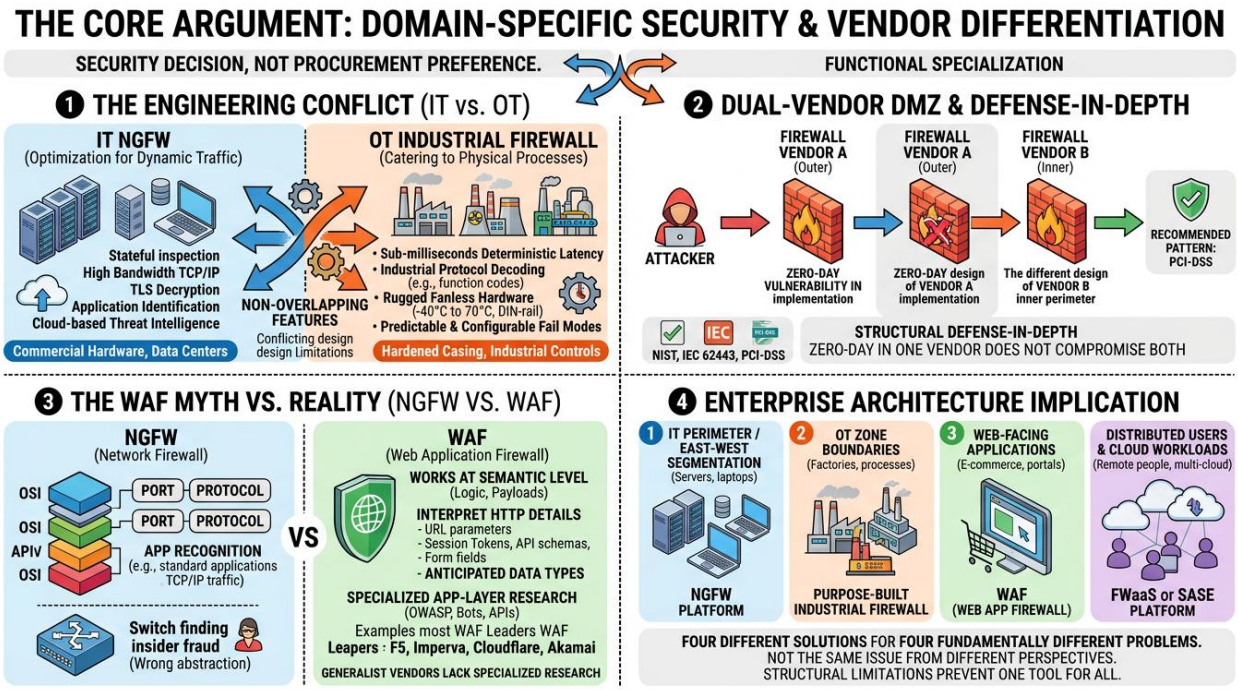

Fig -4: The Core Argument Domain Specific Security & Vendor Differentiation

This is supported by the case of WAF. The fact that a WAF is described as a better NGFW misrepresents the two tools. A WAF works at the semantics of HTTP applications, interpreting URL parameters, session tokens and API schemas, authentication state, form field names and anticipated data types, which no network firewall ever does by design. Requesting an NGFW to filter SQL injection of a web application is analogous to requesting a network switch to identify insider fraud. It is using the wrong layer of abstraction that is required by the problem. The market leaders of WAF vendors (F5, Imperva, Cloudflare and Akamai) have taken years to develop application-layer attack research, OWASP signatures, bot behavior analysis and API security which generalist NGFW vendors just have not matched at the same level.

The practical implication of the enterprise architects is that a multi-domain security approach will generally entail, at least, an NGFW platform to cover the IT perimeter and internal east-west segmentation, a purpose-built industrial firewall to cover the OT zone boundaries, a WAF to cover web-facing applications, and an FWaaS or SASE platform to cover distributed users and cloud workloads. These are not four products that are dealing with the same security issue but in various perspectives. They are four products that address a different issue that cannot be structurally dealt with by the rest.

6. CURRENT TRENDS SHAPING MULTI-DOMAIN FIREWALL STRATEGY

6.1 The Convergence of IT and OT Networks

Convergence of IT/OT has increased at a rapid pace in the last ten years, which is influenced by the necessity of efficiency in operations, remote monitoring, and the opportunities to integrate IoT sensors and enterprise analytics platforms. Where the OT networks used to be air-gapped or attached to the enterprise IT at best via physically controlled, one-way connections, most organizations have now added a

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

bidirectional connection between their OT and IT landscapes without deploying the resulting security architecture to control the risk that the connection presents.

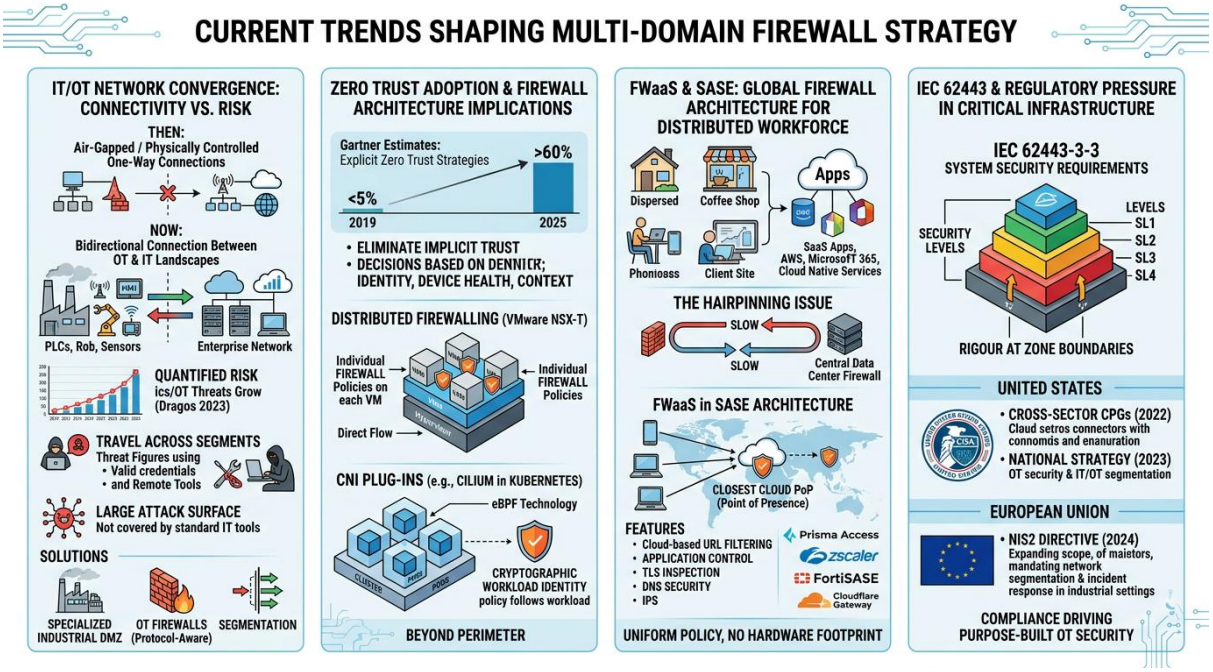

Fig -5: Current Trends Shaping Multi-Domain Firewall Strategy

The outcomes can be quantified. A Year in Review report published by Dragos in 2023 concluded that the number of ICS/OT-focused threat groups grew and the ability of the various groups to travel between the IT and OT network segments using valid credentials and legitimate remote access tools instead of dedicated OT malware had been demonstrated in the year. The implication is obvious: the organizations that have integrated their networks without deploying an appropriate industrial DMZ structure, specifically designed OT firewalls, and protocol-conscious segmentation have an considerably large attack surface that is not sufficiently covered by the standard IT security tools.

6.2 Zero Trust Adoption and Its Firewall Architecture Implications

Zero Trust is no longer a theory but an implementation priority in most of the large organizations. A study by Gartner had estimated that over 60 percent of businesses would have explicit Zero Trust strategies at different phases of deployment by 2025, as compared to less than 5 percent in 2019. The implications of the adoption of the Zero Trust on the firewall architecture are noteworthy. Zero Trust eliminates the unspoken faith that a perimeter security policy applied to traffic that is already on the network and demands that all access control decisions should be based on identity, device health posture and contextual indicators.

Architecturally, the Zero Trust concept is most tangibly applied in the form of micro-segmentation the establishment of small network units, occasionally at the level of each workload or even container, and explicit allow-list controls between these units. Distributed firewalling on platforms like VMware NSX-T are enforced on the hypervisor layer, meaning that every virtual machine has its own policy of enforced security, and there is no need to hairpin the traffic to a physical centralized appliance. CNI plugs like Cilium in Kubernetes are based on extended Berkeley Packet Filter (eBPF) technology to apply per- pod firewall policies that rely on cryptographic workload identity instead of trusting IP addresses, that is, policy is

applied to the workload no matter where it is scheduled within the cluster. Zero Trust does not overhaul the conventional NGFW capabilities on the perimeter. It goes beyond the network to further enforce security as well as threats which the perimeter controls by design never encounter.

6.3 FWaaS and SASE Firewall Architecture for the Distributed Workforce

The increased perimeter firewall practical utility has been altered fundamentally due to the remote work expansion that gained momentum during 2020 and became an inherent part of enterprise operation. The perimeter model is consistent when users are within a corporate structure and applications are operating in in-premises data centers. The presence of users working remotely at home, in coffee shops, and at client sites and using SaaS applications, which are hosted in either AWS or Microsoft 365, results in the fact that the notion of a meaningful network perimeter is mostly melted away.

Firewall-as-a-Service, which is part of SASE architecture, addresses this fact by shifting the processing of firewalls to cloud-native services executed out of the internationally dispersed Points of Presence. The users are linked to the closest PoP where traffic is inspected, irrespective of the physical location or the application destination. This will remove the hairpinning issue where remote user traffic is directed to a central data center firewall, then to the internet resources, which is a trend that was negatively impacting application performance and loading centralized infrastructure. Cloud-based URL filtering, application control, TLS inspection, DNS security, and IPS are provided by platforms such as Palo Alto Networks Prisma Access, Zscaler Internet Access, Fortinet FortiSASE, and Cloudflare Gateway and have no hardware footprint and uniform policy protection irrespective of the location of the user.

6.4 IEC 62443 and Regulatory Pressure in Critical Infrastructure

Regulation of OT cybersecurity has transitioned in most states where it is no longer voluntary but a requirement that can be enforced. The most extensive technical guidelines to industrial automation security are offered by IEC 62443, namely, the ISA/IEC 62443-3-3 system security requirements standard which defines four Security Levels (SL1, SL2, SL3, SL4) defining the rigour necessary at any zone boundary within an ICS environment. Operators of critical infrastructure, insurers of critical infrastructure and regulators of such infrastructure also have an increasing need to comply with IEC 62443.

In the United States, CISA Cross-Sector Cybersecurity Performance Goals (2022) and the National Cybersecurity Strategy (2023) also highlight the areas of priority of OT security and IT/OT segmentation. The NIS2 Directive that was adopted by the European Union in 2024 further extended the scope of the mandated cybersecurity requirements to a much broader group of operators of essential services in the member states with clear terms on network segmentation and incident response in the industrial setting. These trends in regulations are causing the move to purpose-built OT security architecture by organizations that would otherwise have postponed any investment.

7. FIREWALL CATEGORIES, CAPABILITIES, AND THEIR DOMAIN LOGIC

7.1 NGFWs The Right Tool for IT, the Wrong Default for Everything Else

The IT network security presently stands at the NGFW. NGFWs are protocol stack layer 3-7 stateful connection tracking and deep packet inspection, application identification, user identity knowledge with directory service interface, intrusion prevention, TLS decryption and inspection, and cloud-based threat intelligence. The shift to non-stateful firewalls to NGFWs was an arms race: as attackers shifted to

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

application-layer attacks and encrypted tunneling, network defenses needed to support the ability to inspect such layers.

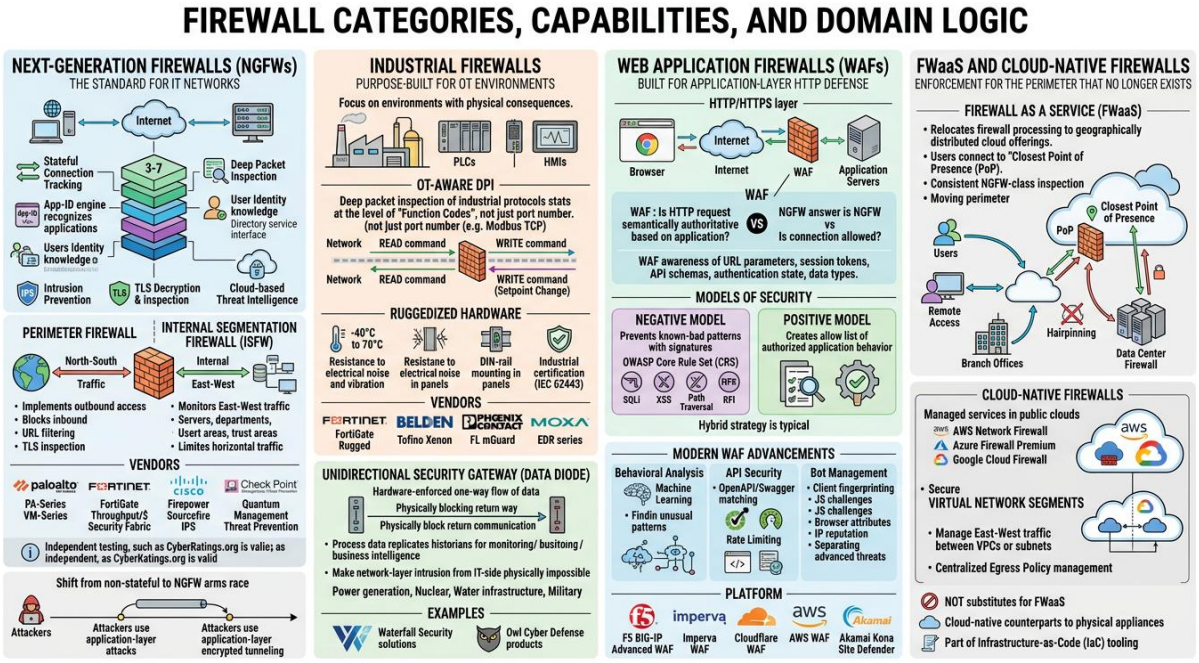

Fig -6: Firewall Categories, Capabilities and Domain Logic

The NGFWs have two architecturally different functions in IT environments. The perimeter firewall manages north south traffic between the internal network and the internet or WAN implementing outbound access policy, blocking unsolicited connections (inbound), ending and examining TLS, and implementing URL filtering. The internal segmentation firewall (ISFW) monitors east-west traffic between the internal areas and limits the horizontal traffic between server levels, departments and trust areas. The same physical platform can fulfill these roles in smaller setups but in large setups with data centres that are used to support high throughput the same hardware might be needed to support east-west traffic as well as north-south traffic which might be as large as east-west traffic.

Dominating NGFW systems incorporate different philosophies of engineering. Application identification using App-ID engine in PAN-OS is commonly considered the standard of application identification when using Palo Alto Networks PA-Series and VM-Series. Fortinet FortiGate is also the leader in throughput per dollar and the most integrated single vendor security architecture with the Security Fabric architecture. Cisco Firepower is a combination of Cisco and networking stack into Sourcefire IPS. Check Point Quantum can boast of maturity in management interface and accuracy in threat prevention. The various trade-offs are performance, application identification coverage and IPS signature update frequency TLS 1.3 inspection performance in each vendor. These trade-offs are practically important and the data set of independent testing given by CyberRatings.org can give more valid comparative results than the datasheet published by the vendor.

7.2 Industrial Firewalls Purpose-Built for Environments Where Failure Has Physical Consequences

The industrial firewall is due to the fact that the normal NGFWs are unable to satisfy the OT needs and the deployment of an NGFW in an OT environment without the knowledge of industrial protocols has already led to reported operational incidents. OT-aware deep packet inspection to the frames of industrial protocols at the level of the functions-code instead of only recognizing traffic as a Modbus TCP one by port number is the minimum capability of any firewall in ICS environment. An operator issue to a PLC that may change a safety-critical setpoint is exactly like a read command at the network layer. They are only differentiated by the level of inspection that is used, which is the function code level.

Physical limitations are also inconclusive. The industrial firewalls should have a temperature range of between minus 40 degrees to 70 degrees Celsius, should be able to withstand electrical noise and vibration, have the option of being mounted in DIN-rail in industrial control panels and have a low power consumption. The FortiGate Rugged series of Fortinet, the Tofino Xenon series by Belden, the FL mGuard series by Phoenix contact, and the EDR series by Moxa are built on exactly these limitations and have industrial certification. Both of them facilitate the adherence to the IEC 62443.

Also a separate and more assured category of OT protection is the unidirectional security gateway, or data diode. Waterfall Security solutions and Owl Cyber Defense products rely on a one-way flow of data which is enforced at the hardware level, which physically blocks any ability of return communication. This enables process data to be passed on to business intelligence systems through the OT networks to replicate historians and monitor operations and make a network-layer intrusion by the IT side physically impossible. Regulators are increasingly requiring the use of data diodes in the generation of power, in nuclear applications, water infrastructure, and military applications.

7.3 WAFs The Only Tool Built for Application-Layer HTTP Defense

A WAF is fully application layer (HTTP/HTTPS) and answers yet another security question altogether as compared to a network firewall. In a place where an NGFW requests as to whether a network connection is allowed, a WAF requests as to whether a particular HTTP request is semantically authoritative based on the application to which it is directed. A WAF is aware of URL parameters, session tokens, API request schemas, authentication state, and anticipated parameter data types and can make no such parallel to NGFW architecture.

WAFs also work on the negative and positive security models. The negative model prevents known-bad patterns with the help of signatures, the OWASP Core Rule Set (CRS) being the most commonly deployed is the signatures of SQL injection payloads, XSS vectors, path traversal sequences, and remote file inclusion patterns. The positive model creates a list of authorized application behavior and blocks all other possible behavior. The majority of systems of production implement a hybrid strategy. The positive-model WAFs are pure, thus produce considerable rates of false-positive at the initial stages of learning, and at the cost of extensive application-specific knowledge to set up.

The modern WAFs have developed significantly over and above the static signature matching. The behavioral analysis is done using machine-learning, which finds unusual request patterns when there is no particular signature. The API security features match requests with the Open API or Swagger schemas and impose rate limiting on each endpoint. The Bot management operates based on fingerprinting client behaviour on JavaScript challenges, analysis of browser attributes, and IP reputation scoring so that legitimate users can be distinguished as against advanced automated threats. Such platforms are F5 BIG-IP Advanced WAF, Imperva WAF, Cloudflare WAF, AWS WAF, and Akamai Kona Site Defender that represent various strengths of deployment models and geographic performance features.

7.4 FWaaS and Cloud-Native Firewalls Enforcement for the Perimeter That No Longer Exists

FWaaS solutions relocate the firewall processing to cloud-native offerings provided by infrastructure that is geographically distributed. Users are linked to the closest Point of Presence and given a consistent inspection of NGFW-class irrespective of location, virtually creating a moving perimeter that follows users instead of standing until they come back to a physical office. The hairpinning issue that had bedeviled the traditional remote access designs wherein all user traffic had to be directed back through a central data center firewall prior to reaching internet resources, is avoided through design. The FWaaS is different from cloud-native firewalls in public cloud providers such as AWS Network Firewall, Azure Firewall Premium, and Google Cloud Firewall. They are managed services which secure the virtual network segments within particular cloud setups and which deal with east-west traffic among the VPCs or subnets and centralized handling of egress policy. They are not supposed to be substitutes of FWaaS. They are cloud-native counterparts to physical appliances, which are managed by cloud-native policy frameworks and part of infrastructure-as-code tooling.

8. ARCHITECTURE AND PLACEMENT GETTING THE STRUCTURE RIGHT BEFORE SELECTING PRODUCTS

8.1 North-South and East-West Two Traffic Problems That Demand Separate Controls

Directionality in traffic dictates the location and actions of firewalls that should be installed. Internet to organizational infrastructure, internal users to the internet, or inter-sites, North-south traffic crosses a perimeter boundary. This has been the solution of perimeter firewalls over decades. East-west traffic remains in the same environment a web server is talking to an application server, a workstation to a domain controller, microservices to one another in a Kubernetes cluster.

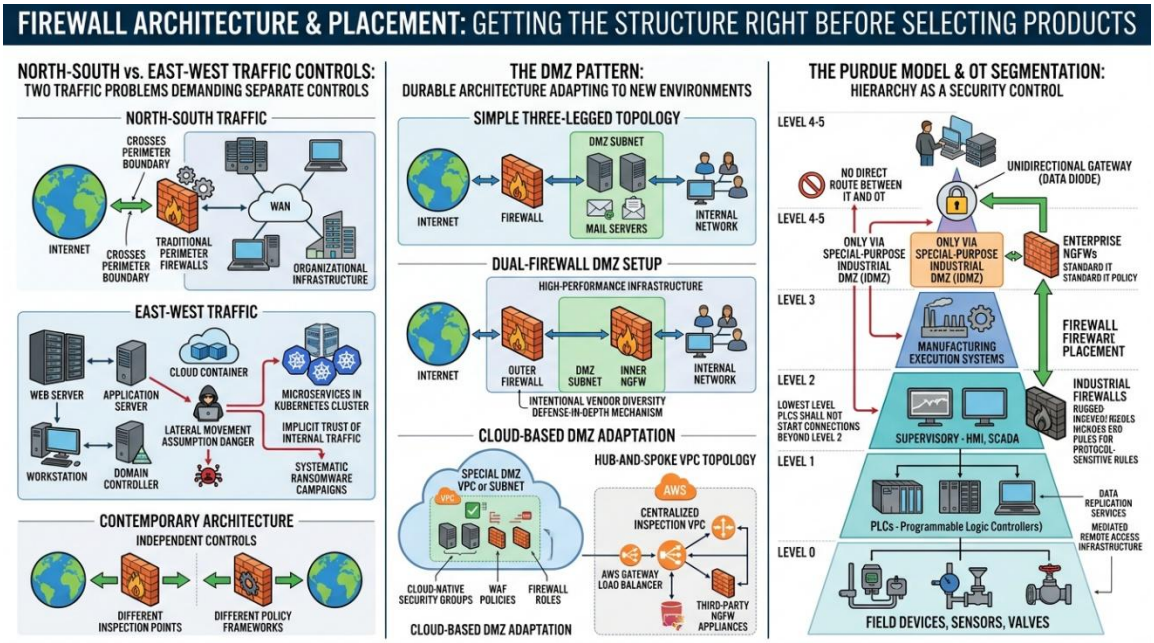

Fig -7: Firewall Architecture & Placement

The commercial history of the internet of most of the time saw the east-west traffic being largely uncontrolled due to the implicit trust of the internal traffic. Ransomware campaigns went through with the

disastrous effects of this assumption in a systematic way. Lateral movement through east-west connectivity will enable an attacker to find high-value targets, privileged accounts and backup systems within the entire network once the attacker has compromised a single endpoint or credential, even though east-west connectivity is not restricted. The contemporary architecture needs to have an independent control of the both directions of traffic with different points of inspection as well as different policy frameworks.

8.2 The DMZ Pattern Durable Architecture Adapting to New Environments

The DMZ is among the most significant trends of network security architecture even now, many decades to date. Its central point, that the resources that are exposed to untrusted networks should be eventually compromised and thus should be not connected to any trusted internal infrastructure, is operationally sound today as it was initially formalized. The simple three-legged topology (internet, DMZ, and internal interfaces on a single firewall) is extended to a dual-firewall DMZ in controlled and high-performance infrastructure setup where an outer firewall is used to deal with internet to DMZ traffic and an inner NGFW is used to deal with DMZ to internal access. The intentional vendor diversity of this pattern is a defensive in-depth mechanism, and not a procurement coincidence. In cloud-based settings, the DMZ would be represented by a special DMZ VPC or subnet which would have cloud-native security groups, WAF policies, and firewall rules that follow the same isolation principles. A hub-and-spoke VPC topology with a centralized inspection VPC with AWS Gateway load balancer is a common AWS environment that is used to enable the addition of third-party NGFW appliances in a transparent manner.

8.3 The Purdue Model and OT Segmentation Hierarchy as a Security Control

In the Purdue Enterprise Reference Architecture, the basic segmentation model of ICS environment is offered. It has a hierarchical structure of Level 0 field devices to Level 1 control, Level 2 supervisory, Level 3 manufacturing, and Level 4 and 5 enterprise business networks with strict levels of control on the inter-level communication. The lowest level of PLC should not even start any connections beyond Level 2. Level 3 systems must only connect to Level 4 enterprise systems via a special purpose Industrial DMZ (IDMZ), containing data replication services, historian mirrors and mediated remote access infrastructure. There should not be a direct route between IT and OT. The industrial firewalls are at Level 2/Level 3 boundary where protocol-sensitive rules are imposed to control the SCADA to control communication. The IDMZ and Level 4 have an enterprise NGFW that applies standard IT policy on this side of the buffer zone that faces the IT. Once in deployment, a unidirectional gateway at the IDMZ-to-Level-4 boundary renders the IT-to-OT intrusion physically impossible, which has the greatest available assurance of isolation.

9. CHALLENGES IN MULTI-DOMAIN FIREWALL DEPLOYMENT

The case of strategic domain-specific and multi-vendor firewall architecture is quite obvious, yet there are indeed real challenges in the implementation that cannot be neglected and tackled by practitioners. The most common barrier is organization resistance. The pressure to insourcing security teams is to simplify by cutting down on the number of vendors, and the rationale of having a firewall with Vendor X, and using it everywhere, is a political challenge to contradict without a clear technical argument as to why it is inadequate. The solution to this dilemma is to convert the functional specialization argument into the language of operational risks which can be assessed by business and finance executives.

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

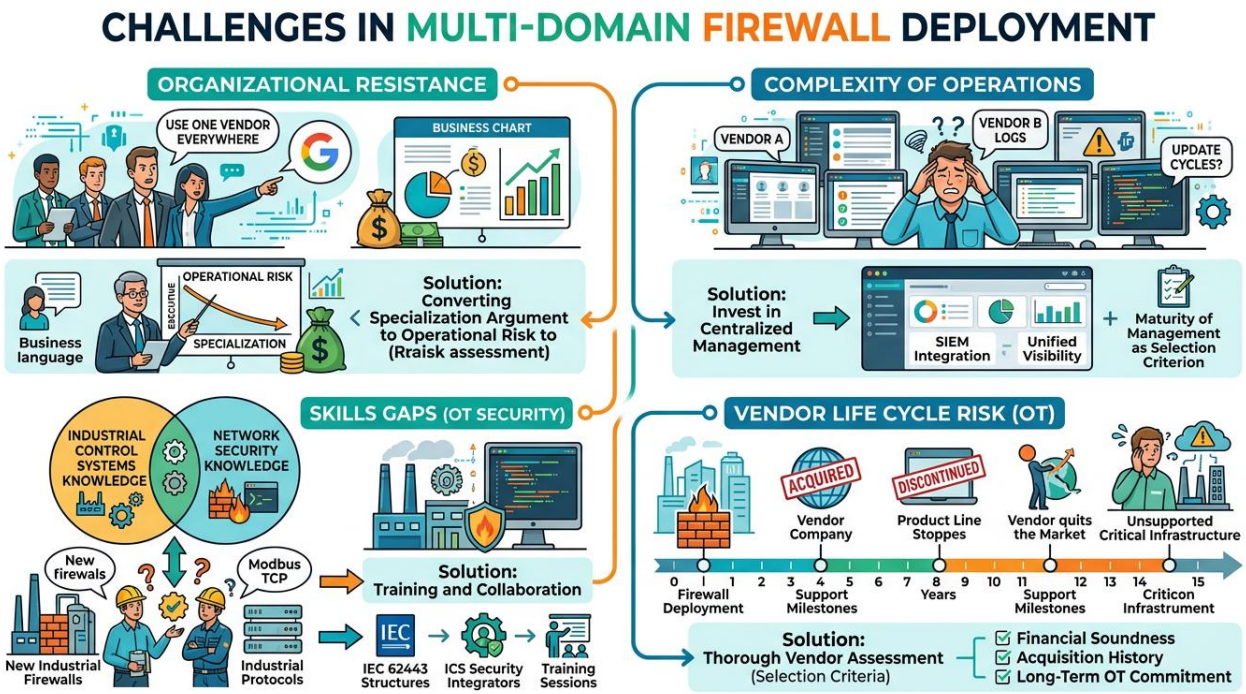

Fig -8: Challenges in Multi-Domain Firewall Deployment

The complexity of operations is an acceptable issue. Operating policies that consist of multiple vendors whose management interfaces, logging formats, update cycles, etc. differ leads to an operational overhead that the security team is under-resourced to handle. The mitigation is not to find the right tool to fit the specific domain but to invest in centralized management where feasible, such as SIEM integration to aggregate the logs, to consider the maturity of management as an explicit selection criterion of each product category.

The existence of skills gaps is a chronic problem, especially in the field of OT security, where the field of industrial control systems knowledge has a relatively narrow overlap with the field of network security knowledge. Companies that implement industrial firewalls initially do not have internal resources equipped with the knowledge of the OT protocols and experience in the administration of firewalls. Collaboration with ICS-specific security integrators and investment in training in opposition to IEC 62443 structures is the right reaction.

The vendor life cycle risk in OT environments is worth being mentioned explicitly. OT firewall implementations can be supported up to ten to fifteen years without a replacement of hardware. An acquired niche industrial firewall vendor who stops selling its OT product line or quits the market can leave critical infrastructure operators without support of deeply embedded equipment, which is a part of operational processes. Assessment of financial soundness of vendors, history of acquisitions and long term OT commitment is hence an important selection criterion in this field.

10. SOLUTIONS A FRAMEWORK FOR PRACTICAL IMPLEMENTATION

10.1 Baseline Before You Deploy

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

The worst error ever made in multi-domain firewall implementation is placing a device between the traffic that it will control and that traffic has not been sensibly understood and documented. This would imply in OT settings, passive baselining of the network with tools like Nozomi Networks Guardian or Claroty Platform, prior to installing any type of firewall in the traffic stream. These tools conduct non-invasive traffic monitoring that traces all the devices, all the flows of communications and all the protocols applied on the OT environment. It is based on this that firewall rules should be written. Rules based on legitimately observed traffic are much more precise, and much less likely to introduce operational disruptions on enforcement initiation, than memory-based or partial network diagram-based rules.

This applies to the same case with IT micro-segmentation projects. Organizations must apply network visibility tools to provide east-west communication paths across application tiers and server groups prior to internal segmentation rules implementation. Undocumented but business-critical application dependencies like an ERP system unexpectedly calling a legacy authentication service will cause application functionality to fail unless the policy of segmentation includes them.

10.2 Policy Design Precision Is the Standard, Not an Aspiration

Security strategy is put into operation where firewall policy design is concerned. The first principle is least-privilege access any rule will only allow the minimum traffic required to document approved business operations. The specifications that must be given by rules include source, destination, port/protocol and application identity as far as possible. The use of any as a service or destination specification must have express business rationale and be signed off. Organizations go uncontrolled risk silently through years of gradual change by permissive rules.

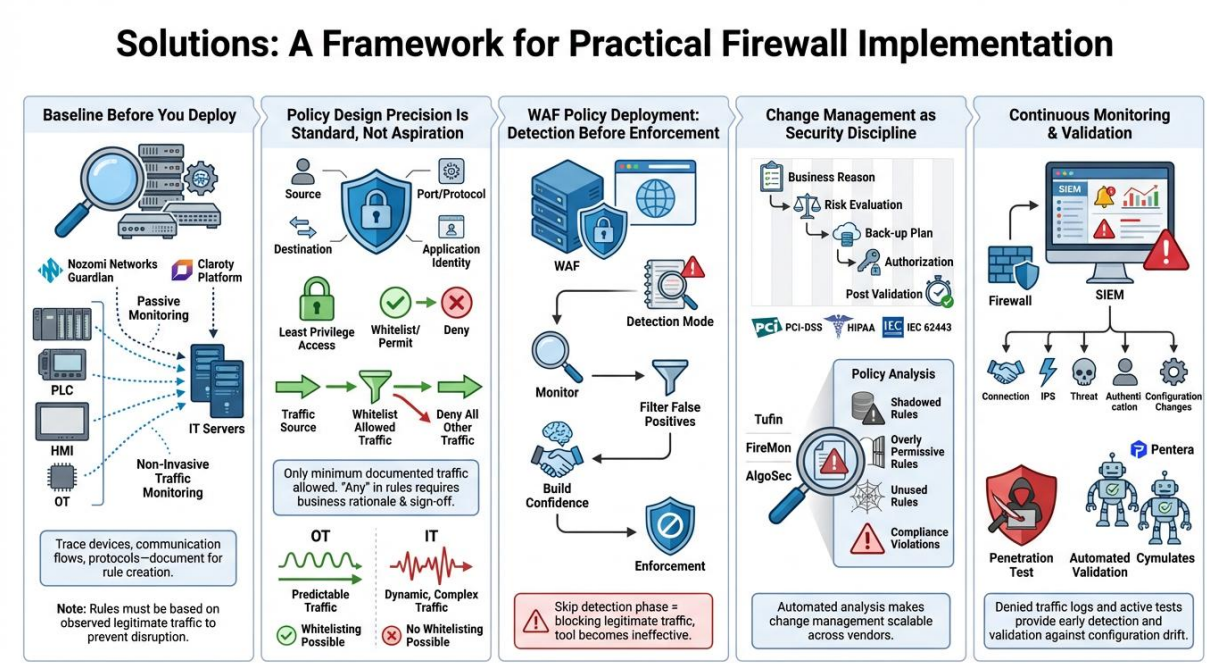

Fig -9: Solutions A Framework for Practical Firewall Implementation

The policy of OT firewall must be based on positive-security whitelisting. The patterns of OT communication are extremely predictable and regular as soon as baselines are identified, which is why the policy of

whitelist is possible when in the dynamic IT environment it is not. All the traffic that does not correspond to a particular permit rule is rejected. Such a model gets rid of the arms race of keeping blacklists and is facing the ever-evolving attackers.

WAF policy deployment is to be started in detection mode and then it can be enforced. The detection phase enables the security teams to monitor what would have been blocked during production traffic, filter out false positives and establish organizational confidence before traffic-affecting enforcement takes place. The most frequent reason why WAF deployments become out of commission by application owners because they are blocked out legitimate traffic is the fact that this step is skipped and organizations are left with a security tool that is a mere piece of paper.

10.3 Change Management as a Security Discipline

Firewall change management isolates security programs which hold significance of control over time as opposed to those which accrue undocumented risk. Each change in rule must pass through a procedure that involves business reason, risk evaluation, back-up plan, implementation authorization and post change validation test. The compliance finding is the unapproved changes, which is stated in the PCI-DSS, HIPAA, IEC 62443, and practically in all other large-scale regulations. Tufin Orchestration Suite, FireMon, and AlgoSec are among the tools that are used to automate policy analysis to find shadowed rules, overly permissive rules, unused rules, and compliance violations which make change management scalable in even complex multi-vendor environments.

10.4 Continuous Monitoring and Validation

The lack of actionable logs and alerts produced by a firewall gives false security. Events related to connection, IPS, threat, authentication and configuration change are supposed to be recorded in a centralized SIEM in real time. Denied traffic logs can also be useful in detecting threats: a burst in the number of denied connection attempts made by a particular internal host is a good early warning of malware that is performing reconnaissance of lateral movement. Active validation should be done as opposed to passive monitoring to ensure that firewall controls are working as desired. Penetration tests that seek to bypass firewall controls, red team exercises that seek to test detection and response against real world techniques of adversaries and automated security validation systems like Pentera and Cymulates have systems that continuously test that enforcement is being applied as intended, and was not eroded by configuration drift or policy accumulation.

11. FUTURE PROSPECTS WHERE MULTI-DOMAIN FIREWALL ARCHITECTURE IS HEADING

The domain-specific firewall strategy will undergo several changes in the coming years based on a number of developments. The use of artificial intelligence in improving detection features is being incorporated in all types of firewalls, and machine learning has been used in anomaly detection in both IT NGFW and OT industrial firewall systems. The practical effect is increased speed of identifying new attack methods that cannot be identified by the existing signatures, but the accuracy and justifiability of AI-based enforcement actions in highly stakes OT settings are both frontiers of assessment and discussion.

The ongoing expansion of 5G as well as private cellular networks in industrial settings will present novel connectivity routes in OT that will disrupt the traditional wired segmentation boundaries, necessitating industrial firewall structures to be adjusted to wireless-native OT traffic. The operational technology and edge computing platform integration where compute assets are physically relocated to the field devices

will demand industrial security controls that are able to run in further distributed and more physically exposed deployments.

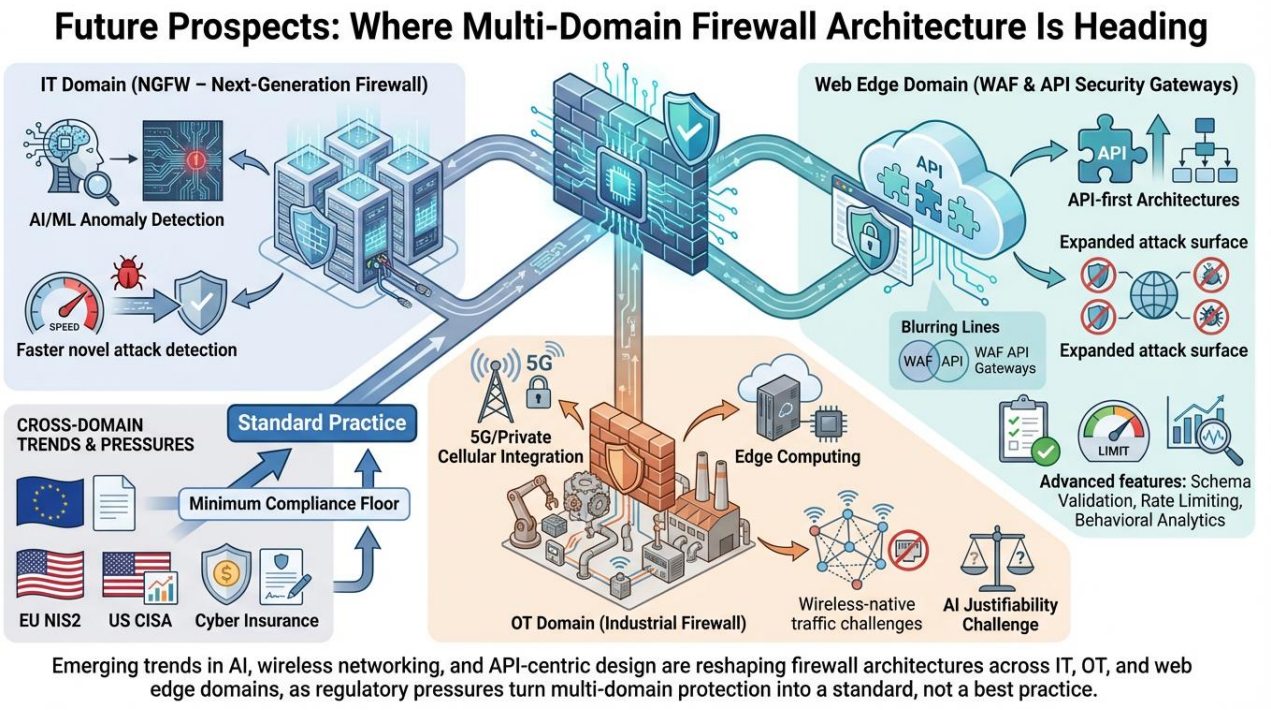

Fig -10: Future Prospects Where Multi-Domain Firewall Architecture is Heading

Within the web edge domain, the overall development of API-first application architectures and the resulting increase in API attack surfaces will cause more specialization of WAF and API security gateway services. The line between the traditional WAF functionality and specific API security platforms will probably become unclear as the vendors of WAF will introduce schema validation, rate limiting, and API behavioral analytics into their product lineup. All three domains will be subject to investment pressures by the authorities. The growth of NIS2 requirements in Europe, the development of CISA mandatory reporting and security requirements in the United States, and the growing role of cyber insurance underwriters in prescriptive specifications of security architecture design are all forming a minimum compliance floor that is turning the multi-domain firewall architecture into a regular expectation and not a best practice.

12. ETHICAL IMPLICATIONS AND GOVERNANCE DIMENSIONS OF MULTI-DOMAIN FIREWALL STRATEGY

In critical infrastructure settings, decisions regarding cybersecurity architecture are not necessarily technical. They have moral implications, administrative burdens, and social implications which practitioners ought to be aware of in addition to the technical needs as mentioned elsewhere in this article.

12.1 Responsible Knowledge and Dual-Use Concerns

The comprehensive listing of the types of OT vulnerabilities, industrial protocol vulnerabilities, and firewall implementation gaps has a valid and useful educational purpose. It also, by definition, makes the

knowledge of the threat landscape aware of enemies who read the same literature. This is the dual-use of all security research and publication. It is not to shun the discussion of vulnerabilities but rather to make sure that architectural advice should be accompanied by practical remediation. Articles and training content that records attack surfaces without commensurate advice on mitigation exacerbate a knowledge asymmetry that favors well-resourced attackers over under resourced defenders. The security architecture guidance published or shared by practitioners is a professional obligation to make the defensive information available as well as the threat description.

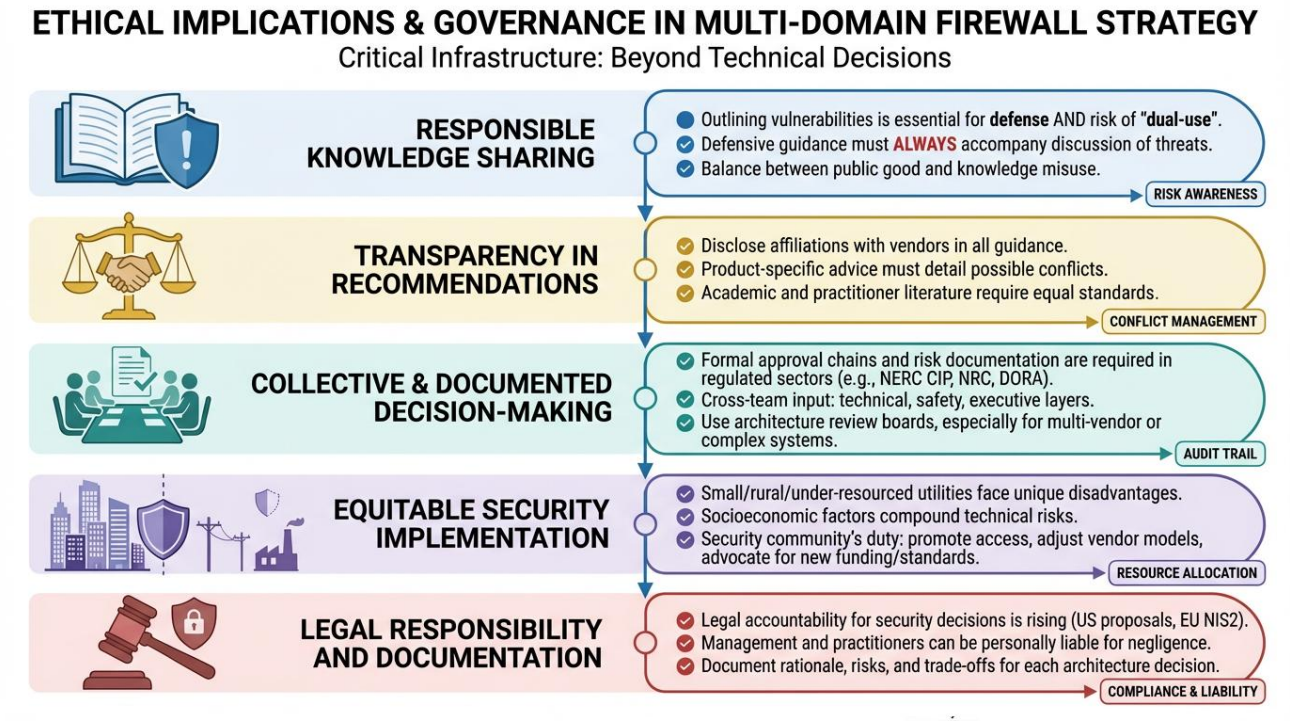

Fig -11: Ethical Implications & Governance in Multi-Domain Firewall Strategy

12.2 Conflict of Interest and Vendor Recommendation Ethics

Architectural advice that identifies particular vendor products without the disclosure of potential affiliations between the author, his or her organization, and the named vendors is below the ethical level of practitioner reference material. This is true of both academic articles, vendor-sponsored white papers, and conference presentations. Explicit conflict of interest declaration is the norm in the world of academic publications. Practitioner literature should be no exception. The readers have the right to find out whether a recommendation to adopt a particular product of a certain vendor came as a result of an independent technical assessment or it was based on a commercial association.

12.3 Governance Frameworks for Security Architecture Decisions

Single security practitioners are not supposed to make critical infrastructure security architecture decisions in isolation. Regulated industries such as electric utilities, NERC CIP, nuclear facilities, NRC cybersecurity, and financial institutions with DORA in the European Union require the governance systems to mandate a particular approval chain, risk acceptance procedures, and documentation of security control decisions. In areas where no regulatory requirements are defined, architecture choices with operational safety consequences, like the implementation of a new firewall in a process control system, must consider

operational technical management, operational safety engineering teams and executive risk acceptance together with security engineers. Decisions related to multi-vendor architecture, especially, due to their ongoing complexity in operation and vendor management, are well served by formal architecture review board procedures that capture the rationale and risk trade-offs in a manner that endures personnel turnover.

12.4 Equity and Access in Critical Infrastructure Security

Large and well-endowed organizations can implement the security architecture outlined in this article. It is quite impossible in small water utilities, rural electric co-operatives, small community hospitals, and the like that provide critical infrastructure in underserved communities with low to no security budgets. This equity has a direct equity aspect populations served by small, under-resourced critical infrastructure operators is more likely to be low-income, rural, or otherwise socially marginal communities that are also less capable of absorbing the impacts of infrastructure failure. The security community is not only supposed to advise the well-endowed. It encompasses lobbying regulatory and funding structures that promote the security enhancements of under-invested critical infrastructure, and the vendors of technology to create products and price structures suited to organizations that genuinely cannot buy enterprise-grade products.

12.5 Legal Liability and Duty of Care

Due to the growing frequency and impact of cyber-physical attacks on critical infrastructure, the question of legal responsibility of security architecture decisions is gaining more and more traction. In the United States, a number of legislative proposals and executive orders have started to develop positive security responsibilities on critical infrastructure operators. NIS2, in the European Union, has provisions on personal liability of management due to negligence in cybersecurity. Security architects and practitioners who recommend or execute security architectures in critical environments must understand that their professional choices can have implications of legal liability that would spill over into areas beyond their immediate employment relationship. Recording of the rationale behind the decision, acceptance of the risk and the trade-offs that have been made in the selection of the architecture is therefore a governance best practice as well as a professional self-protective action.

13. GLOBAL PERSPECTIVES AND REGIONAL CONSIDERATIONS IN MULTI-DOMAIN FIREWALL STRATEGY

The fundamental technical concepts of domain-specific firewall design, trust-boundary segmentation, OT-conscious inspection in industry, web-edge protection in application layers are universal. The environment in which it is implemented, such as the extent of vendors, regulatory needs, profiles of threat actors, and budget constraints, are geographically different. Non-North American and Western European practitioners need to be given guidance that is culturally adjusted, which is not thoroughly offered in the central part of the article.

13.1 Vendor Ecosystems by Region

The US-based vendors, such as Palo Alto Networks, Fortinet, Cisco, and Check Point, dominate the market of the North American and Western European firewall as explained in the main article. Huawei enterprise portfolio of security in Asia-Pacific, specifically in China and those markets that have major investments in Chinese infrastructure, offers a strong and technically viable alternative. The USG series of firewalls by Huawei are deployed at enterprise and carrier level in China, Southeast Asia, Africa and some parts of Latin

America. Their omission in the vendor discussion in this article is a market view, as opposed to a technical view of the markets. The practitioners in these markets should be able to compare Huawei to the same domain specific criteria that is discussed in this article.

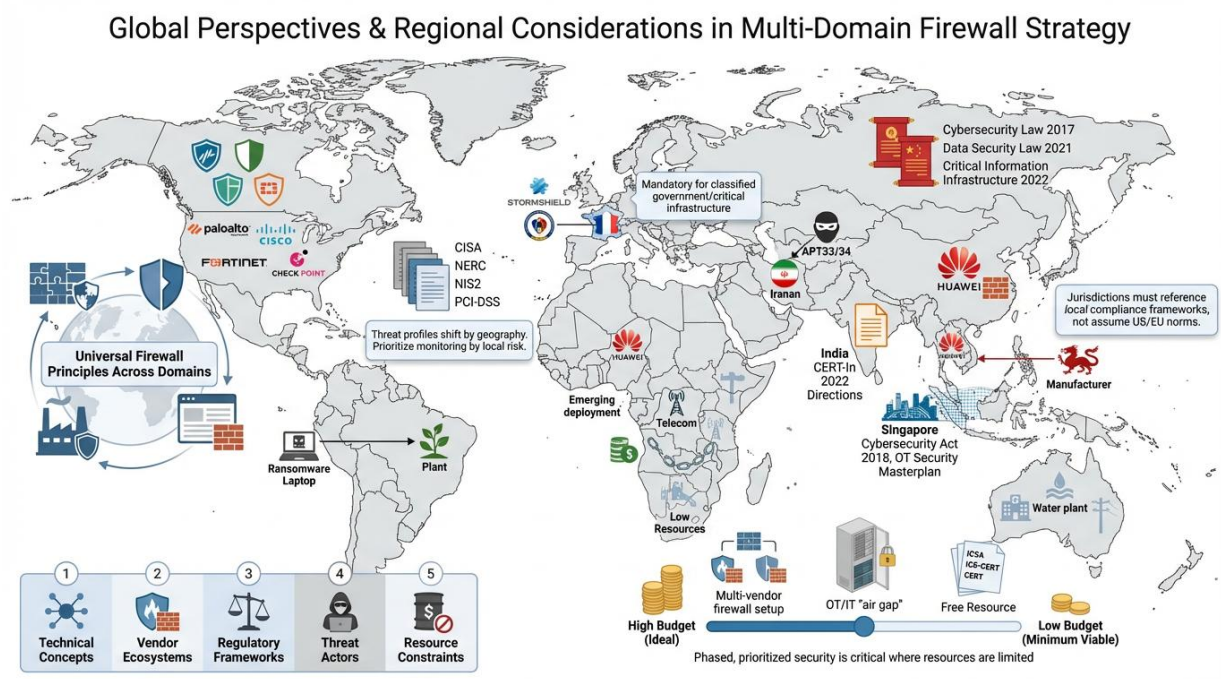

Fig -12: Global Perspectives & Regional Considerations in Multi-Domain Firewall Strategy

Stormshield, an Airbus CyberSecurity subsidiary, enjoys certain regulatory status in France and in the European public sector and defense community. In some French government and critical infrastructure deployments, products with the Restricted classification level certified by the French National Information Systems Security Agency (ANSSI) are mandatory. The Network Security and Industrial Security product lines of Stormshield can cover both IT and OT environments and specifically target sovereignty-sensitive deployments in which US-originated vendor products become a matter of concern regarding data governance.

13.2 Regulatory Landscapes Outside North America and Europe

The regulatory references of the article are focused on the US (CISA, NERC CIP, PCI-DSS) and EU (NIS2) frameworks. Organizations with other jurisdictions have different compliance landscapes because of the critical infrastructure that they operate. The Cybersecurity Law (2017), Data Security Law (2021), and the 2022 Regulations on the Security Protection of Critical Information Infrastructure in China, establish obligatory security criteria on operators of designated critical information infrastructure in China that has network segmentation requirements broadly similar in purpose, however, possibly different in detail, to those of IEC 62443. CERT-In directions (2022) proposed incident reporting requirements and some security architecture requirements on organizations that are present in India. The operational OT security regulatory frameworks were achieved in Singapore when the Cybersecurity Act (2018) and the Operational Technology Security Masterplan required that the industry regulators develop regulatory frameworks on OT security in the critical infrastructure sectors. Such practitioners working in these jurisdictions are advised

to test the requirements they are subjected to against these frameworks instead of thinking that the US or EU standards are in effect.

13.3 Threat Actor Profiles by Region

The geographical differentiation of the threat landscape should be used to shape the architecture and monitoring priorities. Middle Eastern industrial infrastructure has been a continuous target of Iranian actors associated with the state as Mandiant APT33 and APT34 have trailed. The manufacturing and energy industries of Southeast Asia are under a considerable threat of operations by groups that are accredited to Chinese state interests. OT-oriented activity is rife and Latin American critical infrastructure operators are an ever-increasing target of ransomware attacks by financially-driven gangs. African telecommunications infrastructure and energy infrastructure where there is a high level of Chinese-funded investment and this has created dependence on operations presents a unique supply chain risk profile. Knowing what types of threat actors are most applicable to the geographic and industry-specific environment of a particular organization should guide both the choice of firewall vendor (including any issues related to vendor nation-state alignment) and monitoring priorities setting.

13.4 Resource Constraints in the Global South

Critical infrastructure operators in many developing-worlds, such as power utilities, water authorities, and healthcare providers, do not have the budget to support the multi-vendor architecture outlined in this article. OT environments could be running with little or no specific cybersecurity personnel in organizations in Sub-Saharan Africa, some parts of South and Southeast Asia, and Latin America. In such contexts, phased guidance, rather than wholesome architecture frameworks, is more appropriate. Physical separation of the OT network by any IT connection and very stringent control over any equipment that is added to the OT environment is the practical minimum of OT protection in any severely resource-constrained environment. ICSA, the ICS-CERT, and regional CERTs offer free resources that offer baseline guidance, which can be implemented at a low cost.

14. CONCLUSION ARCHITECTURE AND DISCIPLINE DETERMINE OUTCOMES

The main thesis of this paper is that architectural radically different environments have radically different security control demands and firewalls are no exception to this fact. IT networks require NGFWs that perform deep application inspection, TLS decryption and user identity integration, both at the edge and internally to be used to segment east-west. The OT networks require hardened industrial firewalls that are OT-protocol-aware and deep packet inspection, deterministic low latency, fail-safe operation, and physical durability, structured around the Purdue model and the Industrial DMZ between IT and OT. The web facing environments must have WAFs that have OWASP compatible signature coverage, behavioral analysis, API security, and bot management which should be delivered over cloud edge platforms that are distributed globally. Cloud workloads and distributed users require FWaaS or SASE solutions that enforce them in the same way irrespective of location.

No one vendor is so good at all these things. Multi-vendor architecture is not an inconvenience in procurement. In dual-firewall DMZ and dual-perimeter OT designs, a purposely designed security approach means that no individual product vulnerability can be used to compromise two layers of protection at the same boundary simultaneously. The limit of what can be is the product selection. This is dictated by architecture, policy design, and operational discipline, which dictate how close organizations are to that ceiling. When firewalls are installed appropriately at the boundaries between zones where real

trust differences exist, with rules based on documented communication baselines, with disciplined change processes, and continually refined against current threats, provide significantly better security effects than superior products deployed without equivalent discipline. It is only the organizations that are aware of this difference and take action that will construct truly resilient security architectures.

REFERENCES

[1] CXO Revolutionaries. (n.d.). https://www.zscaler.com/cxorevolutionaries/insights
[2] Coleman, S. (n.d.). Defense in depth: The Critical role of data diodes in government industrial control systems. MeriTalk. https://www.meritalk.com/articles/defense-in-depth-the-critical-role-of-data-diodes-in-government-industrial-control-systems/
[3] OWASP Top ten web application Security Risks | OWASP Foundation. (n.d.). https://owasp.org/www-project-top-ten/
[4] STL Partners. (2023, September 28). IT/OT Convergence: The role of edge and operational technology. https://stlpartners.com/articles/edge-computing/it-ot-convergence-edge-operational-technology/
[5] SyC Smart Energy. (2020, July 7). Security Standards and Best Practices for the Smart Energy Operational Environment - SYC Smart Energy. https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/
[6] Team, C. W. (2026, January 7). Top 10 Best Web Application Firewall (WAF) in 2026. Cyber Security News. https://cybersecuritynews.com/best-web-application-firewall-waf/#What
[7] The History of firewalls | Who invented the firewall? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/history-of-firewalls
[8] Time to take action: Insights from the Verizon Data Breach Investigations Report 2024. (2024, September 16). ISMS.online. https://www.isms.online/information-security/time-to-take-action-insights-from-the-verizon-data-breach-investigations-report-2024/
[9] What is the purdue model for ICS security? | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/purdue-model
[10] Wikipedia contributors. (2026, March 3). Unidirectional network. Wikipedia. https://en.wikipedia.org/wiki/Unidirectional_network
[11] Bragaru, T., & Darii, O. (2025). Ensuring web security with OWASP methodology. Creating the Society of Consciousness, TELE-2025. https://doi.org/10.53486/csc2025.16
[12] Daoudi, W., Doumi, K., & Kjiri, L. (2021). Complexity and adaptive enterprise architecture. Proceedings of the 23rd International Conference on Enterprise Information Systems. https://doi.org/10.5220/0010475707590767
[13] Fischer, A. R. H. (2017). Perception of product risks. Consumer Perception of Product Risks and Benefits. https://doi.org/10.1007/978-3-319-50530-5_9
[14] Li, J., & Li, H. (2025). Evolution of application security based on OWASP top 10 and CWE/SANS top 25 with predictions for the 2025 OWASP top 10. 2025 International Conference on Inventive Computation Technologies (ICICT). https://doi.org/10.1109/icict64420.2025.11004742
[15] Madsen, T. (2023). Why zero-trust. Zero-trust – An Introduction. https://doi.org/10.1201/9781003464587-1
[16] Ologunde, E. (2026). Risk acceptance in critical infrastructure cyber incidents: A retrospective analysis of the colonial pipeline ransomware attack. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.6212678
[17] Patil, U. A., Venkatesan, M., & Prasad, S. (2021). An improved wireless network architecture for iot in hospital healthcare. 2021 IEEE Bombay Section Signature Conference (IBSSC). https://doi.org/10.1109/ibssc53889.2021.9673340
[18] Song, Y., Luo, W., Li, J., Xu, P., & Wei, J. (2021). Sdn-based industrial internet security gateway. 2021 International Conference on Security, Pattern Analysis, and Cybernetics（SPAC). https://doi.org/10.1109/spac53836.2021.9539961
[19] Stevens, A. (2025). Enterprise security architecture frameworks. Enterprise Fortress. https://doi.org/10.1201/9781003585923-3

[20] Williams, T. (1993). The purdue enterprise reference architecture. IFAC Proceedings Volumes, 26(2), 559-564. https://doi.org/10.1016/s1474-6670(17)48532-6
[21] Aladi, C. C. (2024). Web application security: A pragmatic exposé. Digital Threats: Research and Practice, 5(2), 1-9. https://doi.org/10.1145/3644394
[22] Aneja, A., & Thapar, V. (2013). Optimizing packet filter firewall using duple decision scheme. The SIJ Transactions on Computer Networks & Communication Engineering, 01(02), 01-07. https://doi.org/10.9756/sijcnce/v1i2/0102510101
[23] Ibrahim, A. (2017). SPIMN stateful packet inspection for multi gigabits networks. International Journal of Computing and Network Technology, 05(02), 77-88. https://doi.org/10.12785/ijcnt/050205
[24] Kapoor, A. (2023). Traffic systems vulnerabilities and cyber-attacks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4430819
[25] Myung, J. W., & Hong, S. (2019). ICS malware triton attack and countermeasures.. IJEMR, 3(2), 13-17. https://doi.org/10.22662/ijemr.2019.3.2.013
[26] Neupane, K., Haddad, R., & Chen, L. (2018). Next generation firewall for network security: A survey. SoutheastCon 2018. https://doi.org/10.1109/secon.2018.8478973
[27] Olorunlana, T. J., & Mohammed, H. (2025). Analysis of the colonial pipeline cybersecurity incident. International Journal of Science, Architecture, Technology and Environment, 9-13. https://doi.org/10.63680/jngh0767as
[28] Paredes, I. (2020). IT/OT convergence – cybersecurity beyond technology. Abu Dhabi International Petroleum Exhibition & Conference. https://doi.org/10.2118/203093-ms
[29] Shin, B. (2017). Architectures and standards. A Practical Introduction to Enterprise Network and Security Management. https://doi.org/10.4324/9781315154206-2
[30] Beverly, G. (2026). Effortless 100% score with ngfw-engineer exam dumps. https://doi.org/10.55277/researchhub.lesra13i
[31] Cabric, M. (2015). Confidentiality, integrity, and availability. Corporate Security Management. https://doi.org/10.1016/b978-0-12-802934-3.00011-1
[32] Davidian, M., Vanetik, N., & Kiperberg, M. (2022). Ransomware detection with deep neural networks. Proceedings of the 8th International Conference on Information Systems Security and Privacy. https://doi.org/10.5220/0011008000003120
[33] Dhiman, P., & Kaur, A. (2025). A comprehensive study on zero-trust frameworks. Zero-Trust Learning. https://doi.org/10.1201/9781779643575-4
[34] George. (2025). India's New Labor Codes A Critical Analysis of Promise, Peril, and the Path Forward. Partners Universal International Research Journal, 4(4), 23–42. https://doi.org/10.5281/zenodo.17871778
[35] Jacques, S. (2023). Activities for annual review, 2023: Mid-year report. https://doi.org/10.21428/7b6d533a.d65b8846/a2519ca6
[36] Pandey, B. K., Pandey, D., Agarwal, A., Mahajan, D. A., Dadheech, P. D., George, A. S., & Kumar Rai, P. (2024). Beyond Data Breaches: Enhancing Security in 6G Communications. In D. Pandey, B. Pandey, & T. Ahmad (Eds.), Security Issues and Solutions in 6G Communications and Beyond (pp. 212-229). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-2931-3.ch013
[37] Jenkinson, A. (2021). Www.avsvmcloud(.)com (solarwinds attack) the modus operandi for attacks since stuxnet. Stuxnet to Sunburst. https://doi.org/10.1201/9781003204145-16
[38] GEORGE, A. SHAJI., GEORGE, A. S. HOVAN., T. Baskar, & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions -Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. Zenodo (CERN European Organization for Nuclear Research), 08(01). https://doi.org/10.5281/zenodo.7028219
[39] Li, J., & Li, H. (2025). Evolution of application security based on OWASP top 10 and CWE/SANS top 25 with predictions for the 2025 OWASP top 10. 2025 International Conference on Inventive Computation Technologies (ICICT). https://doi.org/10.1109/icict64420.2025.11004742
[40] George, Dr. A. Shaji., Dr.T.Baskar, & Dr.Nataliia Siranchuk. (2026). The Gig Career Revolution: How Platform Work Is Transforming Global Employment, Economics, and Human Wellbeing. Zenodo, 03(01). https://doi.org/10.5281/zenodo.18401066
[41] Morgan, M., & Schank, J. (2018). Making it work: Examples of OT within the maker movement. OT Practice. https://doi.org/10.7138/otp.2018.2314.maker
[42] Myung, J. W., & Hong, S. (2019). ICS malware triton attack and countermeasures.. IJEMR, 3(2), 13-17. https://doi.org/10.22662/ijemr.2019.3.2.013

[43] Olorunlana, T. J., & Mohammed, H. (2025). Analysis of the colonial pipeline cybersecurity incident. International Journal of Science, Architecture, Technology and Environment, 9-13. https://doi.org/10.63680/jngh0767as

[44] Soest, H. V. (2025). Cybersecurity in the european electricity system: The role of the NIS2 directive. European Energy Law Report, 345-362. https://doi.org/10.1017/9781839704635.016

[45] (2019). Verizon: 2019 data breach investigations report. Computer Fraud & Security, 2019(6), 4-4. https://doi.org/10.1016/s1361-3723(19)30060-0

[46] (2022). Imperva: The state of security within ecommerce. Computer Fraud & Security, 2022(1). https://doi.org/10.12968/s1361-3723(22)70003-6

[47] Aboalassaad, A., & Malik, T. (2024). The impact of IPS and firewall placement on network security and performance. 2024 Cyber Research Conference - Ireland (Cyber-RCI). https://doi.org/10.1109/cyber-rci60769.2024.10939923

[48] Baloch, R. (2024). Evading web application firewalls (wafs). Web Hacking Arsenal. https://doi.org/10.1201/9781003373568-13

[49] Barakat, R., Catal, F., Tcholtchev, N., Rebahi, Y., & Schieferdecker, I. (2020). Industrial grade methodology for firewall simulation and requirements verification. NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium. https://doi.org/10.1109/noms47738.2020.9110345

[50] Blum, E., Gonzalez, Y., & Teheran, J. (2024). The integration of the cloudflare WAF. The Integration of The Cloudflare WAF. https://doi.org/10.2172/2407272

[51] Bultoc, N. (2026). Master fortigate administration with fortinet NSE4 7.6 prep. https://doi.org/10.55277/researchhub.9vjwc62d

[52] Chinthala, M. M. R., & Kalloji, M. (2025). Policy-oriented zero trust microsegmentation for east-west traffic governance in hybrid cloud architectures. 2025 6th International Conference on Smart Electronics and Communication (ICOSEC), 1330-1335. https://doi.org/10.1109/ICOSEC67334.2025.11459755

[53] Chowdhary, A., Dixit, V. H., Tiwari, N., Kyung, S., Huang, D., & Ahn, G. J. (2017). Science DMZ: SDN based secured cloud testbed. 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). https://doi.org/10.1109/nfv-sdn.2017.8169868

[54] De, B. (2017). API security. API Management. https://doi.org/10.1007/978-1-4842-1305-6_7

[55] Ding, R., & Cheng, M. (2024). Hardware layout of independent metering control. Independent Metering Electro-Hydraulic Control System. https://doi.org/10.1007/978-981-99-6372-0_2

[56] Dr Satya Parkash (2025). Cybersecurity and data breach regulations from a global perspective. Indian Journal of Law, 3(5). https://doi.org/10.36676/ijl.v3.i5.118

[57] Laili, Y., Gong, J., Kong, Y., Wang, F., Ren, L., & Zhang, L. (2025). Communication intensive task offloading with IDMZ for secure industrial edge computing. IEEE Transactions on Cloud Computing, 13(2), 560-577. https://doi.org/10.1109/tcc.2025.3548043

[58] Lee, H. J., & Won, D. (2013). Protection profile for unidirectional security gateway between networks. International Journal of Security and Its Applications, 7(6), 373-384. https://doi.org/10.14257/ijsia.2013.7.6.37

[59] Maulana, A. H., Suyasa, I., & Kurniawan, E. (2023). Analysis of the demilitarized zone implementation in java madura bali electrical systems to increase the level of IT/OT cyber security with the dual DMZ firewall architecture method. 2023 International Conference on Smart Applications, Communications and Networking (SmartNets), 1-6. https://doi.org/10.1109/SmartNets58706.2023.10215960

[60] MK, A., Bala, K. S. S., Sonti, S. S. T., & KP, J. (2026). An empirical study on the evaluation and enhancement of OWASP CRS (core rule set) in modsecurity. Computers & Security, 160, 104714. https://doi.org/10.1016/j.cose.2025.104714

[61] Oh, K. S., & Joo, W. C. (2019). Concept of DMZ peace road for peace and unification, pilgrimage. THE JOURNAL OF PEACE STUDIES, 20(4), 27-52. https://doi.org/10.14363/kaps.2019.20.4.27

[62] Sameh, A., & Selim, S. (2025). Adaptive dual-layer web application firewall (ADL-WAF) leveraging machine learning for enhanced anomaly and threat detection. ArXiv, abs/2511.12643. https://doi.org/10.48550/arXiv.2511.12643

[63] Schäfer, G. (2004). Internet firewalls. Industrial Electronics. https://doi.org/10.1201/9781420036336.ch35

[64] Sichkar, M., & Pavlova, L. (2023). A short survey of the capabilities of next generation firewalls. Computer Science and Cybersecurity. https://doi.org/10.26565/2519-2310-2023-1-02

[65] Singh, B., & ., K. (2024). Cloud-native firewalls with large-scale autonomous policy optimization. Journal of Frontiers in Multidisciplinary Research, 5(1), 344-348. https://doi.org/10.54660/.jfmr.2024.5.1.344-348

[66] Wang, Z., Lu, Z., Wu, J., & Fan, K. (2015). Cpfirewall: A novel parallel firewall scheme for fwaas in the cloud environment. Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-319-26979-5_9
[67] Williams, T. (1993). The purdue enterprise reference architecture. IFAC Proceedings Volumes, 26(2), 559-564. https://doi.org/10.1016/s1474-6670(17)48532-6
[68] Xu, K., Tan, J., Guo, L., & Fang, B. (2011). Traffic-aware frequent elements matching algorithms for deep packet inspection. Journal of Networks, 6(5). https://doi.org/10.4304/jnw.6.5.799-806
[69] (2003). Firewall concepts. The Best Damn Firewall Book Period. https://doi.org/10.1016/b978-193183690-6/50043-1
[70] (2008). Google app engine. Developing with Google App Engine. https://doi.org/10.1007/978-1-4302-1832-6_1
[71] (2015). Remote data access systems. Flow Measurement Handbook. https://doi.org/10.1017/cbo9781107054141.024
[72] (2015). Inside the DMZ. Inside the DMZ. https://doi.org/10.5040/9781350917569
[73] (2018). Understanding the AWS environment. AWS Certified Cloud Practitioner Study Guide. https://doi.org/10.1002/9781119574408.ch4
[74] (2022). Repositórios e sistemas de registro eletrônico em saúde, 2.ed. Cegraf UFG. https://doi.org/10.5216/rep.ebook.978-85-495-0641-2/2022
[75] Busalachi, D. (2024). Bridging the gap between IT and OT to improve industrial cyber security. Cyber Security: A Peer-Reviewed Journal, 7(4), 333. https://doi.org/10.69554/eazh4262
[76] Douillet, M., & Wedin, L. (2023). Multi-domain operations (MDO): From theory to training-complexity and innovation in military operations. Revue Défense Nationale, No 863(8), 73-79. https://doi.org/10.3917/rdna.863.0073
[77] Hakim, A. N., & Setiawan, D. (2025). Multi-criteria decision making (MCDM) analysis in vendor selection decision-making using the analytical hierarchy process (AHP) method. Qomaruna, 2(2), 10-21. https://doi.org/10.62048/qjms.v2i2.89
[78] Khatri, V., Monshizadeh, M., & Tiirikainen, K. (2022). Ethernet communication over IP transport for industrial and private cellular network. 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). https://doi.org/10.23919/softcom55329.2022.9911387
[79] Pandey, D., Pandey, B. K., George, A. S., George, A. S., Sunder, S., Jolly, A., & Verma, S. (2025). Scientific Progress in Artificial Intelligence for Time-Stamped Interpretation of Camera Images in Medical Safety Systems. In B. Pandey, A. George, S. Tiwari, S. Albermany, & H. Hung (Eds.), Advanced Secure Transmission of Telemedicine-Based Bio-Medical Images (pp. 91-114). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9821-0.ch005
[80] Nicholson, A., Janicke, H., & Cau, A. (2014). Safety and security monitoring in ICS/SCADA systems. 2nd International Symposium for ICS & SCADA Cyber Security Research 2014. https://doi.org/10.14236/ewic/ics-csr2014.9
[81] Niemann, K. H., Eßlinger, T., & Waldeck, B. (2025). PROFINET– zukünftige ot-security anforderungen. atp magazin, 67(9), 46-54. https://doi.org/10.17560/atp.v67i9.2796
[82] Porter, K. K. (2019). Common mistakes in design and implementation. Implementing Supplier Diversity. https://doi.org/10.1007/978-3-319-94394-7_7
[83] Sinha, D. A., & Sharma, A. K. (2023). ROLE OF TRADITIONAL FIREWALLS AND AI FIREWALLS IN NETWORK SECURITY. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH, 78-81. https://doi.org/10.36106/ijsr/4120890
[84] George, A. S. (2025). Digital Watermarking in Cloud Environments for Copyright Protection: A Comprehensive Review. Partners Universal Multidisciplinary Research Journal (PUMRJ), 02(06), 54–74. https://doi.org/10.5281/zenodo.17726895
[85] Yuhong, W., & Xiangdong, H. (2021). Industrial internet security protection based on an industrial firewall. 2021 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA). https://doi.org/10.1109/icaica52286.2021.9497973
[86] (2016). Application whitelisting. Information Security Management Handbook, Volume 6. https://doi.org/10.1201/b11802-19
[87] George, Dr. A. Shaji. (2026). Self-Driving Networks: AI Automation for Enterprise IT. Zenodo, 05(01). https://doi.org/10.5281/zenodo.19335608
[88] Ang, B. (2020). Singapore, ASEAN, and international cybersecurity. Routledge Handbook of International Cybersecurity. https://doi.org/10.4324/9781351038904-21

[89] Arnold, S. (2024). African agency in ICT infrastructure provider choice: Navigating access to foreign finance and technology. Telecommunications Policy, 48(5), 102713. https://doi.org/10.1016/j.telpol.2024.102713

[90] Beal, B. (2005). IT security: The product vendor landscape. Network Security, 2005(5), 9-10. https://doi.org/10.1016/s1353-4858(05)70235-x

[91] George, Dr. A. Shaji., George, A. S. Hovan., & Dr.T.Baskar. (2023). SD-WAN Security Threats, Bandwidth Issues, SLA, and Flaws: An In-Depth Analysis of FTTH, 4G, 5G, and Broadband Technologies. Zenodo (CERN European Organization for Nuclear Research), 01(03). https://doi.org/10.5281/zenodo.8057014

[92] A. R. Research Publication. (2026, January 19). Securing Tomorrow: How 6G Networks and AI Are Reshaping the Cybersecurity Landscape. https://doi.org/10.5281/zenodo.18299699

[93] Beverly, G. (2026). Effortless 100% score with ngfw-engineer exam dumps. https://doi.org/10.55277/researchhub.lesra13i

[94] Blum, E., Gonzalez, Y., & Teheran, J. (2024). The integration of the cloudflare WAF. The Integration of The Cloudflare WAF. https://doi.org/10.2172/2407272

[95] George, Dr. A. Shaji. (2025). Cyber Resilience in an AI-Driven World: A Strategic Framework. Zenodo (CERN European Organization for Nuclear Research), 03(06). https://doi.org/10.5281/zenodo.18002783

[96] Bulda, O. (2019). «legal asymmetry»in the context of liability of the state and state-sponsored cyber attacks actors. Proceedings of the conference "Behind the Digital Curtain. Civil Society vs State Sponsored Cyber Attacks". https://doi.org/10.34054/bdc003

[97] Dheeraj, R., Guo, H., Veeravalli, B., & Yu, X. (2019). Design and development of SCADA firewall security features for protecting industrial operations. 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS). https://doi.org/10.1109/vts-apwcs.2019.8851675

[98] George, Dr. A. Shaji., & Dr.T.Baskar. (2025). Security and Privacy Comparison of Arattai, WhatsApp, and WeChat: India's Messaging App Landscape and Digital Sovereignty. Zenodo (CERN European Organization for Nuclear Research), 03(05). https://doi.org/10.5281/zenodo.17483067

[99] Dobson, J. (1990). An architecture for multi-vendor systems. Software Engineering for Large Software Systems. https://doi.org/10.1007/978-94-009-0771-3_6

[100] Ellefsen, I., & von Solms, S. (2010). Critical information infrastructure protection in the developing world. IFIP Advances in Information and Communication Technology. https://doi.org/10.1007/978-3-642-16806-2_3

[101] George, A. S., S Sagayarajan, T Baskar, & Pandey, D. (2024). Assessing the Security and Privacy Implications of India's DigiYatra Initiative. Partners Universal Innovative Research Publication (PUIRP), 02(04), 36–45. https://doi.org/10.5281/zenodo.14599297

[102] Fuller, L. K. (2008). Educational vulnerabilities. African Women's Unique Vulnerabilities to HIV/AIDS. https://doi.org/10.1057/9780230616202_6

[103] George. (2024). Personal Privacy at Risk: The Security Threats of Sharing Boarding Passes Online. Partners Universal International Research Journal, 3(4), 24–40. https://doi.org/10.5281/zenodo.14503012

[104] Hakim, A. N., & Setiawan, D. (2025). Multi-criteria decision making (MCDM) analysis in vendor selection decision-making using the analytical hierarchy process (AHP) method. Qomaruna, 2(2), 10-21. https://doi.org/10.62048/qjms.v2i2.89

[105] George, Dr. A. Shaji. (2025). An Exploratory Study of Friendship Marriage and Its Role in Redefining Partnership for Economic Security and Personal Autonomy in Modern Society. Zenodo, 04(03). https://doi.org/10.5281/zenodo.17137271

[106] Huawei, Z., & Ruixia, L. (2009). A scheme to improve security of SSL. 2009 Pacific-Asia Conference on Circuits, Communications and Systems. https://doi.org/10.1109/paccs.2009.148

[107] Milik, P. (2021). International legal regulations in the area of cybersecurity. Cybersecurity and Law, 1(1), 115-141. https://doi.org/10.35467/cal/133774

[108] Orsini, Y. (2016). Learning from community-company conflicts: Practical approaches. SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility. https://doi.org/10.2118/179417-ms

[109] George, A. S., Baskar, D. T., P. Balaji Srikaanth, & Karthikeyan, M. M. (2025). Building Resilient API Security Through a Five-Dimensional Framework for Data Breach Prevention in Modern Digital Ecosystems. Partners Universal Multidisciplinary Research Journal (PUMRJ), 02(04), 32–50. https://doi.org/10.5281/zenodo.15862111

[110] Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for scada-based critical infrastructure. International Journal of Critical Infrastructure Protection, 25, 14-35. https://doi.org/10.1016/j.ijcip.2019.01.002

[111] Rosén, A., Gaba, G. S., & Gurtov, A. (2025). A strategic roadmap for phased zero trust architecture implementation in organizations. 2025 IEEE Conference on Communications and Network Security (CNS). https://doi.org/10.1109/cns66487.2025.11194934

[112] Sathvick, A., Bangali, S., & Das, S. (2026). Ransomware attacks on smart grids: Challenges and defense strategies. 2026 IEEE PES International Meeting (PES IM), 1-5. https://doi.org/10.1109/PESIM67009.2026.11438311

[113] George, Dr. A. Shaji. (2025). Sanchar Saathi Digital Security versus Civil Liberty in India 's Smartphone Era. Zenodo, 04(04). https://doi.org/10.5281/zenodo.17838468

[114] Soest, H. V. (2025). Cybersecurity in the european electricity system: The role of the NIS2 directive. European Energy Law Report, 345-362. https://doi.org/10.1017/9781839704635.016

[115] Soper, D. S. (2020). Negotiating cloud security requirements with vendors. Cloud Computing Security. https://doi.org/10.1201/9780429055126-24

[116] Wager, E. (2012). Publishing ethics and integrity. Academic and Professional Publishing. https://doi.org/10.1016/b978-1-84334-669-2.50014-7

[117] George, Baskar, D. T., & Balaji, P. (2025). Bridging the Security Skills Gap: A Comprehensive Framework for Developing Application Security Competencies in Modern Software Engineering. Partners Universal Innovative Research Publication, 3(3), 96–123. https://doi.org/10.5281/zenodo.15616416

[118] Zurlo, G. A. (2026). A demographic profile of christianity in sub-saharan africa. Christianity in Sub-Saharan Africa. https://doi.org/10.3366/edinburgh/9781474412032.003.0001

[119] (2003). ISA server installation. The Best Damn Firewall Book Period. https://doi.org/10.1016/b978-193183690-6/50064-9

[120] Dr. A.SHAJI GEORGE, & GEORGE, A. S. HOVAN. (2021). A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall. IJARCCE:International Journal of Advanced Research in Computer and Communication Engineering, 10(05). https://doi.org/10.5281/zenodo.7027397

[121] (2006). Firewall and DMZ design. Designing and Building Enterprise DMZs. https://doi.org/10.1016/b978-159749100-6.50010-x

[122] (2012). Department of homeland security control systems security program - ICS-CERT overview. 2012 Integrated Communications, Navigation and Surveillance Conference. https://doi.org/10.1109/icnsurv.2012.6218507

[123] (2014). Market share analysis techniques: A review and illustration of current US practice. Store Choice, Store Location and Market Analysis (Routledge Revivals). https://doi.org/10.4324/9781315736686-15

[124] (2022). Mandiant: AI support for cyberthreat attribution. Working with AI. https://doi.org/10.7551/mitpress/14453.003.0016

[125] (2024). International cybersecurity laws and regulations. The Cybersecurity Guide to Governance, Risk, and Compliance, 299-314. https://doi.org/10.1002/9781394250226.ch17