ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΑΥΤΟΜΑΤΟΠΟΙΗΣΗ ΠΟΛΙΤΙΚΩΝ ΔΙΚΤΥΑΚΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΜΜΕς»

ΓΕΩΡΓΙΟΣ Η. ΖΗΣΗΣ

Επιβλέπων Καθηγητής:

ΚΩΝΣΤΑΝΤΙΝΟΣ ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ

ΠΕΙΡΑΙΑΣ

ΜΑΡΤΙΟΣ 2026

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΥΤΟΜΑΤΟΠΟΙΗΣΗ ΠΟΛΙΤΙΚΩΝ ΔΙΚΤΥΑΚΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΜΜΕς

ΖΗΣΗΣ Η. ΓΕΩΡΓΙΟΣ

Α.Μ.: MTE24011

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία πραγματεύεται τη σχεδίαση και την αυτοματοποίηση πολιτικών firewall για μικρομεσαίες επιχειρήσεις (SMEs), με στόχο τη βελτίωση του επιπέδου δικτυακής ασφάλειας και τη μείωση της πολυπλοκότητας στη διαχείριση κανόνων. Οι SMEs συχνά αντιμετωπίζουν περιορισμούς σε τεχνική εξειδίκευση και διαθέσιμους πόρους, γεγονός που καθιστά δύσκολη την ορθή υλοποίηση και συντήρηση πολιτικών ασφάλειας.

Στο πλαίσιο της εργασίας αναπτύσσεται ένα πρακτικό πλαίσιο αυτοματοποίησης βασισμένο στο firewall pfSense, το οποίο επιτρέπει τη δημιουργία και εφαρμογή κανόνων μέσω δομημένων αρχείων Excel. Το προτεινόμενο πλαίσιο αξιοποιεί προκαθορισμένες λίστες, ψευδώνυμα (aliases) και μηχανισμούς επικύρωσης δεδομένων, με στόχο τη μείωση σφαλμάτων παραμετροποίησης και τη διασφάλιση της ομοιομορφίας των κανόνων.

Η υλοποίηση πραγματοποιήθηκε σε ελεγχόμενο εργαστηριακό περιβάλλον με χρήση Proxmox, ενώ ενσωματώθηκαν συμπληρωματικοί μηχανισμοί ασφάλειας, όπως το pfBlockerNG και το σύστημα ανίχνευσης/πρόληψης εισβολών Suricata. Τέλος, πραγματοποιήθηκαν δοκιμές επαλήθευσης της λειτουργικότητας των κανόνων και αξιολογήθηκε η αποτελεσματικότητα της προτεινόμενης προσέγγισης σε σχέση με τις ανάγκες μιας τυπικής μικρομεσαίας επιχείρησης, λαμβάνοντας υπόψη βασικές αρχές του προτύπου ISO/IEC 27001.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Δικτυακή Ασφάλεια και Αυτοματοποίηση Πολιτικών Ασφάλειας

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Firewall, pfSense, Αυτοματοποίηση Πολιτικών Ασφάλειας, Μικρομεσαίες Επιχειρήσεις, Δικτυακή Ασφάλεια, IDS/IPS, ISO/IEC 27001

ABSTRACT

This thesis focuses on the design and automation of firewall policies for small and medium-sized enterprises (SMEs), aiming to enhance network security while reducing the complexity associated with firewall rule management. SMEs often face limitations in technical expertise and available resources, which makes the correct implementation and maintenance of security policies particularly challenging.

Within the scope of this work, a practical automation framework based on the pfSense firewall is proposed, enabling the creation and deployment of firewall rules through structured Excel files. The framework utilizes predefined lists, aliases, and data validation mechanisms in order to minimize configuration errors and ensure consistency across security policies.

The implementation was carried out in a controlled laboratory environment using virtualization technologies (Proxmox), while additional security mechanisms, such as pfBlockerNG and the Suricata intrusion detection and prevention system (IDS/IPS), were integrated to strengthen overall protection. Finally, functional tests were conducted to verify the correct application of firewall rules, and the effectiveness of the proposed approach was evaluated in the context of a typical SME environment, considering fundamental principles of the ISO/IEC 27001 standard.

SUBJECT AREA: Network Security and Security Policy Automation

KEYWORDS: Firewall, pfSense, Security Policy Automation, Small and Medium-sized Enterprises, Network Security, IDS/IPS, ISO/IEC 27001

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΙΝΑΚΑ ΣΥΝΤΟΜΕΥΣΕΩΝ – ΑΡΚΤΙΚΟΛΕΞΩΝ

ACL – Access Control List

AES – Advanced Encryption Standard

API – Application Programming Interface

APT – Advanced Persistent Threat

ARP – Address Resolution Protocol

ASLR – Address Space Layout Randomization

BGP – Border Gateway Protocol

BIOS – Basic Input/Output System

BYOD – Bring Your Own Device

CA – Certificate Authority

CAPEX – Capital Expenditure

CERT – Computer Emergency Response Team

CIA – Confidentiality, Integrity, Availability

CIS – Center for Internet Security

CSA – Cloud Security Alliance

CSIRT – Computer Security Incident Response Team

CVE – Common Vulnerabilities and Exposures

CVSS – Common Vulnerability Scoring System

DDoS – Distributed Denial of Service

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

DNSSEC – Domain Name System Security Extensions

DoS – Denial of Service

DR – Disaster Recovery

EAP – Extensible Authentication Protocol

EDR – Endpoint Detection and Response

EOL – End of Life

ERP – Enterprise Resource Planning

ESXi – Elastic Sky X Integrated (VMware Hypervisor)

EU – European Union

FIM – File Integrity Monitoring

FTP – File Transfer Protocol

GDPR – General Data Protection Regulation
GRC – Governance, Risk and Compliance
GUI – Graphical User Interface
HA – High Availability
HIDS – Host-based Intrusion Detection System
HIPS – Host-based Intrusion Prevention System
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol Secure
IaaS – Infrastructure as a Service
IAM – Identity and Access Management
ICS – Industrial Control Systems
IDS – Intrusion Detection System
IEC – International Electrotechnical Commission
IETF – Internet Engineering Task Force
IMAP – Internet Message Access Protocol
IoC – Indicator of Compromise
IoT – Internet of Things
IP – Internet Protocol
IPS – Intrusion Prevention System
IPsec – Internet Protocol Security
ISMS – Information Security Management System
ISO – International Organization for Standardization
ISP – Internet Service Provider
IT – Information Technology
ITIL – Information Technology Infrastructure Library
KPI – Key Performance Indicator
KVM – Kernel-based Virtual Machine
LAN – Local Area Network
LDAP – Lightweight Directory Access Protocol
MAC – Media Access Control
MD5 – Message Digest Algorithm 5
MFA – Multi-Factor Authentication
MITM – Man-in-the-Middle
NAC – Network Access Control

NAT – Network Address Translation

NDR – Network Detection and Response

NIS2 – Network and Information Security Directive 2

NIST – National Institute of Standards and Technology

OSI – Open Systems Interconnection

OT – Operational Technology

OWASP – Open Web Application Security Project

PaaS – Platform as a Service

PCI-DSS – Payment Card Industry Data Security Standard

PKI – Public Key Infrastructure

PoC – Proof of Concept

QoS – Quality of Service

RADIUS – Remote Authentication Dial-In User Service

RAM – Random Access Memory

RBAC – Role-Based Access Control

RFC – Request for Comments

RPO – Recovery Point Objective

RTO – Recovery Time Objective

SaaS – Software as a Service

SAML – Security Assertion Markup Language

SCADA – Supervisory Control and Data Acquisition

SDN – Software Defined Networking

SIEM – Security Information and Event Management

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Management Protocol

SOC – Security Operations Center

SOAR – Security Orchestration, Automation and Response

SQL – Structured Query Language

SSH – Secure Shell

SSL – Secure Sockets Layer

TCP – Transmission Control Protocol

TLS – Transport Layer Security

TPM – Trusted Platform Module

UDP – User Datagram Protocol

URL – Uniform Resource Locator

USB – Universal Serial Bus

VLAN – Virtual Local Area Network

VM – Virtual Machine

VPN – Virtual Private Network

WAN – Wide Area Network

WAF – Web Application Firewall

WLAN – Wireless Local Area Network

XDR – Extended Detection and Response

XSS – Cross-Site Scripting

ZTNA – Zero Trust Network Access

1 ΚΕΦΑΛΑΙΟ 1 – ΕΙΣΑΓΩΓΗ

1.1 Γενικά

Η ασφάλεια δικτύων αποτελεί βασικό μηχανισμό προστασίας των πληροφοριακών υποδομών ενός οργανισμού, καθώς ρυθμίζει και ελέγχει τη ροή της δικτυακής επικοινωνίας μεταξύ εσωτερικών συστημάτων και εξωτερικών δικτύων. Η προστασία των πληροφοριακών συστημάτων και των δικτυακών επικοινωνιών συνδέεται άμεσα με τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών, αρχές που αποτελούν τον πυρήνα των σύγχρονων προτύπων ασφάλειας πληροφοριών (Whitman & Mattord, 2021; Stallings, 2018).

Η αυξανόμενη εξάρτηση των επιχειρήσεων από ψηφιακές υπηρεσίες, υποδομές υπολογιστικού νέφους (cloud infrastructures), μηχανισμούς απομακρυσμένης πρόσβασης και διασυνδεδεμένα πληροφοριακά συστήματα έχει οδηγήσει σε σημαντική ενίσχυση της επιχειρησιακής αποδοτικότητας και της λειτουργικής ευελιξίας. Ωστόσο, η εξέλιξη αυτή συνοδεύεται από σημαντική αύξηση της πολυπλοκότητας των δικτυακών υποδομών και από διεύρυνση της επιφάνειας επίθεσης (attack surface), γεγονός που εντείνει τις απαιτήσεις προστασίας των πληροφοριακών πόρων (ENISA, 2023; Verizon, 2023)

Στο πλαίσιο αυτό, τα τείχη προστασίας (firewalls) αποτελούν θεμελιώδη μηχανισμό ελέγχου και προστασίας της δικτυακής επικοινωνίας, λειτουργώντας ως ο κύριος μηχανισμός επιβολής πολιτικών ασφάλειας μεταξύ διακριτών ζωνών εμπιστοσύνης (trust zones). Μέσω της φιλτραρισμένης διαχείρισης της εισερχόμενης και εξερχόμενης κίνησης, τα firewalls λειτουργούν ως μηχανισμοί μετάφρασης των υψηλού επιπέδου απαιτήσεων ασφάλειας ενός οργανισμού σε τεχνικά εκτελέσιμους κανόνες πρόσβασης (security rules), αποτελώντας βασικό σημείο επιβολής πολιτικών ασφάλειας στο δίκτυο (Scarfone & Mell, 2007; Stallings, 2018).

Παρά τη διαθεσιμότητα ώριμων και τεχνολογικά εξελιγμένων firewall πλατφορμών, η αποτελεσματικότητα της δικτυακής ασφάλειας δεν εξαρτάται αποκλειστικά από τις τεχνικές δυνατότητες του εκάστοτε εργαλείου, αλλά σε μεγάλο βαθμό από τον τρόπο με τον οποίο αυτό σχεδιάζεται, παραμετροποιείται και διαχειρίζεται κατά τη διάρκεια του κύκλου ζωής του. Η έννοια της διαχείρισης κύκλου ζωής των κανόνων firewall (firewall rule lifecycle management), από τη δημιουργία και τεκμηρίωση έως την αναθεώρηση και την απόσυρσή τους, αποκτά

ιδιαίτερη σημασία, καθώς οι κανόνες ασφάλειας εξελίσσονται παράλληλα με τις επιχειρησιακές ανάγκες και τις μεταβαλλόμενες απειλές (Al-Shaer & Hamed, 2024).

Στα περιβάλλοντα των SMEs (Small and Medium-Sized Enterprises - SMEs), η διαχείριση των κανόνων firewall πραγματοποιείται συχνά χειροκίνητα, χωρίς τυποποιημένες διαδικασίες, επαρκή τεκμηρίωση ή συστηματικό έλεγχο αλλαγών (change management). Η απουσία δομημένων μεθοδολογιών διακυβέρνησης οδηγεί σε πρακτικές ad-hoc παραμετροποίησης, όπου οι κανόνες προστίθενται ή τροποποιούνται με γνώμονα άμεσες λειτουργικές απαιτήσεις και όχι βάσει στρατηγικού σχεδιασμού ασφάλειας.

Αποτέλεσμα των πρακτικών αυτών είναι η σταδιακή συσσώρευση πολύπλοκων, αλληλεπικαλυπτόμενων ή παρωχημένων ρυθμίσεων. Δημιουργούνται κανόνες χωρίς σαφή επιχειρησιακή τεκμηρίωση, παραμένουν ενεργές προσωρινές εξαιρέσεις, ενώ η έλλειψη περιοδικής αναθεώρησης οδηγεί στη διατήρηση μη αναγκαίων ανοιγμάτων επικοινωνίας. Το φαινόμενο αυτό, που περιγράφεται στη βιβλιογραφία ως rule sprawl ή policy entropy, αυξάνει την πολυπλοκότητα των πολιτικών ασφάλειας και ενδέχεται να οδηγήσει σε συγκρούσεις κανόνων, σκίαση κανόνων (rule shadowing) και κενά προστασίας (Scarfone & Mell, 2007).

Η κατάσταση αυτή ενισχύει τον κίνδυνο λαθών παραμετροποίησης (misconfigurations), τα οποία συγκαταλέγονται διεθνώς στις σημαντικότερες αιτίες περιστατικών παραβίασης ασφάλειας. Για παράδειγμα, μια συνηθισμένη αμέλεια στις SMEs είναι η έκθεση της θύρας 3389 (RDP - Remote Desktop Protocol) απευθείας στο διαδίκτυο χωρίς κανόνες περιορισμού IP (whitelisting) ή τη χρήση Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks – VPN) (CrowdStrike, 2022). Η συγκεκριμένη ευπάθεια καθιστά τα συστήματα ευάλωτα σε επιθέσεις εξάντλησης κωδικών (brute-force attacks), διευκολύνοντας την εγκατάσταση λυτρισμικού (ransomware), το οποίο κρυπτογραφεί τα δεδομένα της επιχείρησης προκαλώντας τεράστια οικονομική και λειτουργική ζημία. Η ορθή παραμετροποίηση ενός firewall μπορεί να περιορίσει σημαντικά την έκθεση τέτοιων υπηρεσιών, εφαρμόζοντας πολιτικές περιορισμού πρόσβασης, φιλτράροντας μη εξουσιοδοτημένη κίνηση και μειώνοντας την πιθανότητα επιτυχούς εκμετάλλευσης.

Η σημασία της ορθής διαχείρισης των πολιτικών firewall επιβεβαιώνεται και από περιστατικά κυβερνοεπιθέσεων που έχουν καταγραφεί σε SMEs. Σύμφωνα με αναλύσεις του τοπίου απειλών, η απευθείας έκθεση εσωτερικών υπηρεσιών στο διαδίκτυο απόρροια εσφαλμένων ρυθμίσεων στο τείχος προστασίας ή ελλιπούς τμηματοποίησης του δικτύου, συνιστά κύριο

φορέα επιτυχών επιθέσεων λυτρισμικού (ransomware) σε SMEs (Sophos, 2023; ENISA, 2023). Οι επιτιθέμενοι εκμεταλλεύτηκαν τις εσφαλμένες αυτές ρυθμίσεις για να αποκτήσουν αρχική πρόσβαση στο δίκτυο και στη συνέχεια να κινηθούν πλευρικά (lateral movement) προς άλλα συστήματα, εγκαθιστώντας κακόβουλο λογισμικό και προκαλώντας διακοπή λειτουργίας των πληροφοριακών συστημάτων της επιχείρησης. Σύμφωνα με διεθνείς αναφορές κυβερνοασφάλειας, οι SMEs αποτελούν ιδιαίτερα συχνό στόχο τέτοιων επιθέσεων, κυρίως λόγω περιορισμένων πόρων ασφάλειας και ελλιπών διαδικασιών διαχείρισης πολιτικών firewall (ENISA, 2023; Verizon, 2023).

Συνεπώς, το πρόβλημα της δικτυακής ασφάλειας στις SMEs συχνά δεν εντοπίζεται πρωτίστως στο επίπεδο της τεχνολογικής επάρκειας των firewalls, αλλά στον τρόπο οργάνωσης, διαχείρισης και ελέγχου της διαδικασίας δημιουργίας και συντήρησης των κανόνων ασφάλειας. Η απουσία αυτοματοποιημένων μηχανισμών, τυποποιημένων προτύπων παραμετροποίησης και ολοκληρωμένων διαδικασιών διακυβέρνησης καθιστά την πολιτική firewall ευάλωτη σε σφάλματα, ασυνέπειες και αποκλίσεις από τις επιχειρησιακές και κανονιστικές απαιτήσεις.

Υπό το πρίσμα αυτό, αναδεικνύεται η ανάγκη υιοθέτησης δομημένων προσεγγίσεων αυτοματοποίησης και τυποποίησης της διαχείρισης των πολιτικών firewall, οι οποίες να ευθυγραμμίζονται με τις αρχές διαχείρισης κινδύνου, ελέγχου αλλαγών και τεκμηρίωσης που προωθούν τα σύγχρονα πρότυπα ασφάλειας πληροφοριών (ISO/IEC 27001:2022). Η μετάβαση από αποσπασματικές χειροκίνητες πρακτικές σε μοντέλα συστηματοποιημένης διαχείρισης συνιστά κρίσιμο βήμα για την ενίσχυση της ανθεκτικότητας και της κανονιστικής συμμόρφωσης των SMEs.

1.2 Ορισμός του Προβλήματος (Problem Statement)

Παρά την ευρεία χρήση συστημάτων τείχους προστασίας (firewalls) για την προστασία δικτυακών υποδομών, πολλές μικρομεσαίες επιχειρήσεις (SMEs) αντιμετωπίζουν ουσιαστικές προκλήσεις στη διαχείριση και συντήρηση των κανόνων ασφάλειας του τείχους προστασίας (firewall rules). Στην πράξη, η παραμετροποίηση και η εξέλιξη των κανόνων πραγματοποιούνται συχνά χειροκίνητα, χωρίς επαρκώς τυποποιημένες διαδικασίες τεκμηρίωσης, αξιολόγησης κινδύνου και διαχείρισης αλλαγών (change management). Η απουσία τέτοιων δομημένων πρακτικών οδηγεί συχνά στη δημιουργία πολύπλοκων και αλληλοεπικαλυπτόμενων πολιτικών τείχους προστασίας (firewall policies), αυξάνοντας την

πιθανότητα λαθών παραμετροποίησης (misconfigurations) και μειώνοντας την αποτελεσματικότητα των μηχανισμών προστασίας (Scarfone & Mell, 2007· Whitman & Mattord, 2021).

Ένας επιπρόσθετος παράγοντας που επιβαρύνει το πρόβλημα σε περιβάλλοντα SMEs σχετίζεται με το λειτουργικό προφίλ του διαχειριστή της Τεχνολογία Πληροφοριών (Information Technology – IT). Σε πολλές SMEs, ο διαχειριστής συστημάτων (IT administrator) καλείται να καλύψει ταυτόχρονα πολλαπλούς ρόλους (π.χ. υποστήριξη χρηστών, λειτουργία δικτύου, συντήρηση εξυπηρετητών και βασικές λειτουργίες ασφάλειας), γεγονός που περιορίζει τον διαθέσιμο χρόνο για συστηματικό σχεδιασμό και συνεχή αναθεώρηση των πολιτικών firewall. Ως αποτέλεσμα, η σωστή αρχική ρύθμιση, η ορθή ιεράρχηση των κανόνων και η τακτική αξιολόγηση των αλλαγών καθίστανται απαιτητικές διαδικασίες. Αυτό αυξάνει τον κίνδυνο λειτουργικών σφαλμάτων (όπως λανθασμένες διευθύνσεις IP, θύρες ή σειρά εφαρμογής κανόνων) και ενδέχεται να δημιουργήσει είτε διακοπές υπηρεσιών είτε κενά ασφαλείας που επιτρέπουν μη εξουσιοδοτημένη πρόσβαση (Scarfone & Mell, 2007· ENISA, 2023).

Παράλληλα, σε αρκετές περιπτώσεις παρατηρείται περιορισμένη εξοικείωση με διαθέσιμες λύσεις ανοικτού λογισμικού (open-source) που μπορούν να λειτουργήσουν ως ισχυρές πλατφόρμες δικτυακής προστασίας. Παρότι εργαλεία όπως το pfSense προσφέρουν ώριμες δυνατότητες διαχείρισης τείχους προστασίας, δρομολόγησης και πολιτικών πρόσβασης, η εγκατάσταση, η αρχική παραμετροποίηση και η συνεχής συντήρησή τους απαιτούν τεχνική επάρκεια σε δικτυακές έννοιες και πρακτικές ασφάλειας πληροφοριών. Σε οργανισμούς με περιορισμένους πόρους και χωρίς εξειδικευμένο προσωπικό κυβερνοασφάλειας, η αξιοποίηση τέτοιων λύσεων μπορεί να αποδειχθεί δύσκολη χωρίς υποστηρικτικές διαδικασίες τυποποίησης και αυτοματοποίησης, με αποτέλεσμα να παραμένουν είτε αναξιοποίητες είτε να λειτουργούν με ρυθμίσεις που δεν αντανακλούν πλήρως τις πραγματικές ανάγκες ασφάλειας (Whitman & Mattord, 2021· ENISA, 2023).

Η έλλειψη συστηματικής διαχείρισης των κανόνων ασφάλειας δυσκολεύει επιπλέον την παρακολούθηση, τον έλεγχο και την τεκμηρίωση των αλλαγών που πραγματοποιούνται στο τείχος προστασίας. Αυτό ευνοεί την εμφάνιση απόκλισης μεταξύ τεκμηριωμένης πολιτικής και πραγματικής διαμόρφωσης, φαινόμενο γνωστό ως απόκλιση διαμόρφωσης (configuration drift), το οποίο επηρεάζει τόσο την επιχειρησιακή ασφάλεια όσο και την ικανότητα ελέγχου και συμμόρφωσης (NIST, 2012). Η κατάσταση αυτή γίνεται ιδιαίτερα κρίσιμη όταν οι οργανισμοί

επιδιώκουν συμμόρφωση με πρότυπα διαχείρισης ασφάλειας πληροφοριών, όπως το ISO/IEC 27001, τα οποία απαιτούν τεκμηριωμένες διαδικασίες, ελεγχόμενες αλλαγές και επαληθεύσιμη εφαρμογή των μέτρων ασφάλειας (ISO, 2018).

Με βάση τα παραπάνω, προκύπτει η ανάγκη ανάπτυξης πιο δομημένων και αυτοματοποιημένων προσεγγίσεων για τη διαχείριση και παραμετροποίηση των κανόνων firewall. Η αυτοματοποίηση μπορεί να συμβάλει στη μείωση λαθών, στη βελτίωση της διαχειρισιμότητας των πολιτικών ασφάλειας, στην ενίσχυση της ιχνηλασιμότητας των αλλαγών και στη διευκόλυνση της συμμόρφωσης με σύγχρονα πλαίσια διακυβέρνησης ασφάλειας πληροφοριών (ISO, 2018· ENISA, 2023).

1.3 Σκοπός, Ερευνητικοί Στόχοι και Συμβολή της Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία έχει ως σκοπό τη μελέτη και ανάπτυξη ενός δομημένου πλαισίου διαχείρισης της δικτυακής ασφάλειας, προσαρμοσμένου αποκλειστικά στις ανάγκες και τους περιορισμούς των SMEs.

Για την επίτευξη αυτού του σκοπού, τίθενται οι ακόλουθοι επιμέρους ερευνητικοί στόχοι:

1. **Ανάλυση Κινδύνων:** Η διερεύνηση των λειτουργικών κινδύνων που απορρέουν από τη χειροκίνητη και μη συστηματική διαχείριση κανόνων firewall (misconfigurations, rule shadowing).
2. **Σχεδιασμός Αρχιτεκτονικής:** Η ανάπτυξη μιας πρότυπης αρχιτεκτονικής τμηματοποίησης (network segmentation) και «άμυνας σε βάθος» (defense-in-depth) με χρήση τεχνολογιών ανοικτού κώδικα (pfSense, Suricata, pfBlockerNG).
3. **Αυτοματοποίηση Διαδικασιών:** Η μετάβαση από τη χειροκίνητη παραμετροποίηση σε μια δομημένη προσέγγιση «Υποδομής ως Κώδικα» (IaC). Αυτό επιτυγχάνεται μέσω της ανάπτυξης ενός προτύπου υπολογιστικού φύλλου (Excel) που λειτουργεί ως Μοναδική Πηγή Αλήθειας (SSoT), και ενός μηχανισμού μετασχηματισμού (Python script) που παράγει αυτόματα τον κώδικα ρυθμίσεων (XML).
4. **Ευθυγράμμιση με Πρότυπα:** Η αξιολόγηση του βαθμού στον οποίο η αυτοματοποιημένη αυτή προσέγγιση διευκολύνει την κανονιστική συμμόρφωση με τις απαιτήσεις του προτύπου ISO/IEC 27001:2022 (έλεγχος αλλαγών, ιχνηλασιμότητα).

Η ερευνητική συμβολή της εργασίας έγκειται στην εμπειρική απόδειξη (μέσω εργαστηριακού Proof of Concept) ότι οι SMEs μπορούν να επιτύχουν υψηλό επίπεδο δικτυακής προστασίας και διακυβέρνησης, χωρίς την ανάγκη δαπανηρών εμπορικών λύσεων, αξιοποιώντας απλά, ευρέως κατανοητά εργαλεία.

Οι βασικοί ερευνητικοί στόχοι και η αναμενόμενη συμβολή της εργασίας συνοψίζονται στον Πίνακα 1-1.

Πίνακας 1-1: Ερευνητικοί Στόχοι και Συμβολή της Εργασίας

Ερευνητικός Στόχος	**Περιγραφή**	**Τεχνική Υλοποίηση**	**Αναμενόμενη Συμβολή**
Ανάλυση κινδύνων κακής διαχείρισης κανόνων firewall	Εντοπισμός πλεοναζόντων, επικαλυπτόμενων και μη τεκμηριωμένων κανόνων	Ανάλυση κινδύνων και διακυβέρνησης κανόνων	Κατανόηση της πολυπλοκότητας των πολιτικών firewall σε περιβάλλοντα SMEs
Σχεδιασμός πρότυπης αρχιτεκτονικής για SMEs	Τμηματοποίηση δικτύου LAN και διαχωρισμός ζωνών διαχείρισης	Τμηματοποίηση μέσω pfSense και Proxmox	Μείωση της πλευρικής κίνησης επιτιθέμενων και περιορισμός της έκθεσης σε κινδύνους
Αυτοματοποίηση διαχείρισης κανόνων και αντικειμένων πολιτικής	Μετάβαση από χειροκίνητη σε δομημένη διαχείριση κανόνων	Αυτοματοποιημένος μετασχηματισμός πολιτικών ασφαλείας μέσω Python script (Excel-to-XML parser) για απευθείας ενσωμάτωση στο pfSense configuration	Μείωση λανθασμένων παραμετροποιήσεων (misconfigurations) και αύξηση ιχνηλασιμότητας
Πρακτική αξιολόγηση αποτελεσματικότητας	Δοκιμές συνδεσιμότητας και αποκλεισμού κακόβουλης κίνησης	Σενάρια εργαστηριακής αξιολόγησης	Εμπειρική επιβεβαίωση της λειτουργικότητας της προτεινόμενης προσέγγισης

Ερευνητικός Στόχος	Περιγραφή	Τεχνική Υλοποίηση	Αναμενόμενη Συμβολή
Συμβολή στο πεδίο	Οικονομικά βιώσιμο πλαίσιο ασφάλειας ανοικτού κώδικα	pfSense, Suricata, pfBlockerNG	Εφαρμόσιμο μοντέλο διαχείρισης ασφάλειας για SMEs

1.4 Δομή της Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία οργανώνεται σε οκτώ βασικά κεφάλαια, τα οποία παρουσιάζουν σταδιακά το θεωρητικό υπόβαθρο, την ανάλυση του προβλήματος, τον σχεδιασμό της προτεινόμενης λύσης, την υλοποίηση και την πειραματική αξιολόγηση της.

Το Κεφάλαιο 1 (Εισαγωγή) παρουσιάζει το γενικό πλαίσιο της έρευνας, τον σκοπό και τους βασικούς ερευνητικούς στόχους της εργασίας, καθώς και τη συνολική δομή των κεφαλαίων που ακολουθούν. Στόχος του κεφαλαίου είναι η εισαγωγή στο ερευνητικό πρόβλημα και η θεμελίωση του επιστημονικού πλαισίου της εργασίας.

Στο Κεφάλαιο 2 (Θεωρητικό Υπόβαθρο) παρουσιάζονται οι βασικές αρχές της δικτυακής ασφάλειας, η λειτουργία των τειχών προστασίας (firewalls), καθώς και έννοιες που σχετίζονται με τη διαχείριση πολιτικών ασφάλειας, την αξιοποίηση πληροφοριών απειλών (Threat Intelligence) και τις ιδιαιτερότητες των SMEs. Το κεφάλαιο αυτό παρέχει τη θεωρητική βάση που είναι απαραίτητη για την κατανόηση της προτεινόμενης προσέγγισης.

Το Κεφάλαιο 3 (Ανάλυση Προβλήματος και Απαιτήσεων) επικεντρώνεται στην ανάλυση των προβλημάτων που προκύπτουν από τη χειροκίνητη διαχείριση κανόνων firewall, καθώς και στους κινδύνους που σχετίζονται με λανθασμένες ή μη βέλτιστες παραμετροποιήσεις. Παράλληλα, παρουσιάζεται το προφίλ του χρήστη–διαχειριστή, καθώς και οι λειτουργικές και μη λειτουργικές απαιτήσεις της προτεινόμενης λύσης.

Στο Κεφάλαιο 4 (Σχεδίαση Προτεινόμενης Λύσης) παρουσιάζεται ο αρχιτεκτονικός σχεδιασμός της λύσης, η μοντελοποίηση της πολιτικής ασφάλειας και η ανάπτυξη του προτύπου Excel που χρησιμοποιείται για τον ορισμό και τη διαχείριση των κανόνων firewall. Επιπλέον, αναλύεται η διαδικασία χαρτογράφησης των πεδίων του Excel σε τεχνικές παραμέτρους του firewall και η ενσωμάτωση μηχανισμών Threat Intelligence.

Το Κεφάλαιο 5 (Εργαστηριακή Υλοποίηση) περιγράφει την πρακτική υλοποίηση της προτεινόμενης αρχιτεκτονικής σε εργαστηριακό περιβάλλον (Proof of Concept). Συγκεκριμένα παρουσιάζεται η υποδομή του firewall, η δομή του σταθμού διαχείρισης, η δημιουργία και χρήση του Excel template, καθώς και η διαδικασία εισαγωγής των κανόνων στο pfSense και η ενσωμάτωση μηχανισμών Threat Intelligence.

Στο Κεφάλαιο 6 (Πειραματικά Σενάρια και Αξιολόγηση) εξετάζονται τα σενάρια δοκιμών που χρησιμοποιήθηκαν για την αξιολόγηση της προτεινόμενης προσέγγισης, καθώς και τα κριτήρια αξιολόγησης. Περιλαμβάνονται δοκιμές επικύρωσης της πολιτικής firewall, πειραματικά σενάρια ελέγχου κανόνων και αξιολόγηση των μηχανισμών Threat Intelligence μέσω των εργαλείων pfBlockerNG και Suricata, καθώς και συγκριτική προσέγγιση με τη χειροκίνητη διαχείριση κανόνων.

Το Κεφάλαιο 7 (Συζήτηση και Αξιολόγηση Αποτελεσμάτων) παρουσιάζει τη συζήτηση και την ερμηνεία των αποτελεσμάτων που προέκυψαν από τα πειραματικά σενάρια. Επιπλέον, εξετάζονται οι περιορισμοί της έρευνας και οι παράγοντες που επηρεάζουν την εφαρμογή της προτεινόμενης προσέγγισης.

Τέλος, το Κεφάλαιο 8 (Συμπεράσματα και Μελλοντική Έρευνα) συνοψίζει τα βασικά ευρήματα της εργασίας και παρουσιάζει προτάσεις για μελλοντική έρευνα, αναδεικνύοντας τη συμβολή της προτεινόμενης προσέγγισης στη βελτίωση της διαχείρισης πολιτικών ασφάλειας σε περιβάλλοντα SMEs.

2 ΚΕΦΑΛΑΙΟ 2 – ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

2.1 Firewalls και Έλεγχος Δικτυακής Πρόσβασης

Η διαχείριση κανόνων firewall και η αποτροπή απειλών αποτελούν διαρκές αντικείμενο μελέτης, καθώς η πολυπλοκότητα των πολιτικών ασφάλειας αυξάνεται εκθετικά. Ενώ παλαιότερες έρευνες (Al-Shaer & Hamed, 2004; Wool, 2004) εστίαζαν κυρίως στη χειροκίνητη ανάλυση και τον εντοπισμό συγκρούσεων μεταξύ κανόνων (rule conflicts), η σύγχρονη βιβλιογραφία έχει στραφεί στην αυτοματοποίηση, τη χρήση Threat Intelligence και την ενσωμάτωση ανοικτού λογισμικού σε SMEs.

Στον τομέα της ανοικτής αρχιτεκτονικής, πρόσφατες έρευνες υπογραμμίζουν την αποτελεσματικότητα συνδυαστικών λύσεων. Για παράδειγμα, οι Praptodiyono et al. (2023) προτείνουν ένα υβριδικό σύστημα ανίχνευσης εισβολών βασισμένο στο Suricata σε συνδυασμό με το τείχος προστασίας pfSense. Η μελέτη τους κατέδειξε ότι η εν λόγω συνέργεια οδήγησε σε σημαντική μείωση της χρήσης της Κεντρικής Μονάδας Επεξεργασίας (CPU) και σε τεράστια μείωση της καθυστέρησης δικτύου (network latency), παρέχοντας ταυτόχρονα ισχυρή προστασία έναντι επιθέσεων DDoS (Distributed Denial of Service), γεγονός που καθιστά τέτοιες λύσεις ιδανικές για υποδομές με περιορισμένους πόρους.

Επιπρόσθετα, η ενσωμάτωση λιστών φήμης (IP Reputation / Threat Intelligence) στην περίμετρο του δικτύου αποτελεί κυρίαρχο ερευνητικό θέμα. Σε σχετική μελέτη αξιολόγησης απόδοσης, οι Raharjo και Nurmala (2022) ανέλυσαν πώς ο αριθμός των ενεργών κανόνων IP Reputation στο Suricata επηρεάζει το ποσοστό απόρριψης πακέτων (packet drop percentage). Τα ευρήματά τους αποδεικνύουν την αναγκαιότητα ορθολογικής διαχείρισης και αυτοματοποίησης των λίστων αποκλεισμού (blocklists) (όπως αυτές που παρέχονται μέσω του pfBlockerNG), ώστε να αποφεύγεται η υπερφόρτωση του συστήματος ανίχνευσης και η δημιουργία μεγάλου αριθμού ειδοποιήσεων (alert fatigue).

Τέλος, η πρόκληση της λανθασμένης παραμετροποίησης (misconfiguration) παραμένει η κύρια αιτία παραβίασης δικτύων (ENISA, 2023). Στο πλαίσιο αυτό, η σύγχρονη τάση κατευθύνεται προς την πρακτική του «Υποδομή ως Κώδικας» (Infrastructure as Code - IaC) και τον προγραμματιστικό ορισμό των πολιτικών. Η προσέγγιση αυτή, η οποία υιοθετείται και στην παρούσα διπλωματική εργασία μέσω της μετατροπής ενός προτύπου Excel σε κώδικα για το

pfSense, μετατοπίζει την έμφαση από τη χειροκίνητη ανάλυση και διόρθωση σφαλμάτων προς την αυτοματοποιημένη ανάπτυξη και διαχείριση πολιτικών ασφάλειας.

2.2 Ασφάλεια βάσει πολιτικών (Policy-Based Security) και Διαχείριση Κανόνων

Η ασφάλεια βάσει πολιτικών (policy-based security) αποτελεί βασική αρχή διαχείρισης της κυβερνοασφάλειας, σύμφωνα με την οποία οι τεχνικοί μηχανισμοί προστασίας υλοποιούνται βάσει καθορισμένων πολιτικών ασφάλειας και επιχειρησιακών απαιτήσεων (ISO, 2022). Στην περίπτωση των firewalls, οι πολιτικές αυτές μετατρέπονται σε τεχνικούς κανόνες που καθορίζουν ποια δικτυακή επικοινωνία επιτρέπεται ή απορρίπτεται.

Η υλοποίηση της πολιτικής ασφάλειας πραγματοποιείται συνήθως μέσω λιστών ελέγχου πρόσβασης (Access Control Lists – ACLs), οι οποίες αποτελούνται από διατεταγμένες σειρές κανόνων που βασίζονται σε παραμέτρους όπως διευθύνσεις IP, πρωτόκολλα και θύρες επικοινωνίας. Μια θεμελιώδης αρχή στον σχεδιασμό αυτών των πολιτικών είναι η αρχή των ελαχίστων προνομίων (principle of least privilege), σύμφωνα με την οποία κάθε σύστημα ή υπηρεσία πρέπει να διαθέτει μόνο τα απαραίτητα δικαιώματα επικοινωνίας για τη λειτουργία του (Whitman & Mattord, 2021).

Στην πράξη, πολλές πολιτικές firewall βασίζονται στην προσέγγιση «προεπιλεγμένη απόρριψη» (default deny), όπου κάθε μορφή κίνησης απορρίπτεται εκτός εάν επιτρέπεται ρητά από συγκεκριμένο κανόνα. Ωστόσο, η διαχείριση μεγάλου αριθμού κανόνων μπορεί να δημιουργήσει προβλήματα πολυπλοκότητας, όπως σκίαση κανόνων (rule shadowing), συγκρούσεις κανόνων (rule conflicts) και πλεονάζοντες κανόνες (rule redundancies), τα οποία δυσκολεύουν τη διαχείριση και την κατανόηση της πολιτικής ασφάλειας (NIST, 2009).

Για τον λόγο αυτό χρησιμοποιούνται τεχνικές όπως η αντικειμενοστραφής μοντελοποίηση πολιτικών, μέσω της οποίας ομάδες διευθύνσεων ή υπηρεσιών αναπαρίστανται ως λογικά αντικείμενα ή ψευδώνυμα (aliases). Η προσέγγιση αυτή συμβάλλει στη μείωση της πολυπλοκότητας και στη βελτίωση της διαχείρισης των κανόνων firewall.

2.3 Τείχη προστασίας ανοικτού κώδικα (Open-Source Firewalls) και pfSense

Η αγορά συστημάτων δικτυακής ασφάλειας κυριαρχείται παραδοσιακά από εμπορικές λύσεις (commercial solutions), οι οποίες προσφέρουν ολοκληρωμένες δυνατότητες προστασίας αλλά συνοδεύονται συχνά από υψηλό κόστος αδειοδότησης και συντήρησης. Για πολλές SMEs, το κόστος αυτό μπορεί να αποτελεί σημαντικό εμπόδιο στην υιοθέτηση προηγμένων λύσεων ασφάλειας.

Ως εναλλακτική επιλογή, τα λογισμικά ανοιχτού κώδικα (open-source software) έχουν αποκτήσει σημαντική θέση στον τομέα της κυβερνοασφάλειας. Η διαθεσιμότητα του πηγαίου κώδικα επιτρέπει τον ανεξάρτητο έλεγχο της υλοποίησης και ενισχύει τη διαφάνεια των μηχανισμών ασφάλειας (Anderson, 2020).

Ο Πίνακας 2-1 παρουσιάζει μια συνοπτική σύγκριση μεταξύ εμπορικών και ανοικτού κώδικα λύσεων firewall.

Πίνακας 2-1: Σύγκριση Proprietary και Open-source Firewall Λύσεων

Κριτήριο	**Proprietary Firewalls**	**Open-source Firewalls**
Κόστος Απόκτησης	Υψηλό	Χαμηλό / Μηδενικό
Κόστος Αδειοδότησης	Επαναλαμβανόμενο	Μηδενικό
Εξάρτηση από Προμηθευτή (Vendor Lock-in)	Υψηλό	Χαμηλό
Διαφάνεια Κώδικα	Κλειστή αρχιτεκτονική	Πλήρης διαφάνεια
Προσαρμοστικότητα	Περιορισμένη	Υψηλή
Υποστήριξη	Εμπορική	Υποστήριξη Κοινότητας & προαιρετική εμπορική υποστήριξη

Στο πλαίσιο των open-source λύσεων, το pfSense αποτελεί μία από τις πιο διαδεδομένες πλατφόρμες firewall και δρομολόγησης. Βασίζεται στο λειτουργικό σύστημα FreeBSD και αξιοποιεί τον μηχανισμό φιλτραρίσματος πακέτων PF (Packet Filter), ο οποίος είναι γνωστός για την αποδοτικότητα και την ασφάλειά του.

Το pfSense μπορεί να εγκατασταθεί τόσο σε φυσικό εξοπλισμό όσο και σε εικονικές μηχανές, μετατρέποντας ένα σύστημα σε ολοκληρωμένη συσκευή δικτυακής ασφάλειας. Μεταξύ των βασικών δυνατοτήτων του περιλαμβάνονται VPN, εξισορρόπηση φορτίου (load balancing), διαχείριση εύρους ζώνης (traffic shaping) και αρχιτεκτονικές υψηλής διαθεσιμότητας (high availability).

Ένα βασικό χαρακτηριστικό της πλατφόρμας είναι η αρχιτεκτονική πακέτων (package-based architecture), η οποία επιτρέπει την εγκατάσταση πρόσθετων λειτουργιών ασφάλειας. Μέσω των πακέτων αυτών μπορούν να ενσωματωθούν συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems – IDS), μηχανισμοί φιλτραρίσματος κακόβουλων domains και εργαλεία αξιοποίησης πληροφοριών απειλών.

Η ευελιξία και η επεκτασιμότητα της πλατφόρμας καθιστούν το pfSense ιδιαίτερα κατάλληλο για την ανάπτυξη υποδομών ασφάλειας σε περιβάλλοντα SMEs.

2.4 Αυτοματοποίηση στη Δικτυακή Ασφάλεια

Η αυτοματοποίηση αποτελεί βασικό στοιχείο των σύγχρονων προσεγγίσεων διαχείρισης της κυβερνοασφάλειας, ιδιαίτερα σε περιβάλλοντα όπου η πολυπλοκότητα των δικτυακών υποδομών και ο μεγάλος αριθμός παραμέτρων καθιστούν τη χειροκίνητη διαχείριση δύσκολη και επιρρεπή σε σφάλματα (NIST, 2018). Η συνεχής επέκταση των δικτύων, η χρήση εικονικοποιημένων περιβαλλόντων και η αυξανόμενη δυναμική των απειλών απαιτούν πιο ευέλικτους και επαναλήψιμους μηχανισμούς διαχείρισης.

Στο πλαίσιο της δικτυακής ασφάλειας, η αυτοματοποίηση εφαρμόζεται κυρίως στη διαχείριση των πολιτικών firewall και των ACLs. Μέσω αυτοματοποιημένων διαδικασιών μπορούν να δημιουργούνται, να τροποποιούνται ή να αφαιρούνται κανόνες φιλτραρίσματος με βάση προκαθορισμένα πρότυπα. Με τον τρόπο αυτό μειώνεται η εξάρτηση από χειροκίνητες παρεμβάσεις και βελτιώνεται η συνέπεια των ρυθμίσεων.

Ένα από τα βασικά πλεονεκτήματα της αυτοματοποίησης είναι η μείωση ανθρώπινων λαθών (human errors), τα οποία αποτελούν σημαντικό παράγοντα δημιουργίας ευπαθειών σε συστήματα ασφάλειας. Η χρήση τυποποιημένων προτύπων κανόνων επιτρέπει την επαναλαμβανόμενη εφαρμογή πολιτικών με συνεπή τρόπο, περιορίζοντας την πιθανότητα λανθασμένων ρυθμίσεων (NIST, 2018).

Παράλληλα, η αυτοματοποίηση συμβάλλει στην καλύτερη τεκμηρίωση και ιχνηλασιμότητα των αλλαγών. Μέσω μηχανισμών καταγραφής ενεργειών (logging) και διαχείρισης εκδόσεων πολιτικών (policy versioning), είναι δυνατή η παρακολούθηση των αλλαγών που πραγματοποιούνται στους κανόνες ασφάλειας. Η δυνατότητα αυτή είναι ιδιαίτερα σημαντική για την απόδειξη συμμόρφωσης με πρότυπα διαχείρισης ασφάλειας πληροφοριών, όπως το ISO/IEC 27001 (ISO, 2022).

Επιπλέον, η αυτοματοποίηση μπορεί να υποστηρίξει διαδικασίες ελέγχου εγκυρότητας πολιτικών (policy validation). Πριν από την εφαρμογή νέων κανόνων σε ένα firewall, είναι δυνατό να πραγματοποιηθούν δοκιμές που ελέγχουν πιθανές συγκρούσεις κανόνων ή σφάλματα παραμετροποίησης. Με τον τρόπο αυτό μειώνεται ο κίνδυνος διακοπής υπηρεσιών ή δημιουργίας κενών ασφάλειας.

Ωστόσο, η αυτοματοποίηση δεν αντικαθιστά τον σωστό σχεδιασμό πολιτικών ασφάλειας. Αν οι αρχικές πολιτικές είναι λανθασμένες ή ασαφείς, η αυτοματοποίηση μπορεί να αναπαράγει τα ίδια προβλήματα σε μεγαλύτερη κλίμακα. Για τον λόγο αυτό απαιτείται συνδυασμός αυτοματοποιημένων μηχανισμών με διαδικασίες ελέγχου αλλαγών και διακυβέρνησης πολιτικών ασφάλειας (ISO, 2022).

Ο Πίνακας 2-2 παρουσιάζει βασικά επίπεδα αυτοματοποίησης στη διαχείριση πολιτικών τείχους προστασίας (firewall policies), καθώς και τα αντίστοιχα επιχειρησιακά οφέλη που προκύπτουν από την εφαρμογή τους σε περιβάλλοντα SMEs.

Πίνακας 2-2: Επίπεδα και Επιπτώσεις Αυτοματοποίησης στη Διαχείριση Firewall Policies

Επίπεδο Αυτοματοποίησης	**Περιγραφή**	**Επιχειρησιακό Όφελος**	**Σχέση με τη Διπλωματική**
Αυτοματοποίηση δημιουργίας κανόνων (Rule Creation Automation)	Δομημένη δημιουργία κανόνων βάσει προτύπων	Μείωση λαθών παραμετροποίησης	Αυτοματοποιημένος μετασχηματισμός πολιτικών μέσω Python script (Excel-to-XML) και επικύρωση κανόνων.

Επίπεδο Αυτοματοποίησης	Περιγραφή	Επιχειρησιακό Όφελος	Σχέση με τη Διπλωματική
Διαχείριση αντικειμένων και Aliases (Object & Alias Management)	Κεντρική διαχείριση λογικών οντοτήτων	Συνοχή πολιτικής	Δομημένη μοντελοποίηση αντικειμένων (Structured object modeling)
Έκδοση και ιστορικό πολιτικών (Policy Versioning)	Καταγραφή εκδόσεων και αλλαγών πολιτικών	Ιχνηλασιμότητα αλλαγών	Λογική διακυβέρνησης αλλαγών (Change governance logic)
Αυτοματοποιημένη επικύρωση κανόνων (Automated Validation)	Προέλεγχος κανόνων πριν την εφαρμογή τους	Πρόληψη λανθασμένων παραμετροποιήσεων (misconfigurations)	Μηχανισμοί επικύρωσης κανόνων (Rule validation checks)
Threat Intelligence Integration	Δυναμική ενημέρωση λιστών κακόβουλων διευθύνσεων	Ταχύτερη απόκριση σε απειλές	Ενσωμάτωση pfBlockerNG (pfBlockerNG integration)

Συνεπώς, η αυτοματοποίηση στη δικτυακή ασφάλεια συμβάλλει στη δημιουργία πιο διαχειρίσιμων και ανθεκτικών υποδομών, επιτρέποντας στους οργανισμούς να εφαρμόζουν πολιτικές ασφάλειας με μεγαλύτερη συνέπεια και ταχύτητα.

2.5 Βιβλιογραφική Ανασκόπηση

Η διαχείριση κανόνων firewall αποτελεί αντικείμενο μελέτης στη βιβλιογραφία της ασφάλειας δικτύων, καθώς η πολυπλοκότητα των πολιτικών ασφάλειας αυξάνεται σημαντικά όσο μεγαλώνει το μέγεθος και η πολυπλοκότητα ενός δικτύου. Έρευνες έχουν δείξει ότι ένα σημαντικό ποσοστό των firewalls περιέχει σφάλματα παραμετροποίησης, τα οποία μπορεί να οδηγήσουν είτε σε μη εξουσιοδοτημένη πρόσβαση είτε σε μη απαραίτητους περιορισμούς στη δικτυακή επικοινωνία (Wool, 2004).

Στο πλαίσιο αυτό, αρκετές ερευνητικές εργασίες έχουν προτείνει μεθόδους για την ανάλυση και τη διαχείριση πολιτικών firewall με στόχο τον εντοπισμό συγκρούσεων και ασυνεπειών μεταξύ κανόνων. Η εργασία των Al-Shaer και Hamed (2004) παρουσίασε ένα μοντέλο ανάλυσης πολιτικών firewall το οποίο επιτρέπει τον εντοπισμό συγκρουόμενων κανόνων και την κατηγοριοποίηση διαφορετικών τύπων ανωμαλιών που μπορεί να εμφανιστούν σε σύνολα κανόνων firewall.

Επιπλέον, εργαλεία ανάλυσης πολιτικών firewall έχουν αναπτυχθεί για την αυτοματοποιημένη ανίχνευση λαθών σε μεγάλες πολιτικές ασφάλειας. Ένα χαρακτηριστικό παράδειγμα αποτελεί το εργαλείο Fireman, το οποίο επιτρέπει τη μοντελοποίηση και ανάλυση κανόνων firewall με στόχο τον εντοπισμό προβλημάτων πολιτικής ασφάλειας πριν από την εφαρμογή τους στο σύστημα (Yuan et al., 2006).

Παρότι οι παραπάνω ερευνητικές προσεγγίσεις συμβάλλουν σημαντικά στην κατανόηση της πολυπλοκότητας των πολιτικών firewall, πολλές από αυτές επικεντρώνονται κυρίως στην ανάλυση υπαρχόντων κανόνων και όχι στη διαδικασία δημιουργίας και διαχείρισης των πολιτικών με δομημένο τρόπο. Επιπλέον, αρκετές λύσεις απευθύνονται κυρίως σε μεγάλα εταιρικά περιβάλλοντα με εξειδικευμένα εργαλεία διαχείρισης.

Αντίθετα, οι SMEs συχνά αντιμετωπίζουν περιορισμούς σε πόρους και εξειδίκευση σε θέματα κυβερνοασφάλειας. Στο πλαίσιο αυτό, η παρούσα εργασία προτείνει μια πρακτική προσέγγιση για τη διαχείριση πολιτικών firewall βασισμένη σε τεχνολογίες ανοικτού λογισμικού και σε μια δομημένη διαδικασία ορισμού κανόνων μέσω ενός προτύπου Excel. Η προσέγγιση αυτή στοχεύει στη μείωση της πολυπλοκότητας της διαχείρισης κανόνων firewall και στην ενίσχυση της τεκμηρίωσης και της ιχνηλασιμότητας των πολιτικών ασφάλειας σε περιβάλλοντα SMEs.

2.6 Threat Intelligence σε επίπεδο περιμέτρου δικτύου

Το Threat Intelligence αποτελεί βασικό στοιχείο των σύγχρονων στρατηγικών κυβερνοασφάλειας. Ο όρος αναφέρεται στη συλλογή, επεξεργασία και ανάλυση δεδομένων που σχετίζονται με πιθανές ή ενεργές κυβερνοεπιθέσεις, με στόχο τη βελτίωση της πρόληψης και της ανίχνευσης απειλών (ENISA, 2023).

Παραδοσιακά, τα firewalls λειτουργούσαν κυρίως με στατικούς κανόνες φιλτραρίσματος. Ωστόσο, το σύγχρονο απειλητικό τοπίο χαρακτηρίζεται από υψηλή δυναμικότητα. Οι

επιτιθέμενοι χρησιμοποιούν συνεχώς μεταβαλλόμενες διευθύνσεις IP, υποδομές botnet και δυναμικές υπηρεσίες cloud για τη διεξαγωγή επιθέσεων. Αυτό καθιστά απαραίτητη τη χρήση ενημερωμένων πληροφοριών απειλών.

Η ενσωμάτωση Threat Intelligence σε firewalls επιτρέπει την προληπτική αποτροπή επικοινωνίας με κακόβουλες υποδομές. Μέσω δυναμικών λιστών αποκλεισμού (blocklists), το firewall μπορεί να απορρίπτει αυτόματα συνδέσεις προς γνωστές κακόβουλες διευθύνσεις IP ή domains (ENISA, 2023).

Οι λίστες αυτές περιλαμβάνουν συχνά δείκτες παραβίασης (Indicators of Compromise – IoCs), όπως:

- κακόβουλες διευθύνσεις IP
- κακόβουλα domains
- URLs phishing
- υποδομές command-and-control (C2)

Μια σημαντική τεχνική που χρησιμοποιείται σε αυτό το πλαίσιο είναι το DNS blackholing γνωστό και ως DNS-based blocking lists (DNSBL). Η τεχνική αυτή λειτουργεί στο επίπεδο DNS. Όταν ένας χρήστης προσπαθήσει να επισκεφθεί ένα κακόβουλο domain, το αίτημα DNS απορρίπτεται ή ανακατευθύνεται σε ειδικό σύστημα (sinkhole), αποτρέποντας την επικοινωνία με τον κακόβουλο εξυπηρετητή.

Η αποτελεσματικότητα της μεθόδου έγκειται στο γεγονός ότι η απειλή αντιμετωπίζεται πριν ακόμη δημιουργηθεί πραγματική σύνδεση μεταξύ πελάτη και εξυπηρετητή. Με τον τρόπο αυτό παρέχεται ένα επιπλέον επίπεδο προστασίας πέρα από το απλό φιλτράρισμα διευθύνσεων IP.

Ο Πίνακας 2-3 παρουσιάζει βασικές τεχνικές ενσωμάτωσης Threat Intelligence σε firewalls περιμέτρου.

Πίνακας 2-3: Τεχνικές Ενσωμάτωσης Threat Intelligence σε Firewall Περιμέτρου

Τεχνική	**Επίπεδο OSI**	**Τύπος Δεδομένων**	**Πλεονέκτημα**	**Περιορισμός**
IP Blocklists	L3	Κακόβουλες διευθύνσεις IP	Απλή υλοποίηση και χαμηλή υπολογιστική επιβάρυνση	Εύκολη αλλαγή IP από επιτιθέμενο

Τεχνική	Επίπεδο OSI	Τύπος Δεδομένων	Πλεονέκτημα	Περιορισμός
Network Blocking (CIDR)	L3	Κακόβουλα δίκτυα	Ευρύτερη κάλυψη	Πιθανό overblocking νόμιμων δικτύων
DNSBL	L7	Κακόβουλα domains	Αποτροπή σύνδεσης πριν την εγκαθίδρυση επικοινωνίας	Εξάρτηση από την υπηρεσία DNS
URL Filtering	L7	Κακόβουλα URL	Υψηλότερη ακρίβεια στον αποκλεισμό κακόβουλων πόρων	Απαιτεί βαθιά επιθεώρηση πακέτων (Deep Packet Inspection – DPI)
Sinkholing	L7	Ανακατεύθυνση κακόβουλων domain names	Δυνατότητα παρακολούθησης κακόβουλης κίνησης	Αυξημένη διαχειριστική πολυπλοκότητα

Όπως φαίνεται από τον Πίνακα 2-3, οι τεχνικές που βασίζονται σε λίστες αποκλεισμού διευθύνσεων IP (IP blocklists) και network blocking προσφέρουν απλή και αποδοτική προστασία σε επίπεδο δικτύου, ενώ οι τεχνικές επιπέδου εφαρμογής, όπως DNSBL και URL filtering, παρέχουν μεγαλύτερη ακρίβεια στον εντοπισμό κακόβουλων πόρων αλλά ενδέχεται να απαιτούν περισσότερους υπολογιστικούς πόρους ή εξάρτηση από εξωτερικές υπηρεσίες.

Η αξιοποίηση πολλαπλών πηγών Threat Intelligence, όπως κοινοτικές βάσεις δεδομένων και εμπορικά feeds, επιτρέπει τη δημιουργία ενός πιο δυναμικού και προσαρμοστικού συστήματος άμυνας (ENISA, 2023).

2.7 Ιδιαιτερότητες και Ανάγκες SMEs

Οι SMEs αντιμετωπίζουν ιδιαίτερες προκλήσεις στον τομέα της κυβερνοασφάλειας, καθώς καλούνται να προστατεύσουν κρίσιμα εταιρικά δεδομένα με περιορισμένους οικονομικούς και ανθρώπινους πόρους (ENISA, 2023).

Οι περιορισμοί αυτοί δημιουργούν σημαντικές προκλήσεις για την εφαρμογή αποτελεσματικών μέτρων προστασίας. Συχνά, οι λύσεις ασφάλειας πρέπει να ισορροπούν μεταξύ

λειτουργικότητας, κόστους και διαχειρισιμότητας. Πολύπλοκα συστήματα που απαιτούν συνεχή παρακολούθηση ή εξειδικευμένες γνώσεις ενδέχεται να μην αξιοποιούνται σωστά.

Σε αυτό το πλαίσιο, οι επιθέσεις όπως ransomware, phishing και malware αποτελούν σημαντική απειλή για τις SMEs. Η έλλειψη επαρκών μηχανισμών προστασίας μπορεί να οδηγήσει σε απώλεια δεδομένων, διακοπή λειτουργίας ή οικονομικές ζημιές.

Η χρήση τεχνολογιών όπως το pfSense σε συνδυασμό με αυτοματοποιημένες διαδικασίες διαχείρισης μπορεί να προσφέρει μια αποτελεσματική λύση. Μέσω τέτοιων συστημάτων, οι SMEs μπορούν να υλοποιήσουν λειτουργίες όπως:

- VPN για απομακρυσμένη πρόσβαση
- τμηματοποίηση δικτύου (VLANs) για διαχωρισμό υπηρεσιών
- φιλτράρισμα κακόβουλης κίνησης
- αξιοποίηση Threat Intelligence

Η αυτοματοποίηση της διαχείρισης κανόνων και η χρήση δυναμικών λιστών αποκλεισμού μειώνουν σημαντικά τον φόρτο συντήρησης των συστημάτων ασφάλειας. Με τον τρόπο αυτό ακόμη και μικρές ομάδες πληροφορικής μπορούν να διατηρήσουν ένα ικανοποιητικό επίπεδο προστασίας.

Συνεπώς, η αξιοποίηση οικονομικά βιώσιμων και ευέλικτων λύσεων ασφάλειας αποτελεί κρίσιμο παράγοντα για την προστασία των υποδομών SMEs.

3 ΚΕΦΑΛΑΙΟ 3 – ΑΝΑΛΥΣΗ ΠΡΟΒΛΗΜΑΤΟΣ ΚΑΙ ΑΠΑΙΤΗΣΕΩΝ

3.1 Το πρόβλημα της χειροκίνητης διαχείρισης firewall rules

Η διαχείριση των κανόνων σε συστήματα firewalls αποτελεί μία από τις κρισιμότερες λειτουργίες για τη διασφάλιση της δικτυακής ασφάλειας, καθώς οι κανόνες αυτοί υλοποιούν στην πράξη την πολιτική ελέγχου πρόσβασης ενός οργανισμού και καθορίζουν ποια δικτυακή κίνηση επιτρέπεται ή απορρίπτεται μεταξύ διαφορετικών ζωνών του δικτύου (Stallings, 2018). Οι κανόνες firewall αποτελούν το βασικό μηχανισμό επιβολής της πολιτικής ασφάλειας (security policy enforcement), επηρεάζοντας άμεσα την προστασία των πληροφοριακών συστημάτων και τη διαθεσιμότητα των δικτυακών υπηρεσιών.

Παρά τη διαθεσιμότητα γραφικών διεπαφών διαχείρισης, η δημιουργία, τροποποίηση και συντήρηση των κανόνων firewall παραμένει σε μεγάλο βαθμό μια διαδικασία που βασίζεται σε χειροκίνητη διαμόρφωση. Η χειροκίνητη παραμετροποίηση παρουσιάζει γραμμική κλιμάκωση δυσκολίας σε απλά δίκτυα, καθίσταται όμως απαγορευτική σε υποδομές με δυναμικές απαιτήσεις.

Στη βιβλιογραφία της κυβερνοασφάλειας, τέτοιου είδους προβλήματα εντάσσονται συχνά στην ευρύτερη κατηγορία των λανθασμένων παραμετροποιήσεων (misconfigurations), οι οποίες αναγνωρίζονται ως σημαντική αιτία περιστατικών ασφάλειας και λειτουργικών αστοχιών (ENISA, 2023). Ειδικότερα, η μη συστηματική διαχείριση πολιτικών firewall μπορεί να οδηγήσει σε φαινόμενα όπως η λανθασμένη ιεράρχηση κανόνων, η επικάλυψη ή σκίαση κανόνων (rule shadowing), η συσσώρευση παρωχημένων πολιτικών (policy sprawl), καθώς και η απόκλιση μεταξύ τεκμηριωμένης πολιτικής και πραγματικής διαμόρφωσης του συστήματος (configuration drift). Τα φαινόμενα αυτά δυσχεραίνουν τον έλεγχο, τη συντήρηση και τη συνολική διαχείριση της υποδομής ασφάλειας.

Ιδιαίτερα απαιτητική είναι επίσης η διαχείριση μεγάλων λιστών διευθύνσεων IP, δικτύων ή domains, όπως συμβαίνει σε περιπτώσεις αποκλεισμού κακόβουλων πηγών, περιορισμού πρόσβασης μεταξύ διαφορετικών δικτυακών τμημάτων ή εφαρμογής πολιτικών βάσει λιστών εμπιστοσύνης και αποκλεισμού. Η χειροκίνητη ενημέρωση τέτοιων λιστών αυξάνει σημαντικά τόσο τον χρόνο διαχείρισης όσο και την πιθανότητα λαθών, ενώ παράλληλα καθιστά δύσκολη

την αναπαραγωγιμότητα και την παρακολούθηση των αλλαγών που πραγματοποιούνται στο σύστημα.

Τα παραπάνω αναδεικνύουν ότι η παραδοσιακή προσέγγιση διαχείρισης πολιτικών firewall δεν επαρκεί πάντοτε για τις ανάγκες ενός σύγχρονου περιβάλλοντος SME. Για τον λόγο αυτό καθίσταται αναγκαία η υιοθέτηση περισσότερο δομημένων και ελεγχόμενων προσεγγίσεων διαχείρισης πολιτικών firewall, στις οποίες οι πολιτικές ασφάλειας ορίζονται με τυποποιημένο τρόπο, επικυρώνονται πριν από την εφαρμογή τους και μετασχηματίζονται συστηματικά σε ρυθμίσεις συμβατές με το firewall. Η ανάγκη αυτή αποτελεί τη βάση πάνω στην οποία διαμορφώνονται οι απαιτήσεις του προτεινόμενου συστήματος που παρουσιάζονται στις επόμενες ενότητες.

3.2 Ανάλυση Ρόλου Χρήστη (SME IT Administrator)

Ο σχεδιασμός οποιουδήποτε συστήματος αυτοματοποίησης προϋποθέτει την κατανόηση του προφίλ, των επιχειρησιακών περιορισμών και των λειτουργικών αναγκών του τελικού χρήστη. Στο πλαίσιο της παρούσας εργασίας, ο χρήστης είναι ο διαχειριστής IT μιας SMEs, ένας ρόλος που χαρακτηρίζεται από πολυδιάσπαση αρμοδιοτήτων και περιορισμένη εξειδίκευση σε επιμέρους τομείς κυβερνοασφάλειας. Ο ίδιος επωμίζεται ταυτόχρονα τη διαχείριση δικτυακών υποδομών, εξυπηρετητών, τεχνικής υποστήριξης χρηστών και μηχανισμών προστασίας πληροφοριακών συστημάτων.

Ο διαχειριστής IT αναζητά λύσεις που προσφέρουν άμεσα λειτουργικά αποτελέσματα με χαμηλή καμπύλη εκμάθησης. Η εξοικείωσή του με προηγμένα εργαλεία αυτοματοποίησης, γλώσσες προγραμματισμού ή API-based διαχείριση ενδέχεται να είναι περιορισμένη. Αντιθέτως, παρουσιάζει αυξημένη άνεση στη χρήση εργαλείων γραφείου και λογιστικών φύλλων για την οργάνωση και διαχείριση δεδομένων, γεγονός που επηρεάζει άμεσα τις σχεδιαστικές επιλογές του προτεινόμενου συστήματος.

Κατά συνέπεια, το σύστημα αυτοματοποίησης οφείλει να γεφυρώνει το χάσμα μεταξύ ευχρηστίας και τεχνικής αρτιότητας. Απαιτείται ένας μηχανισμός μέσω του οποίου ο διαχειριστής θα μπορεί να ορίζει πολιτικές ασφάλειας σε ένα οικείο και δομημένο περιβάλλον, διασφαλίζοντας παράλληλα ότι η εφαρμογή τους στο firewall πραγματοποιείται με ακρίβεια και

αξιοπιστία. Η αποφυγή πολύπλοκων διαδικασιών scripting ή άμεσης αλληλεπίδρασης με χαμηλού επιπέδου διεπαφές αποτελεί κρίσιμο παράγοντα αποδοχής της λύσης.

Εξίσου σημαντική είναι η ενίσχυση της εμπιστοσύνης του χρήστη προς το σύστημα αυτοματοποίησης. Η διαφάνεια στις εκτελούμενες ενέργειες, η δυνατότητα ελέγχου των αλλαγών και οι μηχανισμοί επαναφοράς σε προηγούμενες καταστάσεις (rollback capability) συνιστούν βασικές προϋποθέσεις λειτουργικής αξιοπιστίας και επιχειρησιακής αποδοχής.

Προκειμένου να αποτυπωθεί το απειλητικό περιβάλλον στο οποίο δραστηριοποιείται μια SME, παρατίθεται στη συνέχεια συγκεντρωτικός πίνακας βασικών κινδύνων, ο οποίος λειτουργεί ως πλαίσιο αναφοράς για τον σχεδιασμό των απαιτήσεων ασφάλειας του προτεινόμενου συστήματος.

Πίνακας 3-1: Βασικοί Κίνδυνοι Ασφάλειας σε Περιβάλλον SMEs και Επιπτώσεις για τον IT Administrator

Κατηγορία Απειλής	**Περιγραφή**	**Επιχειρησιακή Επίπτωση**	**Απαίτηση Συστήματος**
Ransomware	Κρυπτογράφηση εταιρικών δεδομένων	Διακοπή λειτουργίας	Τμηματοποίηση δικτύου (Network Segmentation) και ενσωμάτωση πληροφοριών απειλών (Threat Intelligence)
Phishing	Απόσπαση διαπιστευτηρίων	Παραβίαση λογαριασμών	Φιλτράρισμα DNS μέσω DNS Blackhole Lists (DNSBL) και έλεγχος εξερχόμενης κίνησης
Λανθασμένη παραμετροποίηση (Misconfiguration)	Λανθασμένοι κανόνες firewall	Κενά ασφάλειας	Επικύρωση κανόνων (Rule Validation) και τυποποίηση πολιτικών
Ανθρώπινο σφάλμα διαχειριστή (Insider Error)	Ανθρώπινο λάθος IT	Διακοπή υπηρεσιών	Έλεγχος εκδόσεων (Version Control) και δυνατότητα επαναφοράς ρυθμίσεων (Rollback)
Πλευρική κίνηση επιτιθέμενου (Lateral Movement)	Διάδοση επίθεσης εντός LAN	Εξάπλωση παραβίασης	Απομόνωση δικτύου μέσω VLAN (VLAN-based isolation)

Οι απειλές που παρουσιάζονται στον Πίνακα 3-1 καθορίζουν τις βασικές λειτουργικές και αρχιτεκτονικές απαιτήσεις του προτεινόμενου συστήματος αυτοματοποίησης πολιτικών firewall.

3.3 Λειτουργικές Απαιτήσεις

Οι λειτουργικές απαιτήσεις (functional requirements) περιγράφουν τις βασικές λειτουργίες που πρέπει να υλοποιεί το προτεινόμενο σύστημα προκειμένου να αντιμετωπιστούν τα προβλήματα που αναλύθηκαν στις προηγούμενες ενότητες.

Μία από τις σημαντικότερες απαιτήσεις είναι η δυνατότητα ανάγνωσης και επεξεργασίας δομημένων δεδομένων από εξωτερικές πηγές. Το σύστημα πρέπει να μπορεί να λαμβάνει ως είσοδο αρχεία κοινής μορφής, τα οποία θα περιέχουν λίστες διευθύνσεων IP ή domains που θα χρησιμοποιούνται από το firewall. Τα αρχεία αυτά λειτουργούν ως η κεντρική πηγή δεδομένων του συστήματος, γνωστή και ως Source of Truth.

Μία δεύτερη σημαντική απαίτηση αφορά την ύπαρξη μηχανισμών επικύρωσης δεδομένων (data validation). Το σύστημα πρέπει να ελέγχει την ορθότητα των διευθύνσεων IP, να εντοπίζει διπλότυπες εγγραφές και να αποτρέπει την εισαγωγή μη έγκυρων μορφών δεδομένων. Η διαδικασία αυτή συμβάλλει στη διατήρηση της ακεραιότητας των δεδομένων και αποτρέπει σφάλματα που θα μπορούσαν να επηρεάσουν τη λειτουργία του firewall.

Επιπλέον, το σύστημα πρέπει να μπορεί να επικοινωνεί αυτόματα με το pfSense προκειμένου να ενημερώνει τα αντικείμενα τύπου Alias. Η διαχείριση πραγματοποιείται σε επίπεδο Aliases και όχι απευθείας στους κανόνες firewall, γεγονός που διατηρεί σταθερή τη δομή των πολιτικών ασφάλειας και μειώνει την πιθανότητα σφαλμάτων κατά τη διαμόρφωση.

Τέλος, κάθε λειτουργία του συστήματος πρέπει να καταγράφεται σε αρχεία καταγραφής (logs). Η καταγραφή αυτή περιλαμβάνει τόσο τις επιτυχείς όσο και τις αποτυχημένες ενέργειες, εξασφαλίζοντας πλήρη ιχνηλασιμότητα των αλλαγών και διευκολύνοντας τη διαδικασία διερεύνησης πιθανών προβλημάτων ή περιστατικών ασφάλειας (ISO, 2022).

Με βάση τις απειλές που αναλύθηκαν στην προηγούμενη ενότητα, η κατηγοριοποίηση των κινδύνων σύμφωνα με την πιθανότητα εμφάνισης και το επίπεδο επίπτωσης αποτελεί σημαντικό βήμα για τον σχεδιασμό ενός αποτελεσματικού συστήματος ασφάλειας.

3.4 Μη Λειτουργικές Απαιτήσεις

Οι μη λειτουργικές απαιτήσεις (non-functional requirements) περιγράφουν τα ποιοτικά χαρακτηριστικά του συστήματος, όπως η ασφάλεια, η αξιοπιστία και η απόδοση.

Η ασφάλεια της επικοινωνίας μεταξύ του σταθμού διαχείρισης και του firewall αποτελεί βασική προϋπόθεση για την ασφαλή λειτουργία του συστήματος. Η μεταφορά δεδομένων και η εκτέλεση εντολών πρέπει να πραγματοποιούνται μέσω κρυπτογραφημένων καναλιών επικοινωνίας, όπως το πρωτόκολλο Secure Shell (SSH), με χρήση ισχυρών μηχανισμών αυθεντικοποίησης (authentication) ώστε να αποτρέπεται η υποκλοπή ή η αλλοίωση των εντολών (Stallings, 2018).

Η αξιοπιστία και η διαθεσιμότητα του συστήματος είναι επίσης ιδιαίτερα σημαντικές. Η διαδικασία ενημέρωσης των λιστών δεν πρέπει να προκαλεί διακοπή της λειτουργίας του δικτύου ούτε να επιβαρύνει υπερβολικά τους πόρους του firewall, όπως την CPU ή τη μνήμη.

Το σύστημα πρέπει επίσης να είναι σχεδιασμένο με τρόπο που να επιτρέπει την ασφαλή διαχείριση σφαλμάτων. Σε περίπτωση αποτυχίας κατά την εκτέλεση μιας διαδικασίας, το firewall δεν πρέπει να παραμένει σε ασυνεπή κατάσταση. Η διαδικασία πρέπει να τερματίζεται με ελεγχόμενο τρόπο ώστε να διασφαλίζεται η σταθερότητα της υποδομής.

Ένα επιπλέον σημαντικό χαρακτηριστικό είναι η επεκτασιμότητα (scalability). Η αρχιτεκτονική του συστήματος πρέπει να επιτρέπει τη μελλοντική προσθήκη νέων λειτουργιών χωρίς σημαντικές αλλαγές στον πυρήνα της εφαρμογής. Παράλληλα, η φορητότητα (portability) της λύσης επιτρέπει την εγκατάσταση και λειτουργία της σε τυπικά λειτουργικά συστήματα χωρίς την ανάγκη εξειδικευμένου εξοπλισμού.

Η απλότητα εγκατάστασης και η περιορισμένη εξάρτηση από πρόσθετα λογισμικά αποτελούν επίσης σημαντικούς παράγοντες για την υιοθέτηση της λύσης από SMEs, όπου οι διαθέσιμοι πόροι διαχείρισης είναι συνήθως περιορισμένοι.

3.5 Πεδίο εφαρμογής της προτεινόμενης λύσης (Scope)

Το πεδίο εφαρμογής της παρούσας διπλωματικής εργασίας καθορίζεται με σαφή τρόπο, ώστε να διατηρηθεί η εστίαση στους βασικούς ερευνητικούς στόχους και να αποσαφηνιστούν τα όρια της προτεινόμενης προσέγγισης.

Η προτεινόμενη λύση αφορά την ανάπτυξη ενός μηχανισμού δομημένης και ημι-αυτοματοποιημένης διαχείρισης πολιτικών firewall στο περιβάλλον του pfSense. Η προσέγγιση βασίζεται στη χρήση δομημένων δεδομένων πολιτικής, τα οποία ορίζονται σε εξωτερικά αρχεία και χρησιμοποιούνται για την παραγωγή νέας διαμόρφωσης firewall με ελεγχόμενο τρόπο. Πιο

συγκεκριμένα, το σύστημα αξιοποιεί ένα πρότυπο αρχείο πολιτικής σε μορφή Excel και ένα υφιστάμενο βασικό αρχείο ρυθμίσεων (baseline configuration), από τα οποία παράγεται νέο αρχείο διαμόρφωσης συμβατό με το pfSense.

Στο πλαίσιο αυτό, η λύση υποστηρίζει τον ορισμό και τη διαχείριση κανόνων firewall, καθώς και τη διαχείριση δικτυακών αντικειμένων, όπως αντικείμενα τύπου Alias, τα οποία χρησιμοποιούνται για τον έλεγχο πρόσβασης και τον περιορισμό ανεπιθύμητης ή κακόβουλης δικτυακής δραστηριότητας. Η χρήση δομημένων αντικειμένων και προτύπων πολιτικής επιτρέπει τη συγκεντρωτική διαχείριση μεγάλου αριθμού εγγραφών και συμβάλλει στη βελτίωση της συνέπειας και της διαχειρισιμότητας της πολιτικής ασφάλειας.

Η προτεινόμενη προσέγγιση δεν βασίζεται σε συνεχή ή αμφίδρομο συγχρονισμό μεταξύ του συστήματος και του firewall. Αντίθετα, λειτουργεί ως μηχανισμός ορισμού, επικύρωσης και μετασχηματισμού πολιτικών ασφάλειας, μέσω του οποίου τα δεδομένα πολιτικής μετατρέπονται σε νέο αρχείο ρυθμίσεων προς εφαρμογή στο pfSense. Με τον τρόπο αυτό μειώνεται η ανάγκη χειροκίνητης επεξεργασίας ρυθμίσεων μέσω του γραφικού περιβάλλοντος διαχείρισης, ενώ περιορίζεται και η πιθανότητα σφαλμάτων διαμόρφωσης (misconfigurations), τα οποία αποτελούν συχνή πηγή αδυναμιών ασφάλειας σε περιβάλλοντα με περιορισμένους πόρους διαχείρισης (ENISA, 2023).

Επιπλέον, στο πλαίσιο της εργασίας αξιοποιούνται συμπληρωματικοί μηχανισμοί προστασίας της πλατφόρμας pfSense, όπως το pfBlockerNG και οι DNSBL λίστες αποκλεισμού, για την εφαρμογή πολιτικών φιλτραρίσματος δικτυακής και domain-based κίνησης. Η χρήση αυτών των μηχανισμών εντάσσεται στη συνολική αρχιτεκτονική επιβολής πολιτικών ασφαλείας, χωρίς να αποτελεί αντικείμενο αυτόνομης ανάπτυξης ή ανεξάρτητης έρευνας.

Εκτός του πεδίου της παρούσας εργασίας βρίσκεται η ανάπτυξη ενός νέου λειτουργικού συστήματος firewall ή η δημιουργία ενός πλήρους γραφικού περιβάλλοντος διαχείρισης που θα αντικαθιστούσε το υπάρχον Web Interface του pfSense. Επιπλέον, η εργασία δεν εξετάζει την ανάπτυξη ολοκληρωμένων πλατφορμών ορχήστρωσης ασφάλειας, τη διαχείριση πολλαπλών firewalls σε περιβάλλοντα μεγάλης κλίμακας ή την υλοποίηση μηχανισμών συνεχούς συγχρονισμού και αυτόματης αναπροσαρμογής πολιτικών.

Παράλληλα, δεν εξετάζεται η αξιοποίηση τεχνικών τεχνητής νοημοσύνης ή μηχανικής μάθησης για την ανάλυση δικτυακής κίνησης ή την ανίχνευση επιθέσεων. Ωστόσο αξιοποιούνται μηχανισμοί threat intelligence μέσω blocklists που ενσωματώνονται στο pfSense με τη χρήση

του pfBlockerNG. Η εργασία επικεντρώνεται στη δομημένη και ελεγχόμενη παραγωγή και εφαρμογή πολιτικών firewall και όχι στην ανάπτυξη νέων μηχανισμών ανίχνευσης απειλών. Ομοίως, δεν εξετάζεται η πλήρης διαχείριση όλων των υπηρεσιών της πλατφόρμας pfSense, όπως υπηρεσίες VPN ή DHCP, πέρα από τα σημεία όπου αυτές σχετίζονται με την εφαρμογή της πολιτικής ασφάλειας.

Ο σαφής αυτός καθορισμός του πεδίου εφαρμογής επιτρέπει τη συγκεντρωμένη διερεύνηση μιας δομημένης και ημι-αυτοματοποιημένης προσέγγισης για τη διαχείριση πολιτικών firewall σε περιβάλλοντα SMEs.

3.6 Παραδοχές και Περιορισμοί Σχεδίασης

Η σχεδίαση και υλοποίηση της προτεινόμενης λύσης βασίζεται σε συγκεκριμένες παραδοχές και τεχνικούς περιορισμούς που σχετίζονται με το εργαστηριακό περιβάλλον υλοποίησης.

Βασική παραδοχή αποτελεί η χρήση της πλατφόρμας Proxmox Virtual Environment (Proxmox VE). Η πλατφόρμα αυτή επιτρέπει τη δημιουργία απομονωμένων εικονικών μηχανών και εικονικών δικτύων, καθώς και τη λήψη στιγμιότυπων συστήματος (snapshots). Οι δυνατότητες αυτές διευκολύνουν τη δοκιμή σεναρίων ασφάλειας και επιτρέπουν την επαναληψιμότητα των πειραμάτων σε ελεγχόμενο περιβάλλον, το οποίο προσομοιώνει σε σημαντικό βαθμό την αρχιτεκτονική ενός πραγματικού επιχειρησιακού δικτύου.

Επιπλέον, θεωρείται ότι ο διαχειριστής του συστήματος διαθέτει τα απαραίτητα δικαιώματα διαμόρφωσης στο firewall ώστε να μπορεί να πραγματοποιεί αλλαγές στις παραμέτρους του. Παράλληλα, η δικτυακή υποδομή θεωρείται ότι ακολουθεί μία τυπική αρχιτεκτονική περιμετρικής ασφάλειας (perimeter security architecture), όπου το firewall λειτουργεί ως σημείο ελέγχου μεταξύ διαφορετικών ζωνών εμπιστοσύνης.

Η λύση αναπτύσσεται και αξιολογείται στην Community έκδοση του pfSense. Η έκδοση pfSense Community Edition (CE) αποτελεί την ανοιχτού κώδικα έκδοση της πλατφόρμας, η οποία διατίθεται δωρεάν και χρησιμοποιείται ευρέως για εκπαιδευτικούς, ερευνητικούς και μικρής κλίμακας παραγωγικούς σκοπούς, σε αντίθεση με την εμπορική έκδοση pfSense Plus, η οποία περιλαμβάνει πρόσθετες δυνατότητες και επαγγελματική υποστήριξη.

Ως βασική οργανωτική παραδοχή για την επιτυχή λειτουργία της προτεινόμενης αρχιτεκτονικής, θεωρείται η επιβολή πολιτικής αυστηρού ελέγχου πρόσβασης (read-only) στο γραφικό

περιβάλλον (WebGUI) του pfSense για το τεχνικό προσωπικό. Η παραδοχή αυτή είναι απαραίτητη ώστε το αρχείο Excel να παραμένει αδιαπραγμάτευτα η μοναδική πηγή αλήθειας (Single Source of Truth) και να αποτρέπεται το φαινόμενο της απόκλισης διαμόρφωσης (configuration drift). (Humble & Farley, 2010).

Τέλος, ως σχεδιαστικός περιορισμός θεωρείται η χρήση δομημένων δεδομένων εισόδου. Τα αρχεία που χρησιμοποιούνται για την τροφοδότηση του συστήματος υποτίθεται ότι ακολουθούν προκαθορισμένη μορφή, η οποία επιτρέπει την αυτοματοποιημένη επεξεργασία τους. Η διαχείριση αδόμητων ή ελλιπών δεδομένων δεν εξετάζεται στην παρούσα εργασία, καθώς θα απαιτούσε πρόσθετους μηχανισμούς κανονικοποίησης και επαλήθευσης δεδομένων.

Με βάση την ανάλυση προβλήματος, τις λειτουργικές και μη λειτουργικές απαιτήσεις, καθώς και το καθορισμένο πεδίο εφαρμογής, στο επόμενο κεφάλαιο παρουσιάζεται η αρχιτεκτονική της προτεινόμενης λύσης. Συγκεκριμένα, αναλύεται η συνολική αρχιτεκτονική του συστήματος, τα επιμέρους υποσυστήματα και ο τρόπος με τον οποίο τα δομημένα δεδομένα πολιτικής μετατρέπονται σε ρυθμίσεις συμβατές με το pfSense.

4 ΚΕΦΑΛΑΙΟ 4 – ΣΧΕΔΙΑΣΗ ΠΡΟΤΕΙΝΟΜΕΝΗΣ ΛΥΣΗΣ

4.1 Συνολική αρχιτεκτονική της λύσης

Η σχεδίαση της προτεινόμενης λύσης βασίζεται σε μία αρχιτεκτονική τριών επιπέδων (three-tier architecture), η οποία διαχωρίζει σαφώς το επίπεδο διεπαφής χρήστη, το επίπεδο λογικής επεξεργασίας και το επίπεδο εφαρμογής της υποδομής. Η προσέγγιση αυτή επιλέχθηκε ώστε να διασφαλίζεται η αρθρωτότητα (modularity) του συστήματος, καθώς και η ευκολία συντήρησης και διαχείρισης, χαρακτηριστικά που θεωρούνται ιδιαίτερα σημαντικά για περιβάλλοντα SMEs (Bass, Clements & Kazman, 2013).

Το πρώτο επίπεδο, το οποίο μπορεί να χαρακτηριστεί ως επίπεδο διαχείρισης (Management Plane), περιλαμβάνει το περιβάλλον διεπαφής με τον χρήστη. Στην παρούσα αρχιτεκτονική υλοποιείται μέσω ενός δομημένου προτύπου Excel, το οποίο λειτουργεί ως σημείο καταγραφής και διαχείρισης της πολιτικής ασφάλειας. Σε αυτό το επίπεδο, ο διαχειριστής μπορεί να ορίζει κανόνες πολιτικής σε υψηλό επίπεδο αφαίρεσης, χωρίς να απαιτείται άμεση αλληλεπίδραση με τη γραμμή εντολών ή το περιβάλλον παραμετροποίησης του firewall. Το αρχείο Excel λειτουργεί έτσι ως Single Source of Truth για τη διαμόρφωση της πολιτικής ασφάλειας του δικτύου.

Το δεύτερο επίπεδο αποτελεί το επίπεδο αυτοματοποίησης (Automation Plane). Το επίπεδο αυτό λειτουργεί ως ενδιάμεσο στρώμα μεταξύ της πολιτικής που ορίζεται στο Excel και της τεχνικής υλοποίησής της στο firewall. Το σενάριο αυτοματοποίησης (script logic) επεξεργάζεται τα δεδομένα εισόδου, εκτελεί ελέγχους εγκυρότητας και εξάγει τον κώδικα σε μορφή συμβατή με το pfSense (XML payload), τον οποίο ο διαχειριστής ενσωματώνει ελεγχόμενα στο σύστημα. Στο επίπεδο αυτό πραγματοποιείται επίσης η διαδικασία αντιστοίχισης (mapping) των επιχειρησιακών κανόνων πολιτικής σε τεχνικές παραμέτρους του firewall.

Το τρίτο επίπεδο αποτελεί το επίπεδο υποδομής (Infrastructure Plane), το οποίο φιλοξενείται στο περιβάλλον Proxmox. Στο επίπεδο αυτό υλοποιείται η εγκατάσταση του pfSense, το οποίο λειτουργεί ως το σημείο επιβολής (enforcement point) των κανόνων ασφάλειας του δικτύου. Η χρήση του Proxmox ως hypervisor επιτρέπει τη δημιουργία απομονωμένων εικονικών δικτύων μέσω μηχανισμών Linux Bridges, καθώς και τη χρήση στιγμιότυπων συστήματος (snapshots). Με τον τρόπο αυτό καθίσταται δυνατή η δοκιμή των αυτοματοποιημένων αλλαγών σε ένα

ελεγχόμενο εργαστηριακό περιβάλλον πριν την εφαρμογή τους σε πραγματική λειτουργία, μειώνοντας τον κίνδυνο διακοπής υπηρεσιών.

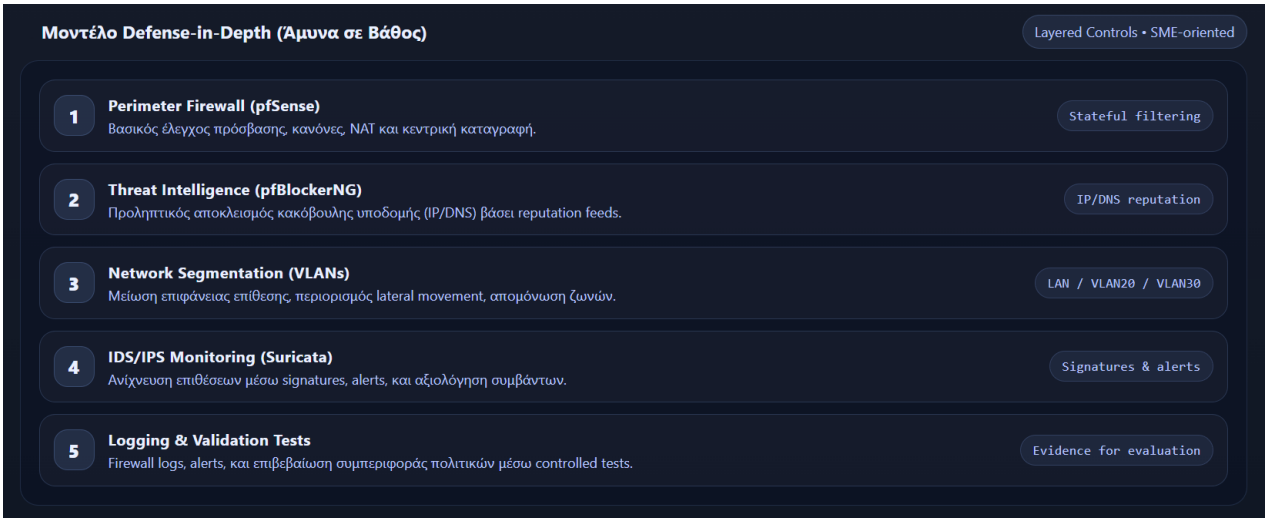
Για την υλοποίηση της προτεινόμενης αρχιτεκτονικής χρησιμοποιήθηκε ένα σύνολο τεχνολογιών ανοικτού λογισμικού και εργαλείων αυτοματοποίησης. Οι βασικές τεχνολογίες που αξιοποιήθηκαν στην υλοποίηση παρουσιάζονται στον Πίνακα 4-1.

Πίνακας 4-1: Τεχνολογίες που χρησιμοποιήθηκαν στην υλοποίηση της προτεινόμενης αρχιτεκτονικής

Εργαλείο	**Έκδοση**	**Ρόλος στο σύστημα**
pfSense	CE 2.7.x	Κεντρικό firewall και επιβολή κανόνων δικτυακής πρόσβασης
Suricata	6.x	Σύστημα ανίχνευσης και πρόληψης εισβολών (IDS/IPS)
pfBlockerNG	3.x	Φιλτράρισμα κακόβουλων IP και domain μέσω threat intelligence
Python	3.x	Αυτοματοποιημένη επεξεργασία και μετατροπή κανόνων
Microsoft Excel	—	Ορισμός και τεκμηρίωση firewall policies
Proxmox VE	7.x	Περιβάλλον Proxmox για το εργαστηριακό περιβάλλον
VLAN (802.1Q)	—	Τμηματοποίηση δικτύου

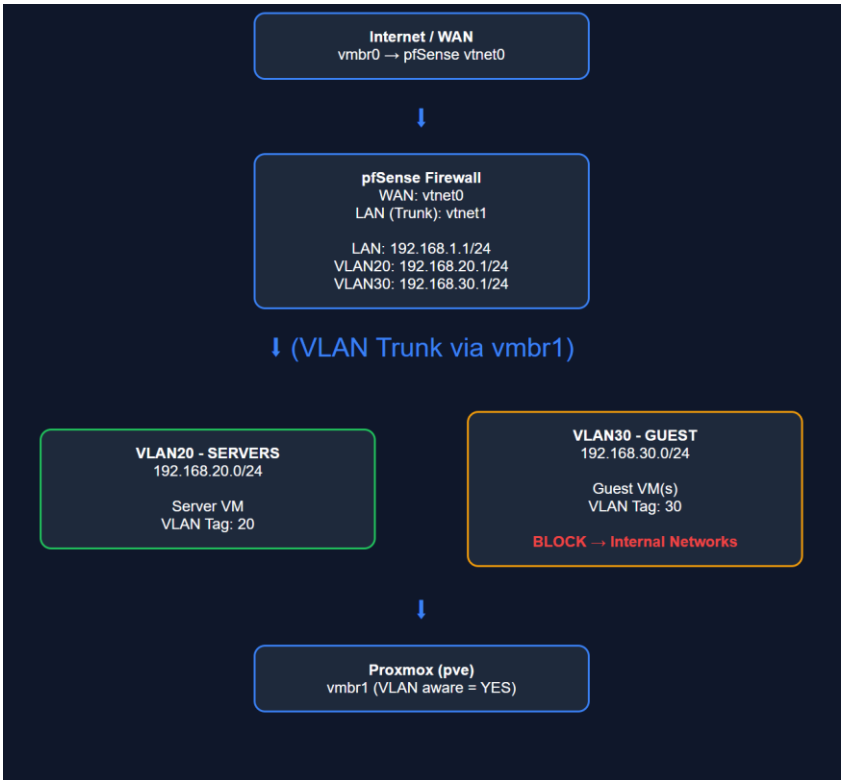
Η προτεινόμενη αρχιτεκτονική δεν βασίζεται σε έναν μόνο μηχανισμό προστασίας, αλλά υιοθετεί την αρχή της άμυνας σε βάθος (Defense-in-Depth). Σύμφωνα με την αρχή αυτή, πολλαπλά επίπεδα ασφάλειας λειτουργούν συμπληρωματικά, ώστε να μειώνεται η πιθανότητα επιτυχούς εκμετάλλευσης μίας μεμονωμένης ευπάθειας ή εσφαλμένης ρύθμισης (NIST, 2020; Stallings, 2018).

Η Εικόνα 4-1 παρακάτω παρουσιάζει τη συνολική πολυεπίπεδη αρχιτεκτονική ασφάλειας που υλοποιήθηκε στο εργαστηριακό περιβάλλον. Στο εξωτερικό επίπεδο βρίσκεται το firewall pfSense, το οποίο λειτουργεί ως κεντρικό σημείο ελέγχου της εισερχόμενης και εξερχόμενης δικτυακής κίνησης. Στα εσωτερικά επίπεδα εφαρμόζονται VLANs και συμπληρωματικά εργαλεία ασφάλειας, όπως το Suricata για ανίχνευση και πρόληψη εισβολών και το pfBlockerNG για φιλτράρισμα κακόβουλων διευθύνσεων.



Εικόνα 4-1: Μοντέλο άμυνας σε βάθος (Defense-in-Depth) της προτεινόμενης αρχιτεκτονικής ασφάλειας

Η Εικόνα 4-2 παρουσιάζει μια απλοποιημένη απεικόνιση της συνδεσμολογίας του εργαστηριακού περιβάλλοντος. Στην αρχιτεκτονική αυτή, το pfSense λειτουργεί ως κεντρικός δρομολογητής και firewall του δικτύου. Η σύνδεση προς το εσωτερικό δίκτυο πραγματοποιείται μέσω trunk διεπαφής (vtnet1) προς το εσωτερικό bridge vmbr1 του Proxmox, το οποίο έχει διαμορφωθεί ως VLAN-aware. Μέσω αυτής της δομής υλοποιείται η τμηματοποίηση του εσωτερικού δικτύου σε πολλαπλά VLANs.



Εικόνα 4-2: Απλοποιημένη απεικόνιση της συνδεσμολογίας του εργαστηριακού περιβάλλοντος.

4.2 Μοντελοποίηση πολιτικής ασφάλειας

Στο πλαίσιο της παρούσας διπλωματικής εργασίας, η πολιτική ασφάλειας δικτύου δεν αντιμετωπίζεται ως ένα σύνολο αποσπασματικών τεχνικών ρυθμίσεων, αλλά ως ένα δομημένο σύνολο κανόνων που βασίζεται σε αναγνωρισμένα πρότυπα ασφάλειας πληροφοριών. Η μοντελοποίηση της πολιτικής βασίζεται στις αρχές του προτύπου ISO/IEC 27001, το οποίο παρέχει κατευθυντήριες γραμμές για τον έλεγχο πρόσβασης (access control), την ασφάλεια δικτύων και τη διαχείριση αλλαγών (ISO/IEC 27001, 2022).

Στο πλαίσιο αυτό, οι απαιτήσεις του προτύπου μεταφράζονται σε αφηρημένες έννοιες πολιτικής ασφάλειας, όπως ο καθορισμός επιτρεπόμενων και μη επιτρεπόμενων ροών δικτύου, ο περιορισμός πρόσβασης βάσει ρόλων και η εφαρμογή της αρχής του ελάχιστου προνομίου (least privilege). Η προσέγγιση αυτή συμβάλλει στη συστηματική ανάπτυξη της πολιτικής, διασφαλίζοντας ότι οι τεχνικές ρυθμίσεις του firewall ευθυγραμμίζονται με τις επιχειρησιακές και κανονιστικές απαιτήσεις του οργανισμού (Whitman & Mattord, 2021).

Παράλληλα, επιτυγχάνεται σαφής διάκριση μεταξύ πολιτικής ασφάλειας και τεχνικής υλοποίησης. Η πολιτική ορίζεται σε υψηλό επίπεδο αφαίρεσης, ανεξάρτητα από συγκεκριμένες τεχνολογικές πλατφόρμες, ενώ η επιβολή της πραγματοποιείται μέσω του pfSense. Με τον τρόπο αυτό η πολιτική παραμένει κατανοητή και επαναχρησιμοποιήσιμη, ενώ η τεχνική υλοποίηση μπορεί να προσαρμοστεί σε διαφορετικές υποδομές.

Στην παρούσα μελέτη, η πολιτική ασφάλειας εξειδικεύεται περαιτέρω μέσω της λογικής τμηματοποίησης του δικτύου (VLAN segmentation). Η δημιουργία διακριτών ζωνών εμπιστοσύνης (trust zones) επιτρέπει τον σαφή καθορισμό των επιτρεπόμενων και μη επιτρεπόμενων ροών επικοινωνίας μεταξύ χρηστών, εξυπηρετητών και επισκεπτών.

Οι βασικές ζώνες που χρησιμοποιήθηκαν στην προτεινόμενη αρχιτεκτονική είναι οι εξής:

• **WAN (Untrusted Zone):** Το εξωτερικό δίκτυο και το Διαδίκτυο, το οποίο θεωρείται πλήρως μη αξιόπιστο.

• **LAN (Internal Trusted Zone):** Το εσωτερικό δίκτυο σταθμών εργασίας και διαχειριστικών συστημάτων.

• **VLAN20_SERVERS (Server Zone):** Ζώνη φιλοξενίας εξυπηρετητών και κρίσιμων υπηρεσιών.

• **VLAN30_GUEST (Guest Zone):** Ζώνη επισκεπτών με απομόνωση από το εσωτερικό δίκτυο.

Ο διαχωρισμός αυτός αποτελεί υλοποίηση πολιτικής ασφάλειας σε επίπεδο αρχιτεκτονικού σχεδιασμού. Κάθε ζώνη αντιστοιχεί σε διαφορετικό επίπεδο εμπιστοσύνης και συνεπάγεται συγκεκριμένους κανόνες φιλτραρίσματος στο firewall.

Η επικοινωνία μεταξύ των ζωνών ακολουθεί την αρχή «απόρριψης εξ ορισμού» (default deny), σύμφωνα με την οποία κάθε μορφή επικοινωνίας απορρίπτεται εκ προεπιλογής, εκτός εάν έχει επιτραπεί ρητά βάσει τεκμηριωμένης επιχειρησιακής ανάγκης. Η προσέγγιση αυτή συμβάλλει στη μείωση της επιφάνειας επίθεσης (attack surface) και επιτρέπει τον αυστηρό έλεγχο των διαθέσιμων υπηρεσιών (NIST, 2020).

4.3 Σχεδίαση προτύπου Excel για τη διαχείριση πολιτικών ασφάλειας

Το πρότυπο αρχείο Excel που προτείνεται στην παρούσα εργασία σχεδιάστηκε ως ενδιάμεσο επίπεδο μεταξύ της αφηρημένης πολιτικής ασφάλειας και της τεχνικής υλοποίησής της στο Firewall. Ο ρόλος του δεν περιορίζεται στην απλή καταγραφή τεχνικών ρυθμίσεων, αλλά επεκτείνεται στη δομημένη αποτύπωση και διαχείριση των πολιτικών ασφάλειας σε μορφή κατανοητή και λειτουργικά αξιοποιήσιμη από τον διαχειριστή μιας SME. Με τον τρόπο αυτό λειτουργεί ως μηχανισμός μετάφρασης πολιτικής (policy translation layer) μεταξύ κανονιστικών απαιτήσεων και τεχνικών ρυθμίσεων.

Η επιλογή του Excel ως διεπαφής πολιτικής (policy interface) βασίζεται κυρίως στη μεγάλη διάδοσή του σε επιχειρησιακά περιβάλλοντα SMEs. Οι περισσότερες SMEs διαθέτουν ήδη εξοικείωση με εργαλεία υπολογιστικών φύλλων, γεγονός που μειώνει την ανάγκη εξειδικευμένης τεχνικής εκπαίδευσης. Παράλληλα, το Excel προσφέρει δυνατότητες δομημένης καταγραφής δεδομένων, όπως προκαθορισμένες λίστες επιλογών (drop-down lists), υποχρεωτικά πεδία και κανόνες επικύρωσης δεδομένων (data validation). Μέσω αυτών των μηχανισμών διασφαλίζεται ότι οι καταχωρήσεις πραγματοποιούνται με ομοιομορφία και συνέπεια, μειώνοντας τον κίνδυνο λανθασμένων ρυθμίσεων (misconfigurations).

Το πρότυπο Excel λειτουργεί ως μέσο επιχειρησιακής αποτύπωσης των πολιτικών που απορρέουν από το πρότυπο ISO/IEC 27001 σε συγκεκριμένα τεχνικά δεδομένα. Οι γενικές απαιτήσεις ασφάλειας, όπως ο έλεγχος πρόσβασης και η τεκμηριωμένη διαχείριση αλλαγών, μετατρέπονται σε συγκεκριμένα πεδία που περιγράφουν τις παραμέτρους ενός κανόνα firewall (ISO/IEC 27001, 2022).

Κάθε στήλη του Excel αντιστοιχεί σε βασική παράμετρο πολιτικής ασφάλειας, όπως:

- η πηγή της δικτυακής κίνησης (source)
- ο προορισμός (destination)
- η υπηρεσία ή το πρωτόκολλο επικοινωνίας
- η ενέργεια εφαρμογής του κανόνα (allow / deny)
- η περιγραφή και τεκμηρίωση του κανόνα

Η δομή αυτή δεν εξυπηρετεί μόνο τεχνικούς σκοπούς, αλλά υποστηρίζει και διαδικασίες διακυβέρνησης της ασφάλειας. Συγκεκριμένα, διασφαλίζεται ότι κάθε κανόνας firewall συνδέεται με τεκμηριωμένη επιχειρησιακή ανάγκη και με συγκεκριμένη απόφαση πολιτικής ασφάλειας.

Η ύπαρξη ενός τέτοιου policy interface ενισχύει τη διαφάνεια και την ιχνηλασιμότητα (traceability) της διαδικασίας διαχείρισης κανόνων. Με τον τρόπο αυτό καθίσταται δυνατή η χαρτογράφηση μεταξύ της πολιτικής ασφάλειας και της τεχνικής υλοποίησης στο firewall, γεγονός που διευκολύνει τόσο τη διαχείριση αλλαγών όσο και τις διαδικασίες ελέγχου συμμόρφωσης (Whitman & Mattord, 2021).

Παράλληλα, περιορίζεται η εξάρτηση από άτυπες διαδικασίες ή εμπειρικές πρακτικές διαχείρισης κανόνων firewall. Αντί για μεμονωμένες και μη τεκμηριωμένες αλλαγές στη διαμόρφωση του firewall, η διαχείριση πραγματοποιείται μέσω ενός τυποποιημένου και ελεγχόμενου μοντέλου πολιτικής ασφάλειας.

4.4 Χαρτογράφηση Excel πεδίων σε firewall rules

Η διαδικασία χαρτογράφησης των πεδίων του Excel template σε κανόνες firewall αποτελεί βασικό στοιχείο της προτεινόμενης αρχιτεκτονικής. Μέσω της διαδικασίας αυτής διασφαλίζεται ότι η πολιτική ασφάλειας που ορίζεται σε υψηλό επίπεδο μετασχηματίζεται με συνεπή τρόπο σε τεχνικές ρυθμίσεις του firewall.

Η πρακτική υλοποίηση της παραπάνω διαδικασίας χαρτογράφησης πραγματοποιείται μέσω του script excel2pfsense.py, το οποίο αναπτύχθηκε στο πλαίσιο της παρούσας εργασίας. Το script διαβάζει τα δεδομένα πολιτικής από το πρότυπο αρχείο Excel χρησιμοποιώντας τη

βιβλιοθήκη openpyxl της Python και τα μετατρέπει σε αντίστοιχες παραμέτρους κανόνων firewall.

Για την παραγωγή του αρχείου διαμόρφωσης του pfSense χρησιμοποιείται η βιβλιοθήκη xml.etree.ElementTree, η οποία επιτρέπει την επεξεργασία του XML αρχείου ρυθμίσεων του firewall. Για λόγους ακεραιότητας της διαμόρφωσης, το script δεν δημιουργεί το αρχείο από το μηδέν αλλά φορτώνει ένα βασικό έγκυρο αρχείο διαμόρφωσης (baseline_config.xml) και ενσωματώνει δυναμικά τους κανόνες που προκύπτουν από το Excel πρότυπο.

Κάθε πεδίο του Excel αντιστοιχίζεται σε συγκεκριμένη παράμετρο ενός κανόνα firewall. Η αντιστοίχιση αυτή πραγματοποιείται βάσει προκαθορισμένης λογικής μετασχηματισμού, η οποία εξαλείφει την αυθαιρεσία κατά τη δημιουργία κανόνων και μειώνει τον κίνδυνο ασυνεπειών μεταξύ πολιτικής και τεχνικής υλοποίησης.

Η χαρτογράφηση δεν περιορίζεται στην απλή μεταφορά δεδομένων. Στόχος της είναι η διατήρηση της σημασιολογίας της πολιτικής ασφάλειας κατά τη μετατροπή της σε τεχνικές ρυθμίσεις. Έννοιες όπως:

- ο έλεγχος πρόσβασης μεταξύ ζωνών εμπιστοσύνης
- ο διαχωρισμός δικτύων
- η ιεράρχηση των κανόνων firewall

μεταφέρονται από το επίπεδο σχεδιασμού πολιτικής στο επίπεδο εφαρμογής χωρίς απώλεια του κανονιστικού τους περιεχομένου.

Επιπλέον, η διαδικασία χαρτογράφησης επιτρέπει την ενσωμάτωση μηχανισμών προληπτικής επικύρωσης (pre-deployment validation). Κατά τη φάση αυτή ελέγχονται τα δεδομένα που έχουν καταχωρηθεί στο Excel προκειμένου να εντοπιστούν μη έγκυρες, ελλιπείς ή ασυνεπείς τιμές πριν την εφαρμογή τους στο firewall.

Η προσέγγιση αυτή είναι ιδιαίτερα σημαντική, καθώς οι λανθασμένες ρυθμίσεις firewall αποτελούν μία από τις συχνότερες αιτίες παραβιάσεων ασφάλειας σε οργανισμούς (ENISA, 2023). Μέσω της προληπτικής επικύρωσης μειώνεται σημαντικά ο κίνδυνος δημιουργίας προβληματικών κανόνων και ενισχύεται η αξιοπιστία της συνολικής αρχιτεκτονικής.

Συνολικά, η διαδικασία χαρτογράφησης συμβάλλει στη γεφύρωση του χάσματος μεταξύ σχεδιασμού πολιτικής ασφάλειας και τεχνικής εφαρμογής της. Με τον τρόπο αυτό διασφαλίζεται

ότι οι κανόνες που εφαρμόζονται στο firewall αντικατοπτρίζουν με συνέπεια τις απαιτήσεις της πολιτικής ασφάλειας του οργανισμού.

4.5 Διαχείριση εξαιρέσεων και προτεραιότητας κανόνων

Ένα από τα συνηθέστερα προβλήματα στη χειροκίνητη διαχείριση κανόνων firewall είναι η ανεξέλεγκτη εισαγωγή εξαιρέσεων. Σε πολλές περιπτώσεις, οι εξαιρέσεις δημιουργούνται για την επίλυση άμεσων λειτουργικών αναγκών, χωρίς όμως να συνοδεύονται από σαφή τεκμηρίωση ή χρονικό περιορισμό. Ως αποτέλεσμα, οι κανόνες αυτοί παραμένουν ενεργοί για μεγάλα χρονικά διαστήματα και οδηγούν σταδιακά σε αποδυνάμωση της πολιτικής ασφάλειας.

Η προτεινόμενη αρχιτεκτονική αντιμετωπίζει το ζήτημα σε επίπεδο σχεδιασμού, εισάγοντας τη λογική της ρητής και τεκμηριωμένης εξαίρεσης (explicit exception handling). Σύμφωνα με την προσέγγιση αυτή, κάθε εξαίρεση αντιμετωπίζεται ως συνειδητή απόκλιση από τη γενική πολιτική ασφάλειας, η οποία πρέπει να καταγράφεται και να αιτιολογείται.

Η πληροφορία αυτή ενσωματώνεται στη διεπαφή πολιτικής (policy interface) του Excel, επιτρέποντας την καταγραφή της επιχειρησιακής αιτιολόγησης κάθε εξαίρεσης. Με τον τρόπο αυτό ενισχύεται η ιχνηλασιμότητα των αλλαγών και καθίσταται δυνατή η επανεξέταση των εξαιρέσεων στο πλαίσιο διαδικασιών αναθεώρησης της πολιτικής ασφάλειας.

Παράλληλα, ιδιαίτερη σημασία δίνεται στη σωστή προτεραιοποίηση των κανόνων firewall. Στα περισσότερα firewalls, οι κανόνες αξιολογούνται σειριακά, γεγονός που καθιστά κρίσιμη τη σωστή σειρά εφαρμογής τους. Εάν ένας γενικός κανόνας τοποθετηθεί πριν από έναν πιο συγκεκριμένο κανόνα, ενδέχεται να οδηγήσει σε απρόβλεπτη συμπεριφορά του συστήματος.

Στην προτεινόμενη μεθοδολογία, η σειρά των κανόνων δεν αποτελεί αποτέλεσμα τυχαίας συσσώρευσης αλλαγών, αλλά εντάσσεται στον αρχικό σχεδιασμό της πολιτικής ασφάλειας. Η ιεράρχηση των κανόνων καθορίζεται με βάση το επίπεδο εμπιστοσύνης των ζωνών δικτύου και τη σημασία των υπηρεσιών που προστατεύονται. Η σειριακή εκτέλεση εξασφαλίζεται με τη διατήρηση της σειράς των γραμμών (row index) του υπολογιστικού φύλλου κατά την παραγωγή του XML κώδικα. Ο κανόνας στη γραμμή 2 του Excel θα εισαχθεί ψηλότερα στο δέντρο XML (XML tree) από τον κανόνα στη γραμμή 3, εγγυώμενος την επιθυμητή ιεραρχία ελέγχου (Top-Down evaluation).

Η προσέγγιση αυτή ενισχύει τη διαφάνεια και τη διαχειρισιμότητα των κανόνων firewall, ιδιαίτερα σε περιβάλλοντα SMEs όπου οι διαθέσιμοι πόροι διαχείρισης είναι περιορισμένοι.

4.6 Σχεδίαση ενσωμάτωσης Threat Intelligence (pfBlockerNG)

Στο πλαίσιο της προτεινόμενης λύσης, η αξιοποίηση Threat Intelligence αντιμετωπίζεται ως συμπληρωματικό επίπεδο προστασίας της αρχιτεκτονικής ασφάλειας. Οι πληροφορίες αυτές χρησιμοποιούνται για την προληπτική αναγνώριση και φιλτράρισμα γνωστών κακόβουλων διευθύνσεων IP, domains και δικτυακών υποδομών που συνδέονται με κακόβουλη δραστηριότητα (ENISA, 2021).

Η ενσωμάτωση του Threat Intelligence υλοποιείται μέσω του μηχανισμού pfBlockerNG, ο οποίος αποτελεί επέκταση του pfSense και παρέχει δυνατότητες δυναμικής εισαγωγής και διαχείρισης blocklists. Οι λίστες αυτές προέρχονται από εξωτερικές πηγές πληροφοριών απειλών (threat intelligence feeds) και ενημερώνονται σε τακτική βάση.

Ωστόσο, η αρχιτεκτονική της προτεινόμενης λύσης δεν βασίζεται αποκλειστικά σε αυτοματοποιημένο αποκλεισμό διευθύνσεων. Οι πληροφορίες απειλών εντάσσονται στο συνολικό πλαίσιο της πολιτικής ασφάλειας και υπόκεινται στον έλεγχο του διαχειριστή. Με τον τρόπο αυτό αποφεύγονται περιπτώσεις υπερβολικού φιλτραρίσματος που θα μπορούσαν να επηρεάσουν τη νόμιμη λειτουργία του δικτύου.

Οι λίστες threat intelligence λειτουργούν επομένως ως εξωτερική πηγή πληροφορίας που ενισχύει την αμυντική ικανότητα του firewall, χωρίς να παρακάμπτει τη βασική λογική της πολιτικής ασφάλειας και της ιεράρχησης των κανόνων.

Η προσέγγιση αυτή είναι ιδιαίτερα κατάλληλη για περιβάλλοντα SMEs, καθώς επιτρέπει την ενσωμάτωση σύγχρονων μηχανισμών προληπτικής άμυνας χωρίς την ανάγκη πολύπλοκων αρχιτεκτονικών ασφάλειας ή εξειδικευμένων υποδομών.

Επομένως, το pfBlockerNG δεν λειτουργεί ως αυτόνομος μηχανισμός λήψης αποφάσεων, αλλά ως υποστηρικτικό στοιχείο της συνολικής πολιτικής ασφάλειας που επιβάλλεται μέσω του pfSense.

5 ΚΕΦΑΛΑΙΟ 5 – ΕΡΓΑΣΤΗΡΙΑΚΗ ΥΛΟΠΟΙΗΣΗ (PoC)

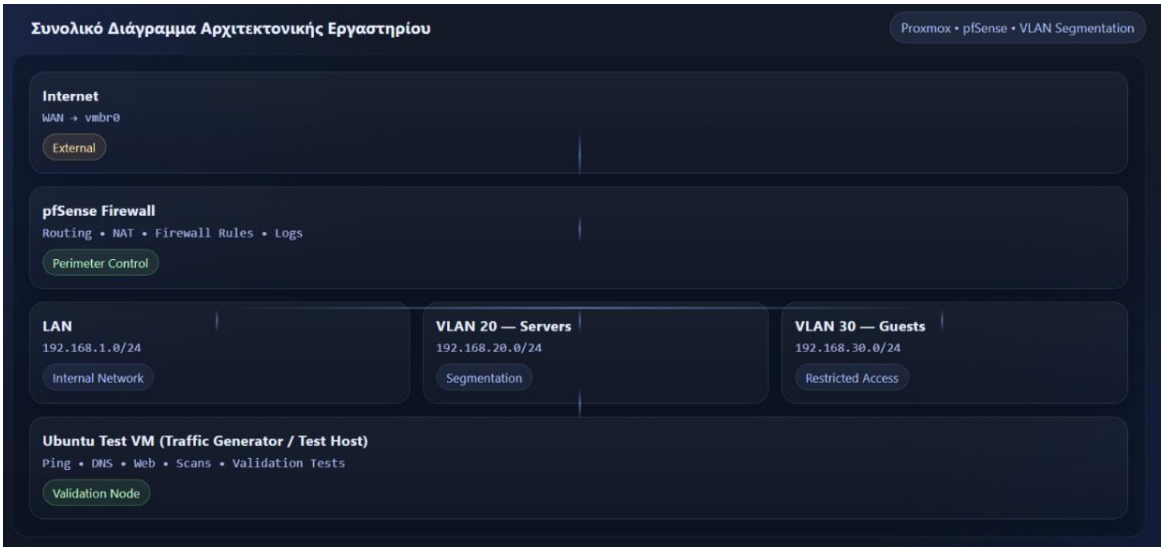
5.1 Περιγραφή εργαστηριακής αρχιτεκτονικής

Η εργαστηριακή υλοποίηση της προτεινόμενης λύσης σχεδιάστηκε με στόχο την όσο το δυνατόν πιστότερη προσομοίωση ενός πραγματικού περιβάλλοντος SME, στο οποίο η διαχείριση των κανόνων firewall πραγματοποιείται από περιορισμένο αριθμό διαχειριστών υπό αυξημένες απαιτήσεις ασφάλειας, ιχνηλασιμότητας και ελέγχου αλλαγών (ISO/IEC 27001, 2022).

Η αρχιτεκτονική βασίζεται σε εικονικοποιημένη υποδομή τύπου υπερδιαχειριστή επιπέδου 1 (Type-1 hypervisor), με χρήση του Proxmox. Στο περιβάλλον αυτό εγκαταστάθηκε το pfSense Community Edition ως κεντρικό firewall και σημείο ελέγχου της δικτυακής κίνησης. Το pfSense τοποθετήθηκε λογικά μεταξύ του εξωτερικού δικτύου (WAN) και των εσωτερικών ζωνών του δικτύου, αναλαμβάνοντας τον ρόλο του προεπιλεγμένου δρομολογητή (default gateway) και του μηχανισμού επιβολής πολιτικών ασφάλειας (policy enforcement).

Η εργαστηριακή διάταξη περιλαμβάνει επίσης σταθμό διαχείρισης για τον ορισμό και τον μετασχηματισμό των πολιτικών ασφάλειας, καθώς και απομονωμένα εσωτερικά συστήματα δοκιμών τοποθετημένα πίσω από το pfSense. Τα συστήματα αυτά χρησιμοποιήθηκαν για την παραγωγή δικτυακής κίνησης και την επαλήθευση της ορθής εφαρμογής των κανόνων firewall σε ελεγχόμενο περιβάλλον.

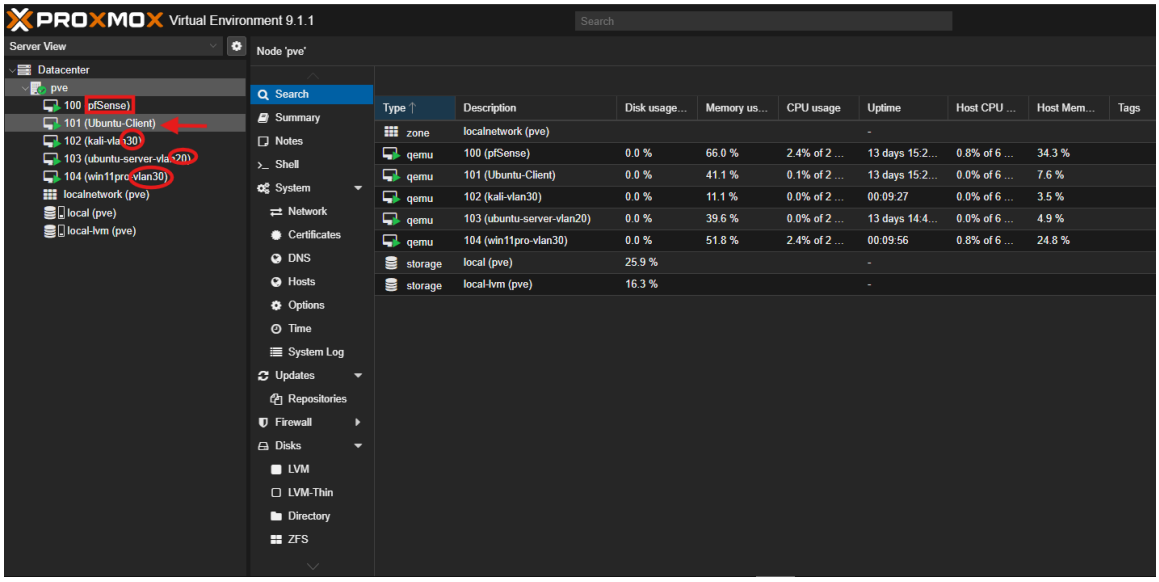
Πριν από την παρουσίαση των επιμέρους παραμέτρων, η Εικόνα 5-1 αποτυπώνει συνοπτικά το σύνολο της εργαστηριακής αρχιτεκτονικής από το επίπεδο WAN έως τις εσωτερικές ζώνες, ώστε να είναι σαφής η θέση του pfSense ως κεντρικού σημείου ελέγχου.



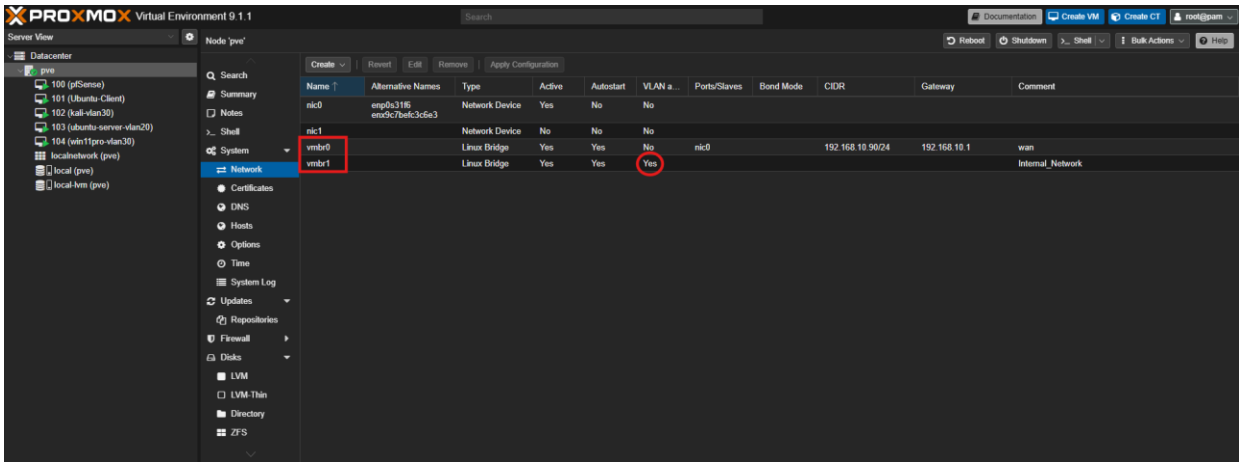
Εικόνα 5-1: Συνολικό διάγραμμα εργαστηριακής αρχιτεκτονικής (PoC) με pfSense ως κεντρικό σημείο ελέγχου, τμηματοποίηση σε LAN/VLANs και Ubuntu test VM για παραγωγή κίνησης και επικύρωση πολιτικών.

Η επιλογή της συγκεκριμένης διάταξης επιτρέπει την πλήρη απομόνωση της κίνησης δοκιμών από το σύστημα διαχείρισης, διασφαλίζοντας ότι κάθε πακέτο που παράγεται από το Ubuntu Test VM διέρχεται υποχρεωτικά από το pfSense. Με τον τρόπο αυτό καθίσταται δυνατή η ακριβής συσχέτιση κάθε επιτρεπόμενης ή απορριπτόμενης σύνδεσης με τον αντίστοιχο κανόνα firewall, όπως αυτός έχει οριστεί μέσω του Excel template και έχει εισαχθεί στο σύστημα.

Η Εικόνα 5-2 παρουσιάζει την κεντρική διεπαφή διαχείρισης του Proxmox VE με επισκόπηση των εικονικών μηχανών του εργαστηριακού περιβάλλοντος. Παράλληλα, η Εικόνα 5-3 απεικονίζει τη ρύθμιση των εικονικών γεφυρών (Linux Bridges), μέσω των οποίων διαχωρίζεται το WAN από το LAN. Με τον τρόπο αυτό, κάθε πακέτο που παράγεται από τις δοκιμαστικές εικονικές μηχανές διέρχεται υποχρεωτικά από το pfSense, επιτρέποντας την εφαρμογή και αξιολόγηση των κανόνων firewall που έχουν οριστεί στο σύστημα.



Εικόνα 5-2: Κεντρική οθόνη διαχείρισης του Proxmox VE με επισκόπηση των εικονικών μηχανών



Εικόνα 5-3: Ρύθμιση εικονικών γεφυρών (Linux Bridges). Η vmbr0 συνδέεται στο φυσικό δίκτυο (WAN), ενώ η vmbr1 αποτελεί το απομονωμένο εσωτερικό δίκτυο (LAN).

5.2 Υποδομή Firewall

Η υλοποίηση του Firewall Host βασίστηκε στο pfSense Community Edition, το οποίο επιλέχθηκε λόγω της ευρείας χρήσης του σε περιβάλλοντα SMEs και της δυνατότητάς του να συνδυάζει λειτουργίες firewall, δρομολόγησης (routing) και μηχανισμούς ασφάλειας σε ένα ενιαίο σύστημα. Η εγκατάσταση πραγματοποιήθηκε ως εικονική μηχανή σε περιβάλλον

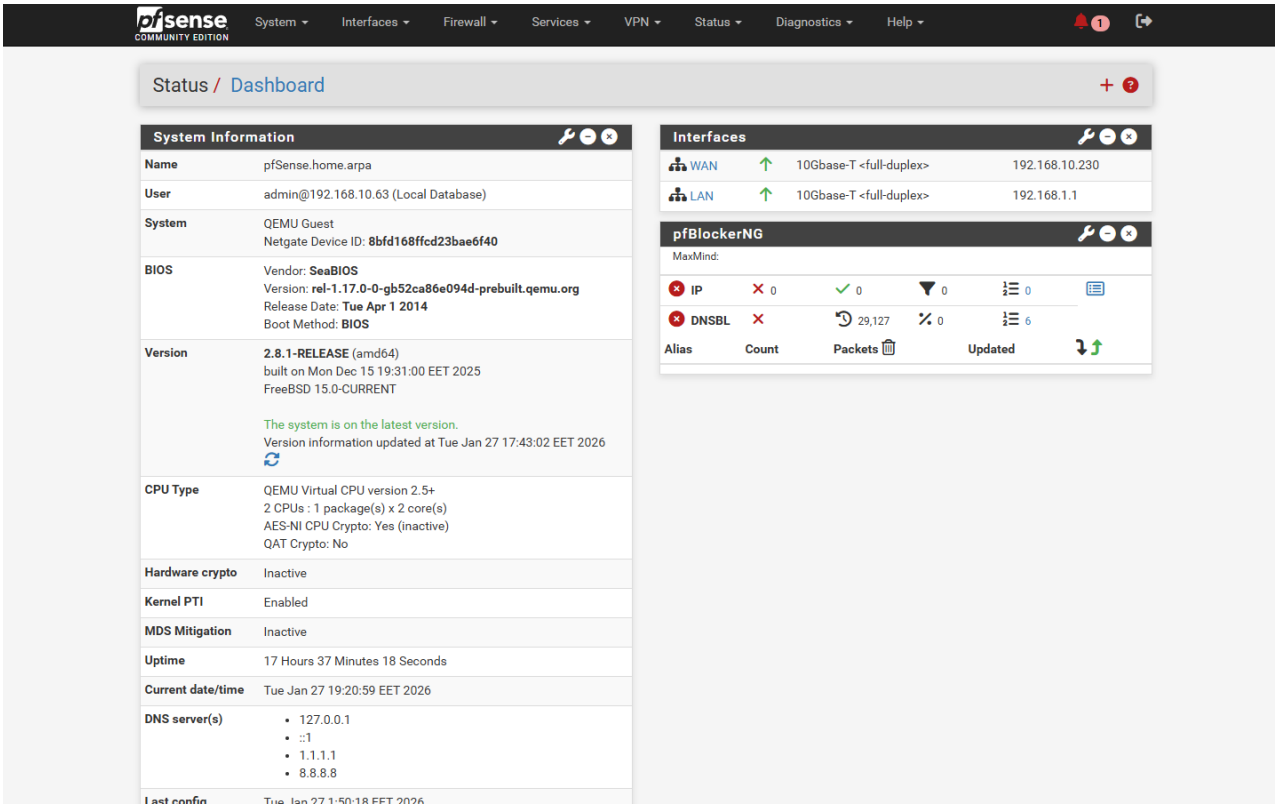
εικονικοποίησης, επιτρέποντας ευελιξία στην κατανομή πόρων και ασφαλή επαναφορά της κατάστασης του συστήματος κατά τη διάρκεια των πειραματικών δοκιμών μέσω snapshots.

Το firewall διαθέτει δύο κύριες δικτυακές διεπαφές. Η διεπαφή WAN συνδέεται με το εξωτερικό δίκτυο και χρησιμοποιείται για την προσομοίωση πρόσβασης στο Διαδίκτυο, ενώ η διεπαφή LAN εξυπηρετεί το εσωτερικό δίκτυο στο οποίο βρίσκεται το Test VM (Ubuntu Client). Η διάκριση αυτή είναι κρίσιμη, καθώς επιτρέπει σαφή διαχωρισμό μεταξύ εξωτερικής και εσωτερικής κίνησης, πρακτική που αποτελεί θεμελιώδη αρχή στον σχεδιασμό ασφαλών δικτυακών υποδομών (NIST, 2020).

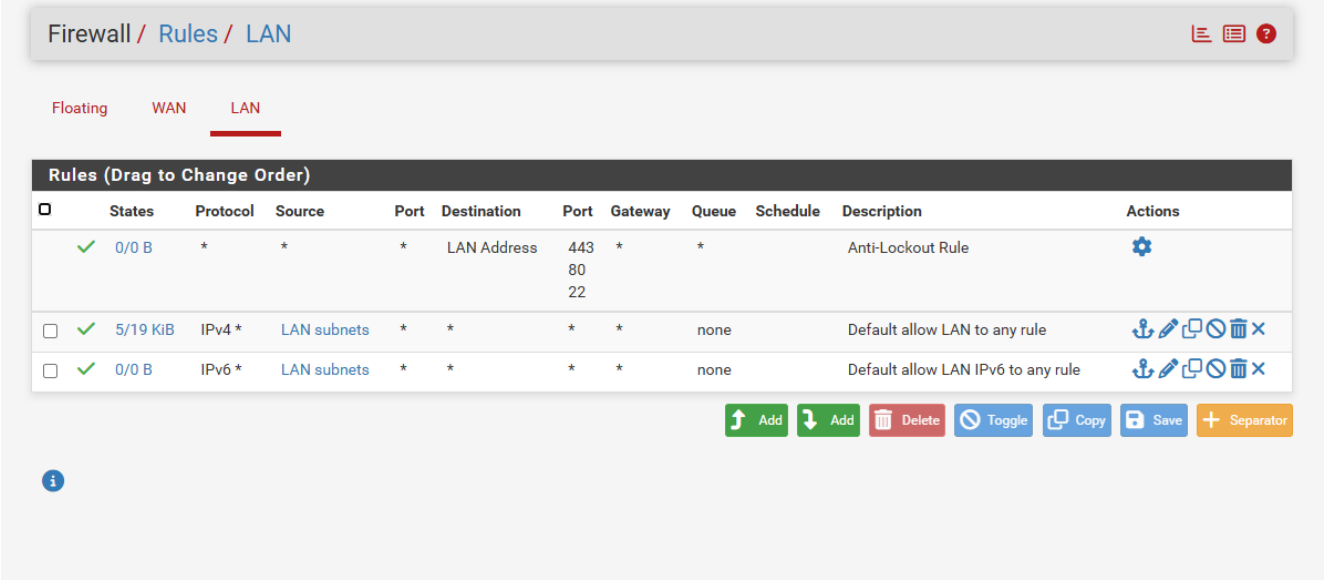
Κατά τη ρύθμιση του pfSense διατηρήθηκαν προεπιλεγμένοι κανόνες ασφαλείας, όπως ο κανόνας anti-lockout στη διεπαφή LAN, ώστε να διασφαλίζεται η συνεχής πρόσβαση στο περιβάλλον διαχείρισης. Οι βασικές ρυθμίσεις του firewall περιλαμβάνουν επιθεώρηση πακέτων με κατάσταση (stateful packet inspection), καταγραφή συμβάντων (logging) για τους κανόνες που ενεργοποιούνται στο πλαίσιο της πειραματικής διαδικασίας, καθώς και υποστήριξη πρόσθετων πακέτων ασφάλειας για threat intelligence.

Η κεντρική θέση του pfSense στην αρχιτεκτονική καθιστά το Firewall Host μοναδικό σημείο επιβολής πολιτικών ασφάλειας (policy enforcement point). Κάθε εισερχόμενη ή εξερχόμενη σύνδεση από το εσωτερικό δίκτυο διέρχεται υποχρεωτικά από το firewall, γεγονός που επιτρέπει ακριβή παρακολούθηση και αξιολόγηση της αποτελεσματικότητας των κανόνων που εισάγονται μέσω της προτεινόμενης αυτοματοποιημένης διαδικασίας.

Η κατάσταση του Firewall Host και οι ενεργές διεπαφές του παρουσιάζονται στην Εικόνα 5-4. Επιπλέον, στην Εικόνα 5-5 αποτυπώνεται το σύνολο των βασικών κανόνων Lan πριν από την εισαγωγή των κανόνων που παράγονται από το πρότυπο Excel, ώστε να υπάρχει σαφές σημείο αναφοράς (baseline) για τη σύγκριση πριν και μετά την αυτοματοποίηση.



Εικόνα 5-4:pfSense Dashboard

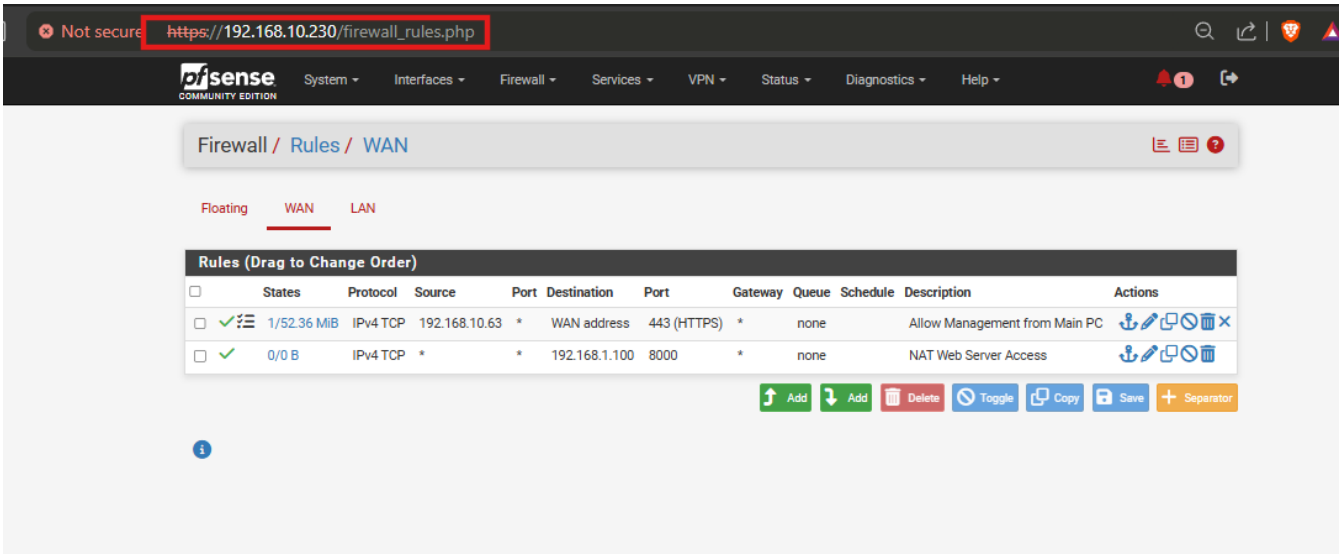


Εικόνα 5-5: Προεπιλεγμένοι κανόνες firewall στο pfSense απεικονίζεται το σύνολο των βασικών κανόνων firewall πριν από την εισαγωγή των κανόνων που προκύπτουν από το Excel templateοκύπτουν από το Excel template

Για λόγους ασφαλούς απομακρυσμένης διαχείρισης, το pfSense δεν επιτρέπει default deny πρόσβαση από το WAN προς το διαχειριστικό του περιβάλλον (WebGUI). Στο παρόν σενάριο

υλοποιήθηκε ελεγχόμενη πρόσβαση διαχείρισης, επιτρέποντας συνδέσεις μόνο από συγκεκριμένη διεύθυνση IP διαχειριστή και μόνο της υπηρεσίας ιστού Hypertext Transfer Protocol Secure (HTTPS) (TCP/443), ως πρακτική περιορισμού της επιφάνειας επίθεσης (attack surface) (NIST, 2020).

Δημιουργήθηκε κανόνας στο WAN interface, ο οποίος επιτρέπει την πρόσβαση στο WebGUI του pfSense αποκλειστικά από τον υπολογιστή διαχείρισης (Admin PC) με IP: 192.168.10.63, μέσω του πρωτοκόλλου HTTPS (TCP/443). Όπως φαίνεται στην Εικόνα 5-6, ο κανόνας επιτρέπει μόνο τη συγκεκριμένη σύνδεση διαχείρισης, περιορίζοντας την πρόσβαση στο περιβάλλον διαχείρισης του firewall από μη εξουσιοδοτημένα συστήματα



Εικόνα 5-6: Επιτρεπόμενη ασφαλής πρόσβαση διαχείρισης από τον υπολογιστή διαχειριστή

Απόπειρα πρόσβασης στο WebGUI από διαφορετική διεύθυνση IP εκτός της επιτρεπόμενης απέτυχε, με την κίνηση να απορρίπτεται από το firewall. Η απόρριψη επιβεβαιώθηκε μέσω των αρχείων καταγραφής κανόνων (Firewall Logs), όπου καταγράφεται ενέργεια απόρριψης (block) στο WAN interface:

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Jan 29 15:49:37	WAN	Default deny rule IPv4 (1000000103)	192.168.10.164:33506	192.168.10.230:443	TCP:S
✕	Jan 29 15:49:05	WAN	Default deny rule IPv4 (1000000103)	192.168.10.164:33506	192.168.10.230:443	TCP:S
✕	Jan 29 15:48:49	WAN	Default deny rule IPv4 (1000000103)	192.168.10.164:33506	192.168.10.230:443	TCP:S
✕	Jan 29 15:48:40	WAN	Default deny rule IPv4 (1000000103)	192.168.10.164:33506	192.168.10.230:443	TCP:S
✕	Jan 29 15:48:36	WAN	Default deny rule IPv4 (1000000103)	192.168.10.164:33506	192.168.10.230:443	TCP:S
✕	Jan 29 15:48:34	WAN	Default deny rule IPv4 (1000000103)	192.168.10.164:33506	192.168.10.230:443	TCP:S
✕	Jan 29 15:48:33	WAN	Default deny rule IPv4 (1000000103)	192.168.10.164:33506	192.168.10.230:443	TCP:S
✕	Jan 29 15:48:32	WAN	Default deny rule IPv4 (1000000103)	192.168.10.164:33506	192.168.10.230:443	TCP:S

Εικόνα 5-7: pfSense WAN firewall logs – Απόρριψη μη εξουσιοδοτημένης σύνδεσης (TCP/443)- Source: 192.168.10.164(kali) -Destination: 192.168.10.230:443(webgui firewall) – Rule: Default Deny Rule IPv4

5.3 Υποδομή Σταθμού Διαχείρισης (Management) και Συστήματος Δοκιμών

Η εργαστηριακή υποδομή συμπληρώνεται από τον κύριο σταθμό εργασίας (Main Workstation) και το Test Vm, τα οποία διαδραματίζουν διακριτούς αλλά συμπληρωματικούς ρόλους στην πειραματική διαδικασία. Ο Main Workstation χρησιμοποιήθηκε ως σύστημα διαχείρισης και ανάπτυξης, ενώ το Test VM τοποθετήθηκε πίσω από το pfSense και αξιοποιήθηκε αποκλειστικά για την παραγωγή και τον έλεγχο δικτυακής κίνησης.

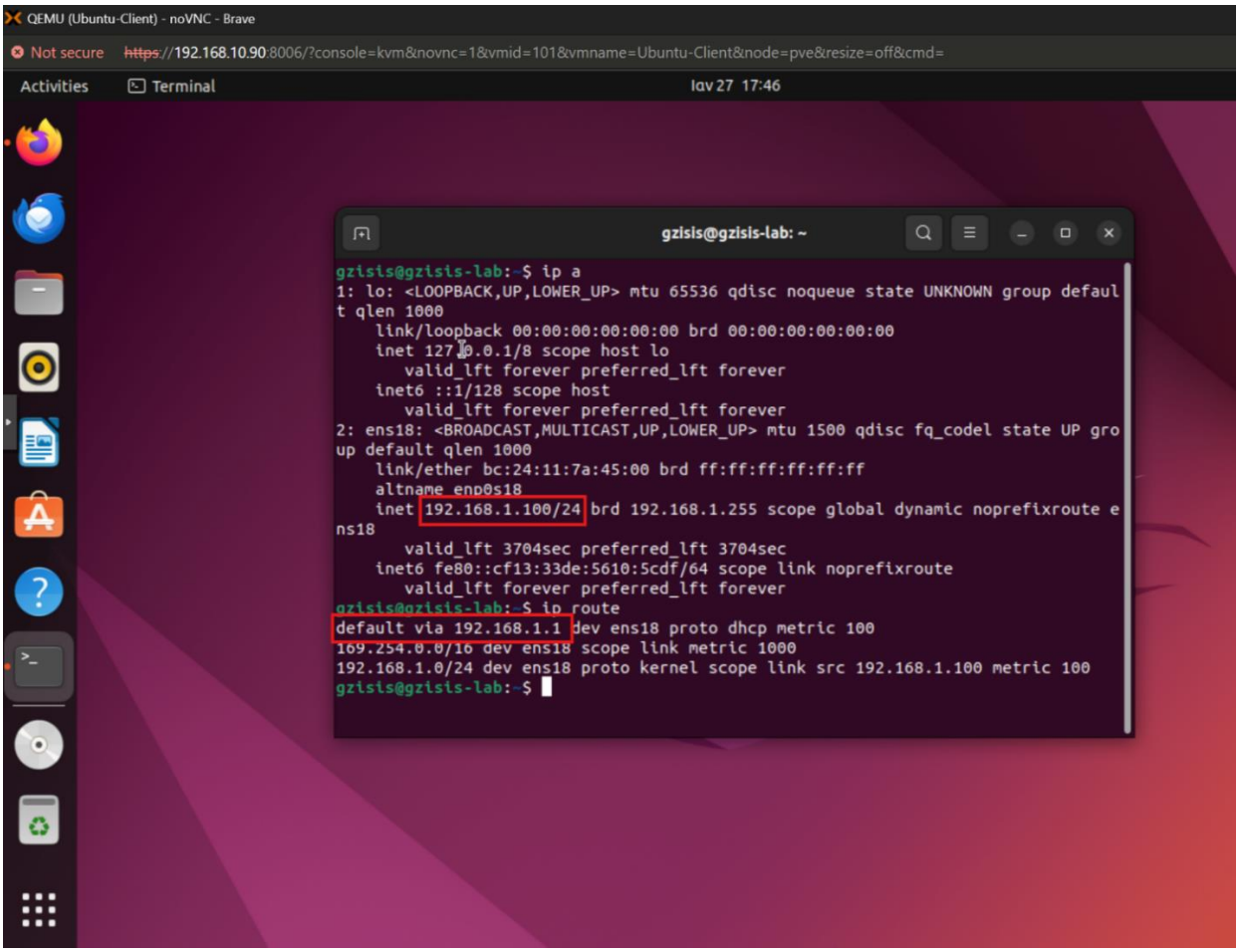
Ο Main Workstation φιλοξενεί τα εργαλεία που απαιτούνται για τη δημιουργία και επεξεργασία του προτύπου Excel, καθώς και για την εκτέλεση των αυτοματοποιημένων διαδικασιών μετασχηματισμού των κανόνων σε μορφή συμβατή με τις ρυθμίσεις του pfSense. Με τον τρόπο αυτό, προσομοιώνεται ο ρόλος ενός IT administrator σε SME, ο οποίος κατά κανόνα βασίζεται σε δομημένα εργαλεία πολιτικής και όχι σε χειροκίνητες παρεμβάσεις στο firewall σε χαμηλό επίπεδο παραμετροποίησης.

Το Test VM βασίστηκε σε Ubuntu Linux και τοποθετήθηκε αποκλειστικά στο LANS πίσω από το pfSense. Η διεύθυνση IP εκχωρήθηκε από το LAN υποδίκτυο του firewall, διασφαλίζοντας ότι κάθε εξερχόμενη σύνδεση προς το Διαδίκτυο διέρχεται υποχρεωτικά από τους μηχανισμούς ελέγχου του pfSense. Το Test VM δεν διαθέτει άμεση πρόσβαση στο WAN και δεν παρακάμπτει τους κανόνες ασφάλειας που εφαρμόζονται στο firewall.

Στο Test VM εκτελέστηκαν οι δοκιμές επαλήθευσης των κανόνων firewall, όπως προσπάθειες σύνδεσης σε συγκεκριμένες θύρες, έλεγχοι επιτρεπόμενης και απορριπτόμενης κίνησης, καθώς και δοκιμές βασικών πρωτοκόλλων δικτύου. Η χρήση απομονωμένου εικονικού συστήματος για τις δοκιμές επιτρέπει ασφαλή αξιολόγηση των πολιτικών, χωρίς κίνδυνο επίδρασης στον σταθμό διαχείρισης ή σε άλλους κρίσιμους πόρους.

Η σαφής διάκριση μεταξύ Main Workstation και Test VM ενισχύει τη μεθοδολογική καθαρότητα της πειραματικής διαδικασίας: ο σχεδιασμός και η εισαγωγή πολιτικών πραγματοποιούνται σε ελεγχόμενο περιβάλλον, ενώ η λειτουργική επαλήθευση βασίζεται σε πραγματική κίνηση από σύστημα πίσω από το firewall. Η προσέγγιση αυτή διευκολύνει την επαναληψιμότητα και την τεκμηρίωση των δοκιμών (NIST, 2020).

Για την επιβεβαίωση της σωστής δικτυακής διαμόρφωσης του δοκιμαστικού συστήματος πραγματοποιήθηκε έλεγχος της IP διεύθυνσης και του προεπιλεγμένου δρομολογητή (default gateway) στο Test VM.



Εικόνα 5-8: Επαλήθευση IP διευθυνσιοδότησης και default gateway στον σταθμό διαχείρισης.

Όπως φαίνεται στην Εικόνα 5-8, το σύστημα έχει λάβει τη διεύθυνση 192.168.1.100/24, ενώ ως προεπιλεγμένος δρομολογητής έχει οριστεί η διεύθυνση 192.168.1.1, η οποία αντιστοιχεί στη διεπαφή του pfSense στο εσωτερικό δίκτυο. Η ρύθμιση αυτή διασφαλίζει ότι όλη η εξερχόμενη κίνηση του Test VM διέρχεται από το firewall, επιτρέποντας την εφαρμογή και αξιολόγηση των κανόνων ασφάλειας.

5.4 Απομόνωση δικτυακής κίνησης και σχεδιαστική λογική της αρχιτεκτονικής

Η απομόνωση της δικτυακής κίνησης αποτέλεσε βασική σχεδιαστική αρχή της εργαστηριακής υλοποίησης, καθώς επιτρέπει την αξιόπιστη αξιολόγηση της αποτελεσματικότητας των κανόνων firewall χωρίς παρεμβολές από εξωτερικούς παράγοντες. Στο πλαίσιο της

προτεινόμενης αρχιτεκτονικής, η απομόνωση επιτεύχθηκε μέσω της λογικής τμηματοποίησης του εσωτερικού δικτύου σε διακριτές ζώνες εμπιστοσύνης (trust zones), συγκεκριμένα στα VLAN20_SERVERS και VLAN30_GUEST, πίσω από το pfSense, το οποίο λειτουργεί ως το μοναδικό σημείο ελέγχου της δικτυακής κίνησης.

Η συγκεκριμένη διάταξη διασφαλίζει ότι κάθε εξερχόμενη σύνδεση από τα εσωτερικά συστήματα προς το διαδίκτυο, καθώς και κάθε απόκριση εισερχόμενης κίνησης, διέρχεται υποχρεωτικά από τους μηχανισμούς φιλτραρίσματος του pfSense. Με τον τρόπο αυτό καθίσταται δυνατή η πλήρης επιβολή των κανόνων ασφαλείας και η ακριβής καταγραφή των αποφάσεων αποδοχής ή απόρριψης της κίνησης σε επίπεδο firewall. Η απουσία εναλλακτικών διαδρομών επικοινωνίας αποτρέπει την παράκαμψη των πολιτικών και ενισχύει την εγκυρότητα των πειραματικών αποτελεσμάτων.

Η πολιτική απομόνωσης υλοποιήθηκε ως εξής:

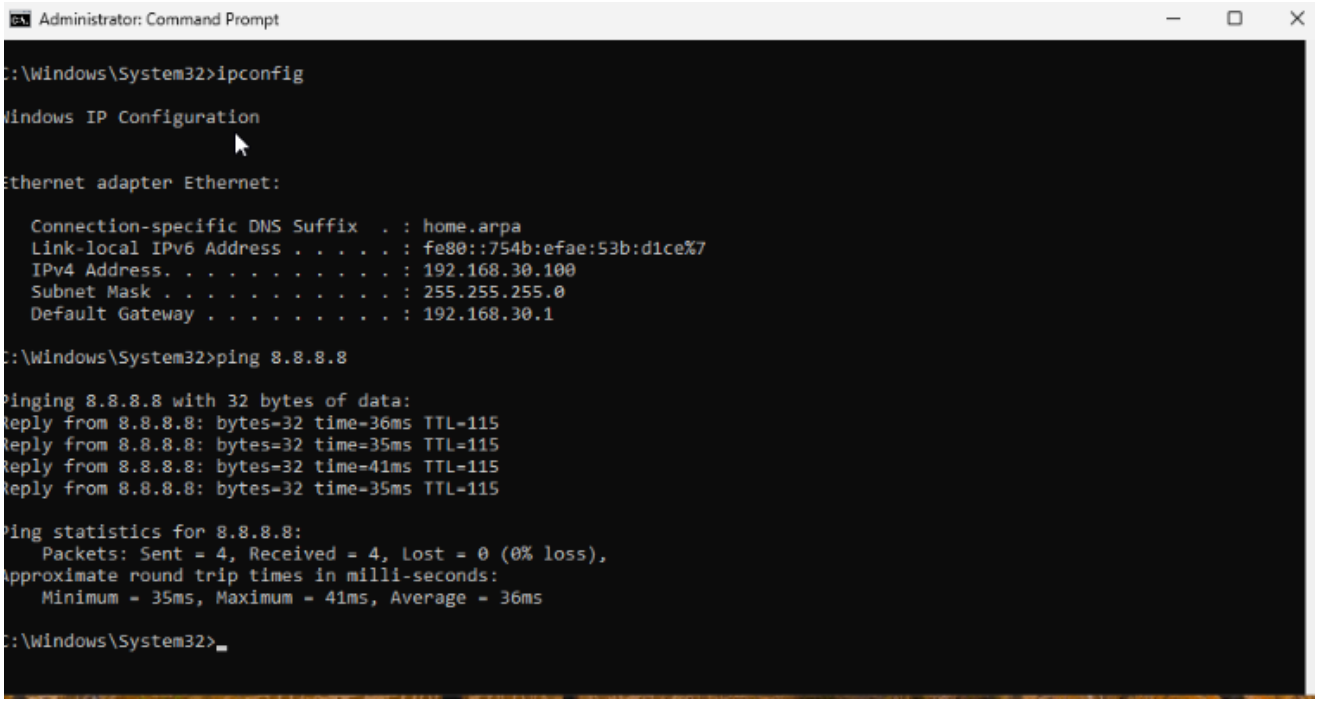
- Το VLAN30_GUEST διαθέτει πρόσβαση μόνο προς το διαδίκτυο.
- Απαγορεύεται η πρόσβαση του VLAN30_GUEST προς τα εσωτερικά δίκτυα (RFC1918).
- Απαγορεύεται η πρόσβαση του VLAN30_GUEST στο διαχειριστικό περιβάλλον του firewall.
- Το VLAN20_SERVERS διαθέτει πρόσβαση προς το διαδίκτυο.
- Απαγορεύεται η επικοινωνία μεταξύ VLAN20_SERVERS και VLAN30_GUEST.

Η προσέγγιση αυτή ενσωματώνει την αρχή του ελάχιστου προνομίου (least privilege) και περιορίζει δραστικά την πλευρική κίνηση (lateral movement) σε περίπτωση παραβίασης ενός συστήματος χαμηλής εμπιστοσύνης.

Για την επιβεβαίωση της ορθής εφαρμογής των παραπάνω κανόνων, πραγματοποιήθηκε σειρά λειτουργικών δοκιμών (functional validation tests).

1. Έλεγχος πρόσβασης VLAN30_GUEST προς Διαδίκτυο

   Από σταθμό εργασίας του VLAN30_GUEST (192.168.30.100) πραγματοποιήθηκε δοκιμή ICMP επικοινωνίας προς εξωτερικό εξυπηρετητή (8.8.8.8). Η επικοινωνία ολοκληρώθηκε επιτυχώς, επιβεβαιώνοντας τη σωστή λειτουργία των κανόνων NAT και των επιτρεπτικών κανόνων εξερχόμενης κίνησης.



Εικόνα 5-9: Λειτουργική επαλήθευση παραμετροποίησης δικτύου και εξερχόμενης συνδεσιμότητας από σταθμό εργασίας (LAN) προς εξωτερικό προορισμό στο πλαίσιο ελέγχου της εφαρμογής των firewall policies

Η επιτυχής δρομολόγηση της κίνησης επιβεβαιώθηκε και από τα αρχεία καταγραφής του firewall (pfSense Firewall Logs), όπου καταγράφεται η επιτρεπόμενη εξερχόμενη σύνδεση από τον σταθμό εργασίας του VLAN30_GUEST προς τον εξωτερικό προορισμό 8.8.8.8 μέσω του κανόνα “Guest to Internet”. Η καταγραφή αυτή επιβεβαιώνει ότι η κίνηση διήλθε από τον μηχανισμό ελέγχου του firewall και εγκρίθηκε σύμφωνα με την εφαρμοζόμενη πολιτική ασφάλειας.

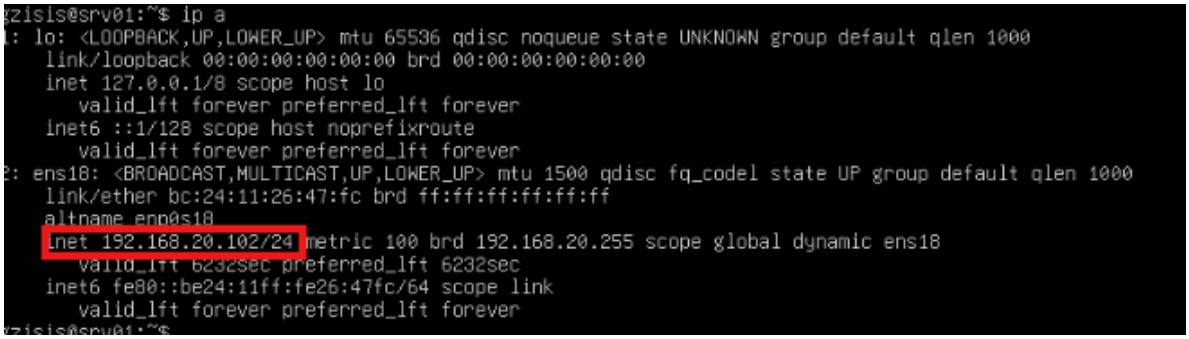
✕	Mar 4 17:05:16	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✕	Mar 4 17:05:12	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Mar 4 17:05:11	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✕	Mar 4 17:05:06	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✓	Mar 4 17:05:06	VLAN30_GUEST	USER_RULE (1772615798)	192.168.30.100:60556	192.168.30.1:53	UDP
✓	Mar 4 17:05:05	VLAN30_GUEST	Guest to Internet (1770287515)	192.168.30.100	8.8.8.8	ICMP
✓	Mar 4 17:05:02	VLAN30_GUEST	Guest to Internet (1770287515)	192.168.30.100:64272	51.104.136.2:443	TCP:S
✓	Mar 4 17:05:02	VLAN30_GUEST	Guest to Internet (1770287515)	192.168.30.100:64271	40.126.53.10:443	TCP:S
✓	Mar 4 17:05:02	VLAN30_GUEST	USER_RULE (1772615798)	192.168.30.100:51557	192.168.30.1:53	UDP
✓	Mar 4 17:05:01	VLAN30_GUEST	USER_RULE (1772615798)	192.168.30.100:57095	192.168.30.1:53	UDP
✕	Mar 4 17:05:01	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✕	Mar 4 17:05:01	WAN	Default deny rule IPv4 (1000000103)	192.168.10.17:56700	255.255.255.255:56700	UDP
✓	Mar 4 17:05:01	VLAN30_GUEST	Guest to Internet (1770287515)	192.168.30.100:64270	204.79.197.222:443	TCP:S
✓	Mar 4 17:05:00	VLAN30_GUEST	USER_RULE (1772615798)	192.168.30.100:56700	192.168.30.1:53	UDP
✓	Mar 4 17:05:00	VLAN30_GUEST	USER_RULE (1772615798)	192.168.30.100:63142	192.168.30.1:53	UDP
✕	Mar 4 17:05:00	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP

Εικόνα 5-10: pfSense firewall logs – Επιτρεπόμενη εξερχόμενη επικοινωνία από το VLAN30_GUEST (192.168.30.100) προς εξωτερικό προορισμό (8.8.8.8) μέσω του κανόνα "Guest to Internet".

2. Έλεγχος αποκλεισμού πρόσβασης VLAN30_GUEST προς VLAN20_SERVERS Πραγματοποιήθηκε προσπάθεια επικοινωνίας από 192.168.30.100 προς διεύθυνση του δικτύου 192.168.20.0/24. Η σύνδεση απορρίφθηκε επιτυχώς από το firewall όπως φαίνεται στην Εικόνα 5-13, γεγονός που επιβεβαιώθηκε τόσο από την αποτυχία ICMP επικοινωνίας όσο και από σχετικές καταγραφές "Default deny rule" στα αρχεία καταγραφής του pfSense.

```
C:\Windows\System32>ping 192.168.20.102

Pinging 192.168.20.102 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 192.168.20.102:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Windows\System32>
```

Εικόνα 5-11: Προσπάθεια επικοινωνίας από 192.168.30.100 προς διεύθυνση του δικτύου 192.168.20.0/24



Εικόνα 5-12: Διεύθυνση IP του Ubuntu server στο VLAN20_SERVERS (192.168.20.102)

Η απόρριψη της επικοινωνίας επιβεβαιώθηκε και από τα αρχεία καταγραφής του firewall (pfSense Firewall Logs) (*Εικόνα 5 -13*), όπου καταγράφεται ρητά η απόπειρα επικοινωνίας από τον σταθμό του VLAN30_GUEST (192.168.30.100) προς τον εξυπηρετητή του VLAN20_SERVERS (192.168.20.102) μέσω ICMP. Η κίνηση απορρίφθηκε από τον κανόνα “Block Guest to Internal Networks”, ο οποίος απαγορεύει την πρόσβαση του δικτύου επισκεπτών προς τα εσωτερικά δίκτυα της υποδομής.

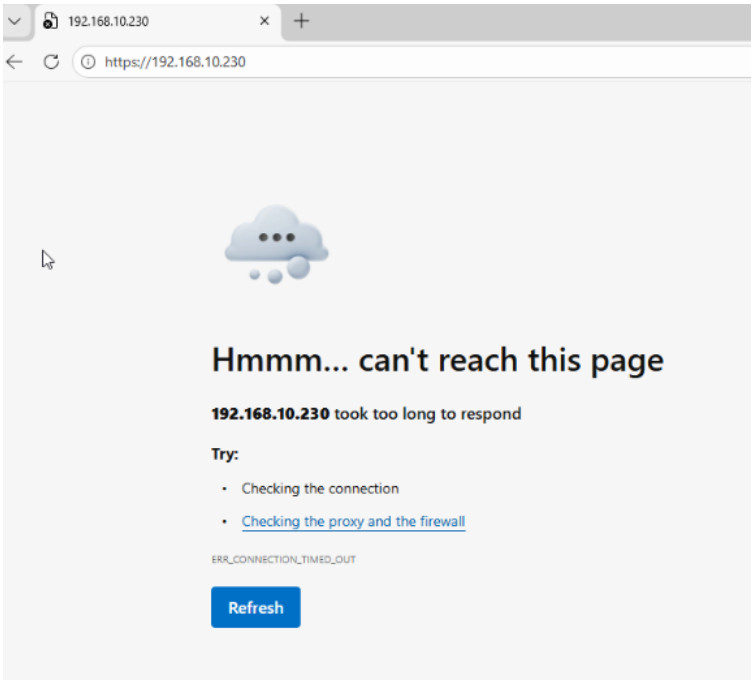
Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Mar 4 17:11:16	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✕	Mar 4 17:11:15	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Mar 4 17:11:11	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✕	Mar 4 17:11:06	VLAN30_GUEST	Block Guest to Internal Networks (1770287704)	192.168.30.100	192.168.20.102	ICMP
✕	Mar 4 17:11:06	WAN	Default deny rule IPv4 (1000000103)	192.168.10.17:56934	255.255.255.255:9999	UDP
✕	Mar 4 17:11:06	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✕	Mar 4 17:11:03	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Mar 4 17:11:01	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✕	Mar 4 17:11:01	WAN	Default deny rule IPv4 (1000000103)	192.168.10.17:56700	255.255.255.255:56700	UDP

Εικόνα 5-13: pfSense firewall logs – Απόρριψη επικοινωνίας ICMP από το VLAN30_GUEST (192.168.30.100) προς τον εξυπηρετητή του VLAN20_SERVERS (192.168.20.102) σύμφωνα με τον κανόνα “Block Guest to Internal Networks”.

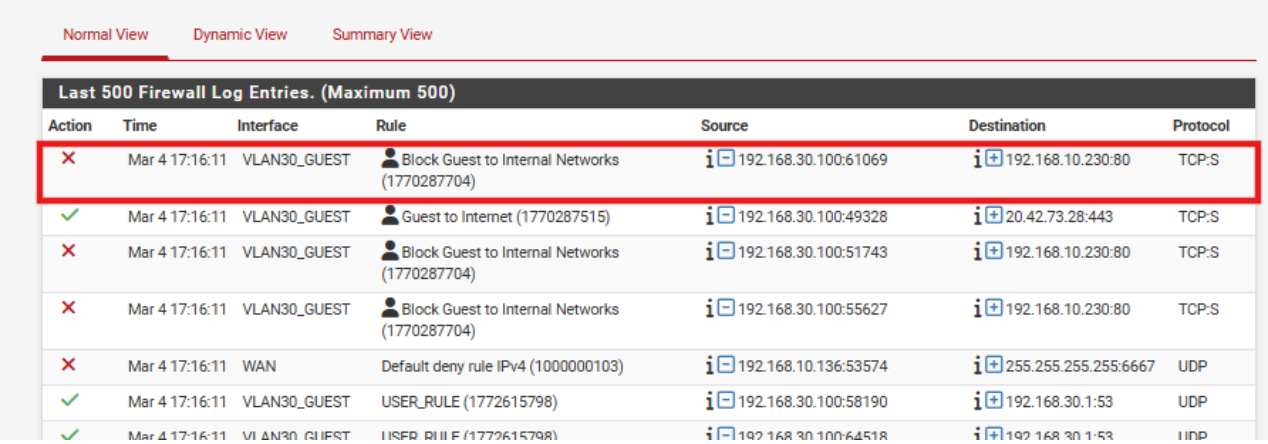
3. Έλεγχος προστασίας διαχειριστικού περιβάλλοντος firewall

Επιχειρήθηκε πρόσβαση στο HTTPS interface του pfSense από το VLAN30_GUEST. Η πρόσβαση αποκλείστηκε, αποδεικνύοντας την ορθή εφαρμογή του κανόνα προστασίας του firewall management interface.



Εικόνα 5-14: Απόπειρα πρόσβασης στο διαχειριστικό περιβάλλον του pfSense από το VLAN30_GUEST, αποδεικνύοντας την ορθή εφαρμογή του κανόνα προστασίας του firewall management interface.

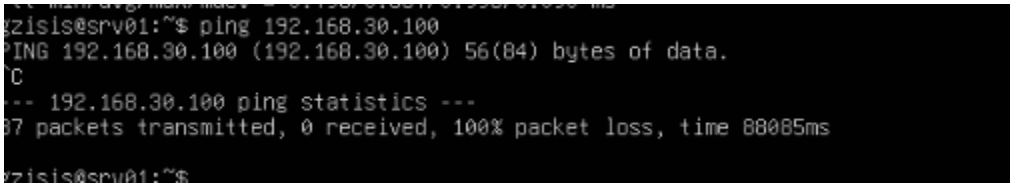
Η απόρριψη της σύνδεσης επιβεβαιώθηκε και από τα αρχεία καταγραφής του firewall (pfSense Firewall Logs) *(Εικόνα 5-15)*, όπου καταγράφεται η προσπάθεια πρόσβασης από τον σταθμό του VLAN30_GUEST (192.168.30.100) προς τη διεύθυνση διαχείρισης του pfSense (192.168.10.230). Η κίνηση απορρίφθηκε από τον κανόνα “Block Guest to Internal Networks”, ο οποίος απαγορεύει την πρόσβαση του δικτύου επισκεπτών προς εσωτερικά συστήματα και το διαχειριστικό περιβάλλον του firewall.



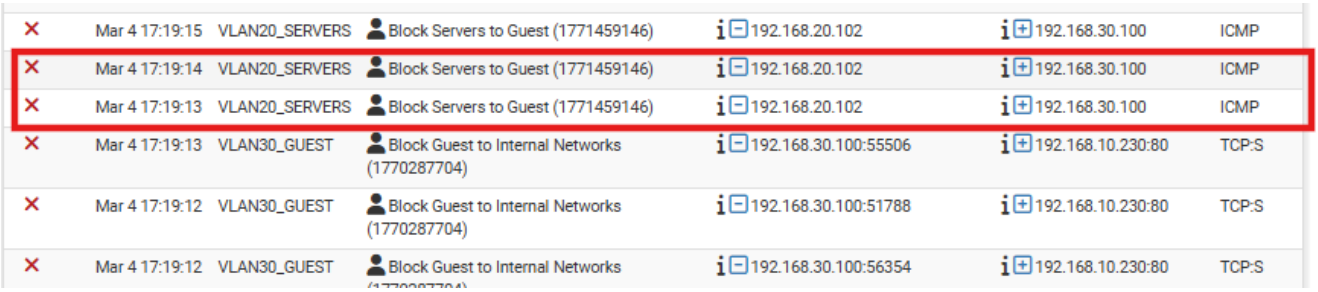
Εικόνα 5-15: pfSense firewall logs – Απόρριψη προσπάθειας πρόσβασης από το VLAN30_GUEST (192.168.30.100) προς το διαχειριστικό περιβάλλον του pfSense (192.168.10.230) σύμφωνα με τον κανόνα “Block Guest to Internal Networks”.

4. Έλεγχος απομόνωσης από πλευράς VLAN20_SERVERS

Από σύστημα του VLAN20_SERVERS πραγματοποιήθηκε δοκιμή επικοινωνίας (*Εικόνα 5-16*) προς διεύθυνση του VLAN30_GUEST. Η σύνδεση απορρίφθηκε, επιβεβαιώνοντας τον αμφίδρομο διαχωρισμό των δύο ζωνών *(Εικόνα 5-16).*



Εικόνα 5-16: η σύνδεση αποκλείστηκε επιτυχώς, επιβεβαιώνοντας τον αμφίδρομο διαχωρισμό των ζωνών.



Εικόνα 5-17: Καταγραφή απορριφθείσας κίνησης από το VLAN20_SERVERS (192.168.20.102) προς εσωτερικές διευθύνσεις (192.168.30.100), επιβεβαιώνοντας την ενεργή εφαρμογή του κανόνα απομόνωσης και την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Η απομόνωση της δικτυακής κίνησης επιτρέπει τον καθαρό διαχωρισμό μεταξύ λειτουργιών διαχείρισης και λειτουργιών δοκιμής. Το Main Workstation χρησιμοποιείται αποκλειστικά για τον σχεδιασμό και την εισαγωγή των κανόνων, ενώ τα συστήματα των επιμέρους VLAN χρησιμοποιούνται για την παραγωγή δικτυακής κίνησης. Αυτή η διάκριση αντικατοπτρίζει πρακτικές που εφαρμόζονται σε πραγματικά περιβάλλοντα SMEs, όπου τα συστήματα διαχείρισης δεν εκτίθενται άμεσα σε μη αξιόπιστες ζώνες.

Ένα επιπλέον πλεονέκτημα της συγκεκριμένης αρχιτεκτονικής είναι η δυνατότητα αξιόπιστης συσχέτισης των αποτελεσμάτων των δοκιμών με τους αντίστοιχους κανόνες firewall. Κάθε απορριπτόμενη ή επιτρεπόμενη σύνδεση καταγράφεται στα αρχεία καταγραφής του pfSense μαζί με την περιγραφή του κανόνα που την ενεργοποίησε, γεγονός που επιτρέπει την άμεση επαλήθευση της ορθής εφαρμογής των πολιτικών που ορίστηκαν μέσω του Excel template.

Η συγκεκριμένη αρχιτεκτονική απομόνωσης διασφαλίζει ότι τα δεδομένα καταγραφής (logs) που παράγονται από το firewall μπορούν να συσχετιστούν άμεσα με τις πειραματικές δοκιμές, οι οποίες παρουσιάζονται και αξιολογούνται στο Κεφάλαιο 6.

5.5 Δημιουργία και χρήση Excel template

Η δημιουργία του προτύπου Excel αποτέλεσε κεντρικό στοιχείο της προτεινόμενης λύσης, καθώς λειτουργεί ως ενδιάμεσο επίπεδο ορισμού πολιτικής (policy abstraction layer) μεταξύ του IT administrator και του firewall. Στόχος του template δεν είναι μόνο η καταγραφή κανόνων, αλλά η τυποποίηση της διαδικασίας ορισμού πολιτικών ασφάλειας με τρόπο δομημένο, ελεγχόμενο και επαναλήψιμο, περιορίζοντας σφάλματα που συχνά προκύπτουν από χειροκίνητη διαχείριση μέσω γραφικού περιβάλλοντος (ENISA, 2023).

Το Excel σχεδιάστηκε ώστε να μπορεί να χρησιμοποιηθεί από διαχειριστές SMEs χωρίς να απαιτείται γνώση της εσωτερικής δομής ή της συντακτικής πολυπλοκότητας του pfSense. Κάθε γραμμή του template αντιστοιχεί σε έναν κανόνα firewall και περιλαμβάνει σαφώς ορισμένα πεδία, όπως η διεπαφή εφαρμογής, το πρωτόκολλο, ο τύπος και η τιμή πηγής και προορισμού, οι θύρες επικοινωνίας, η ενέργεια του κανόνα και η κατάστασή του (ενεργός ή ανενεργός).

Ιδιαίτερη έμφαση δόθηκε στο πεδίο περιγραφής (description), το οποίο χρησιμοποιείται για τεκμηρίωση και για τη διευκόλυνση της ανάλυσης των logs στη φάση αξιολόγησης. Με τον τρόπο αυτό επιτυγχάνεται άμεση συσχέτιση μεταξύ της πολιτικής που ορίστηκε στο Excel και της συμπεριφοράς του firewall κατά την εφαρμογή των κανόνων.

Βασικό χαρακτηριστικό του προτύπου (template) αποτελεί η υιοθέτηση ενός alias-based policy model. Στο μοντέλο αυτό αποφεύγεται η άμεση χρήση διευθύνσεων IP και αριθμητικών θυρών μέσα στους κανόνες firewall. Αντίθετα, όλοι οι κανόνες αναφέρονται αποκλειστικά σε λογικά aliases, τα οποία ορίζονται σε ξεχωριστό φύλλο του Excel.
Τα aliases διακρίνονται σε aliases διευθύνσεων (hosts και δίκτυα) και aliases υπηρεσιών (θύρες). Η προσέγγιση αυτή επιτρέπει τον διαχωρισμό των κανόνων πολιτικής από τις χαμηλού επιπέδου τεχνικές παραμέτρους, διευκολύνοντας τη συντήρηση, την αναγνωσιμότητα και τη διαχείριση της πολιτικής ασφάλειας.

Για τη μείωση λαθών εισαγωγής, ενσωματώθηκαν μηχανισμοί ελέγχου εγκυρότητας (data validation). Κρίσιμα πεδία όπως η ενέργεια του κανόνα, η διεπαφή, το πρωτόκολλο, ο τύπος πηγής/προορισμού και οι θύρες επικοινωνίας περιορίζονται σε προκαθορισμένες τιμές μέσω

αναπτυσσόμενων λιστών. Έτσι, το Excel λειτουργεί ως ενδιάμεσο επίπεδο ελέγχου ποιότητας πριν από την εφαρμογή των κανόνων στο firewall.

Η χρήση του Excel template στο εργαστηριακό περιβάλλον ακολουθεί σαφή και επαναλήψιμη ροή: ο IT administrator ορίζει ή τροποποιεί κανόνες και aliases στο αρχείο, το οποίο αποτελεί single source of truth για τις πολιτικές firewall. Το αρχείο αυτό τροφοδοτεί τη διαδικασία αυτοματοποίησης χωρίς άμεση επέμβαση στο γραφικό περιβάλλον του pfSense, υποστηρίζοντας πρακτικές ελεγχόμενης διαχείρισης αλλαγών (ISO/IEC 27001, 2022).

Το πρότυπο Excel *(Εικόνα 5-18)* που χρησιμοποιείται υλοποιεί στην πράξη τις αρχές μοντελοποίησης πολιτικής ασφάλειας που παρουσιάστηκαν στο Κεφάλαιο 4. Μέσω της τυποποιημένης δομής και της υποχρεωτικής χρήσης aliases *(Εικόνα 5-19)*, υποστηρίζει συνεπή εφαρμογή πολιτικών ασφάλειας δικτύου σε συμφωνία με βέλτιστες πρακτικές (NIST, 2020).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Rule_ID	Enabled	Action	Interface	IP_Version	Protocol	Source_Type	Source_Value	Source_Port	Destination_Type	Destination_Value	Destination_Port	Log	Description	Change_Ticket
2	BP-001	TRUE	PASS	LAN	IPv4	TCP/UDP	ALIAS	LAN_NET	ANY	ALIAS	FIREWALL_IP	DNS	TRUE	Allow DNS to internal firewall resolver	CHG-001
3	BP-002	TRUE	PASS	LAN	IPv4	TCP	ALIAS	LAN_NET	ANY	ANY		HTTPS	TRUE	Allow HTTPS from LAN	CHG-002
4	BP-003	TRUE	BLOCK	LAN	IPv4	TCP	ALIAS	UBUNTU_HOST	ANY	ANY		SSH	TRUE	Block outbound SSH from Ubuntu	CHG-003
5	BP-004	TRUE	PASS	LAN	IPv4	TCP	ANY		ANY	ANY		HTTP	TRUE	Allow HTTP fallback	CHG-004
6	BP-005	TRUE	PASS	LAN	IPv4	UDP	ANY		ANY	ANY		NTP	TRUE	Allow NTP time sync	CHG-005
7	BP-006	TRUE	BLOCK	LAN	IPv4	TCP	ANY		ANY	ANY		TELNET	TRUE	Block Telnet outbound	CHG-006
8	BP-007	TRUE	BLOCK	LAN	IPv4	TCP	ANY		ANY	ANY		SMB	TRUE	Block SMB outbound (malware prevention)	CHG-007
9	BP-008	TRUE	BLOCK	LAN	IPv4	TCP	ANY		ANY	ANY		NETBIOS	TRUE	Block NetBIOS outbound	CHG-008
10	BP-009	TRUE	BLOCK	LAN	IPv4	TCP	ANY		ANY	ANY		FTP	TRUE	Block FTP outbound (clear-text)	CHG-009
11	BP-010	FALSE	BLOCK	LAN	IPv4	TCP	ANY		ANY	ANY		SMTP	TRUE	Block direct SMTP (prevent data exfiltration)	CHG-010
12	BP-011	TRUE	BLOCK	LAN	IPv4	TCP	ANY		ANY	ANY		SMTP_SUBMISSION	TRUE	Block SMTP submission (controlled email)	CHG-011
13	BP-012	FALSE	BLOCK	LAN	IPv4	ICMP	ANY		ANY	ANY		ANY	TRUE	Block ICMP outbound (optional hardening)	CHG-012
14	BP-013	FALSE	PASS	LAN	IPv4	UDP	ANY		ANY	ANY		OPENVPN	TRUE	Allow OpenVPN outbound	CHG-013
15	BP-014	FALSE	BLOCK	LAN	IPv4	TCP	ANY		ANY	ANY		TOR	TRUE	Block TOR outbound (policy enforcement)	CHG-014
16	BP-015	FALSE	BLOCK	LAN	IPv4	TCP/UDP	ANY		ANY	ANY		DNS	TRUE	Block external DNS – enforce firewall DNS	CHG-015
17	BP-016	TRUE	PASS	LAN	IPv4	ICMP	ALIAS	LAN_NET	ANY	ALIAS	FIREWALL_IP	ANY	TRUE	Allow ICMP to firewall for monitoring	CHG-016
18	BP-017	TRUE	BLOCK	LAN	IPv4	ANY	ANY		ANY	ANY		ANY	TRUE	Default deny – enforce least privilege	CHG-017
19	BP-018	TRUE	BLOCK	LAN	IPv4	TCP/UDP	ALIAS	LAN_NET	ANY	ANY		DNS	TRUE	Block external DNS – force internal DNS	CHG-018

Εικόνα 5-18: Πίνακας ορισμού κανόνων firewall στο Excel policy template με χρήση aliases και περιγραφικών κανόνων.

	A	B	C	D
1	Alias_Name	Alias_Type	Alias_Value	Description
2	LAN_NET	Network	192.168.1.0/24	Internal LAN subnet
3	DNS_SERVERS	Host	1.1.1.1,8.8.8.8	Public DNS resolvers
4	HTTP	Port	80	HTTP service port
5	HTTPS	Port	443	HTTPS service port
6	DNS	Port	53	DNS service port
7	HIGH_RISK_PORTS	Port	23,135,139,445,3389	Example high-risk ports (telnet, SMB, RDP etc.)
8	UBUNTU_HOST	Host	192.168.1.100	Ubuntu host to restrict SSH
9	FIREWALL_IP	Host	192.168.1.1	pfSense firewall IP (for 'this firewall')
10	SSH	Port	22	SSH
11	NTP	Port	123	NTP
12	TELNET	Port	23	Telnet
13	SMB	Port	445	SMB
14	NETBIOS	Port	137	NetBIOS
15	FTP	Port	21	FTP
16	SMTP	Port	25	SMTP
17	SMTP_SUBMISSION	Port	587	SMTP submission
18	OPENVPN	Port	1194	OpenVPN
19	TOR	Port	9001	Tor
20	RFC1918	Network	10.0.0.0/8,172.16.0.0/12,192.168.0.0/16	Private IPv4 Networks (RFC1918)

Εικόνα 5-19: Πίνακας ορισμού aliases (διευθύνσεων και θυρών) στο Excel policy template.

	A	B	C	D	E	F	G	H	I	J
1	Enabled	Action	Interface	IP_Version	Protocol	Type	Log	PortOrAny	Address_Aliases	Port_Aliases
2	TRUE	PASS	LAN	IPv4	TCP	ALIAS	TRUE	ANY	LAN_NET	DNS
3	FALSE	BLOCK	WAN	IPv6	UDP	ANY	FALSE	DNS	UBUNTU_HOST	HTTP
4		REJECT	OPT1	ANY	TCP/UDP			HTTP	FIREWALL_IP	HTTPS
5			OPT2		ICMP			HTTPS	DNS_SERVERS	SSH
6			OPT3		ANY			SSH	RFC1918	SMTP
7			DMZ					NTP		SMTP_SUBMISSION
8			VPN					SMTP		FTP
9								SMTP_SUBMISSION		TELNET
10								FTP		SMB
11								TELNET		NETBIOS
12								SMB		OPENVPN
13								NETBIOS		TOR
14								OPENVPN		
15								TOR		

Εικόνα 5-20: Φύλλο προκαθορισμένων λιστών (LISTS) του Excel policy template για την τυποποίηση παραμέτρων κανόνων firewall.

Για τη διασφάλιση της ιχνηλασιμότητας και του ελέγχου των αλλαγών στην πολιτική firewall, υλοποιήθηκε ένας πίνακας καταγραφής αλλαγών (Change Register) στο Excel πρότυπο διαχείρισης κανόνων. Κάθε κανόνας firewall συνδέεται με ένα μοναδικό αναγνωριστικό αλλαγής (Change_Ticket), το οποίο αντιστοιχεί σε καταχώρηση στο μητρώο αλλαγών. Στο μητρώο αυτό καταγράφονται βασικές πληροφορίες όπως η ημερομηνία αλλαγής, ο σχετικός κανόνας firewall, η περιγραφή της αλλαγής, καθώς και τα πρόσωπα που αιτήθηκαν, ενέκριναν και υλοποίησαν την αλλαγή.

Η προσέγγιση αυτή ενισχύει τη λογοδοσία και επιτρέπει την τεκμηριωμένη διαχείριση των τροποποιήσεων της πολιτικής ασφάλειας, ενώ παράλληλα διευκολύνει διαδικασίες ελέγχου και audit. Η πρακτική αυτή ευθυγραμμίζεται με τις αρχές διαχείρισης αλλαγών που προτείνονται από το πρότυπο ISO/IEC 27001 για την ελεγχόμενη τροποποίηση κρίσιμων ρυθμίσεων ασφάλειας (ISO, 2022).

5.6 Εισαγωγή κανόνων στο pfSense

Η εισαγωγή των κανόνων firewall στο pfSense υλοποιήθηκε με αυτοματοποιημένο τρόπο, χωρίς χειροκίνητη παραμετροποίηση μέσω του γραφικού περιβάλλοντος διαχείρισης. Η διαδικασία βασίζεται στη δομημένη αξιοποίηση του αρχείου ρυθμίσεων config.xml, το οποίο αποτελεί τον κεντρικό μηχανισμό αποθήκευσης και εφαρμογής πολιτικών στο pfSense. Η επιλογή αυτή είναι κρίσιμη, καθώς η πλατφόρμα δεν παρέχει επίσημη προγραμματιστική διεπαφή (REST API) για πλήρη διαχείριση κανόνων firewall, γεγονός που καθιστά αναγκαία την υιοθέτηση εναλλακτικών, τεχνικά τεκμηριωμένων προσεγγίσεων αυτοματοποίησης.

Το αρχείο διαμόρφωσης του pfSense δημιουργήθηκε μέσω του script excel2pfsense.py, το οποίο περιγράφηκε στο Κεφάλαιο 4. Το script επεξεργάζεται τα δεδομένα πολιτικής από το πρότυπο Excel και δημιουργεί ενημερωμένη έκδοση του αρχείου config.xml, το οποίο στη συνέχεια εισάγεται στο pfSense για την εφαρμογή των κανόνων firewall. Στη συνέχεια, χρησιμοποιώντας τη βιβλιοθήκη openpyxl, επεξεργάζεται τα δεδομένα εισόδου από το πρότυπο Excel.

1. Επικύρωση Δεδομένων (Data Validation)

Πριν από τη δημιουργία των κανόνων firewall, το script καλεί την εσωτερική συνάρτηση validate_rules(). Σε αυτό το στάδιο ελέγχεται η μοναδικότητα των αναγνωριστικών (Rule_ID), η εγκυρότητα των IP/CIDR και επαληθεύεται ότι τα aliases που χρησιμοποιούνται στους κανόνες έχουν οριστεί σωστά στα αντίστοιχα φύλλα του Excel. Η υλοποίηση της διαδικασίας αυτής αποτυπώνεται ενδεικτικά στην Εικόνα 5-21, όπου παρουσιάζεται η συνάρτηση validate_rules() που λειτουργεί ως μηχανισμός προελέγχου πριν από την παραγωγή της τελικής ρύθμισης του pfSense.

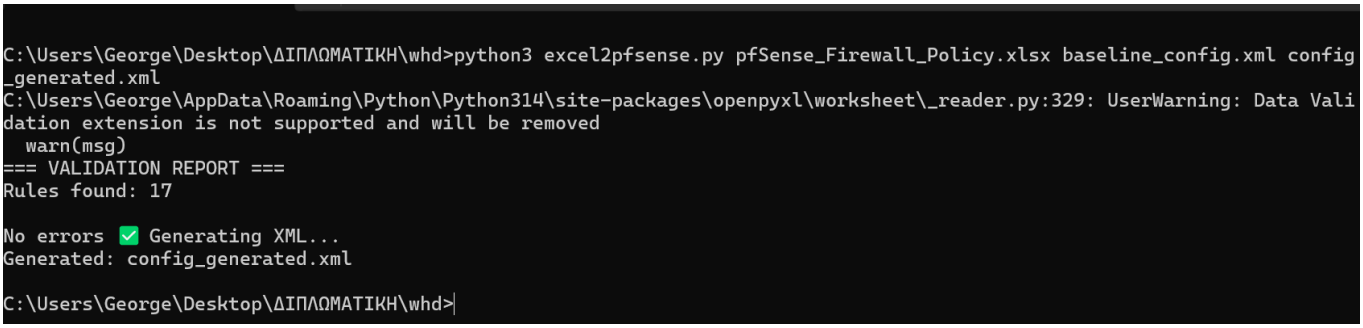
Ενδεικτικά πραγματοποιούνται οι ακόλουθοι έλεγχοι:

• Έλεγχος μοναδικότητας των αναγνωριστικών κανόνων (Rule_ID), ώστε να αποφεύγονται διπλοεγγραφές.
• Έλεγχος εγκυρότητας βασικών πεδίων πολιτικής, όπως Enabled, Action, Interface, IP_Version και Protocol.
• Επαλήθευση της ορθής χρήσης τύπων πηγής και προορισμού (Source_Type, Destination_Type).
• Έλεγχος ύπαρξης υποχρεωτικών πεδίων, όπως η περιγραφή (Description) κάθε κανόνα.
• Επικύρωση διευθύνσεων IP και υποδικτύων (CIDR) όταν χρησιμοποιούνται τύποι SINGLE_IP ή SUBNET.
• Έλεγχος ότι τα aliases που χρησιμοποιούνται στους κανόνες έχουν οριστεί στα αντίστοιχα φύλλα του Excel.
• Επικύρωση των θυρών πηγής και προορισμού (Source_Port, Destination_Port) σύμφωνα με τα ορισμένα port aliases.

```python
def validate_rules(
    rules: List[Dict[str, str]],
    addr_aliases: Optional[Set[str]] = None,
    port_aliases: Optional[Set[str]] = None
) -> Tuple[List[str], List[str]]:
    errors: List[str] = []
    warnings: List[str] = []
    seen_ids: Set[str] = set()

    for n, r in enumerate(rules, start=2):
        rid = r["Rule_ID"]

        if rid in seen_ids:
            errors.append(f"Row {n}: duplicate Rule_ID {rid}")
        seen_ids.add(rid)

        for field, allowed_key in [
            ("Enabled", "Enabled"),
            ("Action", "Action"),
            ("Interface", "Interface"),
            ("IP_Version", "IP_Version"),
            ("Protocol", "Protocol"),
            ("Log", "YesNo"),
        ]:
            if norm(r[field]).upper() not in ALLOWED[allowed_key]:
                errors.append(f"Row {n} ({rid}): invalid {field}='{r[field]}'")

        for field in ("Source_Type", "Destination_Type"):
            if norm(r[field]).upper() not in ALLOWED["Type"]:
                errors.append(f"Row {n} ({rid}): invalid {field}='{r[field]}'")

        if not norm(r["Description"]):
            errors.append(f"Row {n} ({rid}): Description is required")

        # Validate address side values
        for side in ("Source", "Destination"):
            t = norm(r[f"{side}_Type"]).upper()
            v = norm(r[f"{side}_Value"])

            if t in ("SINGLE_IP", "SUBNET", "ALIAS") and not v:
                errors.append(f"Row {n} ({rid}): {side}_Value required for {t}")

            if t == "ANY" and v not in ("", "ANY"):
                warnings.append(f"Row {n} ({rid}): {side}_Value ignored because {side}_Type=ANY")

            if t == "ALIAS" and v and addr_aliases is not None:
                if v.upper() not in addr_aliases and v.upper() not in (port_aliases or set()):
                    warnings.append(f"Row {n} ({rid}): {side}_Value alias '{v}' not found in ALIASES sheet

            try:
                if t == "SINGLE_IP" and v:
                    validate_ip(v)
                if t == "SUBNET" and v:
                    validate_cidr(v)
            except Exception as e:
                errors.append(f"Row {n} ({rid}): {side}_Value '{v}' invalid ({e})")

        # Validate ports
        try:
            validate_port(r.get("Source_Port", "") or "ANY", port_aliases)
        except Exception as e:
            errors.append(f"Row {n} ({rid}): Source_Port '{r.get('Source_Port','')}' invalid ({e})")

        try:
            validate_port(r.get("Destination_Port", "") or "ANY", port_aliases)
```

Εικόνα 5-21: Συνάρτηση validate_rules() για επικύρωση κανόνων firewall από το Excel template πριν από την παραγωγή του αρχείου ρυθμίσεων του pfSense.

Μόνο εφόσον δεν εντοπιστούν κρίσιμα σφάλματα, η εκτέλεση προχωρά, παράγοντας μια αναλυτική αναφορά στο τερματικό.



Εικόνα 5-22: Εκτέλεση του Python script excel2pfsense.py για τη μετατροπή της πολιτικής firewall από το αρχείο Excel σε δομή XML συμβατή με το pfSense, με επιτυχή επαλήθευση 17 κανόνων και δημιουργία του αρχείου config_generated.xml.

2. Λογική Μετασχηματισμού (XML Generation)

Αν οι κανόνες περάσουν επιτυχώς τον έλεγχο επικύρωσης, το script εντοπίζει τον κεντρικό κόμβο <filter> στο δέντρο XML του pfSense. Μέσω δομών επανάληψης (iteration), διατρέχει τις ενεργές εγγραφές του Excel και προσαρτά (appends) τους νέους κανόνες, διατηρώντας την ιεραρχική τους σειρά. Στο παρακάτω απόσπασμα κώδικα παρουσιάζεται η δομική λογική του κώδικα Python για τον μετασχηματισμό των δεδομένων.

```
# ----------------------------
# Inject rules into pfSense config.xml
# ----------------------------
def inject_rules_into_config(baseline_xml: str, rules: List[Dict[str, str]]) -> ET.ElementTree:
    tree = ET.parse(baseline_xml)
    root = tree.getroot()

    filter_node = root.find("filter")
    if filter_node is None:
        raise SystemExit("config.xml has no <filter> section")

    new_rules: List[ET.Element] = []

    # Build rules in EXACT Excel order (top->bottom)
    for r in rules:
        if norm_bool(r.get("Enabled", "")) != "YES":
            continue

        rule = ET.Element("rule")
        ET.SubElement(rule, "type").text = map_action(r["Action"])
        ET.SubElement(rule, "interface").text = map_interface(r["Interface"])
        ET.SubElement(rule, "ipprotocol").text = map_ipproto(norm_ip_version(r.get("IP_Version", "
        ET.SubElement(rule, "protocol").text = map_protocol(norm_protocol(r.get("Protocol", "")))

        # tracker for log traceability
        ET.SubElement(rule, "tracker").text = rule_tracker_from_id(r["Rule_ID"])

        src = ET.SubElement(rule, "source")
        build_addr_node(src, r["Source_Type"], r["Source_Value"])
        build_port_node(src, r["Source_Port"])

        dst = ET.SubElement(rule, "destination")
        build_addr_node(dst, r["Destination_Type"], r["Destination_Value"])
        build_port_node(dst, r["Destination_Port"])

        ET.SubElement(rule, "descr").text = r["Description"]

        if norm_bool(r.get("Log", "")) == "YES":
            ET.SubElement(rule, "log")

        new_rules.append(rule)

    # Append to the end of <filter> in the SAME order as Excel
    for rule_el in new_rules:
        filter_node.append(rule_el)

    return tree
```

Εικόνα 5-23: Η δομική λογική μετασχηματισμού των κανόνων από το Excel στο XML δέντρο του pfSense μέσω Python.

Ιδιαίτερη έμφαση δίνεται στη δημιουργία των aliases ως αυτόνομων αντικειμένων πριν από την εισαγωγή των firewall rules. Επιπλέον, οι νέοι κανόνες εισάγονται διαδοχικά (με τη σειρά που έχουν στο Excel), διατηρώντας ανέπαφους τους προεπιλεγμένους κανόνες προστασίας του συστήματος (anti-lockout rules), αποτρέποντας έτσι καταστάσεις απώλειας διαχειριστικής πρόσβασης.

3. Παραγόμενο Αποτέλεσμα (XML Payload)

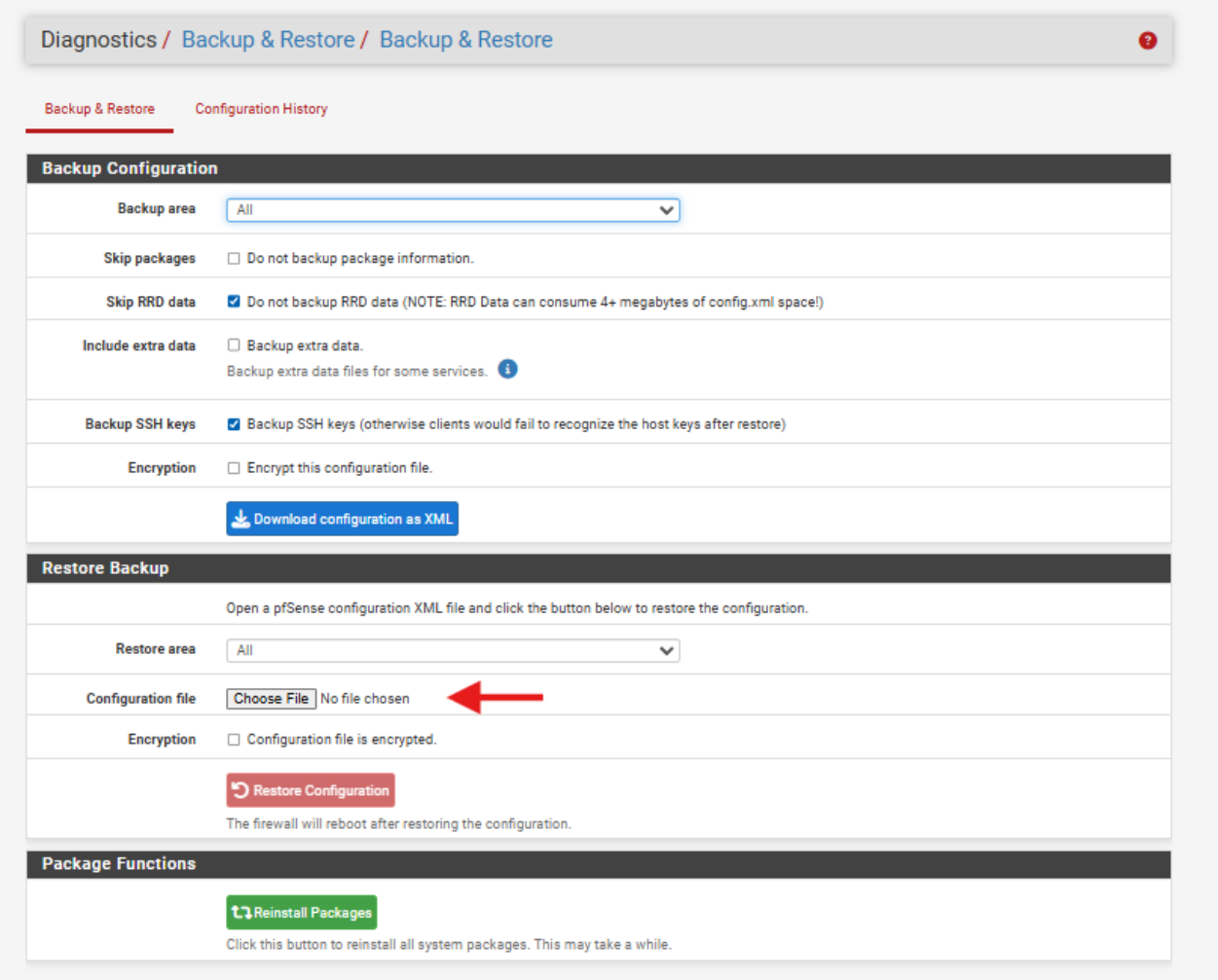
Το αποτέλεσμα της παραπάνω διαδικασίας είναι η παραγωγή καθαρού και συντακτικά ορθού κώδικα XML. Για παράδειγμα, ο κανόνας με Rule ID BP-001 από το Excel, ο οποίος επιτρέπει την κίνηση DNS από το τοπικό δίκτυο (LAN_NET) προς το firewall (FIREWALL_IP), μετασχηματίζεται αυτόματα στην ακόλουθη XML δομή.

```xml
<rule>
    <id />
    <tracker>1001</tracker>
    <type>pass</type>
    <interface>lan</interface>
    <ipprotocol>inet</ipprotocol>
    <tag />
    <tagged />
    <max />
    <max-src-nodes />
    <max-src-conn />
    <max-src-states />
    <statetimeout />
    <statepolicy />
    <statetype>keep state</statetype>
    <os />
    <protocol>tcp/udp</protocol>
    <source>
        <network>lan</network>
    </source>
    <destination>
        <network>(self)</network>
        <port>DNS</port>
    </destination>
    <log />
    <descr>Allow DNS to internal firewall resolver</descr>
    <updated>
        <time>1770482379</time>
        <username>admin@192.168.10.63 (Local Database)</username>
    </updated>
</rule>
```

Εικόνα 5-24: Το παραγόμενο XML για τον επιτρεπτικό κανόνα πρόσβασης DNS (Rule ID: BP-001).

4. Εφαρμογή της Πολιτικής (Configuration Restore)

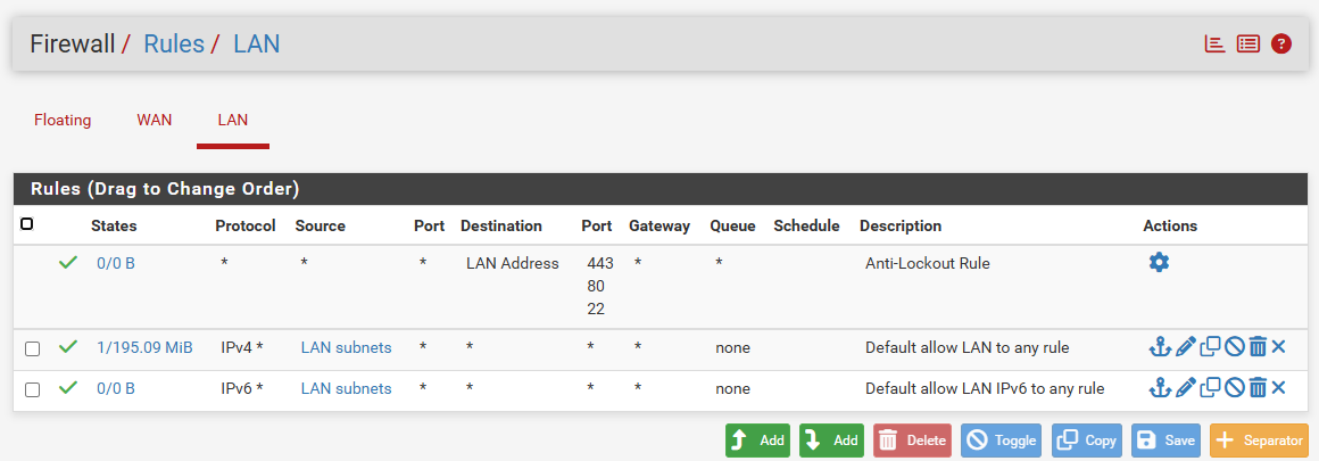
Αυτή η δομή ενσωματώνεται στο τελικό αρχείο config_generated.xml. Στη συνέχεια, το παραγόμενο αρχείο εισάγεται στο pfSense μέσω της διαδικασίας επαναφοράς ρυθμίσεων (Backup & Restore), επιτρέποντας την ημι-αυτόματη εφαρμογή της πολιτικής firewall χωρίς καμία χειροκίνητη δημιουργία κανόνων στο WebGUI.



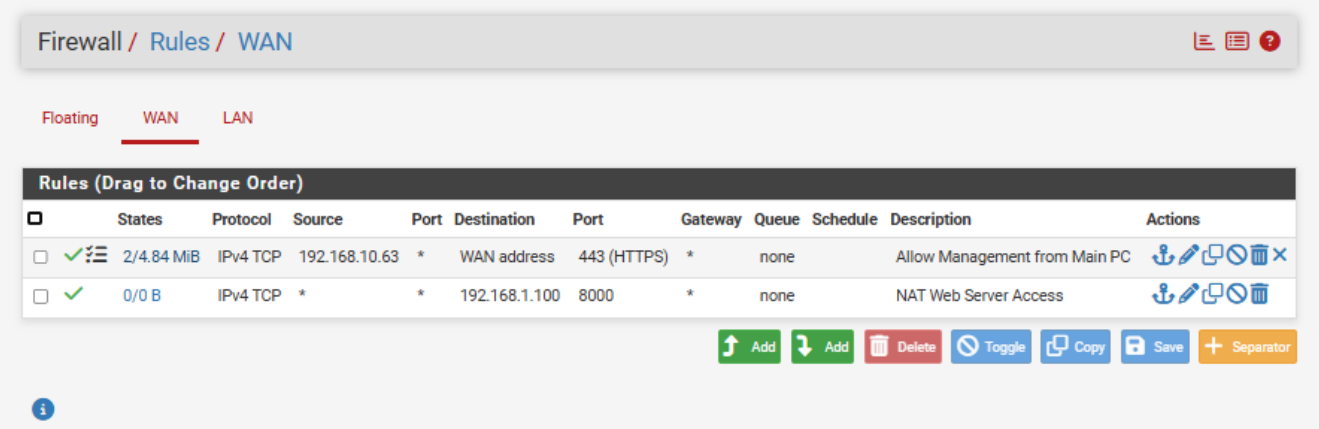
Εικόνα 5-25: Διαδικασία εισαγωγής του αρχείου ρυθμίσεων config_generated.xml στο pfSense μέσω της λειτουργίας Backup & Restore, επιτρέποντας την εφαρμογή της παραγόμενης πολιτικής firewall χωρίς χειροκίνητη δημιουργία κανόνων στο WebGUI.

Η επιτυχής εφαρμογή της προσέγγισης τεκμηριώνει ότι είναι εφικτή η αυτοματοποίηση της διαχείρισης κανόνων firewall ακόμη και σε περιβάλλοντα όπου δεν παρέχεται επίσημο API, ενισχύοντας την τεκμηρίωση, την επαναληψιμότητα και τον έλεγχο των πολιτικών ασφάλειας (ISO/IEC 27001, 2022).

Πριν από την εφαρμογή της προτεινόμενης πολιτικής ασφάλειας, καταγράφηκε η αρχική κατάσταση των κανόνων firewall στο pfSense. Οι εικόνες που ακολουθούν παρουσιάζουν τους προεπιλεγμένους κανόνες που ήταν ενεργοί στις διεπαφές LAN και WAN πριν από την εισαγωγή των κανόνων που παράγονται από το Excel template.

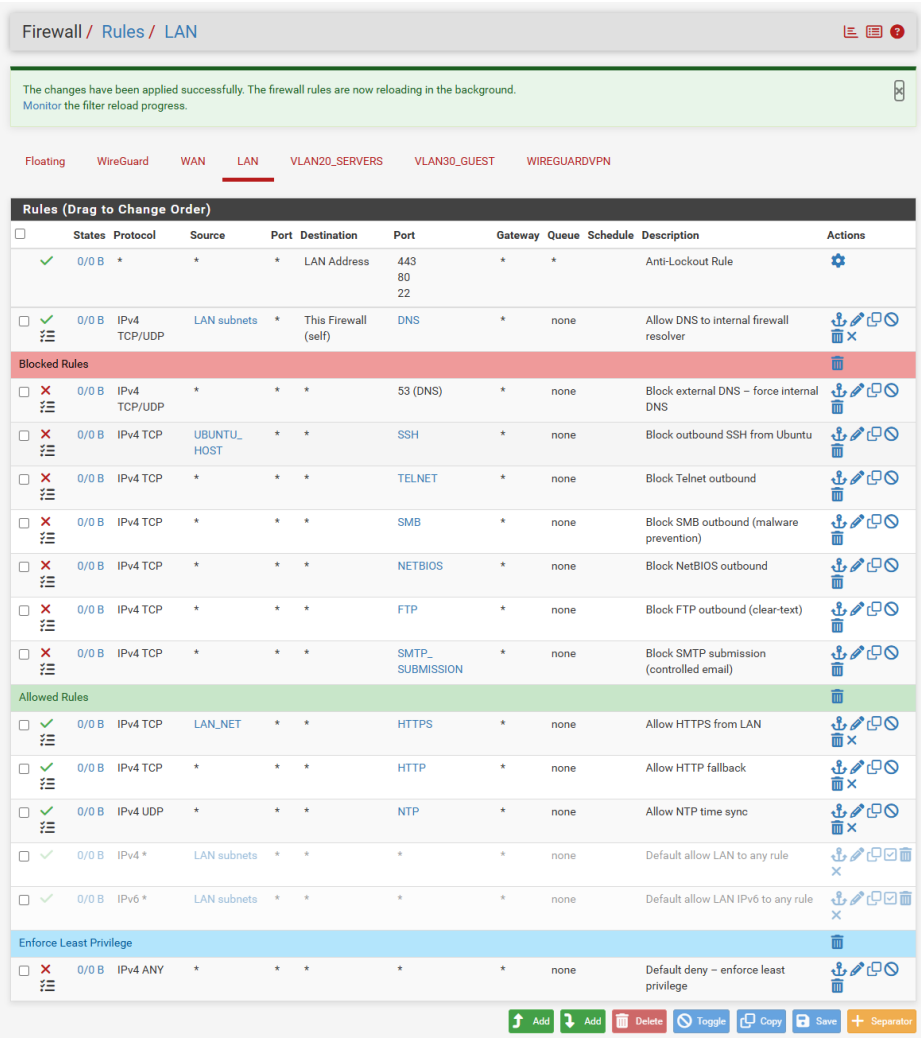


Εικόνα 5-26: Εφαρμοσμένοι κανόνες firewall στη διεπαφή LAN του pfSense πριν την εισαγωγή της πολιτικής ασφάλειας

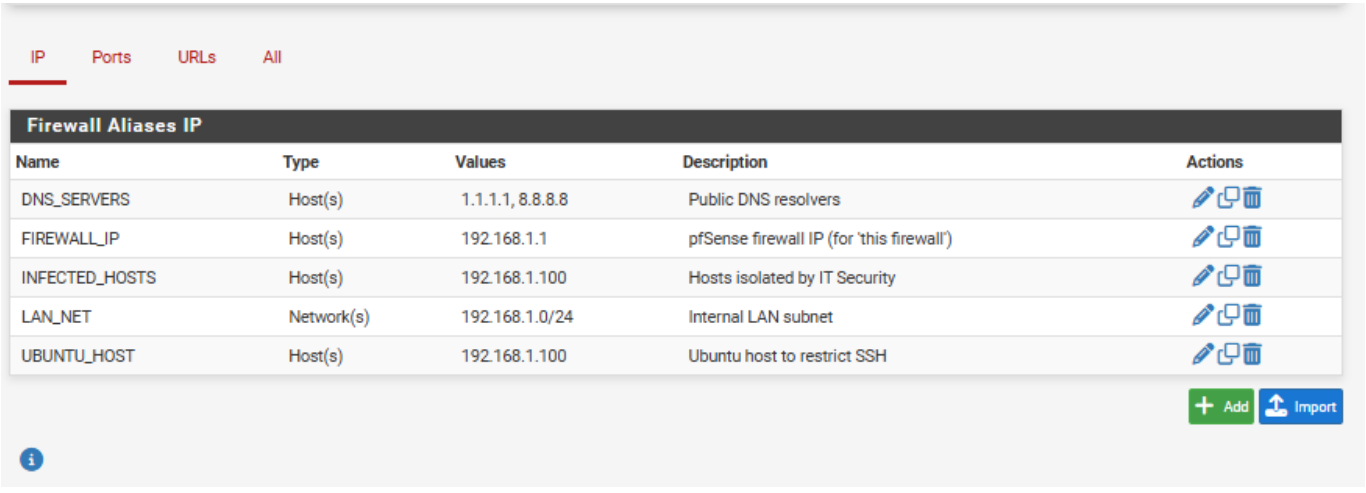


Εικόνα 5-27: Εφαρμοσμένοι κανόνες firewall στη διεπαφή WAN του pfSense πριν την εισαγωγή της πολιτικής ασφάλειας.

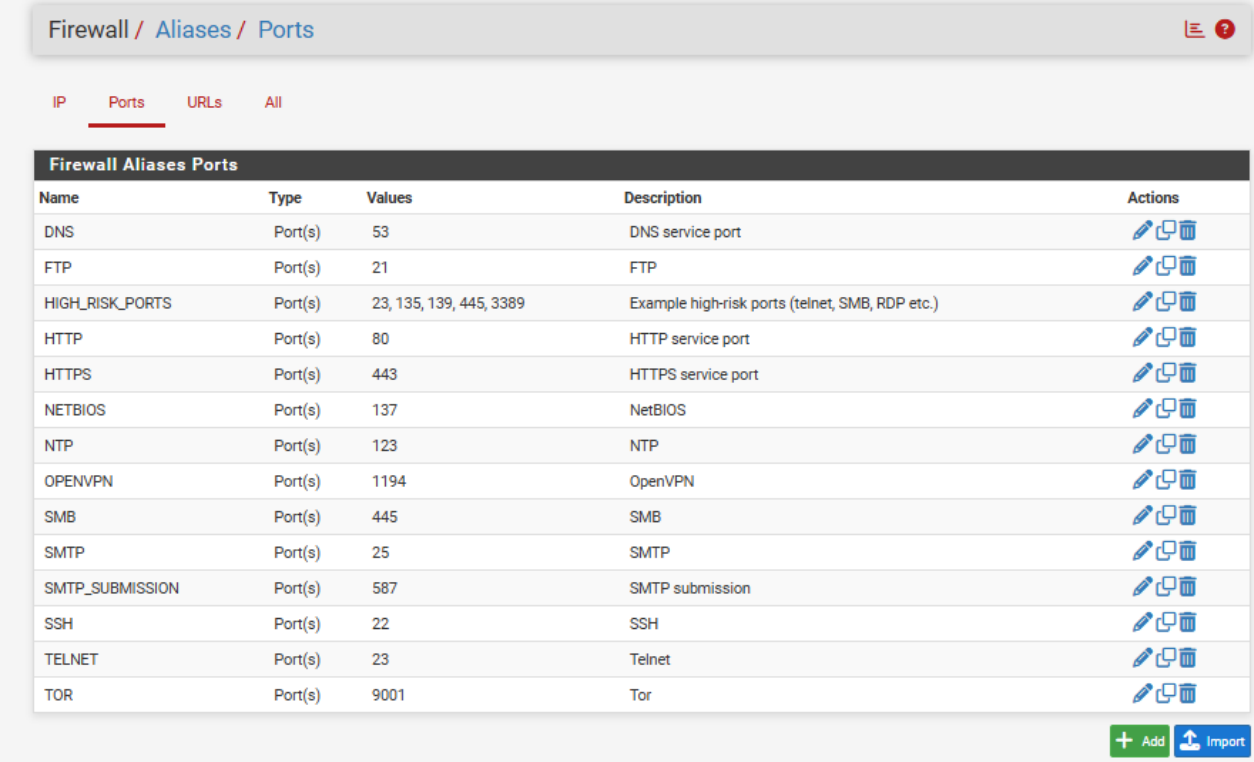
Η τελική κατάσταση των κανόνων firewall, aliases και ports μετά την εισαγωγή τους στο pfSense παρουσιάζονται στις εικόνες 5-28 με 5-30



Εικόνα 5-28: Κανόνες firewall στο pfSense μετά την εισαγωγή από το Excel template.



Εικόνα 5-29: Ορισμός και διαχείριση IP aliases στο pfSense.



Εικόνα 5-30: Port aliases που χρησιμοποιούνται στους κανόνες firewall για την εφαρμογή της πολιτικής ασφάλειας.

Οι Εικόνες 5-31 και 5-32 παρουσιάζουν ενδεικτικές καταγραφές από το firewall του pfSense μετά την εφαρμογή της πολιτικής ασφάλειας.

✓	Jan 28 15:09:26	LAN	Allow DNS for all LAN (1001)	192.168.1.100:46583	192.168.1.1:53	UDP
✓	Jan 28 15:09:26	LAN	Allow DNS for all LAN (1001)	192.168.1.100:40340	192.168.1.1:53	UDP
✗	Jan 28 15:09:26	LAN	Block FTP outbound (clear-text) (1009)	192.168.1.100:43220	146.75.118.132:21	TCP:S
✗	Jan 28 15:09:27	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✗	Jan 28 15:09:27	LAN	Block FTP outbound (clear-text) (1009)	192.168.1.100:43220	146.75.118.132:21	TCP:S
✗	Jan 28 15:09:28	LAN	Block FTP outbound (clear-text) (1009)	192.168.1.100:43220	146.75.118.132:21	TCP:S
✗	Jan 28 15:09:29	LAN	Block FTP outbound (clear-text) (1009)	192.168.1.100:43220	146.75.118.132:21	TCP:S
✗	Jan 28 15:09:30	LAN	Block FTP outbound (clear-text) (1009)	192.168.1.100:43220	146.75.118.132:21	TCP:S

Εικόνα 5-31: Καταγραφές firewall (logs) του pfSense που επιβεβαιώνουν την επιτυχή εφαρμογή επιτρεπτικών και απαγορευτικών κανόνων.

✕	Jan 28 15:08:49	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Jan 28 15:08:52	LAN	Default deny – enforce least privilege! (1017)	192.168.1.100:33604	34.107.243.93:443	TCP:A
✕	Jan 28 15:08:52	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✕	Jan 28 15:08:53	LAN	Default deny – enforce least privilege! (1017)	192.168.1.100:33604	34.107.243.93:443	TCP:A
✕	Jan 28 15:08:54	LAN	Default deny – enforce least privilege! (1017)	192.168.1.100:33604	34.107.243.93:443	TCP:A
✕	Jan 28 15:08:54	WAN	Default deny rule IPv4 (1000000103)	192.168.10.17:56700	255.255.255.255:56700	UDP
✕	Jan 28 15:08:55	LAN	Default deny – enforce least privilege! (1017)	192.168.1.100:33604	34.107.243.93:443	TCP:A
✕	Jan 28 15:08:56	LAN	Default deny – enforce least privilege! (1017)	192.168.1.100:33604	34.107.243.93:443	TCP:RA
✕	Jan 28 15:08:57	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✕	Jan 28 15:09:00	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✓	Jan 28 15:09:01	LAN	Allow DNS for all LAN (1001)	192.168.1.100:35974	192.168.1.1:53	UDP
✓	Jan 28 15:09:01	LAN	Allow DNS for all LAN (1001)	192.168.1.100:42875	192.168.1.1:53	UDP
✓	Jan 28 15:09:01	LAN	Allow HTTPS from LAN (1002)	192.168.1.100:60808	34.107.243.93:443	TCP:S
✓	Jan 28 15:09:01	LAN	Allow HTTPS from LAN (1002)	192.168.1.100:60810	34.107.243.93:443	TCP:S
✓	Jan 28 15:09:02	LAN	Allow DNS for all LAN (1001)	192.168.1.100:40178	192.168.1.1:53	UDP
✓	Jan 28 15:09:02	LAN	Allow DNS for all LAN (1001)	192.168.1.100:41306	192.168.1.1:53	UDP
✕	Jan 28 15:09:02	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✓	Jan 28 15:09:02	LAN	Allow HTTPS from LAN (1002)	192.168.1.100:47614	146.75.117.91:443	TCP:S
✕	Jan 28 15:09:07	WAN	Default deny rule IPv4 (1000000103)	192.168.10.137:5353	224.0.0.251:5353	UDP

Εικόνα 5-32: Επαλήθευση της πολιτικής default deny μέσω καταγραφών απορριπτόμενης και επιτρεπόμενης κίνησης στο pfSense.

5.7 Ενσωμάτωση Threat Intelligence (pfBlockerNG & Suricata)

Στο πλαίσιο της εργαστηριακής υλοποίησης, η βασική λειτουργικότητα του firewall ενισχύθηκε με μηχανισμούς threat intelligence, με στόχο την αξιολόγηση της αποτελεσματικότητας συνδυαστικών πολιτικών ασφάλειας. Για τον σκοπό αυτό αξιοποιήθηκαν τα πακέτα pfBlockerNG και Suricata, τα οποία ενσωματώθηκαν στο pfSense ως συμπληρωματικά επίπεδα προστασίας πέραν των στατικών κανόνων firewall.

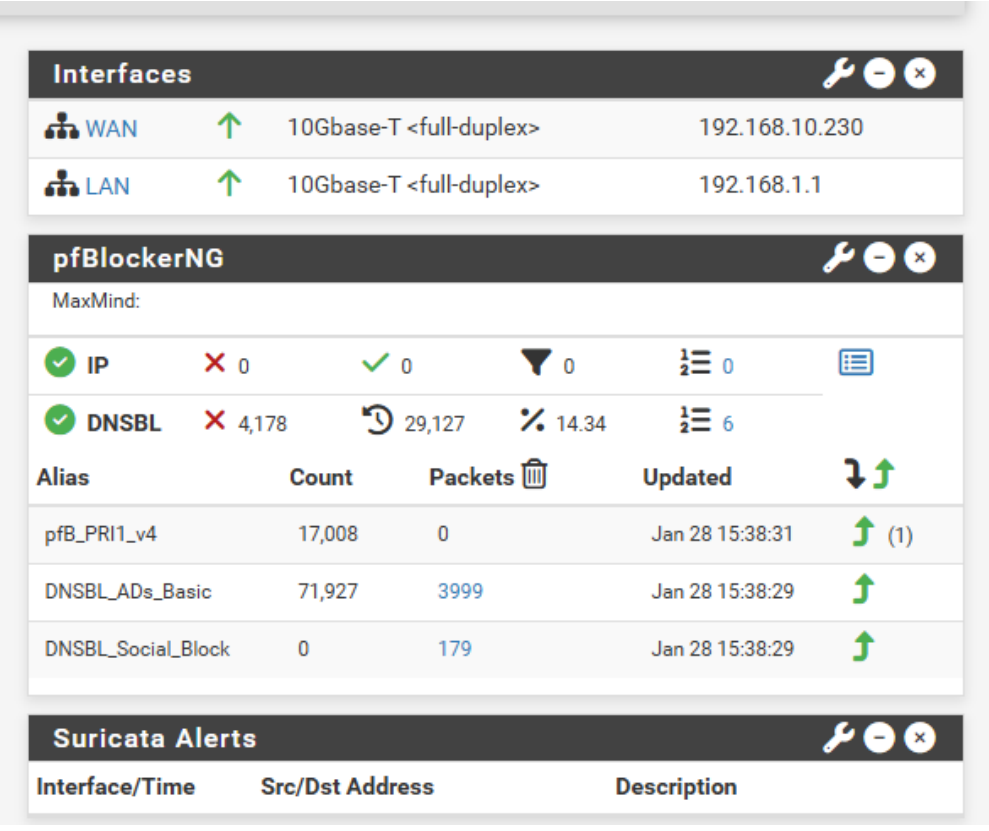
Το pfBlockerNG χρησιμοποιήθηκε για την εφαρμογή πολιτικών αποκλεισμού βάσει εξωτερικών πηγών πληροφοριών απειλών, όπως λίστες κακόβουλων διευθύνσεων IP και domains. Η λειτουργία του βασίζεται στην περιοδική ενημέρωση των πηγών δεδομένων (feeds) από επιλεγμένες πηγές threat intelligence και στην εφαρμογή φιλτραρίσματος σε επίπεδο DNS (DNSBL) και IP, ενισχύοντας την προληπτική προστασία του δικτύου (ENISA, 2021).

Παράλληλα, το Suricata ενσωματώθηκε σε λειτουργία συστήματος IDS. Το Suricata παρακολουθεί τη διερχόμενη δικτυακή κίνηση σε σχεδόν πραγματικό χρόνο και τη συγκρίνει με γνωστά μοτίβα επιθέσεων, όπως αυτά ορίζονται από ενεργά σύνολα κανόνων (rule sets). Σε περίπτωση ανίχνευσης ύποπτης ή κακόβουλης δραστηριότητας, το σύστημα καταγράφει

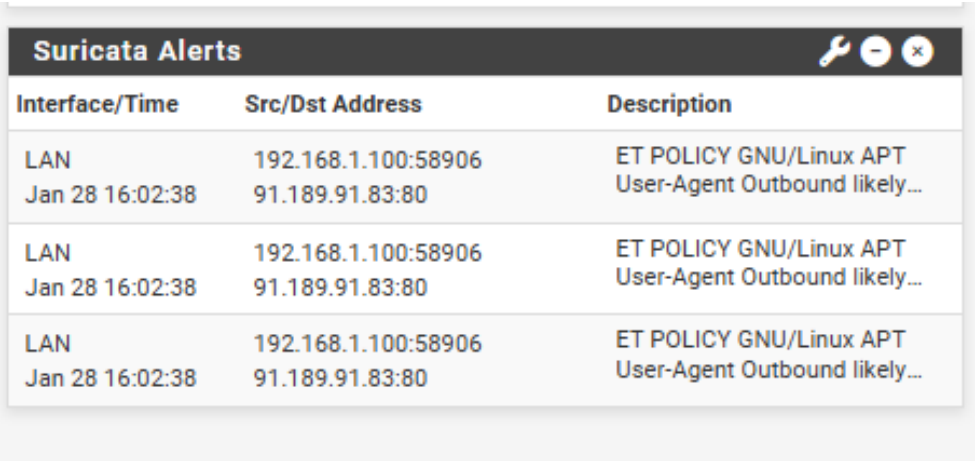
ειδοποιήσεις (alerts), οι οποίες μπορούν να συσχετιστούν με συγκεκριμένες δοκιμές και σενάρια ελέγχου (Scarfone & Mell, 2007).

Η ενσωμάτωση των μηχανισμών threat intelligence επιτρέπει την αξιολόγηση πολυεπίπεδης προσέγγισης ασφάλειας. Οι στατικοί κανόνες firewall που ορίζονται μέσω του Excel template λειτουργούν ως πρώτη γραμμή άμυνας, ενώ τα δυναμικά εργαλεία παρέχουν πρόσθετη προστασία έναντι απειλών που δεν είναι εύκολο να προβλεφθούν εκ των προτέρων. Η συνδυαστική χρήση των μηχανισμών αυτών αντανακλά πρακτικές που εφαρμόζονται σε περιβάλλοντα SMEs, όπου επιδιώκεται ισορροπία μεταξύ αποτελεσματικότητας και λειτουργικής απλότητας (ENISA, 2021).

Η λειτουργία του pfBlockerNG και η ενσωμάτωσή του στο pfSense παρουσιάζονται στην Εικόνα 5-33, ενώ στην Εικόνα 5-34 αποτυπώνονται ενδεικτικές ειδοποιήσεις του Suricata που καταγράφηκαν κατά τη διάρκεια δοκιμών. Τα στιγμιότυπα αυτά τεκμηριώνουν ότι το περιβάλλον είναι σε θέση να εφαρμόζει φιλτράρισμα βάσει threat intelligence και να καταγράφει ύποπτη δραστηριότητα σε επίπεδο IDS.



Εικόνα 5-33: Ενοποιημένη επισκόπηση μηχανισμών ασφάλειας στο pfSense με pfBlockerNG (Threat Intelligence) και Suricata (IDS/IPS).



Εικόνα 5-34: Ενδεικτικές ειδοποιήσεις Suricata από ανίχνευση ύποπτης δικτυακής κίνησης

5.1 Βελτιστοποίηση Διαδικασίας Εφαρμογής Πολιτικών

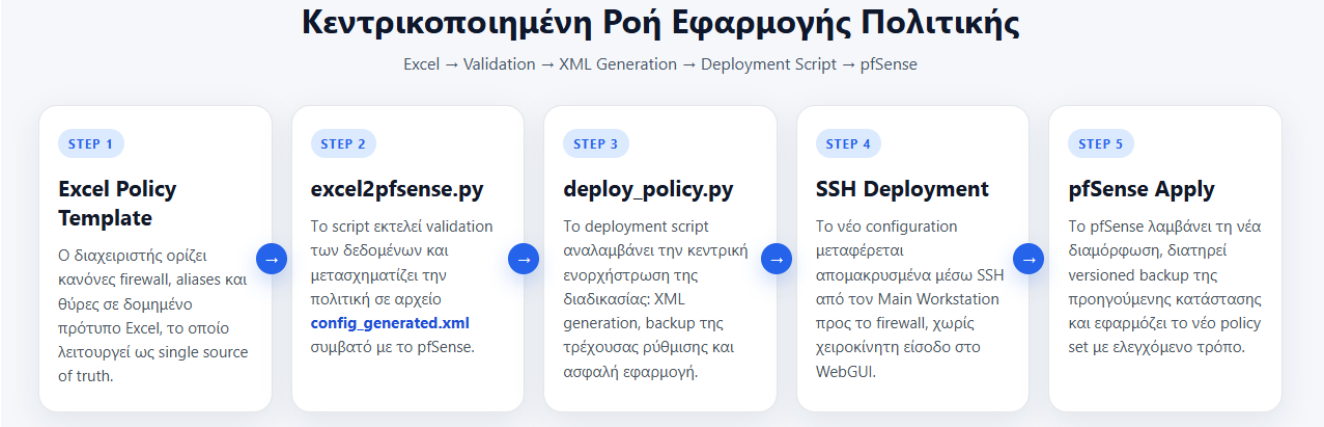
Στο αρχικό στάδιο της υλοποίησης, η διαδικασία εφαρμογής των κανόνων firewall βασιζόταν στη χρήση του υπολογιστικού φύλλου Excel ως σημείου ορισμού της πολιτικής και στη μετατροπή των δεδομένων σε αρχείο XML, το οποίο εισαγόταν στο pfSense μέσω της λειτουργίας backup/restore του γραφικού περιβάλλοντος. Παρότι η προσέγγιση αυτή εξασφάλιζε συνέπεια στη δομή των κανόνων, απαιτούσε χειροκίνητη παρέμβαση για την τελική εφαρμογή των ρυθμίσεων.

Για την περαιτέρω ενίσχυση της αποδοτικότητας και της λειτουργικής συνέπειας, σχεδιάστηκε και υλοποιήθηκε ένας μηχανισμός κεντρικοποιημένης εφαρμογής πολιτικών. Στο προτεινόμενο μοντέλο, το υπολογιστικό φύλλο Excel διατηρεί τον ρόλο του ως ενιαία πηγή ορισμού των κανόνων (single source of truth), ενώ το σενάριο excel2pfsense.py αναλαμβάνει την επικύρωση των δεδομένων και τη μετατροπή τους σε κατάλληλη μορφή XML. Στη συνέχεια, το σενάριο deploy_policy.py χρησιμοποιεί το παραγόμενο αρχείο για την απευθείας εφαρμογή της πολιτικής στο pfSense.

Η διαδικασία εκτελείται κεντρικά από τον σταθμό διαχείρισης (main workstation), χωρίς να απαιτείται η είσοδος στο γραφικό περιβάλλον του firewall για κάθε τροποποίηση. Η επικοινωνία με το pfSense πραγματοποιείται μέσω ασφαλούς σύνδεσης SSH, επιτρέποντας την απομακρυσμένη μεταφορά και εφαρμογή του αρχείου ρυθμίσεων με ελεγχόμενο τρόπο. Παράλληλα, πριν από κάθε νέα εφαρμογή πολιτικής, λαμβάνεται αυτόματα αντίγραφο

ασφαλείας (backup) της προηγούμενης κατάστασης, διασφαλίζοντας τη δυνατότητα άμεσης επαναφοράς (rollback) σε περίπτωση αστοχίας.

Η εξέλιξη αυτή μετασχηματίζει τη διαδικασία διαχείρισης πολιτικών από ένα μοντέλο που απαιτούσε χειροκίνητη εισαγωγή σε ένα πλήρως κεντρικοποιημένο σύστημα εφαρμογής, η οποία απεικονίζεται στην Εικόνα 5-35. Με τον τρόπο αυτό, μειώνεται περαιτέρω η πιθανότητα ανθρώπινου σφάλματος, ενισχύεται η επαναληψιμότητα των διαδικασιών και επιτυγχάνεται καλύτερος έλεγχος των αλλαγών στο σύστημα.



Εικόνα 5-35: Κεντρικοποιημένη ροή εφαρμογής πολιτικών firewall μέσω Excel, μηχανισμού επικύρωσης και απομακρυσμένης ανάπτυξης μέσω SSH στο pfSense.

6 ΚΕΦΑΛΑΙΟ 6 – ΠΕΙΡΑΜΑΤΙΚΑ ΣΕΝΑΡΙΑ & ΑΞΙΟΛΟΓΗΣΗ

6.1 Σενάρια ελέγχου

Η αξιολόγηση της προτεινόμενης λύσης βασίστηκε σε σύνολο προκαθορισμένων σεναρίων ελέγχου, τα οποία σχεδιάστηκαν για να επαληθεύσουν την ορθή εφαρμογή των κανόνων firewall και τη συνολική συμπεριφορά του συστήματος υπό ελεγχόμενες συνθήκες. Η λογική επιλογής των σεναρίων ακολουθεί πρακτικές ελέγχου ασφάλειας και επικύρωσης ρυθμίσεων, όπως προτείνεται στη σχετική βιβλιογραφία (NIST, 2008) (Scarfone & Hoffman, 2009).

Τα σενάρια δοκιμών (test cases) περιλαμβάνουν τόσο επιτρεπόμενη όσο και απορριπτόμενη δικτυακή κίνηση, σύμφωνα με τις πολιτικές που έχουν οριστεί στο Excel template. Ειδικότερα, εξετάστηκαν σενάρια πρόσβασης σε βασικές υπηρεσίες δικτύου, όπως επίλυση ονομάτων DNS, συγχρονισμός ώρας (Network Time Protocol – NTP) και πρόσβαση σε υπηρεσίες ιστού (HTTP / HTTPS), καθώς και σενάρια απόπειρας χρήσης μη επιτρεπόμενων πρωτοκόλλων και θυρών επικοινωνίας. Η επιλογή των υπηρεσιών αυτών στηρίζεται στο ότι αποτελούν τυπικές λειτουργικές ανάγκες ενός περιβάλλοντος SMES, αλλά και κοινά σημεία κατάχρησης όταν απουσιάζουν περιορισμοί εξερχόμενης κίνησης (egress filtering) (NIST, 2009) (ENISA, 2023).

Η επιλογή των σεναρίων πραγματοποιήθηκε με γνώμονα ρεαλιστικές περιπτώσεις χρήσης που συναντώνται σε περιβάλλοντα SMEs, ώστε η αξιολόγηση να αντανακλά λειτουργικές και επιχειρησιακές απαιτήσεις, και όχι θεωρητικά σενάρια χωρίς πρακτικό αντίκρισμα. Τα σενάρια σχεδιάστηκαν επαναλήψιμα, ώστε να μειωθεί η επίδραση τυχαίων παραγόντων και να ενισχυθεί η αξιοπιστία των συμπερασμάτων (NIST, 2008).

6.2 Κριτήρια αξιολόγησης

Η αξιολόγηση της προτεινόμενης λύσης πραγματοποιήθηκε βάσει συγκεκριμένων, σαφώς ορισμένων κριτηρίων, τα οποία καλύπτουν τόσο τη λειτουργική ορθότητα του συστήματος όσο και τη χρηστικότητα της διαδικασίας διαχείρισης των κανόνων firewall. Τα κριτήρια αποσκοπούν σε αντικειμενική αποτίμηση της αποτελεσματικότητας της αυτοματοποιημένης προσέγγισης σε σύγκριση με την παραδοσιακή χειροκίνητη διαχείριση μέσω γραφικού περιβάλλοντος (Graphical User Interface – GUI) (NIST, 2009).

Πρωταρχικό κριτήριο αποτέλεσε η ορθότητα εφαρμογής των κανόνων. Για κάθε κανόνα που ορίστηκε μέσω του Excel template εξετάστηκε αν η αντίστοιχη δικτυακή κίνηση επιτράπηκε ή απορρίφθηκε, όπως είχε σχεδιαστεί. Η επαλήθευση πραγματοποιήθηκε με συνδυασμό αποτελεσμάτων από τα σενάρια δοκιμών και αντιστοίχισή τους με τις εγγραφές των logs του pfSense, ώστε να ελεγχθεί ότι δεν προκύπτουν αποκλίσεις μεταξύ ορισμού πολιτικής και πραγματικής συμπεριφοράς (Scarfone & Hoffman, 2009).

Δεύτερο κριτήριο αποτέλεσε η ελεγκσιμότητα (auditability) της διαδικασίας. Η ύπαρξη περιγραφικών πεδίων στους κανόνες και η εμφάνισή τους στις εγγραφές καταγραφής του pfSense επιτρέπουν άμεση τεκμηρίωση του «γιατί» μιας απόφασης αποδοχής ή απόρριψης κίνησης. Το στοιχείο αυτό είναι κρίσιμο σε περιβάλλοντα SMEs, όπου οι διαδικασίες τεκμηρίωσης και ελέγχου αλλαγών συχνά είναι περιορισμένες, αλλά παραμένουν απαραίτητες για διακυβέρνηση ασφάλειας και συμμόρφωση (ISO, 2022) (Whitman & Mattord, 2021).

Επιπλέον, αξιολογήθηκε η επαναληψιμότητα και η συνέπεια της διαδικασίας. Η χρήση του Excel template ως single source of truth επιτρέπει την εκ νέου εφαρμογή του ίδιου συνόλου κανόνων σε διαφορετικό χρονικό σημείο ή/και σε διαφορετικό περιβάλλον χωρίς διαφοροποιήσεις. Έτσι μειώνεται η εξάρτηση από εμπειρικές πρακτικές ή από τη μνήμη του διαχειριστή και ενισχύεται η τυποποίηση της διαχείρισης κανόνων (ISO, 2022).

Τέλος, εξετάστηκε η πρακτική χρησιμότητα της λύσης για περιβάλλοντα SMEs. Ελέγχθηκε κατά πόσο η προσέγγιση μπορεί να ενταχθεί σε καθημερινές διαδικασίες διαχείρισης χωρίς να απαιτείται εξειδικευμένη γνώση χαμηλού επιπέδου ρυθμίσεων του τείχους προστασίας. Η μείωση πολυπλοκότητας και η δυνατότητα ελέγχου αλλαγών μέσω ενός ευρέως διαδεδομένου εργαλείου, όπως το Excel, αποτελούν κρίσιμους παράγοντες αποδοχής σε πραγματικά επιχειρησιακά περιβάλλοντα (Whitman & Mattord, 2021).

Η εφαρμογή των παραπάνω κριτηρίων στα πειραματικά σενάρια επιτρέπει σφαιρική και τεκμηριωμένη αξιολόγηση της προτεινόμενης λύσης και δημιουργεί σταθερή βάση για την ανάλυση των αποτελεσμάτων στα επόμενα υποκεφάλαια.

6.3 Επικύρωση προτύπου πολιτικής (Policy Template) και μηχανισμού επικύρωσης (Validation)

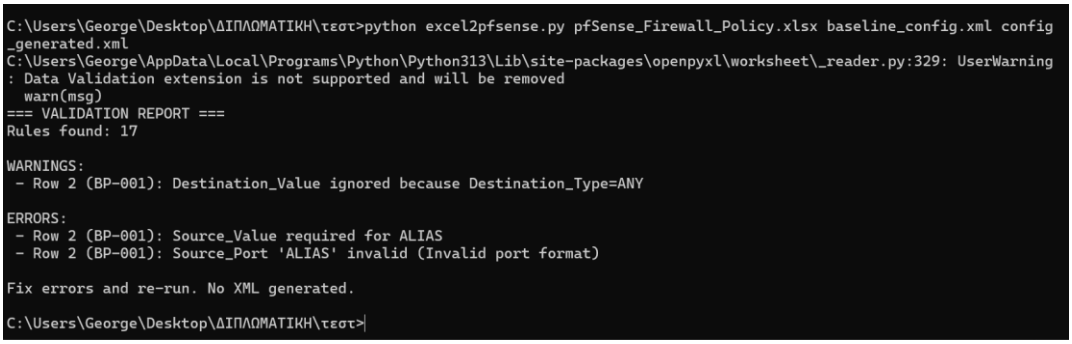
Κατά τη διαδικασία μετασχηματισμού του policy template από μορφή Excel σε αρχείο ρυθμίσεων XML για το pfSense, εφαρμόστηκε μηχανισμός επικύρωσης (validation) των πεδίων. Σκοπός του μηχανισμού είναι να διασφαλίζει τη συντακτική και λογική ορθότητα των κανόνων πριν από την εφαρμογή τους στο τείχος προστασίας, μειώνοντας τον κίνδυνο εσφαλμένων αλλαγών και μη αναμενόμενης συμπεριφοράς (NIST, 2009) (Whitman & Mattord, 2021).

Στο συγκεκριμένο πειραματικό σενάριο εισήχθη σκόπιμα μη έγκυρη πολιτική, με χρήση τύπου πηγής ALIAS χωρίς αντίστοιχη τιμή Source_Value, καθώς και με λανθασμένη καταχώριση της τιμής ALIAS στο πεδίο Source_Port. Οι ασυνέπειες αυτές παραβιάζουν κανόνες ορισμού πολιτικής και, αν εφαρμόζονταν, θα μπορούσαν να οδηγήσουν σε μη έγκυρη ή δυνητικά επικίνδυνη ρύθμιση.

Ο μηχανισμός επικύρωσης εντόπισε τα σφάλματα σε επίπεδο γραμμής (Rule ID), παρήγαγε αναλυτική αναφορά σφαλμάτων και διέκοψε τη διαδικασία δημιουργίας του XML, αποτρέποντας την εφαρμογή λανθασμένης πολιτικής στο pfSense. Ως αποτέλεσμα, δεν παρήχθη αρχείο ρυθμίσεων και δεν εφαρμόστηκε καμία αλλαγή στο τείχος προστασίας, στοιχείο που είναι ιδιαίτερα σημαντικό για έλεγχο αλλαγών και αποφυγή «μερικώς εφαρμοσμένων» ρυθμίσεων (configuration drift) (ISO, 2022).

Η προσέγγιση ευθυγραμμίζεται με αρχές ασφαλούς σχεδίασης (secure-by-design), διαχείρισης αλλαγών και λειτουργικής αξιοπιστίας συστημάτων ασφάλειας (ISO, 2022) (NIST, 2009).

Πριν από την παρουσίαση των επιμέρους υποπεριπτώσεων, η Εικόνα 6-1 αποτυπώνει το σημείο στο οποίο απορρίπτεται η πολιτική στο στάδιο validation, πριν παραχθεί το XML. Το στιγμιότυπο λειτουργεί ως τεκμήριο ότι ο έλεγχος προηγείται της εφαρμογής στο firewall.



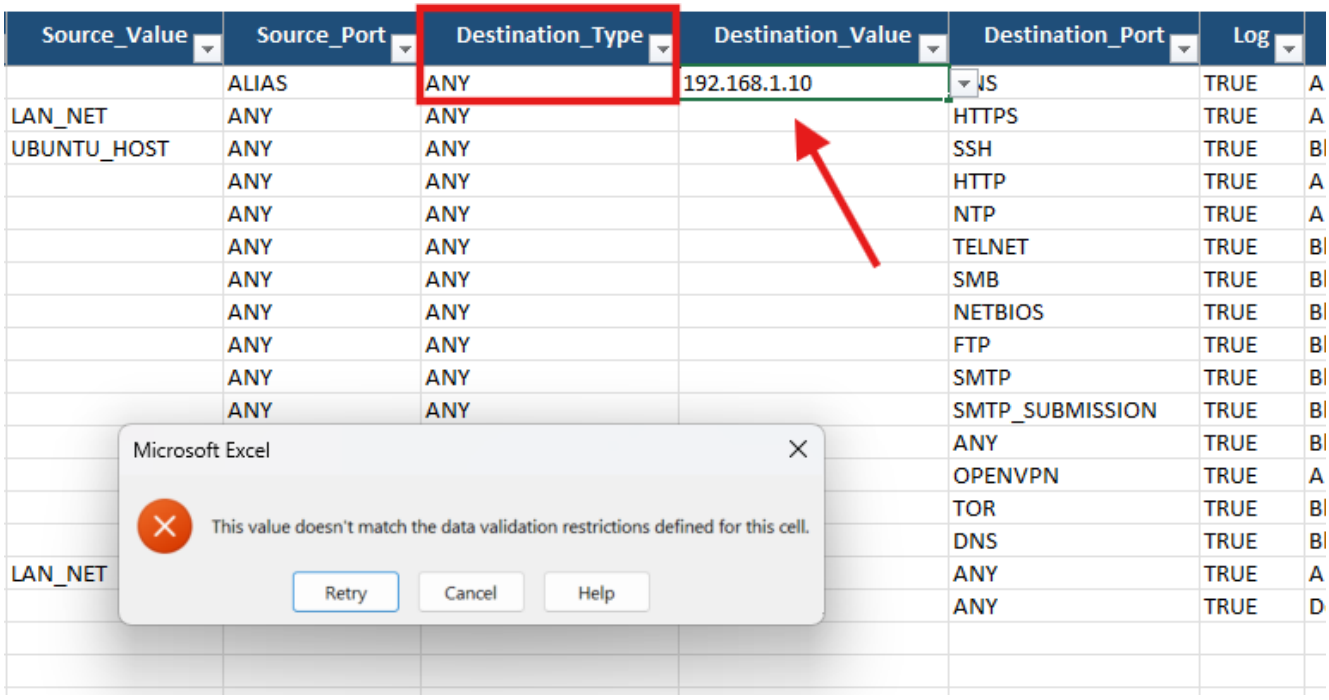
Εικόνα 6-1: Απόρριψη μη έγκυρης πολιτικής κατά το στάδιο validation πριν τη δημιουργία XML

6.3.1 Έλεγχος ασυνέπειας Destination_Type και Destination_Value

Στο πλαίσιο της λειτουργικής επικύρωσης του policy template πραγματοποιήθηκε έλεγχος λογικής ασυνέπειας μεταξύ των πεδίων Destination_Type και Destination_Value. Δοκιμάστηκε σενάριο στο οποίο το Destination_Type ορίστηκε ως ANY, ενώ ταυτόχρονα συμπληρώθηκε τιμή στο Destination_Value.

Η καταχώριση αυτή δεν συνιστά συντακτικό σφάλμα, αλλά αποτελεί λογική ασυνέπεια: όταν ο προορισμός ορίζεται ως ANY, οποιαδήποτε επιπλέον τιμή προορισμού δεν έχει επιχειρησιακή σημασία και πρακτικά αγνοείται. Ο μηχανισμός validation εντόπισε την ασυνέπεια και παρήγαγε προειδοποίηση (warning), χωρίς να απορρίψει τη συνολική πολιτική. Η διάκριση μεταξύ κρίσιμων σφαλμάτων και μη κρίσιμων ασυνεπειών υποστηρίζει ορθολογική λειτουργία, καθώς αποφεύγεται η άσκοπη απόρριψη πολιτικών όταν δεν επηρεάζεται η ασφάλεια ή η ορθότητα (Whitman & Mattord, 2021).

Η Εικόνα 6-2 παρουσιάζει την προειδοποίηση που εκδόθηκε κατά το validation.



Εικόνα 6-2: Προειδοποίηση (warning) λόγω ασυνέπειας μεταξύ Destination_Type=ANY και συμπληρωμένου Destination_Value κατά το στάδιο validation.

Ενδεικτικά, καταγράφηκε προειδοποίηση σε περίπτωση όπου ο χρήστης όρισε Destination_Type = ANY και ταυτόχρονα συμπλήρωσε Destination_Value. Σε αυτή τη λογική,

οποιαδήποτε τιμή στο Destination_Value θεωρείται περιττή και αγνοείται. Ο μηχανισμός validation κατέγραψε σχετική προειδοποίηση (“Destination_Value ignored because Destination_Type=ANY”) και συνέχισε τη δημιουργία του XML (*Εικόνα 6-4*), διατηρώντας την ορθότητα του παραγόμενου κανόνα.

Source_Port	Destination_Type	Destination_Value	Destination_Port	Log
ANY	ALIAS	FIREWALL_IP	DNS	TRUE
ANY	ANY		HTTPS	TRUE
ANY	ANY		SSH	TRUE
ANY	ANY		HTTP	TRUE
ANY	ANY		NTP	TRUE
ANY	ANY		TELNET	TRUE
ANY	ANY	FIREWALL_IP	[illegible]	TRUE
ANY	ANY		NETBIOS	TRUE
ANY	ANY		FTP	TRUE
ANY	ANY		SMTP	TRUE
ANY	ANY		SMTP_SUBMISSION	TRUE
ANY	ANY		ANY	TRUE
ANY	ANY		OPENVPN	TRUE
ANY	ANY		TOR	TRUE
ANY	ANY		DNS	TRUE
ANY	ALIAS	FIREWALL_IP	ANY	TRUE
ANY	ANY		ANY	TRUE
ANY	ANY		DNS	TRUE

Εικόνα 6-3: Παράδειγμα καταχώρησης στο Excel με ασύμβατο συνδυασμό (Destination_Type = ANY και συμπληρωμένο Destination_Value).

```
C:\Users\George\Desktop\ΔΙΠΛΩΜΑΤΙΚΗ\τεστ>python excel2pfsense.py pfSense_Firewall_Policy.xlsx baseline_config.xml config
_generated.xml
C:\Users\George\AppData\Local\Programs\Python\Python313\Lib\site-packages\openpyxl\worksheet\_reader.py:329: UserWarning
: Data Validation extension is not supported and will be removed
  warn(msg)
=== VALIDATION REPORT ===
Rules found: 18

WARNINGS:
 - Row 8 (BP-007): Destination_Value ignored because Destination_Type=ANY

No errors ✅ Generating XML...
Generated: config_generated.xml

C:\Users\George\Desktop\ΔΙΠΛΩΜΑΤΙΚΗ\τεστ>
```

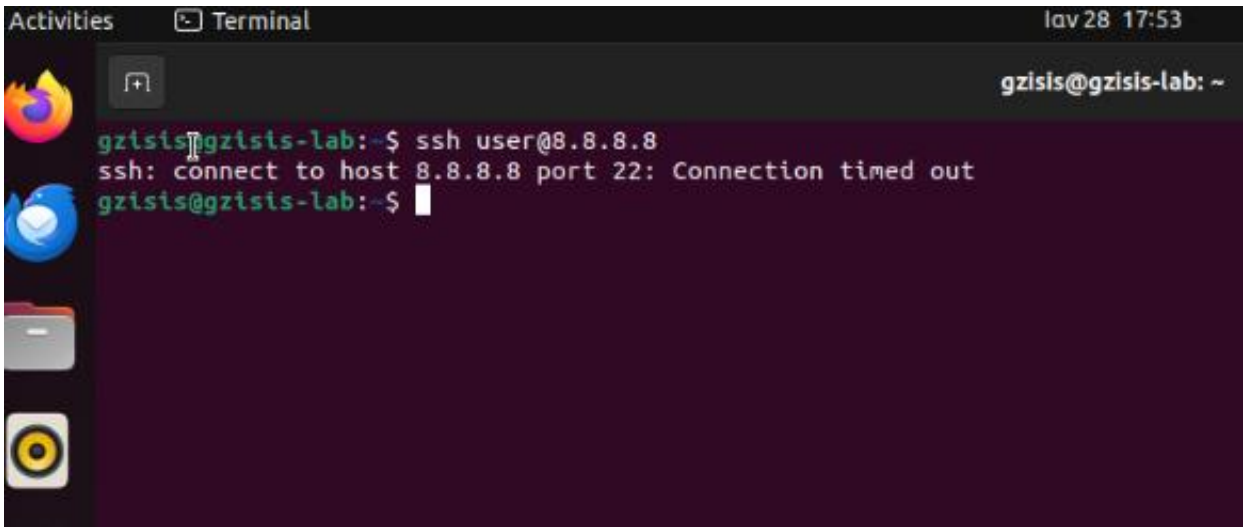
Εικόνα 6-4: Output του validation report στο terminal όπου εμφανίζεται η προειδοποίηση και η επιτυχής παραγωγή του XML.

6.3.2 Σενάριο 1 – Απαγόρευση εξερχόμενης σύνδεσης SSH(TCP/22)

Ο κανόνας “Block outbound SSH from Ubuntu” στοχεύει στην αποτροπή εξερχόμενων συνδέσεων Secure Shell (SSH) μέσω Transmission Control Protocol (TCP) στη θύρα 22 (TCP/22) από το Test VM προς το διαδίκτυο. Η πολιτική αυτή περιορίζει δυνατότητες κατάχρησης του πρωτοκόλλου για μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση ή για

εξαγωγή δεδομένων (data exfiltration), ειδικά σε περιπτώσεις παραβίασης εσωτερικού σταθμού (ENISA, 2023) (NIST, 2009).

Η δοκιμή πραγματοποιήθηκε με απόπειρα σύνδεσης SSH προς εξωτερική διεύθυνση IP. Η σύνδεση απορρίφθηκε και στα firewall logs καταγράφηκε αντιστοίχιση με τον συγκεκριμένο κανόνα αποκλεισμού, επιβεβαιώνοντας την ορθή εφαρμογή της πολιτικής. Οι Εικόνες 6-5 και 6-6 αποτυπώνουν αντίστοιχα την απόπειρα σύνδεσης και την καταγραφή απόρριψης.



Εικόνα 6-5: απόπειρα σύνδεσης SSH προς εξωτερική διεύθυνση IP

Normal View | Dynamic View | Summary View

Last 500 Firewall Log Entries. (Maximum 500)

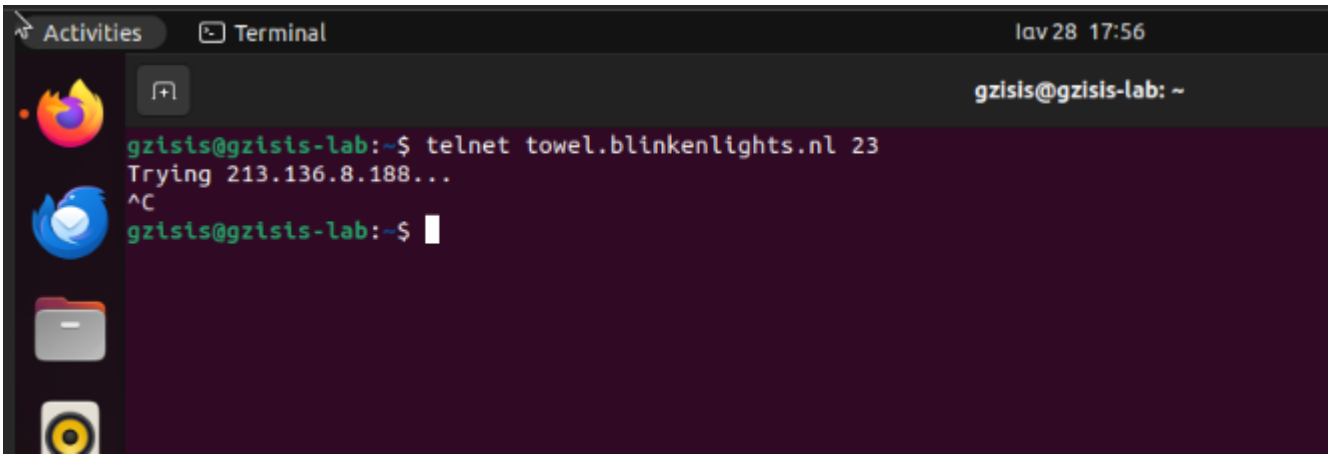
Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Jan 28 17:48:36	LAN	Block outbound SSH from Ubuntu (1003)	192.168.1.100:43786	8.8.8.8:22	TCP:S
✕	Jan 28 17:48:32	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Jan 28 17:48:32	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✕	Jan 28 17:48:27	LAN	Block outbound SSH from Ubuntu (1003)	192.168.1.100:43786	8.8.8.8:22	TCP:S
✕	Jan 28 17:48:27	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✕	Jan 28 17:48:23	WAN	Default deny rule IPv4 (1000000103)	192.168.10.17:56700	255.255.255.255:56700	UDP
✕	Jan 28 17:48:23	LAN	Block outbound SSH from Ubuntu (1003)	192.168.1.100:43786	8.8.8.8:22	TCP:S
✕	Jan 28 17:48:22	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✕	Jan 28 17:48:21	LAN	Block outbound SSH from Ubuntu (1003)	192.168.1.100:43786	8.8.8.8:22	TCP:S
✕	Jan 28 17:48:20	LAN	Block outbound SSH from Ubuntu (1003)	192.168.1.100:43786	8.8.8.8:22	TCP:S
✕	Jan 28 17:48:20	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Jan 28 17:48:19	LAN	Block outbound SSH from Ubuntu (1003)	192.168.1.100:43786	8.8.8.8:22	TCP:S

Εικόνα 6-6: Firewall logs που καταγράφουν τον αποκλεισμό εξερχόμενης σύνδεσης SSH από Ubuntu

6.3.3 Σενάριο 2 – Απαγόρευση μη ασφαλούς διαχείρισης μέσω Telnet (TCP/23)

Ο κανόνας “Block Telnet outbound” ελέγχει τη χρήση του μη ασφαλούς πρωτοκόλλου Telnet μέσω TCP στη θύρα 23 (TCP/23). Η απαγόρευση Telnet αποτελεί συνήθη πολιτική σκλήρυνσης (hardening), λόγω μετάδοσης διαπιστευτηρίων σε μη κρυπτογραφημένη μορφή (clear-text) (Stallings, 2018) (NIST, 2009).

Η δοκιμή τεκμηριώνεται στις Εικόνες 6-7 και 6-8, όπου παρουσιάζεται η αποτυχημένη απόπειρα σύνδεσης και η αντίστοιχη εγγραφή απόρριψης στα logs του pfSense.



Εικόνα 6-7: Απόπειρα εξερχόμενης σύνδεσης Telnet (TCP/23) από σταθμό Ubuntu, η οποία απορρίπτεται σύμφωνα με την πολιτική ασφάλειας.

Η σύνδεση δεν ολοκληρώθηκε και καταγράφηκε σχετική εγγραφή απόρριψης στο pfSense firewall, επιβεβαιώνοντας την απαγόρευση του πρωτοκόλλου.

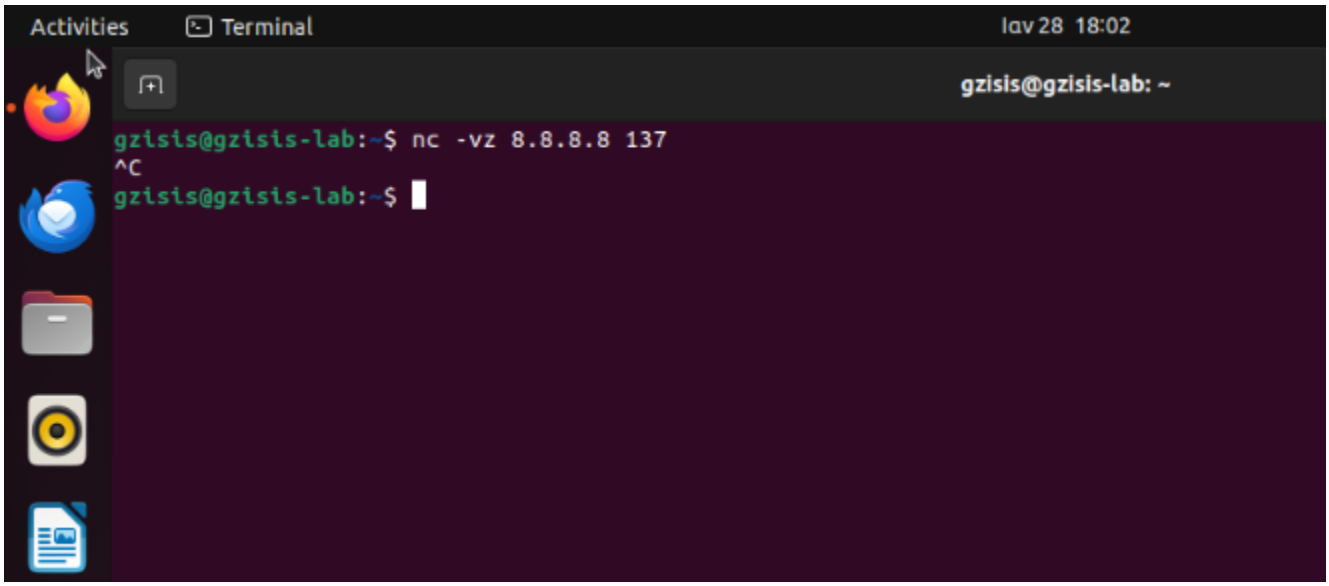
✕	Jan 28 17:56:32	WAN	Default deny rule IPv4 (1000000103)	192.168.10.17:5353	224.0.0.251:5353	UDP
✕	Jan 28 17:56:32	WAN	Default deny rule IPv4 (1000000103)	192.168.10.63:5353	224.0.0.251:5353	UDP
✕	Jan 28 17:56:32	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✕	Jan 28 17:56:31	LAN	Block Telnet outbound (1006)	192.168.1.100:53472	213.136.8.188:23	TCP:S
✕	Jan 28 17:56:30	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Jan 28 17:56:27	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP

Εικόνα 6-8: Καταγραφή firewall που επιβεβαιώνει τον αποκλεισμό εξερχόμενης σύνδεσης Telnet (TCP/23) από τον σταθμό Ubuntu.

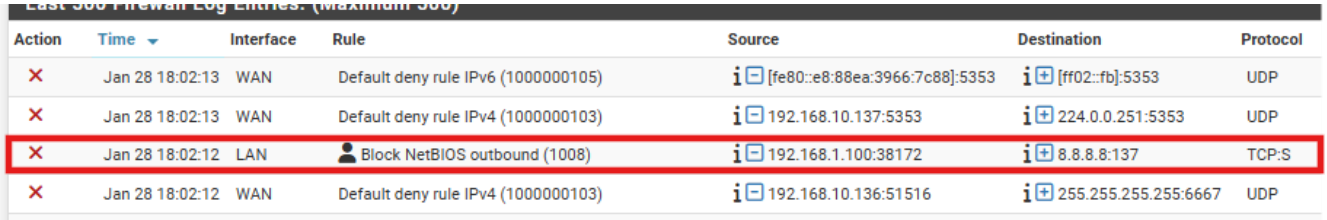
6.3.4 Σενάριο 3 – Απαγόρευση SMB και NetBIOS εξερχόμενης κίνησης

Οι κανόνες “Block SMB outbound” (TCP/445) και “Block NetBIOS outbound” (TCP/137) εφαρμόστηκαν για την αποτροπή μη απαραίτητων και δυνητικά επικίνδυνων πρωτοκόλλων, τα οποία έχουν ιστορικά συσχετιστεί με επιθέσεις εξάπλωσης και πλευρικής κίνησης (lateral movement) σε εσωτερικά δίκτυα (ENISA, 2023) (NIST, 2009).

Οι δοκιμές πραγματοποιήθηκαν με χρήση του εργαλείου netcat (nc). Οι Εικόνες 6-9 και 6-10 παρουσιάζουν αντίστοιχα την αποτυχημένη απόπειρα σύνδεσης NetBIOS και την επιβεβαίωση του αποκλεισμού στα logs του pfSense.



Εικόνα 6-9: Απόπειρα εξερχόμενης σύνδεσης NetBIOS (TCP/137) από σταθμό Ubuntu, η οποία αποτυγχάνει λόγω ενεργού κανόνα αποκλεισμού.

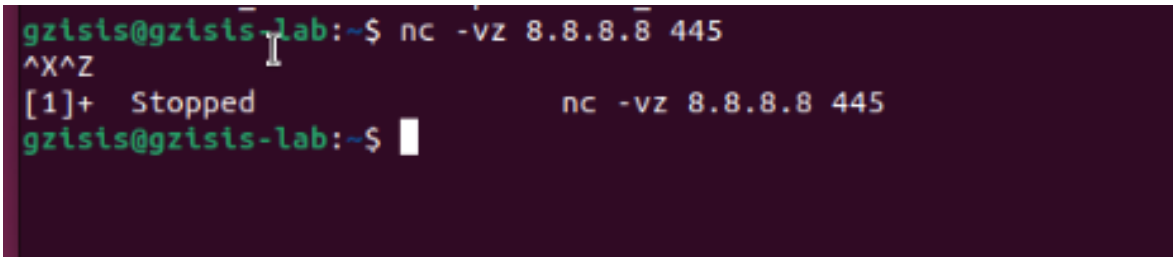


Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Jan 28 18:02:13	WAN	Default deny rule IPv6 (1000000105)	[fe80::e8:88ea:3966:7c88]:5353	[ff02::fb]:5353	UDP
✕	Jan 28 18:02:13	WAN	Default deny rule IPv4 (1000000103)	192.168.10.137:5353	224.0.0.251:5353	UDP
✕	Jan 28 18:02:12	LAN	Block NetBIOS outbound (1008)	192.168.1.100:38172	8.8.8.8:137	TCP:S
✕	Jan 28 18:02:12	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP

Εικόνα 6-10: Καταγραφή firewall που επιβεβαιώνει τον αποκλεισμό εξερχόμενης κίνησης NetBIOS (TCP/137) από σταθμό Ubuntu.

Για την επαλήθευση του κανόνα “Block SMB outbound” (TCP/445) πραγματοποιήθηκε δοκιμή εξερχόμενης σύνδεσης SMB από τον σταθμό Ubuntu προς εξωτερικό προορισμό με χρήση του εργαλείου Netcat (nc).

Η εκτέλεση της εντολής nc -vz 8.8.8.8 445 επιχειρεί τη δημιουργία TCP σύνδεσης προς τη θύρα SMB. Η αποτυχία της σύνδεσης επιβεβαιώνει ότι ο κανόνας αποκλεισμού SMB εφαρμόζεται ορθά από το firewall.



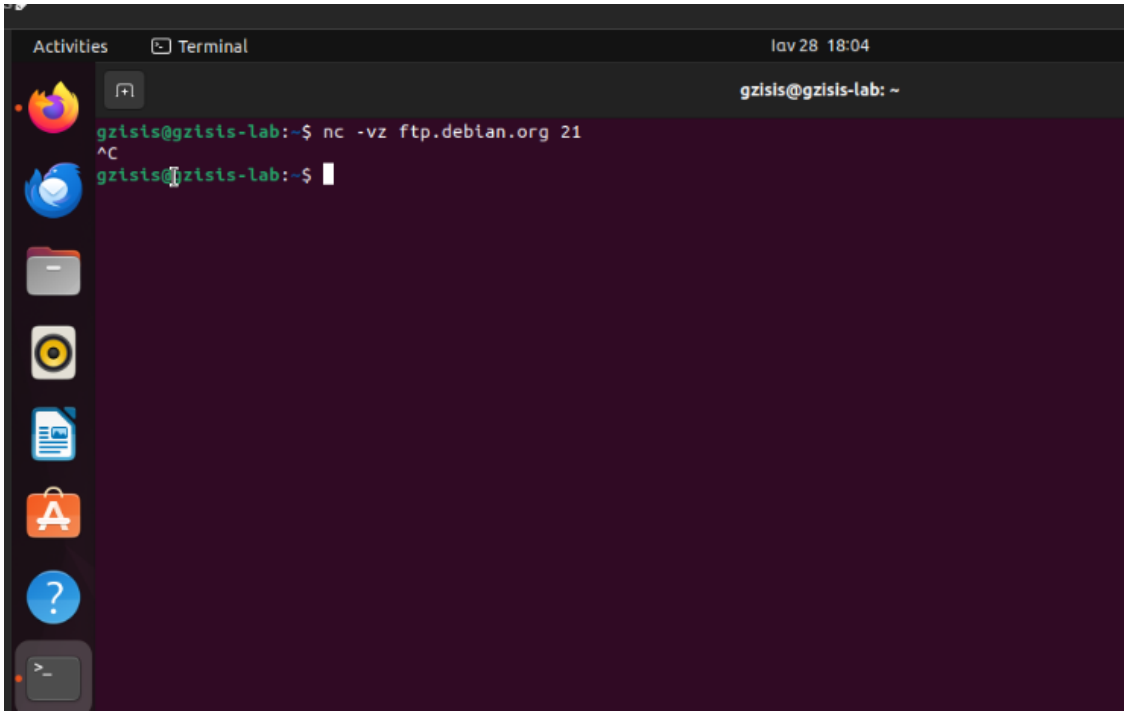
Εικόνα 6-11: Απόπειρα εξερχόμενης σύνδεσης SMB (TCP/445) από σταθμό Ubuntu προς εξωτερικό προορισμό με χρήση του εργαλείου Netcat (nc), η οποία αποτυγχάνει λόγω ενεργού κανόνα αποκλεισμού.

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Mar 4 18:03:37	WAN	Default deny rule IPv4 (1000000103)	192.168.10.17:56934	255.255.255.255:9999	UDP
✕	Mar 4 18:03:37	LAN	Block SMB outbound (malware prevention) (1007)	192.168.1.100:56800	8.8.8.8:445	TCP:S
✕	Mar 4 18:03:36	LAN	Block SMB outbound (malware prevention) (1007)	192.168.1.100:56800	8.8.8.8:445	TCP:S
✕	Mar 4 18:03:35	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Mar 4 18:03:34	LAN	Block SMB outbound (malware prevention)	192.168.1.100:56800	8.8.8.8:445	TCP:S

Εικόνα 6-12: Απόπειρα εξερχόμενης σύνδεσης SMB (TCP/445) από σταθμό Ubuntu προς εξωτερικό προορισμό με χρήση του εργαλείου Netcat (nc), η οποία αποτυγχάνει λόγω ενεργού κανόνα αποκλεισμού.

6.3.5 Σενάριο 4 – Απαγόρευση FTP

Ο κανόνας *"Block FTP outbound (clear-text)"* ελέγχει την απαγόρευση του πρωτοκόλλου FTP (TCP/21). Για την επαλήθευση του κανόνα πραγματοποιήθηκε δοκιμή εξερχόμενης σύνδεσης FTP από σταθμό Ubuntu προς εξωτερικό διακομιστή (ftp.debian.org) στη θύρα 21. Όπως φαίνεται στην Εικόνα 6-13, η προσπάθεια σύνδεσης αποτυγχάνει, γεγονός που επιβεβαιώνει ότι ο κανόνας αποκλεισμού εφαρμόζεται σωστά.



Εικόνα 6-13: Απόπειρα εξερχόμενης σύνδεσης FTP (TCP/21) από σταθμό Ubuntu, η οποία απορρίπτεται σύμφωνα με την πολιτική ασφάλειας.

Η απόρριψη της κίνησης καταγράφεται επίσης στο σύστημα καταγραφών του firewall, όπως παρουσιάζεται στην Εικόνα 6-14, επιβεβαιώνοντας την ορθή λειτουργία της πολιτικής απαγόρευσης εξερχόμενης FTP κίνησης.

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Jan 28 18:03:58	WAN	Default deny rule IPv4 (1000000103)	192.168.10.17:5353	224.0.0.251:5353	UDP
✕	Jan 28 18:03:58	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1:5353	224.0.0.251:5353	UDP
✕	Jan 28 18:03:57	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✕	Jan 28 18:03:56	LAN	Block FTP outbound (clear-text) (1009)	192.168.1.100:44912	146.75.118.132:21	TCP:S
✕	Jan 28 18:03:55	LAN	Block FTP outbound (clear-text) (1009)	192.168.1.100:44912	146.75.118.132:21	TCP:S
✕	Jan 28 18:03:54	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Jan 28 18:03:54	LAN	Block FTP outbound (clear-text) (1009)	192.168.1.100:44912	146.75.118.132:21	TCP:S
✕	Jan 28 18:03:53	LAN	Block FTP outbound (clear-text) (1009)	192.168.1.100:44912	146.75.118.132:21	TCP:S
✕	Jan 28 18:03:52	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP

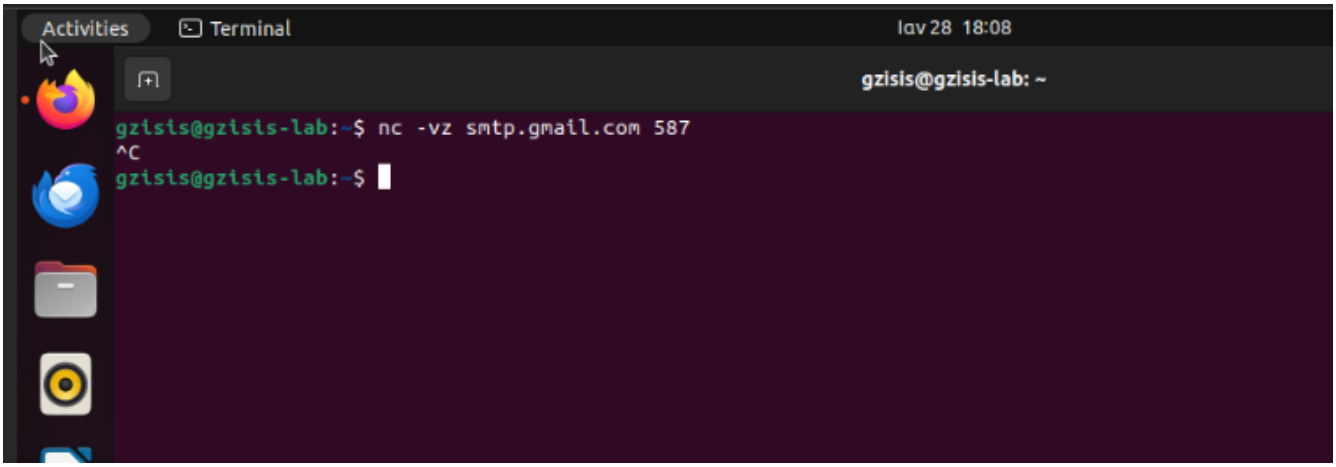
Εικόνα 6-14: Καταγραφή firewall που επιβεβαιώνει τον αποκλεισμό εξερχόμενης FTP κίνησης (clear-text, TCP/21) από σταθμό Ubuntu.

6.3.6 Σενάριο 5 – Έλεγχος πολιτικών SMTP (TCP/587)

Ο κανόνας “Block SMTP submission” εφαρμόστηκε για τον περιορισμό της ανεξέλεγκτης αποστολής ηλεκτρονικής αλληλογραφίας (Simple Mail Transfer Protocol – SMTP) μέσω TCP στη θύρα 587 (TCP/587). Τέτοιες πολιτικές χρησιμοποιούνται για μείωση κινδύνου κατάχρησης σταθμών (π.χ. από κακόβουλο λογισμικό) για αποστολή ανεπιθύμητης αλληλογραφίας ή για εξαγωγή δεδομένων μέσω email (ENISA, 2023).

Η αποτυχία σύνδεσης και η αντίστοιχη καταγραφή αποκλεισμού τεκμηριώνονται στις Εικόνες 6-15 και 6-16.

Η δοκιμή πραγματοποιήθηκε με την εντολή:



Εικόνα 6-15: Αποτυχία σύνδεσης SMTP Submission λόγω ενεργών κανόνων περιορισμού εξερχόμενης email κίνησης.

Η σύνδεση απορρίφθηκε, γεγονός που επιβεβαιώνει την εφαρμογή πολιτικής ελέγχου εξερχόμενης SMTP επικοινωνίας.

✕	Jan 28 18:08:39	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1	224.0.0.1	IGMP
✕	Jan 28 18:08:37	LAN	Block SMTP submission (controlled email) (1011)	192.168.1.100:50944	74.125.71.108:587	TCP:S
✕	Jan 28 18:08:37	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP
✕	Jan 28 18:08:36	LAN	Block SMTP submission (controlled email) (1011)	192.168.1.100:50944	74.125.71.108:587	TCP:S
✕	Jan 28 18:08:35	LAN	Block SMTP submission (controlled email) (1011)	192.168.1.100:50944	74.125.71.108:587	TCP:S
✕	Jan 28 18:08:34	LAN	Block SMTP submission (controlled email) (1011)	192.168.1.100:50944	74.125.71.108:587	TCP:S
✕	Jan 28 18:08:33	LAN	Block SMTP submission (controlled email) (1011)	192.168.1.100:50944	74.125.71.108:587	TCP:S
✕	Jan 28 18:08:32	LAN	Block SMTP submission (controlled email) (1011)	192.168.1.100:50944	74.125.71.108:587	TCP:S
✕	Jan 28 18:08:32	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:51516	255.255.255.255:6667	UDP

Εικόνα 6-16: Firewall logs του pfSense που επιβεβαιώνουν τον αποκλεισμό εξερχόμενης σύνδεσης SMB (TCP/445) από τον σταθμό Ubuntu προς εξωτερικό προορισμό

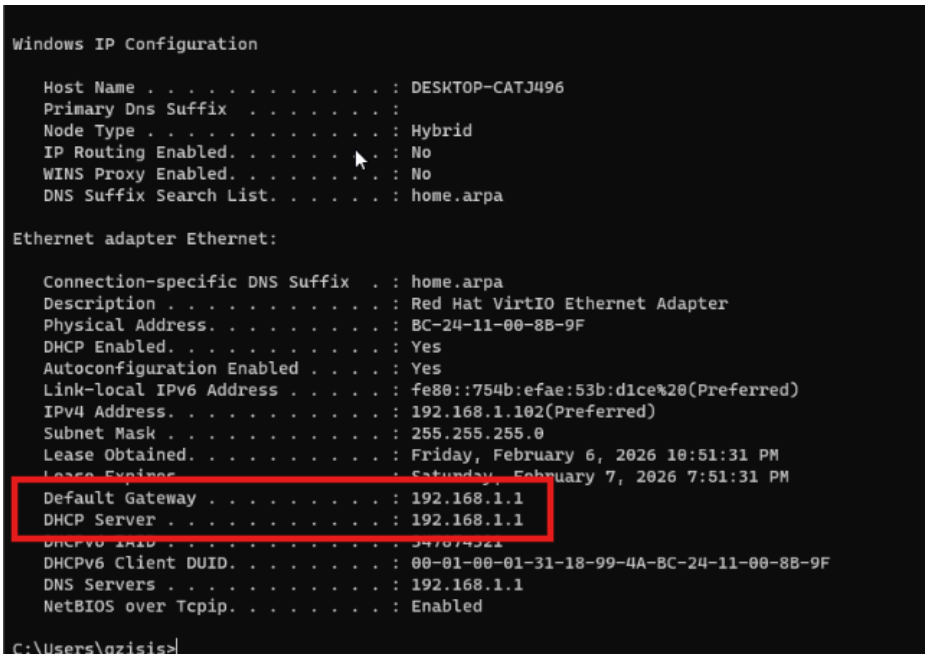
6.3.7 Σενάριο 6 – Επιτρεπόμενες βασικές υπηρεσίες (DNS, HTTPS)

Για την επαλήθευση της βασικής λειτουργικότητας του συστήματος, δοκιμάστηκαν υπηρεσίες που επιτρέπονται ρητά από την πολιτική τείχους προστασίας. Οι δοκιμές DNS πραγματοποιήθηκαν με χρήση εικονικής μηχανής Windows 11 Pro, η οποία εκτελέστηκε στο Proxmox Virtual Environment και λειτούργησε ως τυπικός πελάτης (client) του εσωτερικού δικτύου πίσω από το pfSense.

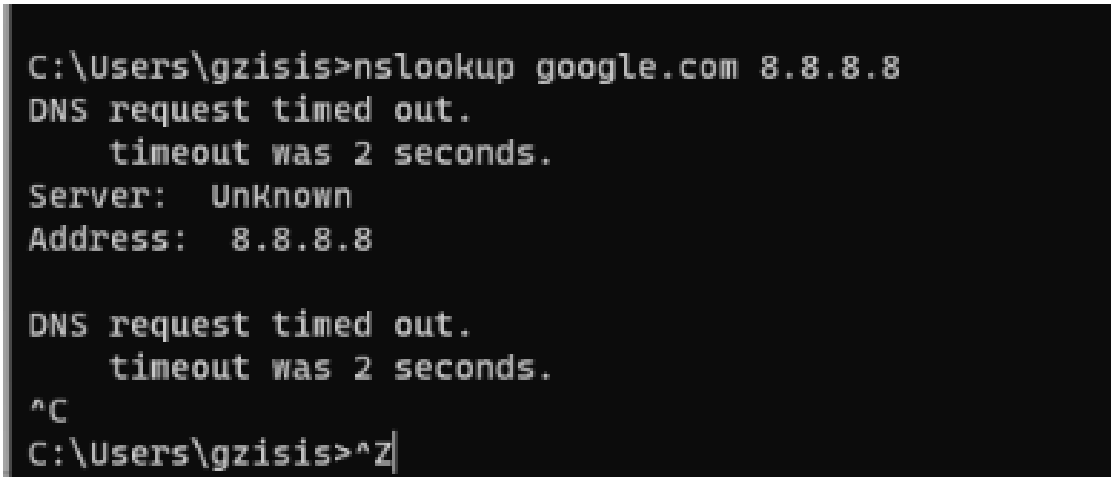
DNS – Επιβολή κεντρικού resolver μέσω firewall

Στο παρόν σενάριο αξιολογείται η επιτρεπόμενη παροχή υπηρεσίας DNS προς τις τελικές συσκευές, υπό τον περιορισμό ότι η επίλυση ονομάτων πραγματοποιείται αποκλειστικά μέσω του τείχους προστασίας. Η πολιτική αυτή στοχεύει στην αποτροπή παράκαμψης μηχανισμών φιλτραρίσματος και στην κεντρική επιβολή πολιτικών πληροφοριών απειλών (threat intelligence) μέσω DNS-based ελέγχων (ENISA, 2023).

Υλοποιήθηκαν δύο διαδοχικοί κανόνες: (α) επιτρεπτός κανόνας DNS αποκλειστικά προς τον resolver του pfSense και (β) απαγορευτικός κανόνας για κάθε άλλη DNS επικοινωνία προς εξωτερικούς προορισμούς. Η ορθότητα της πολιτικής επαληθεύτηκε μέσω δοκιμών επίλυσης ονομάτων και ανάλυσης των firewall logs, όπου καταγράφηκαν τόσο οι επιτρεπόμενες όσο και οι απορριπτόμενες προσπάθειες παράκαμψης.



Εικόνα 6-17: Ρυθμίσεις δικτύου Windows 11 – Ανάθεση IP, Gateway και DNS από το pfSense firewall μέσω DHCP.



Εικόνα 6-18: Αποτυχημένη απόπειρα επίλυσης ονομάτων μέσω εξωτερικού DNS server (8.8.8.8), λόγω επιβολής πολιτικής κεντρικού DNS

✓	Feb 7 18:46:05	LAN	Allow DNS to internal firewall resolver (1001)	192.168.1.102:55491	192.168.1.1:53	UDP
✓	Feb 7 18:46:05	LAN	Allow DNS to internal firewall resolver (1001)	192.168.1.102:62935	192.168.1.1:53	UDP
✗	Feb 7 18:46:04	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✗	Feb 7 18:46:03	WAN	Default deny rule IPv4 (1000000103)	192.168.10.42:5353	224.0.0.251:5353	UDP
✗	Feb 7 18:46:03	WAN	Default deny rule IPv4 (1000000103)	192.168.10.1:5353	224.0.0.251:5353	UDP
✗	Feb 7 18:45:59	WAN	Default deny rule IPv4 (1000000103)	192.168.10.136:53574	255.255.255.255:6667	UDP
✗	Feb 7 18:45:59	LAN	Block external DNS – force internal DNS (1770411519)	192.168.1.102:50301	8.8.8.8:53	UDP
✗	Feb 7 18:45:57	LAN	Block external DNS – force internal DNS (1770411519)	192.168.1.102:50300	8.8.8.8:53	UDP
✗	Feb 7 18:45:55	LAN	Block external DNS – force internal DNS (1770411519)	192.168.1.102:50299	8.8.8.8:53	UDP

Εικόνα 6-19: Καταγραφή απορριπτόμενων DNS αιτημάτων προς εξωτερικούς προορισμούς στα firewall logs του pfSense.

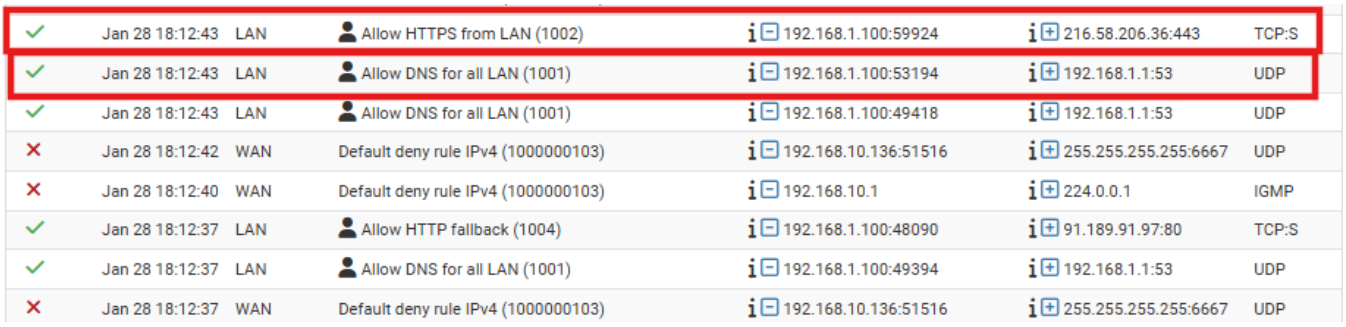
Όπως απεικονίζεται στις Εικόνες 6-18 και 6-19, κάθε απόπειρα απευθείας επικοινωνίας με εξωτερικούς DNS servers απορρίπτεται και καταγράφεται επιτυχώς.

HTTPS πρόσβαση:

Για την επαλήθευση της επιτρεπόμενης εξερχόμενης πρόσβασης σε ασφαλείς υπηρεσίες ιστού, πραγματοποιήθηκε δοκιμή σύνδεσης HTTPS από σταθμό Ubuntu που βρίσκεται στο εσωτερικό δίκτυο πίσω από το pfSense firewall. Η δοκιμή εκτελέστηκε με χρήση της εντολής curl, αποστέλλοντας αίτημα προς εξωτερικό εξυπηρετητή ιστού μέσω της θύρας TCP/443.

Εικόνα 6-20: Επιτυχής εξερχόμενη σύνδεση HTTPS (TCP/443) από σταθμό Ubuntu, επιβεβαιώνοντας την επιτρεπτική πολιτική για ασφαλείς υπηρεσίες.

Όλες οι δοκιμές ολοκληρώθηκαν επιτυχώς και καταγράφηκαν στα firewall logs ως επιτρεπόμενη (pass) κίνηση, επιβεβαιώνοντας ότι οι εφαρμοζόμενοι κανόνες επιτρέπουν τις απαραίτητες υπηρεσίες του δικτύου.



Εικόνα 6-21: Καταγραφές firewall που επιβεβαιώνουν την επιτρεπόμενη εξερχόμενη επικοινωνία DNS και HTTPS από το LAN, σύμφωνα με την πολιτική ασφάλειας.

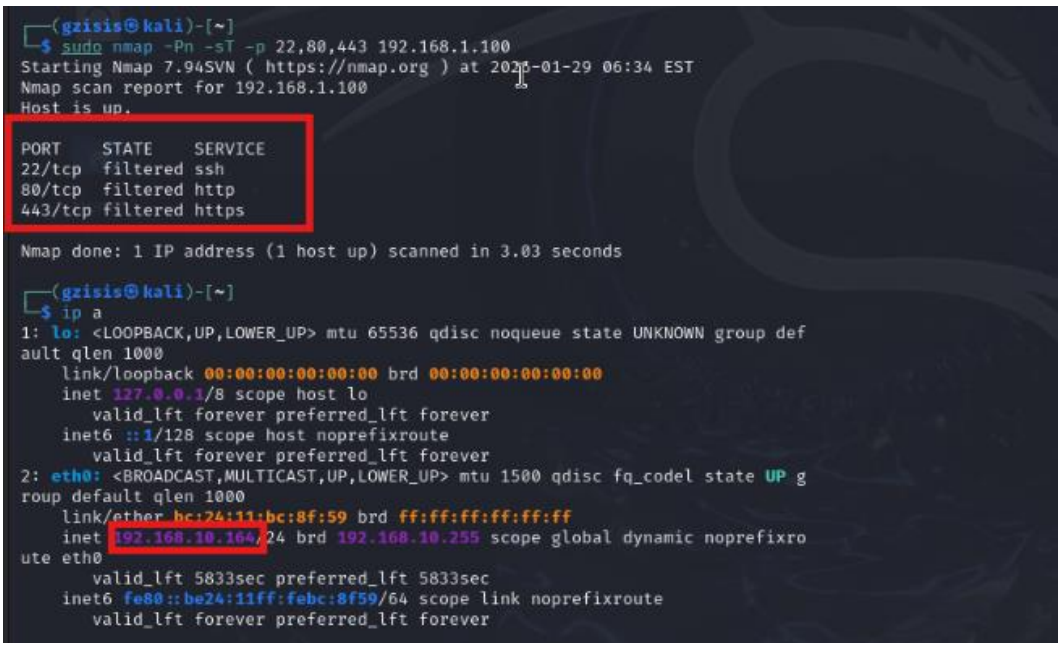
Όλες οι εντολές εκτελέστηκαν από σύστημα τοποθετημένο πίσω από το firewall, γεγονός που διασφαλίζει ότι τα αποτελέσματα αντικατοπτρίζουν πραγματική συμπεριφορά δικτύου σε περιβάλλον SME.

6.3.8 Σενάριο 7 – Λειτουργική επαλήθευση κανόνων firewall

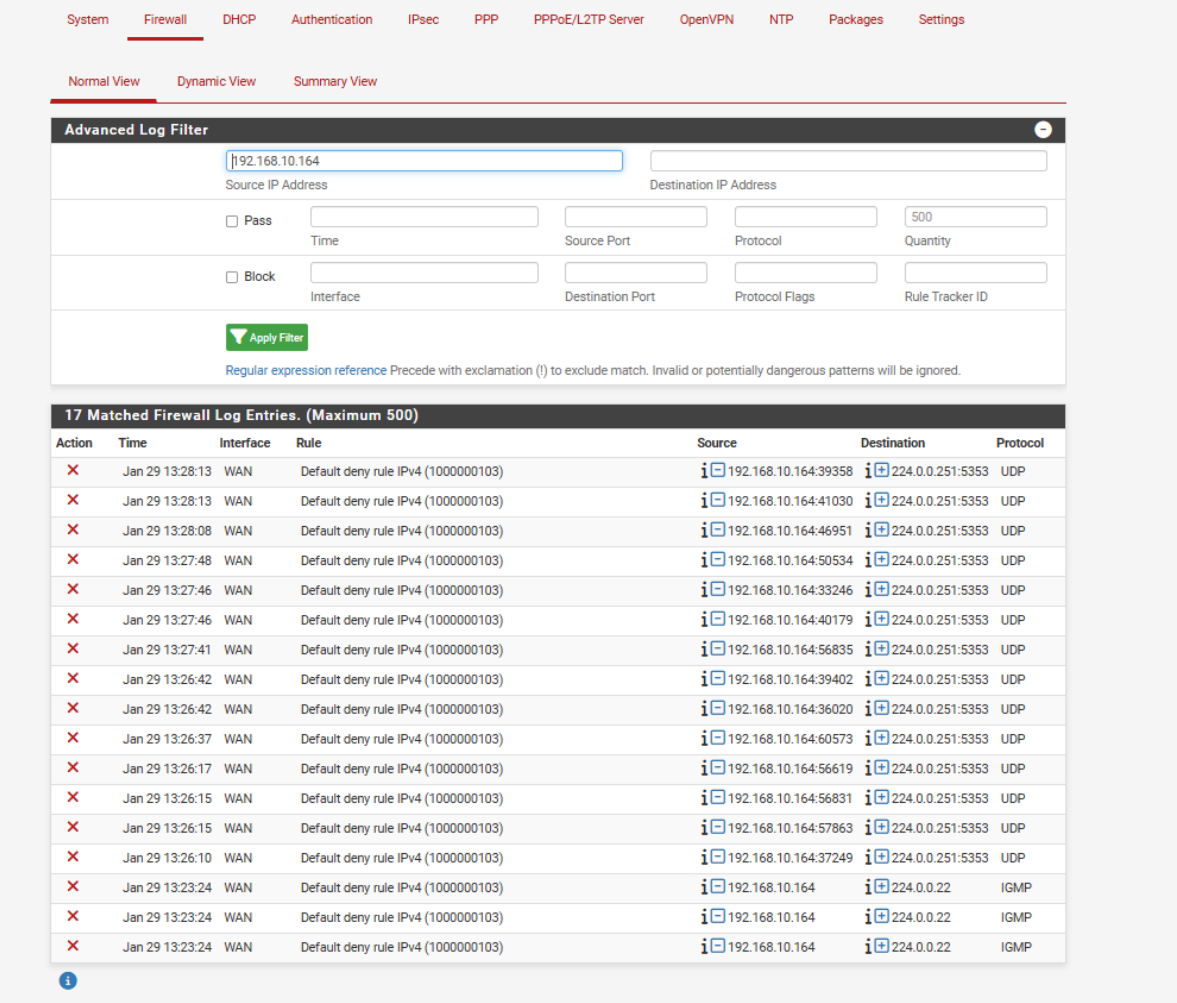
Στο παρόν σενάριο εξετάστηκε η συμπεριφορά του τείχους προστασίας σε περιπτώσεις απόρριψης δικτυακής κίνησης, με έμφαση στη διάκριση μεταξύ των καταστάσεων “blocked” και “filtered”, όπως εμφανίζονται στα αποτελέσματα εργαλείων ελέγχου δικτύου (π.χ. nmap). Η διάκριση αυτή έχει σημασία επειδή επηρεάζει τη δυνατότητα αναγνώρισης υπηρεσιών από έναν επιτιθέμενο, άρα συνδέεται με πρακτικές σκλήρυνσης (hardening) και μείωσης πληροφοριακής διαρροής (information disclosure) (NIST, 2009).

Κατά την εκτέλεση σαρώσεων από το Attacker Virtual Machine (Kali Linux) προς το Test Virtual Machine, παρατηρήθηκε ότι ορισμένες θύρες εμφανίζονται ως “filtered”. Η ένδειξη αυτή υποδηλώνει ότι τα πακέτα δεν απορρίπτονται ρητά με απάντηση (reject), αλλά αποσιωπώνται (drop) από το τείχος προστασίας, σύμφωνα με την προεπιλεγμένη πολιτική απόρριψης (default deny). Η συμπεριφορά αυτή επιβεβαιώνεται από τις εγγραφές των firewall logs του pfSense, όπου η αντίστοιχη κίνηση καταγράφεται ως απορριπτόμενη από τον κανόνα “Default deny IPv4”.

Οι Εικόνες 6-22 και 6-23 παρουσιάζουν αντίστοιχα το αποτέλεσμα της σάρωσης με “filtered” θύρες και την καταγραφή της απόρριψης στο pfSense, τεκμηριώνοντας τη συσχέτιση μεταξύ παρατηρούμενης συμπεριφοράς και εφαρμοζόμενης πολιτικής.



Εικόνα 6-22: Αποτελέσματα σάρωσης θυρών από Attacker VM με ένδειξη “filtered”



Εικόνα 6-23: Καταγραφή απορριπτόμενης κίνησης από τον κανόνα Default deny IPv4

6.4 Αξιολόγηση Threat Intelligence πολιτικών

Στην παρούσα ενότητα αξιολογείται η αποτελεσματικότητα των πολιτικών threat intelligence που υλοποιήθηκαν στο πλαίσιο της προτεινόμενης αρχιτεκτονικής ασφάλειας. Η αξιολόγηση εστιάζει σε δύο συμπληρωματικούς μηχανισμούς: (α) την προληπτική αποτροπή απειλών μέσω του pfBlockerNG και (β) την ανίχνευση και καταγραφή ύποπτης/κακόβουλης δραστηριότητας μέσω του συστήματος Suricata σε ρόλο συστήματος IDS και IPS. Η διάκριση αυτή επιτρέπει να αποτυπωθεί η συμβολή κάθε μηχανισμού στο συνολικό μοντέλο άμυνας σε βάθος (defense-in-depth) (Stallings, 2018) (ENISA, 2023).

Πριν την ανάλυση των επιμέρους μηχανισμών, ο Πίνακας 6-1 συνοψίζει συγκριτικά το είδος προστασίας, το σημείο ελέγχου και τη χρονική στιγμή απόκρισης, ώστε να είναι σαφές πώς οι μηχανισμοί αλληλοσυμπληρώνονται επιχειρησιακά.

Πίνακας 6-1: Συγκριτική Αξιολόγηση Μηχανισμών Threat Intelligence

Μηχανισμός	**Τύπος Προστασίας**	**Σημείο Ελέγχου**	**Χρόνος Απόκρισης**	**Επίπεδο Φιλτραρίσματος**	**Συνεισφορά στο Defense-in-Depth**
pfBlockerNG	Proactive Blocking	Perimeter (DNS/IP)	Πριν τη σύνδεση	Layer 3 / Layer 7 (DNSBL)	Προληπτική αποτροπή
Suricata IDS	Detection	Inline / Traffic Inspection	Μετά την έναρξη επικοινωνίας	Layer 4–7	Εντοπισμός ύποπτης συμπεριφοράς
Suricata IPS	Active Prevention	Inline	Real-time	Layer 4–7	Δυναμικός αποκλεισμός

6.4.1 pfBlockerNG

Το pfBlockerNG χρησιμοποιήθηκε ως συμπληρωματικό επίπεδο ασφάλειας, με στόχο την προληπτική αποτροπή επικοινωνίας με γνωστή κακόβουλη υποδομή, αξιοποιώντας δεδομένα threat intelligence. Ο ρόλος του δεν είναι να αντικαταστήσει τους κανόνες τείχους προστασίας, αλλά να μειώσει την επιφάνεια επίθεσης μέσω φιλτραρίσματος διευθύνσεων IP και domain names πριν η κίνηση φτάσει σε ανώτερα επίπεδα ελέγχου (ENISA, 2023).

Η λειτουργία DNS Block List (DNSBL) ενεργοποιήθηκε ώστε να αποτρέπεται η επίλυση domain names που έχουν συσχετιστεί με κακόβουλη δραστηριότητα. Η επιλογή των feeds βασίστηκε σε κατηγορίες υψηλής αξιοπιστίας (high-confidence), όπως:

- domains διανομής κακόβουλου λογισμικού,
- υποδομές ηλεκτρονικού «ψαρέματος» (phishing),
- command-and-control endpoints,

- compromised domains με επιβεβαιωμένη κακόβουλη χρήση (ENISA, 2023).

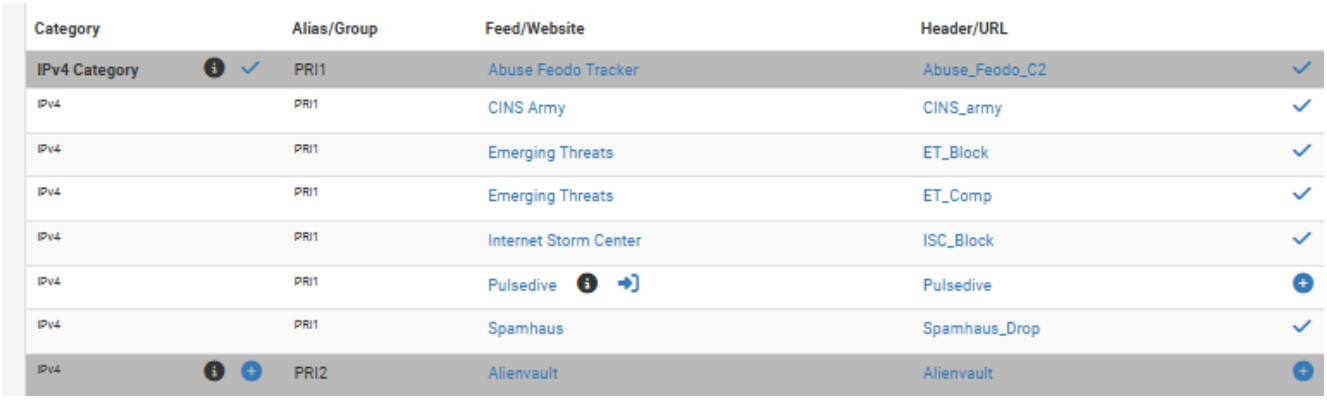
Αντίθετα, κατηγορίες γενικού σκοπού ή επιθετικού χαρακτήρα (π.χ. social media, CDN, video platforms, heuristic lists) αποκλείστηκαν σκόπιμα, ώστε να περιοριστούν τα ψευδώς θετικά (false positives) και να διατηρηθεί επιχειρησιακή συνέχεια, που είναι κρίσιμο ζητούμενο σε περιβάλλον SME (Whitman & Mattord, 2021). Για λόγους διαχειριστικής σαφήνειας και ελεγκσιμότητας (auditability), δημιουργήθηκε ένα μοναδικό DNSBL group, αποφεύγοντας επικαλύψεις και πολλαπλές ομάδες με παρόμοια λειτουργία.

Παράλληλα με το DNSBL ενεργοποιήθηκε φιλτράρισμα IP βάσει φήμης (IP reputation), με έμφαση στην εισερχόμενη κίνηση από το διαδίκτυο. Χρησιμοποιήθηκαν αποκλειστικά feeds υψηλής αξιοπιστίας, που σχετίζονται με botnets, exploit hosts και γνωστές κακόβουλες πηγές. Υπηρεσίες ανωνυμοποίησης (π.χ. TOR exit nodes) αξιολογήθηκαν ξεχωριστά και εφαρμόστηκαν μόνο WAN, κατόπιν εκτίμησης κινδύνου, ώστε να επιτευχθεί ισορροπία μεταξύ μείωσης έκθεσης και λειτουργικότητας (ENISA, 2023).

Η αποτελεσματικότητα των πολιτικών pfBlockerNG αξιολογήθηκε μέσω: (α) καταγραφής μπλοκαρισμένων DNS queries, (β) αυτόματα παραγόμενων firewall rules και (γ) συμβάντων που τεκμηριώνουν αποτροπή επικοινωνίας με κακόβουλους προορισμούς. Η χρήση logs ως τεκμήρια ενισχύει την ιχνηλασιμότητα (traceability) και υποστηρίζει πρακτικές ελέγχου συμμόρφωσης (ISO, 2022).

Οι Εικόνες 6-24 έως 6-28 αποτυπώνουν τις βασικές ρυθμίσεις DNSBL, την ενεργοποίηση επιλεγμένων IP reputation feeds, την risk-based εφαρμογή TOR πολιτικών στο WAN και τους αυτόματα παραγόμενους κανόνες pfBlockerNG. Τα στιγμιότυπα αυτά τεκμηριώνουν τη μετάβαση από πολιτική επιλογή feeds σε πραγματική επιβολή κανόνων στο firewall.

Εικόνα 6-24: Παραμετροποίηση και ενεργοποίηση του μηχανισμού DNSBL (DNS Block List) στο pfBlockerNG για φιλτράρισμα κακόβουλων και ανεπιθύμητων domains.



Εικόνα 6-25: Ενεργοποίηση επιλεγμένων IP reputation feeds υψηλής αξιοπιστίας (PR1) για τον προληπτικό αποκλεισμό γνωστής κακόβουλης δικτυακής υποδομής.

IPv4	TOR	Binary Defense	BDS_TOR	✓
IPv4	TOR	Dan.me	DMe_TOR_EN	✓
IPv4	TOR	Rueckgr Tor	RUECKGR_TOR_All	+
IPv4	TOR	Emerging Threats	ET_TOR_All	✓
IPv4	TOR	Tor Project Bulk Exit List	PROJECT_TOR_EN	✓
IPv4	TOR	Internet Storm Center	ISC_TOR	+

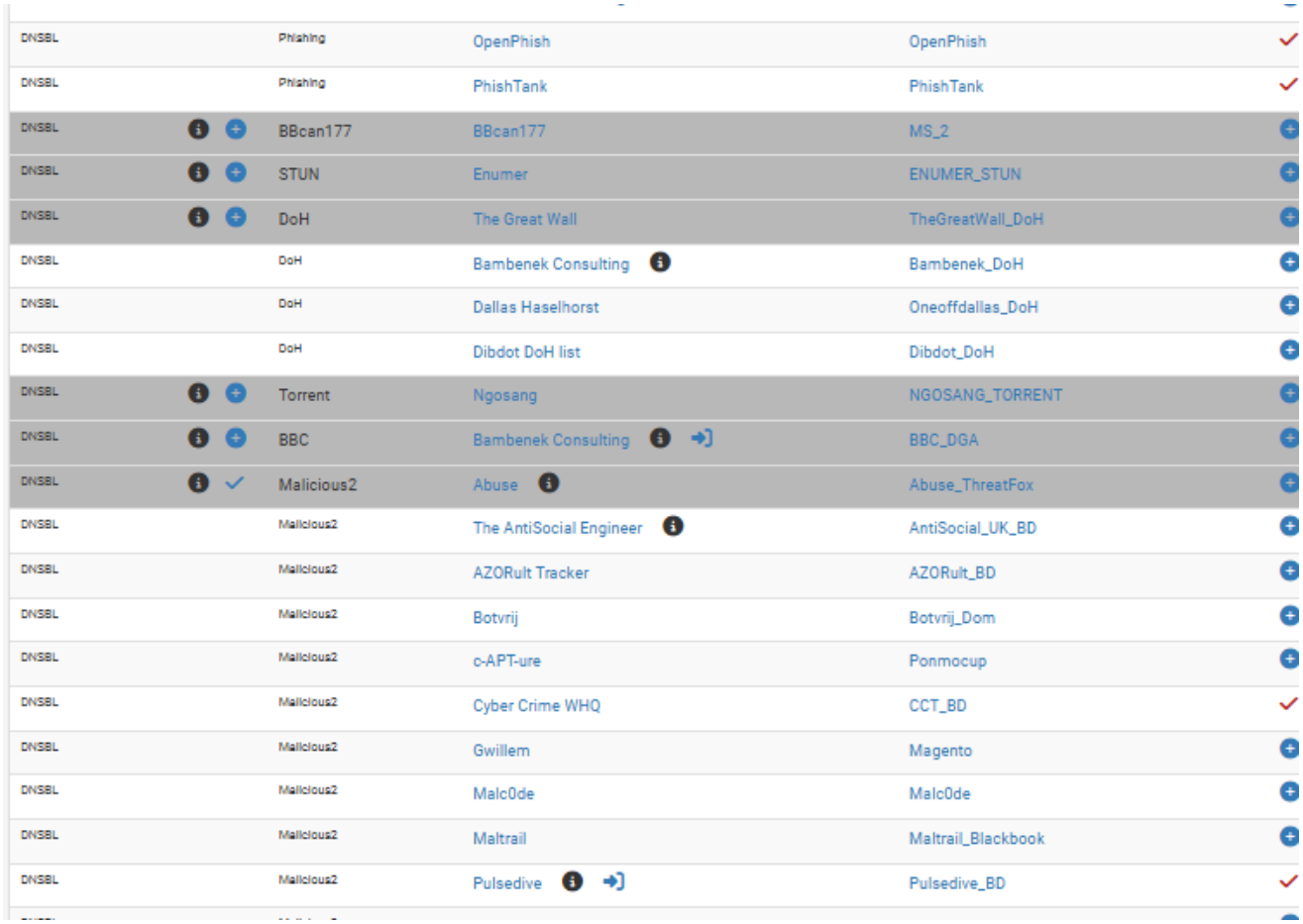
Εικόνα 6-26: Risk-based εφαρμογή IP reputation feeds για TOR exit nodes στο WAN interface.

Η Εικόνα 6-26 παρουσιάζει την επιλογή IP reputation feeds που σχετίζονται με TOR exit nodes. Οι συγκεκριμένες λίστες αξιολογήθηκαν και εφαρμόστηκαν αποκλειστικά στο όριο του δικτύου (WAN), ακολουθώντας προσέγγιση βάσει εκτίμησης κινδύνου. Η ρύθμιση αυτή δεν στοχεύει στον καθολικό αποκλεισμό της ανωνυμοποιημένης κίνησης, αλλά στη μείωση της έκθεσης σε επιθετικές ή ύποπτες εισερχόμενες συνδέσεις, διατηρώντας ταυτόχρονα τη λειτουργικότητα και την επιχειρησιακή συνέχεια

DNSBL	Malicious	Dan Pollock	SWC	✓
DNSBL	Malicious	Disconnect.Me	D_Me_Malv	✓
DNSBL	Malicious	Disconnect.Me	D_Me_Malw	✓
DNSBL	Malicious	Maltrail	Maltrail_BD	✓
DNSBL	Malicious	MVPS Hosts	MVPS	✓
DNSBL	Malicious	Spam404	Spam404	✓
DNSBL	Malicious	Stop Forum Spam	SFS_Toxic_BD	✓
DNSBL	Phishing	Abuse URLhaus	Abuse_urlhaus	+

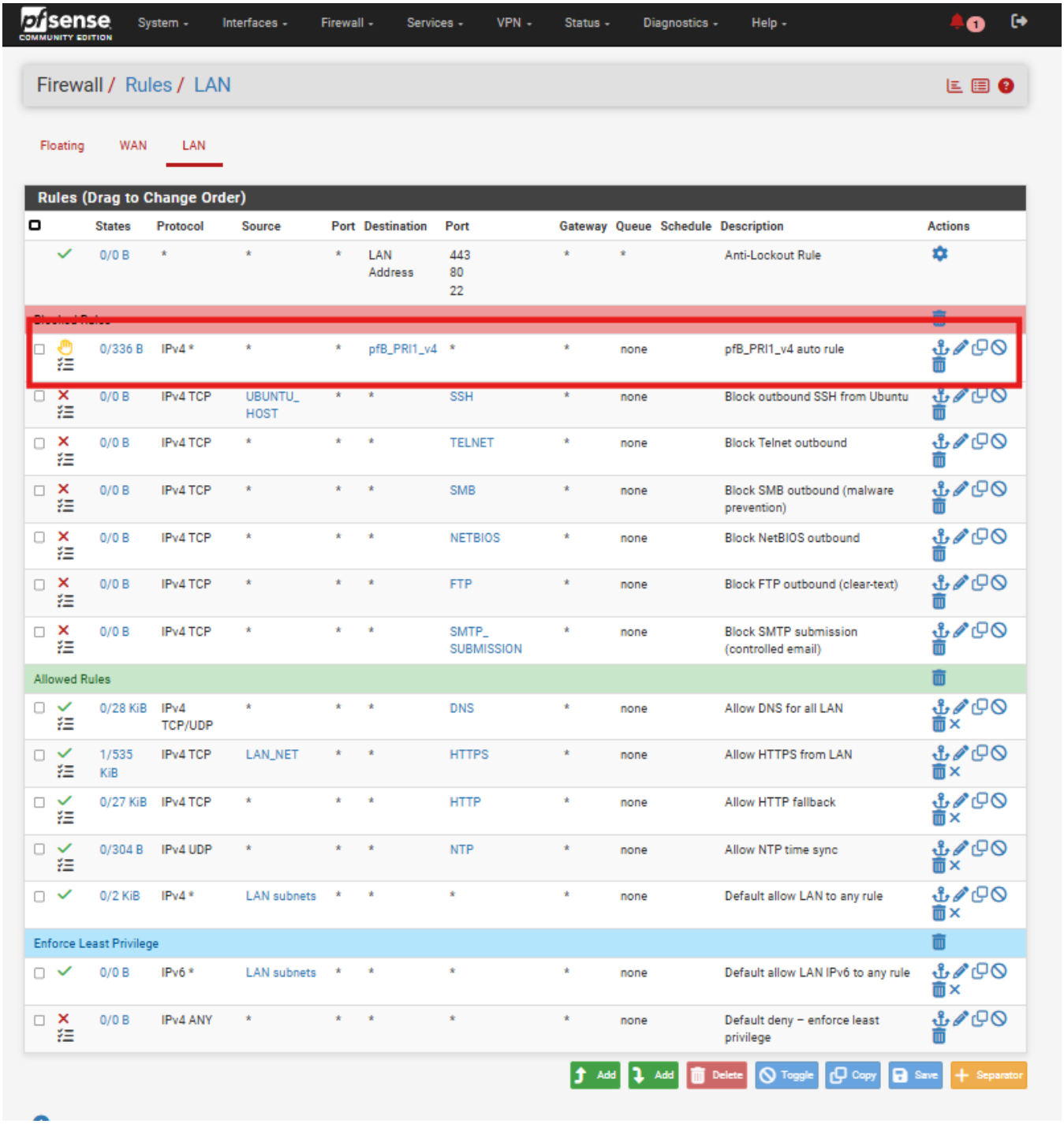
Εικόνα 6-27: Ενεργοποίηση επιλεγμένων DNSBL feeds για κακόβουλα και phishing domains στο πλαίσιο πολιτικής Threat Intelligence.

Η Εικόνα 6-27 παρουσιάζει την ενεργοποίηση DNSBL feeds που αφορούν κακόβουλα και phishing domains, προερχόμενα από αξιόπιστες πηγές Threat Intelligence. Τα επιλεγμένα feeds επικεντρώνονται σε υποδομές διανομής κακόβουλου λογισμικού, phishing καμπάνιες και command-and-control επικοινωνία. Η χρήση περιορισμένου αριθμού στοχευμένων feeds αποσκοπεί στη μείωση της επιφάνειας επίθεσης, διατηρώντας ταυτόχρονα χαμηλό ποσοστό false positives σε περιβάλλον μικρομεσαίας επιχείρησης.



Εικόνα 6-28: Ενεργοποίηση DNSBL feeds υψηλής αξιοπιστίας για κακόβουλες υποδομές και σκόπιμος αποκλεισμός μη συναφών ή επιθετικών κατηγοριών.

Η Εικόνα 6-28 παρουσιάζει την επιλεκτική ενεργοποίηση DNSBL feeds που σχετίζονται με κακόβουλη δραστηριότητα υψηλής αξιοπιστίας (Malicious2), όπως compromised domains, command-and-control υποδομές και γνωστά botnets. Παράλληλα, κατηγορίες που δεν σχετίζονται άμεσα με την ασφάλεια του δικτύου (π.χ. DoH, STUN, Torrent, DGA γενικού σκοπού ή content-based λίστες) παραμένουν απενεργοποιημένες, στο πλαίσιο μιας συντηρητικής και προσανατολισμένης στον κίνδυνο πολιτικής Threat Intelligence για περιβάλλοντα SMEs.

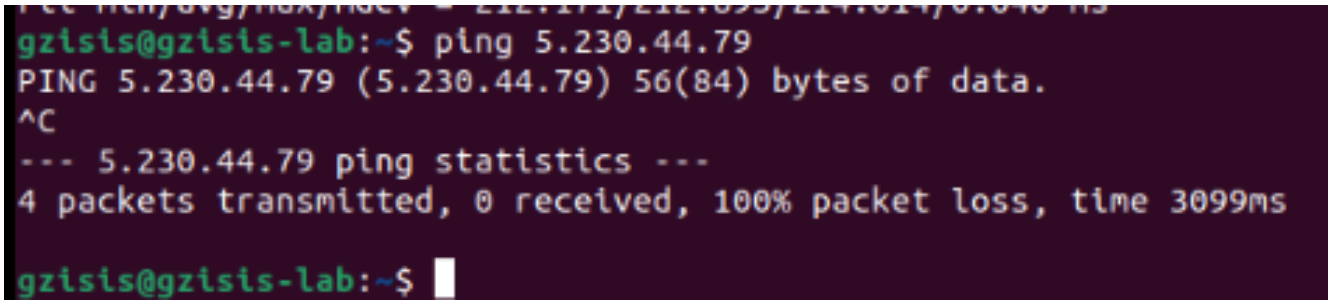


Εικόνα 6-29: Αυτόματα παραγόμενοι κανόνες pfBlockerNG στο firewall

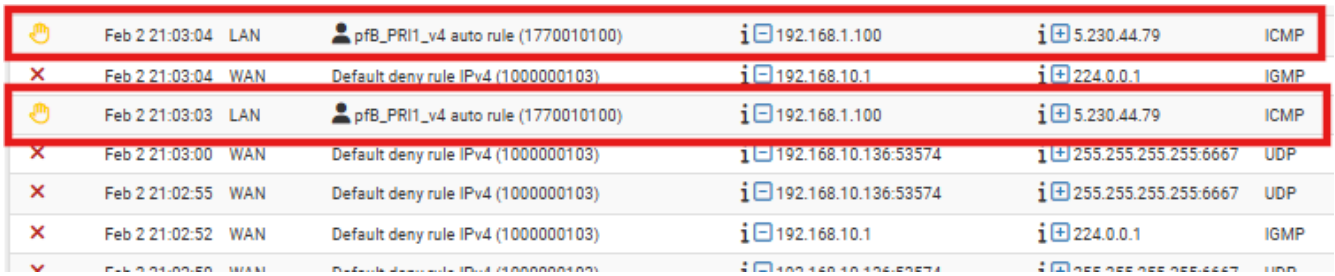
Στην Εικόνα 6-29 παρουσιάζονται ενδεικτικά οι αυτόματα δημιουργημένοι κανόνες που εφαρμόστηκαν στο firewall μέσω του pfBlockerNG.

Η επιλογή των DNSBL feeds πραγματοποιήθηκε με βάση τη συνάφεια τους με πραγματικές απειλές ασφάλειας και όχι με κριτήρια γενικού φιλτραρίσματος περιεχομένου. Κατηγορίες που

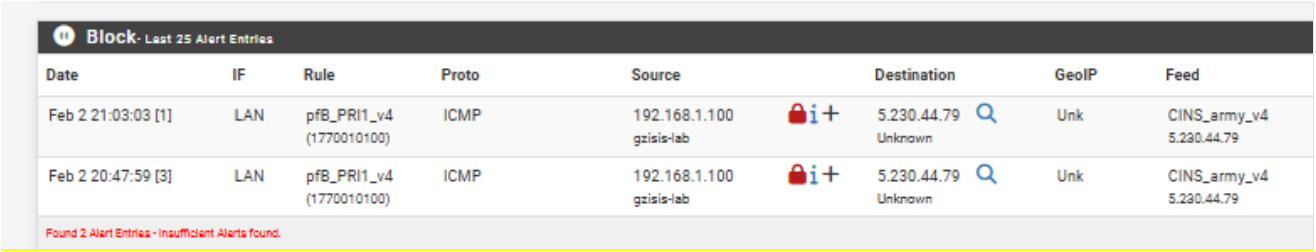
σχετίζονται με τεχνικές παράκαμψης (π.χ. DNS-over-HTTPS), peer-to-peer δραστηριότητα ή traffic classification αποκλείστηκαν, καθώς δεν συνεισφέρουν άμεσα στη μείωση του κινδύνου κακόβουλης δραστηριότητας στο εξεταζόμενο περιβάλλον.



Εικόνα 6-30: Προσπάθεια επικοινωνίας με έναν απο τους κακόβουλους προορισμούς.



Εικόνα 6-31: Καταγραφές DNSBL / IP reputation σε firewall logs



Εικόνα 6-32: Καταγεγραμμένα alerts του pfBlockerNG που αποτυπώνουν τον αποκλεισμό κακόβουλης επικοινωνίας βάσει IP reputation feeds.

Παράλληλα, εμφανίζονται απορρίψεις πακέτων από τον προεπιλεγμένο κανόνα απόρριψης (default deny rule), γεγονός που επιβεβαιώνει τη συνεργασία των μηχανισμών threat intelligence με το βασικό rulebase του firewall.

Οι καταγραφές αποδεικνύουν ότι οι πολιτικές Threat Intelligence εφαρμόζονται προληπτικά, δημιουργώντας αυτόματα κανόνες φιλτραρίσματος πριν η κίνηση φτάσει στους γενικούς κανόνες απόρριψης του firewall. Με τον τρόπο αυτό, κακόβουλη δικτυακή δραστηριότητα

αποκόπτεται έγκαιρα, μειώνοντας την επιφάνεια επίθεσης και το φορτίο ανάλυσης σε ανώτερα επίπεδα ασφάλειας.

Η υλοποίηση του pfBlockerNG απέδειξε ότι το προτεινόμενο περιβάλλον υποστηρίζει μηχανισμό προληπτικής μείωσης της επιφάνειας επίθεσης μέσω αξιοποίησης Threat Intelligence feeds. Η επιλεκτική ενεργοποίηση DNSBL και IP reputation πολιτικών υψηλής αξιοπιστίας επέτρεψε τον αποκλεισμό κακόβουλων προορισμών πριν την έναρξη σύνδεσης ή την ανάγκη περαιτέρω ανάλυσης από μηχανισμούς IDS.

Η προσέγγιση αυτή θεωρείται ιδιαίτερα κατάλληλη για περιβάλλον SME, όπου απαιτείται ισορροπία μεταξύ επιπέδου προστασίας και επιχειρησιακής σταθερότητας.

6.4.2 Suricata

Το Suricata αξιοποιήθηκε ως σύστημα ανίχνευσης και απόκρισης σε δικτυακές απειλές (IDS/IPS), με σκοπό την παροχή ορατότητας και την ανίχνευση επιθετικής δραστηριότητας που δεν αποκόπτεται προληπτικά από τους μηχανισμούς Threat Intelligence. Σε αντίθεση με το pfBlockerNG, το οποίο βασίζεται σε δεδομένα φήμης, το Suricata λειτουργεί μέσω ανάλυσης της πραγματικής δικτυακής κίνησης και αντιστοίχισης με γνωστά signatures επιθέσεων.

Ο ρόλος του Suricata στο εξεταζόμενο περιβάλλον είναι συμπληρωματικός και εντάσσεται στο συνολικό μοντέλο άμυνας σε βάθος (defense-in-depth), ενισχύοντας την ικανότητα ανίχνευσης, καταγραφής και αξιολόγησης κακόβουλων ενεργειών εντός του δικτύου.

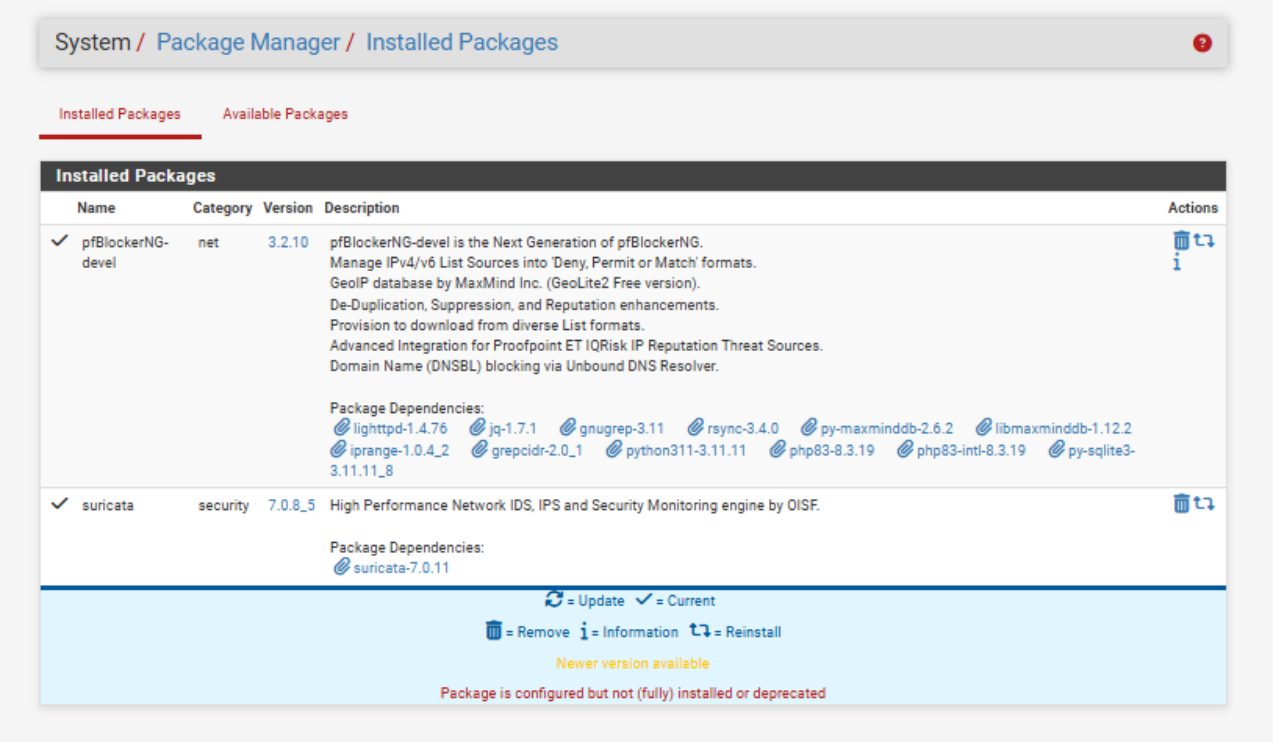
Πίνακας 6-2: Τεχνική Αξιολόγηση Λειτουργίας Suricata IDS/IPS

Παράμετρος	**Περιγραφή**	**Ρόλος στο Μοντέλο Ασφάλειας**
Τύπος Λειτουργίας	Σύστημα ανίχνευσης / πρόληψης εισβολών (IDS/IPS) σε λειτουργία inline	Ενεργή ή παθητική επιτήρηση
Τύπος Ανάλυσης	Ανίχνευση βάσει υπογραφών (signature-based detection)	Αντιστοίχιση γνωστών επιθετικών μοτίβων
Σημείο Εφαρμογής	Διεπαφές WAN ή LAN του firewall	Παρακολούθηση εξερχόμενης & εισερχόμενης κίνησης

Παράμετρος	Περιγραφή	Ρόλος στο Μοντέλο Ασφάλειας
Απόκριση	Ειδοποίηση ή απόρριψη πακέτων (alert / drop)	Άμεσος αποκλεισμός κακόβουλης ροής
Logging	Αναλυτικά αρχεία καταγραφής συμβάντων (detailed event logs)	Ιχνηλασιμότητα & forensic ανάλυση
Συνεισφορά	Ανίχνευση μετά την έναρξη επικοινωνίας (post-connection detection)	Εντοπισμός επιθέσεων που δεν μπλοκαρίστηκαν προληπτικά

Το Suricata εγκαταστάθηκε μέσω του Package Manager του pfSense, προκειμένου να λειτουργήσει ως σύστημα ανίχνευσης και πρόληψης εισβολών (IDS/IPS) στο εργαστηριακό περιβάλλον.

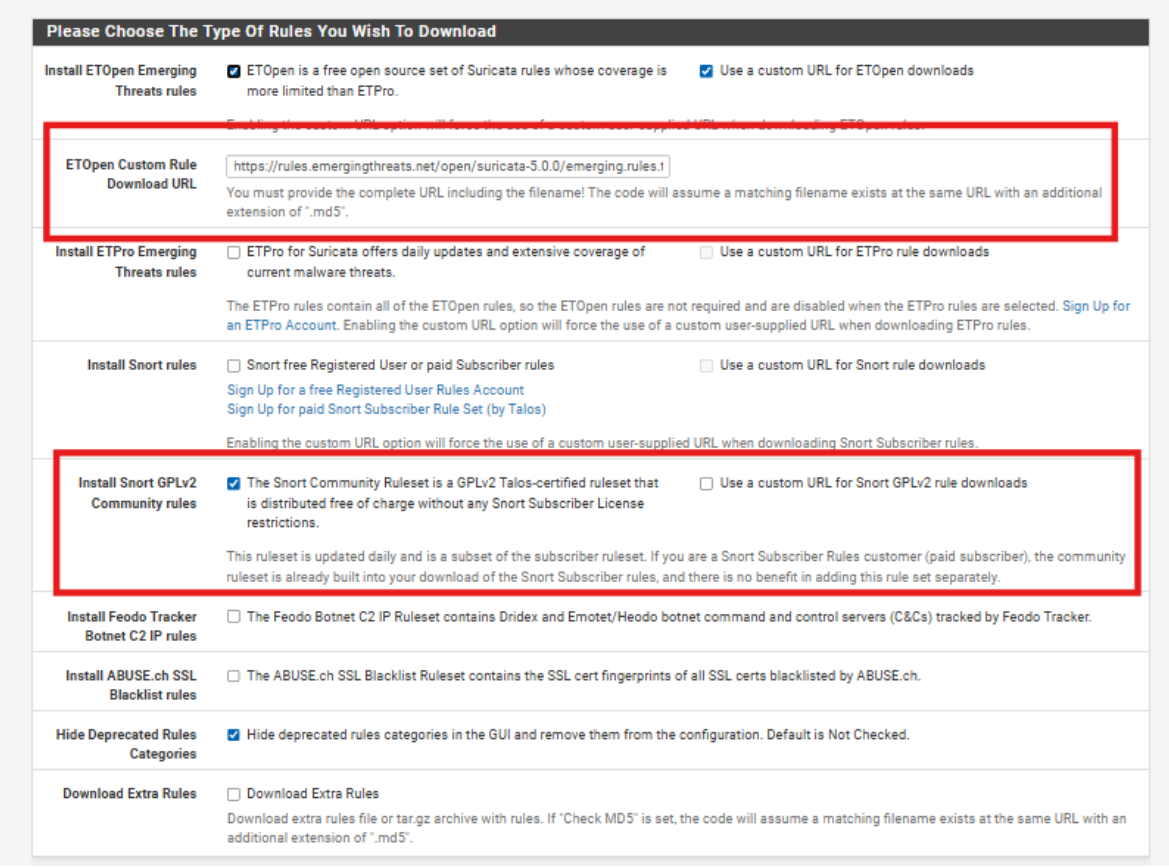
Η επιλογή του Suricata βασίστηκε στην υποστήριξη λειτουργίας inline IPS, στην ανάλυση πακέτων σε επίπεδο Deep Packet Inspection (DPI) και στη συμβατότητα με κανόνες Emerging Threats.



Εικόνα 6-33: Εγκατάσταση Suricata μέσω Package Manager στο pfSense.

Για την ενεργοποίηση μηχανισμών ανίχνευσης επιλέχθηκε η χρήση του ανοικτού συνόλου κανόνων (rule set) *Emerging Threats Open (ET Open)*. Η λήψη των κανόνων πραγματοποιήθηκε μέσω προσαρμοσμένου συνδέσμου (custom URL) από το αποθετήριο κανόνων της Emerging Threats, το οποίο παρέχει ενημερωμένες υπογραφές ανίχνευσης (signatures) για το σύστημα Suricata. Η προσέγγιση αυτή διασφαλίζει τη συμβατότητα με την εγκατεστημένη έκδοση του Suricata και επιτρέπει ελεγχόμενη διαδικασία ενημέρωσης των κανόνων.

Επιπλέον ενεργοποιήθηκε το σύνολο κανόνων κοινότητας Snort GPLv2 (Snort GPLv2 Community Ruleset), προκειμένου να ενισχυθεί η κάλυψη γνωστών επιθετικών προτύπων.



Εικόνα 6-34: Παραμετροποίηση custom URL για λήψη Emerging Threats Open rules & επιλογή πρόσθετων rulesets (Snort GPLv2 Community Rules).

Το Suricata ενεργοποιήθηκε στο LAN interface του firewall, ώστε να επιτηρεί την εσωτερική δικτυακή κίνηση και να εντοπίζει πιθανές lateral movement επιθέσεις εντός του ίδιου VLAN.

Το Suricata ενεργοποιήθηκε αποκλειστικά στο LAN interface του firewall, προκειμένου να επιτηρεί την εσωτερική δικτυακή κίνηση μεταξύ των συστημάτων του οργανισμού.

Η επιλογή αυτή βασίστηκε στη μείωση του θορύβου (noise) και των ψευδώς θετικών (false positives) που παρατηρούνται συνήθως στο WAN interface, λόγω της μεγάλης και μη ελεγχόμενης εισερχόμενης κίνησης από το Διαδίκτυο.
Σε περιβάλλον SME, η προτεραιότητα δόθηκε στην ανίχνευση lateral movement και εσωτερικών απειλών (insider threats), που αποτελούν ρεαλιστικότερο σενάριο κινδύνου.

Μετά τη λήψη των rulesets Emerging Threats Open και Snort GPLv2 Community Rules, πραγματοποιήθηκε επιλεκτική ενεργοποίηση κατηγοριών κανόνων (rule categories), με στόχο τη βελτιστοποίηση της ανίχνευσης και τη μείωση ψευδώς θετικών (false positives).

Η επιλογή των κατηγοριών βασίστηκε σε risk-based προσέγγιση, λαμβάνοντας υπόψη τις συνήθεις απειλές που αντιμετωπίζει μία μικρομεσαία επιχείρηση, όπως:

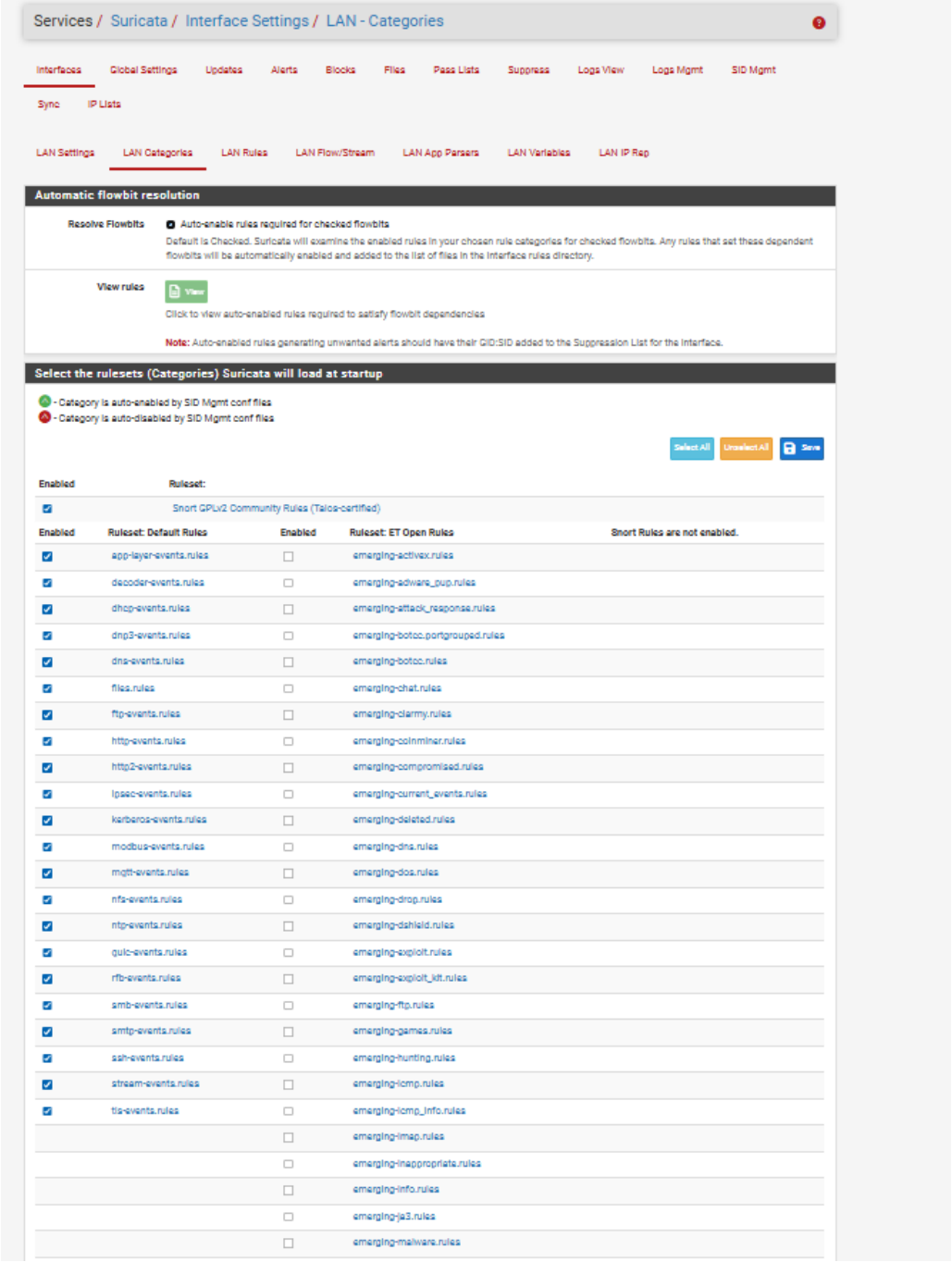
• Reconnaissance δραστηριότητες (port scanning)

• Web-based επιθέσεις

• Exploit attempts

• Malware communication

• Denial-of-Service patterns



Εικόνα 6-35: Επιλογή και ενεργοποίηση κατηγοριών κανόνων στο LAN interface του Suricata.

Όπως παρατηρείται στην Εικόνα 6-35, ενεργοποιήθηκαν κανόνες που αφορούν HTTP, DNS, exploit detection, malware, reconnaissance και botnet δραστηριότητες.

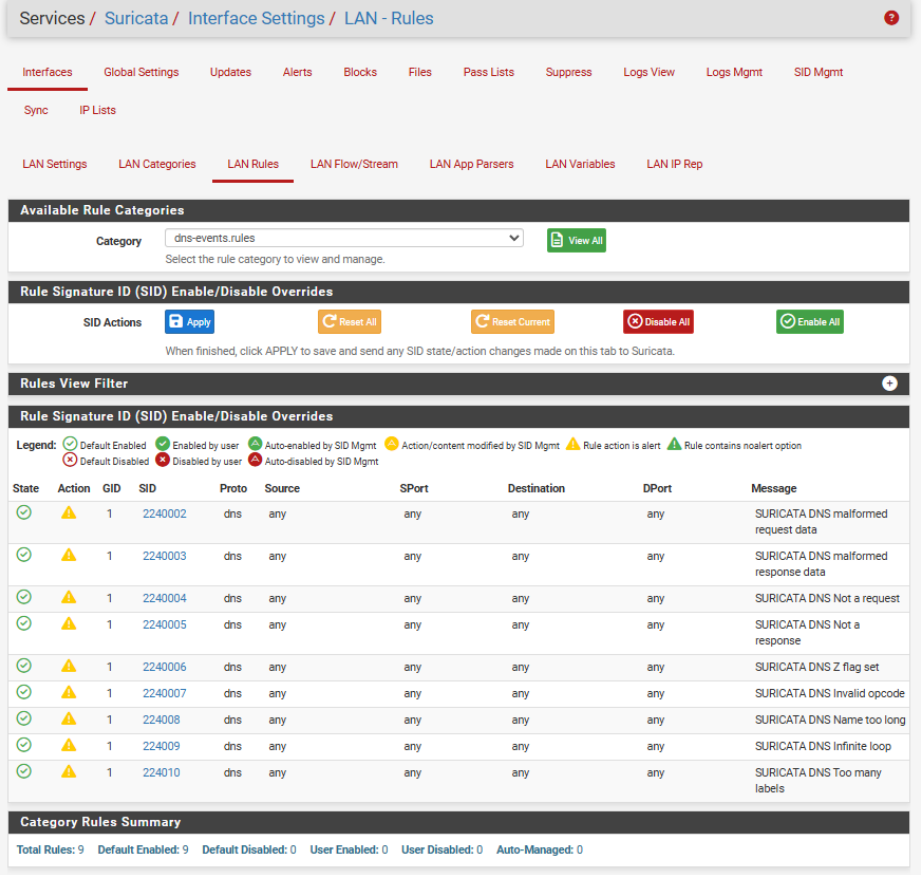
Η επιλεκτική ενεργοποίηση περιορίζει την υπερβολική καταγραφή συμβάντων, βελτιώνει την απόδοση του συστήματος και επιτρέπει στο IDS να εστιάζει σε απειλές υψηλής σημασίας.

Η συγκεκριμένη παραμετροποίηση κρίνεται κατάλληλη για περιβάλλον SME, όπου απαιτείται ισορροπία μεταξύ επιπέδου προστασίας και διαχειριστικού φόρτου.

Πέραν της ενεργοποίησης κατηγοριών κανόνων (rule categories), παρέχεται η δυνατότητα λεπτομερούς διαχείρισης σε επίπεδο Signature ID (SID).

Η λειτουργία αυτή επιτρέπει την ενεργοποίηση, απενεργοποίηση ή τροποποίηση συγκεκριμένων signatures, προσφέροντας αυξημένο έλεγχο στη συμπεριφορά του IDS/IPS.

Στο παρόν εργαστηριακό περιβάλλον, πραγματοποιήθηκε έλεγχος των DNS-related signatures, προκειμένου να επιβεβαιωθεί η ορθή φόρτωση και ενεργοποίηση των κανόνων που σχετίζονται με ανωμαλίες DNS πρωτοκόλλου.



Εικόνα 6-36: Διαχείριση κανόνων Suricata σε επίπεδο Signature ID (SID) – Παράδειγμα DNS category.

Όπως παρατηρείται, κάθε κανόνας διαθέτει SID, τύπο πρωτοκόλλου, προορισμό, θύρα και περιγραφή ανίχνευσης.

Η ύπαρξη SID-level ελέγχου επιτρέπει:

• Μείωση ψευδώς θετικών (false positives)

• Προσαρμογή κανόνων σε συγκεκριμένο περιβάλλον

• Στοχευμένη απενεργοποίηση noisy signatures

• Βελτιστοποίηση απόδοσης συστήματος

Σε ένα περιβάλλον SME, η δυνατότητα αυτή θεωρείται κρίσιμη για την αποφυγή alert fatigue και την αποτελεσματική διαχείριση συμβάντων ασφαλείας.

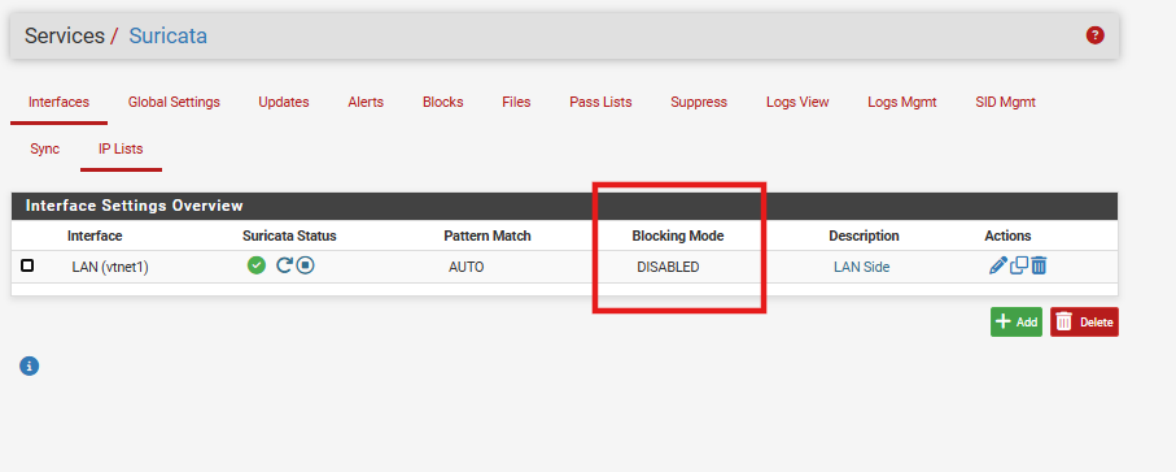
6.4.2.1 Τρόπος Λειτουργίας (IDS έναντι IPS)

Το Suricata στο παρόν εργαστηριακό περιβάλλον λειτούργησε σε IDS mode (alert-only), χωρίς ενεργοποίηση ενεργού αποκλεισμού (drop actions), όπως φαίνεται στην Εικόνα 6-37. Η επιλογή αυτή πραγματοποιήθηκε προκειμένου να αξιολογηθεί αρχικά η συμπεριφορά των κανόνων και το επίπεδο ανίχνευσης, χωρίς να επηρεαστεί η κανονική λειτουργία του δικτύου.

Η λειτουργία σε IDS mode επιτρέπει:

- Παρακολούθηση της δικτυακής κίνησης σε πραγματικό χρόνο
- Καταγραφή και ειδοποίηση ύποπτων μοτίβων
- Αξιολόγηση της ποιότητας των rulesets
- Σταδιακό tuning πριν από ενδεχόμενη μετάβαση σε IPS mode

Η συγκεκριμένη προσέγγιση θεωρείται βέλτιστη πρακτική σε περιβάλλον SME, όπου η ανεξέλεγκτη ενεργοποίηση μηχανισμών drop μπορεί να προκαλέσει διακοπές υπηρεσιών λόγω ψευδώς θετικών (false positives).



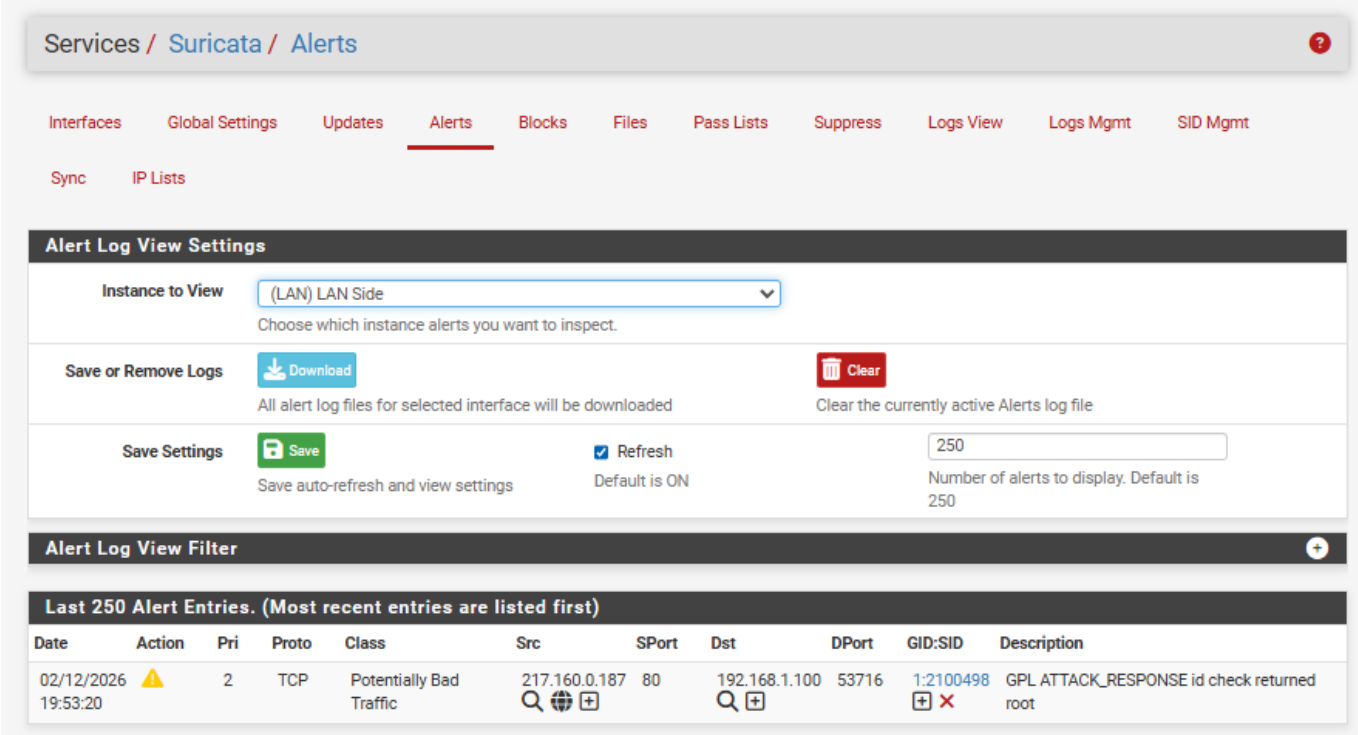
Εικόνα 6-37: Παραμετροποίηση και ενεργοποίηση επιλεγμένων Suricata rulesets στο pfSense, στο πλαίσιο της πολιτικής IDS/IPS για ενίσχυση της ανίχνευσης κακόβουλης δραστηριότητας στο περιμετρικό επίπεδο.

6.4.2.2 Επαλήθευση Ανίχνευσης σε Επίπεδο Εφαρμογής (Application Layer Detection Validation)

Για την επαλήθευση της λειτουργίας application-layer inspection, πραγματοποιήθηκε πρόσβαση στο ελεγχόμενο test domain testmyids.com από το Ubuntu VM (*Εικόνα 6-38).*

Το συγκεκριμένο domain περιέχει προκαθορισμένα test signatures που ενεργοποιούν κανόνες IDS, επιτρέποντας την επιβεβαίωση της ορθής λειτουργίας του συστήματος ανίχνευσης.

Εικόνα 6-38: Εκτέλεση HTTP αιτήματος προς το testmyids.com από το Ubuntu VM.



Εικόνα 6-39: Ανίχνευση HTTP-based test signature από το Suricata (GPL ATTACK_RESPONSE rule).

Όπως παρατηρείται στην εικόνα 6-39, το Suricata ενεργοποίησε τον κανόνα "GPL ATTACK_RESPONSE id check returned root", ταξινομημένο ως Potentially Bad Traffic.

Εικόνα 6-40: Εκτέλεση της εντολής curl http://testmyids.com από σταθμό Ubuntu για την ενεργοποίηση δοκιμαστικής IDS υπογραφής. Η απόκριση του server επιστρέφει το μοτίβο uid=0(root), το οποίο χρησιμοποιείται για την επαλήθευση της λειτουργίας των κανόνων ανίχνευσης

Η Εικόνα 6-40 παρουσιάζει το πλήρες κείμενο του κανόνα (rule) του Suricata, όπως εμφανίζεται στο περιβάλλον διαχείρισης του pfSense. Ο συγκεκριμένος κανόνας προέρχεται από το rule set emerging-attack_response.rules και ενεργοποιείται όταν ανιχνευθεί στο δικτυακό φορτίο (payload) το μοτίβο "uid=0(root)", το οποίο αποτελεί χαρακτηριστική ένδειξη απόκρισης συστήματος τύπου Unix/Linux που επιστρέφει πληροφορίες για τον χρήστη root. Η ανίχνευση τέτοιου μοτίβου μπορεί να υποδηλώνει πιθανή επιτυχή εκτέλεση εντολών ή απόκριση από ευάλωτο σύστημα μετά από προσπάθεια εκμετάλλευσης.

Το αποτέλεσμα επιβεβαιώνει την επιτυχή λειτουργία signature-based detection σε επίπεδο εφαρμογής (Layer 7), καθώς και τη σωστή επιτήρηση της εσωτερικής δικτυακής κίνησης στο LAN interface.

Η εγκατάσταση του Suricata στο pfSense επιλέχθηκε για να καλύψει την ανάγκη ανίχνευσης και καταγραφής δικτυακών απειλών σε πραγματικό χρόνο, πέρα από τον έλεγχο πρόσβασης που υλοποιείται μέσω απλών firewall κανόνων. Σε αντίθεση με μηχανισμούς threat intelligence που βασίζονται σε reputation lists, το Suricata επιθεωρεί την πραγματική κίνηση (Deep Packet Inspection) και εντοπίζει ύποπτα μοτίβα (π.χ. reconnaissance/port scanning, κακόβουλα web

requests, indicators of compromise). Η λειτουργία της εντάσσεται σε μοντέλο defense-in-depth και ενισχύει ουσιαστικά την ικανότητα έγκαιρης ανίχνευσης, τη δυνατότητα διερεύνησης περιστατικών (incident response) και την τήρηση ιχνηλασιμότητας μέσω καταγραφών (logging), στοιχεία κρίσιμα για ένα περιβάλλον μικρομεσαίας επιχείρησης.

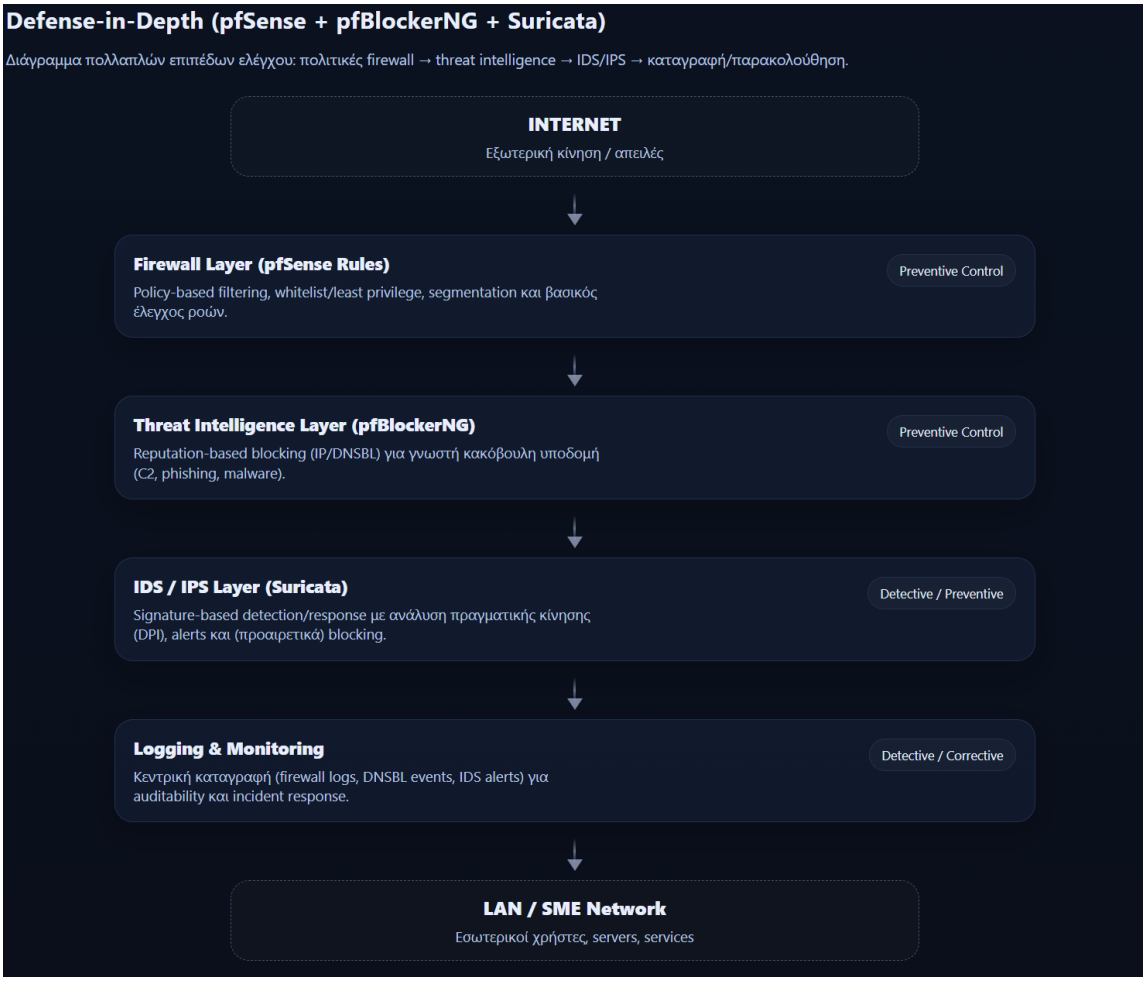
Η επιτήρηση ενεργοποιήθηκε στο LAN interface ώστε να δοθεί έμφαση σε εσωτερικές απειλές και lateral movement, ενώ παράλληλα μειώθηκε ο θόρυβος και τα false positives που εμφανίζονται συνήθως σε WAN επιτήρηση.

Συνολικά, η ενσωμάτωση του Suricata στο pfSense απέδειξε ότι το προτεινόμενο εργαστηριακό περιβάλλον υποστηρίζει μηχανισμό ανίχνευσης επιθέσεων σε πραγματικό χρόνο. Η λειτουργία σε IDS mode επέτρεψε την αξιολόγηση των ενεργοποιημένων κανόνων χωρίς διατάραξη της δικτυακής λειτουργίας, ενώ η επιτυχής ενεργοποίηση test signatures επιβεβαίωσε τη σωστή επιθεώρηση σε επίπεδο εφαρμογής.

Το Suricata ενισχύει ουσιαστικά το μοντέλο άμυνας σε βάθος (defense-in-depth) της προτεινόμενης αρχιτεκτονικής SME, παρέχοντας μηχανισμό έγκαιρης ανίχνευσης, καταγραφής και τεκμηρίωσης δικτυακών απειλών.

6.4.3 Συνδυαστική αξιολόγηση και άμυνα σε βάθος

Η μεμονωμένη αξιολόγηση των μηχανισμών pfBlockerNG και Suricata δεν αποτυπώνει πλήρως το συνολικό επίπεδο προστασίας. Η πραγματική ενίσχυση της ασφάλειας προκύπτει από τον συνδυασμό των πολιτικών firewall, του threat intelligence φιλτραρίσματος και της ανίχνευσης επιθέσεων μέσω IDS/IPS. Ο συνδυασμός αυτός διαμορφώνει μία πολυεπίπεδη αρχιτεκτονική άμυνας σε βάθος (defense-in-depth), όπου κάθε επίπεδο καλύπτει διαφορετικό φάσμα απειλών και μειώνει την πιθανότητα επιτυχούς εκμετάλλευσης.



Εικόνα 6-41: Αρχιτεκτονική άμυνας σε βάθος (defense-in-depth) με διαδοχική εφαρμογή πολιτικών firewall, φιλτραρίσματος threat intelligence και IDS/IPS, με τελικό στόχο την προληπτική αποτροπή, την ανίχνευση και την τεκμηριωμένη καταγραφή συμβάντων στο δίκτυο μίας μικρομεσαίας επιχείρησης.

Συνεπώς, το firewall αποτελεί το πρώτο επίπεδο προληπτικού ελέγχου πολιτικών, το pfBlockerNG μειώνει την επιφάνεια επίθεσης μέσω αποκλεισμού γνωστής κακόβουλης υποδομής, ενώ το Suricata προσφέρει δυνατότητα ανίχνευσης (και προαιρετικά αποτροπής) επιθετικής δραστηριότητας σε επίπεδο δικτυακής κίνησης.

Η συνδυαστική αυτή προσέγγιση βελτιώνει την ανθεκτικότητα σε περιβάλλοντα SME και ενισχύει την ικανότητα τεκμηριωμένης παρακολούθησης συμβάντων μέσω καταγραφών. Η συνέργεια των τριών μηχανισμών παρέχει προληπτικό φιλτράρισμα, ανίχνευση επιθέσεων και τεκμηριωμένη καταγραφή, ενισχύοντας τη συνολική στάση ασφάλειας.

6.5 Συγκριτική προσέγγιση με χειροκίνητη διαχείριση

Η πειραματική αξιολόγηση ανέδειξε ξεκάθαρα τις διαφορές μεταξύ της παραδοσιακής χειροκίνητης παραμετροποίησης μέσω GUI και της προτεινόμενης αυτοματοποιημένης λύσης. Ενώ η χειροκίνητη μέθοδος απαιτεί συνεχή αλληλεπίδραση με το σύστημα, αυξάνοντας γεωμετρικά τον κίνδυνο λαθών (misconfigurations) και καθιστώντας την αναδρομή (audit) εξαιρετικά δυσχερή, η προσέγγιση μέσω Excel εξάλειψε πλήρως τα συντακτικά σφάλματα πριν καν αυτά φτάσουν στο firewall.

Η σύγκριση ανέδειξε επίσης διαφορές ως προς την επαναληψιμότητα και τη συνέπεια. Στη χειροκίνητη διαχείριση, η επανεφαρμογή του ίδιου συνόλου κανόνων σε διαφορετικό περιβάλλον ή χρονική στιγμή απαιτεί εκ νέου χειροκίνητη εργασία, με κίνδυνο αποκλίσεων. Αντιθέτως, η αυτοματοποιημένη προσέγγιση επιτρέπει την επανεισαγωγή του ίδιου αρχείου πολιτικής χωρίς διαφοροποιήσεις, εξασφαλίζοντας ομοιομορφία στη διαχείριση και διευκολύνοντας διαδικασίες ανάκτησης ή μεταφοράς ρυθμίσεων.

Τέλος, από οργανωτικής άποψης, η προτεινόμενη λύση ευθυγραμμίζεται περισσότερο με βασικές αρχές change management και ελέγχου πρόσβασης, καθώς διαχωρίζει τον ορισμό της πολιτικής από την εφαρμογή της. Ο IT administrator μπορεί να σχεδιάζει, να ελέγχει και να εγκρίνει αλλαγές σε επίπεδο αρχείου πολιτικής πριν αυτές εφαρμοστούν στο firewall, γεγονός που είναι ιδιαίτερα σημαντικό για SMEs με περιορισμένους πόρους και αυξημένες απαιτήσεις αξιοπιστίας.

Συνολικά, η συγκριτική αξιολόγηση καταδεικνύει ότι η αυτοματοποιημένη προσέγγιση προσφέρει σαφή πλεονεκτήματα έναντι της χειροκίνητης διαχείρισης, χωρίς να αναιρεί τη δυνατότητα ελέγχου και προσαρμογής που παρέχει το pfSense. Η λύση που προτείνεται στην παρούσα εργασία δεν αντικαθιστά το firewall, αλλά επαναπροσδιορίζει τον τρόπο με τον οποίο οι πολιτικές ασφάλειας σχεδιάζονται, εφαρμόζονται και αξιολογούνται σε περιβάλλοντα SMEs.

6.6 Ποσοτική Αξιολόγηση και Μετρικές Απόδοσης

Πέραν της λειτουργικής επιβεβαίωσης των κανόνων, η αξιολόγηση του συστήματος περιέλαβε και την ποσοτική αποτίμηση της προτεινόμενης λύσης, με κύριο άξονα τη μείωση του διαχειριστικού χρόνου και την κατανάλωση υπολογιστικών πόρων. Στο εργαστηριακό περιβάλλον, η χειροκίνητη εισαγωγή ενός συνόλου 50 σύνθετων κανόνων μέσω του γραφικού

περιβάλλοντος του pfSense εκτιμήθηκε ότι απαιτεί περίπου 45–60 λεπτά, ενώ η αντίστοιχη διαδικασία με χρήση του προτύπου Excel και του αυτοματοποιημένου σεναρίου ολοκληρώθηκε σε περίπου 5 λεπτά. Η παρατήρηση αυτή υποδηλώνει σημαντική μείωση του διαχειριστικού χρόνου, χωρίς ωστόσο να αποτελεί γενικεύσιμη μέτρηση για κάθε περιβάλλον. Με τη χρήση του προτεινόμενου προτύπου Excel και του αυτοματοποιημένου σεναρίου μετατροπής, ο συνολικός χρόνος από την εισαγωγή των δεδομένων έως την πλήρη εφαρμογή τους στο σύστημα μειώθηκε σε περίπου 5 λεπτά. Η προσέγγιση αυτή επιτυγχάνει μια εκτιμώμενη μείωση της τάξης του 90% στον χρόνο διαχείρισης, αυξάνοντας ταυτόχρονα την ακρίβεια των ρυθμίσεων μέσω των μηχανισμών επικύρωσης δεδομένων.

Αναφορικά με την επιβάρυνση του συστήματος, η ενσωμάτωση του μηχανισμού Suricata προσθέτει ένα απαραίτητο επίπεδο εις βάθος επιθεώρησης πακέτων, το οποίο ωστόσο συνοδεύεται από μετρήσιμο λειτουργικό κόστος. Κατά τη διάρκεια της κανονικής λειτουργίας του δικτύου, η χρήση CPU κυμαινόταν σε επίπεδα κάτω του 5%. Ωστόσο, κατά τη διάρκεια των εντατικών δοκιμών δικτυακής σάρωσης (nmap scanning) και της ενεργοποίησης των κανόνων ανίχνευσης, παρατηρήθηκε αύξηση της χρήσης του επεξεργαστή η οποία έφτασε το 15% με 20%, καθώς και αυξημένη δέσμευση μνήμης RAM για τη διατήρηση των πινάκων κατάστασης. Αν και η συγκεκριμένη επιβάρυνση κρίνεται απολύτως αποδεκτή για τις σύγχρονες υποδομές μιας SME, αποτελεί έναν κρίσιμο παράγοντα που πρέπει να συνυπολογίζεται κατά τον αρχικό σχεδιασμό του υλικού, ειδικά στην περίπτωση μελλοντικής λειτουργίας του συστήματος σε IPS mode.

7 ΚΕΦΑΛΑΙΟ 7 – ΣΥΖΗΤΗΣΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

7.1 Ερμηνεία Αποτελεσμάτων και Επιχειρησιακή Αξία

Το παρόν κεφάλαιο επικεντρώνεται στην ερμηνεία των πειραματικών αποτελεσμάτων που προέκυψαν από την υλοποίηση της προτεινόμενης αρχιτεκτονικής δικτυακής ασφάλειας, συνδέοντας τα τεχνικά ευρήματα με τους αρχικούς ερευνητικούς στόχους της εργασίας. Η ανάλυση των δεδομένων επιβεβαιώνει ότι η μετάβαση από τη χειροκίνητη διαχείριση σε ένα δομημένο μοντέλο αυτοματοποίησης, προσαρμοσμένο στις ανάγκες των SMEs, προσφέρει μετρήσιμα πλεονεκτήματα τόσο σε επιχειρησιακό όσο και σε τεχνικό επίπεδο.

Ένα από τα βασικά ευρήματα της πειραματικής αξιολόγησης είναι η σημαντική μείωση του διαχειριστικού φόρτου που απαιτείται για τη δημιουργία και εφαρμογή των κανόνων firewall. Η χρήση του προτύπου Excel ως ενιαίας πηγής ορισμού πολιτικών (single source of truth) οδήγησε σε εκτιμώμενη μείωση του χρόνου παραμετροποίησης κατά περίπου 90% (από 45-60 λεπτά σε μόλις 5 λεπτά για 50 σύνθετους κανόνες). Το εύρημα αυτό σχετίζεται άμεσα με τον περιορισμό των διαθέσιμων πόρων πληροφορικής που χαρακτηρίζει τις SMEs. Παράλληλα, ο μηχανισμός επικύρωσης δεδομένων (data validation) του υπολογιστικού φύλλου λειτούργησε ως επιτυχημένο προληπτικό μέτρο, μειώνοντας σημαντικά την πιθανότητα τυπογραφικών και λογικών σφαλμάτων που συχνά οδηγούν σε τρωτότητες (misconfigurations).

Από την πλευρά της αρχιτεκτονικής άμυνας σε βάθος (defense-in-depth), η συνδυαστική χρήση του pfBlockerNG και του Suricata IDS αποδείχθηκε λειτουργικά επαρκής. Ωστόσο, η συζήτηση των αποτελεσμάτων αναδεικνύει μια σημαντική επιχειρησιακή πρόκληση σχετικά με την αντιμετώπιση των ψευδώς θετικών συναγερμών (false positives). Σε περιπτώσεις όπου το σύστημα Threat Intelligence αποκλείσει λανθασμένα ένα νόμιμο domain, η επαναφορά της πρόσβασης (allow-listing) απαιτεί την τροποποίηση του κεντρικού Excel, την εκτέλεση του σεναρίου Python και την επαναφορά (restore) του αρχείου XML. Ο κύκλος αυτός δημιουργεί μια μικρή, αλλά υπολογίσιμη, χρονοκαθυστέρηση στην αποκατάσταση κρίσιμων υπηρεσιών, αναδεικνύοντας την ανάγκη εξισορρόπησης μεταξύ αυστηρής ασφάλειας και επιχειρησιακής συνέχειας.

Αναφορικά με την επιβάρυνση των υπολογιστικών πόρων, το καταγεγραμμένο overhead της τάξης του 15-20% στη χρήση της CPU κατά τη διάρκεια δικτυακών σαρώσεων κρίνεται

απολύτως βιώσιμο. Επιβεβαιώνει, ωστόσο, ότι η λειτουργία μηχανισμών Layer 7 σε περιβάλλοντα με περιορισμένο hardware απαιτεί προσεκτικό σχεδιασμό (sizing), ειδικά εάν στο μέλλον επιλεγεί η μετάβαση από κατάσταση ανίχνευσης (ID) σε κατάσταση IPS.

7.2 Αξιολόγηση Ερευνητικών Στόχων

Στην εισαγωγή της παρούσας εργασίας παρουσιάστηκαν οι βασικοί ερευνητικοί στόχοι, οι οποίοι συνοψίζονται στον Πίνακα 1.1. Η πειραματική υλοποίηση της προτεινόμενης αρχιτεκτονικής και η αξιολόγηση των αποτελεσμάτων επιτρέπουν την εκτίμηση του βαθμού επίτευξης των στόχων αυτών. Συνολικά, τα ευρήματα της έρευνας δείχνουν ότι οι στόχοι επιτεύχθηκαν σε σημαντικό βαθμό, τόσο σε τεχνικό όσο και σε επιχειρησιακό επίπεδο.

Πρώτον, η ανάλυση των κινδύνων που σχετίζονται με την κακή διαχείριση κανόνων firewall ανέδειξε προβλήματα όπως πλεονάζοντες κανόνες, επικαλύψεις και ελλιπή τεκμηρίωση, τα οποία μπορούν να οδηγήσουν σε σφάλματα παραμετροποίησης και αυξημένο κίνδυνο ασφάλειας. Η υιοθέτηση ενός δομημένου μοντέλου πολιτικών μέσω του προτύπου Excel συνέβαλε στη βελτίωση της οργάνωσης και της διακυβέρνησης των κανόνων firewall.

Δεύτερον, επιτεύχθηκε ο στόχος του σχεδιασμού μιας πρότυπης αρχιτεκτονικής ασφάλειας για περιβάλλοντα SMEs. Η αρχιτεκτονική αυτή βασίζεται στη χρήση του pfSense ως κεντρικού σημείου επιβολής πολιτικών και στην υλοποίηση δικτυακής τμηματοποίησης μέσω VLANs, επιτρέποντας τον διαχωρισμό διαφορετικών ζωνών δικτύου και περιορίζοντας την πιθανότητα πλευρικής κίνησης επιτιθέμενων.

Τρίτον, η αυτοματοποίηση της διαχείρισης κανόνων firewall υλοποιήθηκε μέσω της ανάπτυξης του σεναρίου Python excel2pfsense.py, το οποίο μετατρέπει τα δεδομένα πολιτικής από το πρότυπο Excel σε αρχείο διαμόρφωσης του pfSense. Η προσέγγιση αυτή επέτρεψε τη σημαντική μείωση του χρόνου παραμετροποίησης και τον περιορισμό σφαλμάτων διαμόρφωσης (misconfigurations), ενισχύοντας παράλληλα την ιχνηλασιμότητα των αλλαγών.

Τέλος, πραγματοποιήθηκε πρακτική αξιολόγηση της αποτελεσματικότητας της προτεινόμενης λύσης μέσω εργαστηριακών δοκιμών συνδεσιμότητας και σεναρίων αποκλεισμού κακόβουλης κίνησης. Τα αποτελέσματα επιβεβαίωσαν ότι οι κανόνες firewall εφαρμόζονται ορθά και ότι οι μηχανισμοί ασφάλειας που ενσωματώθηκαν στην αρχιτεκτονική συμβάλλουν στη βελτίωση της συνολικής προστασίας του δικτύου.

Συνολικά, η εργασία παρουσιάζει ένα εφαρμόσιμο και οικονομικά βιώσιμο μοντέλο διαχείρισης πολιτικών ασφάλειας βασισμένο σε εργαλεία ανοικτού κώδικα, το οποίο μπορεί να αξιοποιηθεί από SMEs για τη βελτίωση της ασφάλειας των πληροφοριακών τους συστημάτων.

7.3 Ευθυγράμμιση με το Πρότυπο ISO/IEC 27001

Η προτεινόμενη λύση δεν εξυπηρετεί μόνο λειτουργικούς σκοπούς, αλλά αποτελεί μηχανισμό κανονιστικής συμμόρφωσης (compliance), ικανοποιώντας άμεσα βασικές απαιτήσεις του προτύπου ISO/IEC 27001. Συγκεκριμένα, η αρχιτεκτονική που αναπτύχθηκε ευθυγραμμίζεται με τα ακόλουθα σημεία ελέγχου (Controls) του Παραρτήματος Α (Annex A):

- A.8.20 (Networks Security): Η χρήση του pfSense ως κεντρικού σημείου επιβολής και η λογική "Default Deny" διασφαλίζουν την προστασία των πληροφοριών στα δίκτυα από μη εξουσιοδοτημένη πρόσβαση.
- A.8.22 (Segregation of Networks): Η υλοποίηση 802.1Q VLANs (π.χ. διαχωρισμός LAN, GUEST, SERVERS) μέσω του Proxmox και του pfSense, καλύπτει την απαίτηση για διαχωρισμό ομάδων υπηρεσιών πληροφοριών, χρηστών και πληροφοριακών συστημάτων.
- A.8.32 (Change Management): Η μετάβαση από τις ad-hoc ρυθμίσεις στο WebGUI σε μια δομημένη διαδικασία "Policy as Code" μέσω του προτύπου Excel, εισάγει αυστηρό έλεγχο αλλαγών. Το Validation script διασφαλίζει ότι οι αλλαγές ελέγχονται πριν εφαρμοστούν, μειώνοντας τον κίνδυνο διακοπής υπηρεσιών.
- A.5.37 (Documented Operating Procedures): Το ίδιο το Excel Template, με την υποχρεωτική στήλη "Description" και την καρτέλα του "Change Register", λειτουργεί ως δυναμικά τεκμηριωμένη διαδικασία λειτουργίας, αποτρέποντας την απώλεια γνώσης (knowledge loss) στην επιχείρηση.

7.4 Περιορισμοί της Προτεινόμενης Λύσης (Limitations)

Παρότι τα αποτελέσματα της πειραματικής αξιολόγησης κρίνονται ιδιαίτερα θετικά, η παρούσα έρευνα υπόκειται σε συγκεκριμένους λειτουργικούς και τεχνικούς περιορισμούς. Αρχικά, η αξιολόγηση πραγματοποιήθηκε σε ελεγχόμενο εργαστηριακό περιβάλλον εικονικοποίησης, το

οποίο δεν αναπαριστά πλήρως την πολυπλοκότητα ενός παραγωγικού δικτύου. Κατά συνέπεια, δεν εξήχθησαν συμπεράσματα για τη συμπεριφορά του τείχους προστασίας υπό συνθήκες πραγματικού, βαρέος φόρτου (real-world heavy traffic) πολλών ταυτόχρονων χρηστών ή κρυπτογραφημένης κίνησης (SSL/TLS Inspection), η οποία απαιτεί πολλαπλάσιους πόρους.

Ο σημαντικότερος λειτουργικός περιορισμός της λύσης αφορά τον κίνδυνο απόκλισης διαμόρφωσης (configuration drift). Λόγω της μονόδρομης (one-way) φύσης του αυτοματισμού, το σύστημα δεν υποστηρίζει αμφίδρομο συγχρονισμό (two-way synchronization). Εάν πραγματοποιηθεί χειροκίνητη αλλαγή απευθείας WebGUI του pfSense, αυτή δεν καταγράφεται στο Excel και θα αντικατασταθεί (overwritten) στην επόμενη εφαρμογή του παραγόμενου αρχείου XML. Επομένως, προαπαιτούμενο για την επιτυχή λειτουργία της αρχιτεκτονικής σε παραγωγικό περιβάλλον είναι η οργανωτική επιβολή πολιτικής "Read-Only" πρόσβασης στο WebGUI για το τεχνικό προσωπικό, ώστε το Excel να παραμένει αδιαπραγμάτευτα η μοναδική πηγή αλήθειας.

Τέλος, η επιλογή της έκδοσης Community Edition (CE) του pfSense, η οποία δεν διαθέτει RESTful API, καθιστά την τρέχουσα υλοποίηση μια ημι-αυτοματοποιημένη διαδικασία, ή ακριβέστερα, μια προσέγγιση Διαχείρισης Πολιτικών ως Κώδικα (Policy as Code), καθώς απαιτείται η χειροκίνητη εισαγωγή του αρχείου ρυθμίσεων μέσω της λειτουργίας επαναφοράς.

Παρά τους παραπάνω περιορισμούς, η προτεινόμενη αρχιτεκτονική αποδεικνύει ότι η αυτοματοποίηση της διαχείρισης πολιτικών firewall σε περιβάλλοντα SMEs είναι τεχνικά εφικτή και επιχειρησιακά ωφέλιμη, υπό την προϋπόθεση ύπαρξης κατάλληλων διαδικασιών διακυβέρνησης και ελέγχου αλλαγών.

8 ΚΕΦΑΛΑΙΟ 8 – ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

8.1 Συμπεράσματα

Το βασικό συμπέρασμα που εξάγεται από την παρούσα διπλωματική εργασία είναι ότι η εφαρμογή σύγχρονων αρχών υποδομής ως κώδικα (Infrastructure as Code - IaC), μέσω απλών και ευρέως κατανοητών εργαλείων όπως τα υπολογιστικά φύλλα, μπορεί να καταστήσει τις πρακτικές κυβερνοασφάλειας πιο προσβάσιμες για τις SMEs. Η μετάβαση από τις αποσπασματικές, ad-hoc παρεμβάσεις στα γραφικά περιβάλλοντα διαχείρισης των firewalls σε μια κεντρικά ελεγχόμενη, τυποποιημένη και ημι-αυτοματοποιημένη διαδικασία ενισχύει σημαντικά την ανθεκτικότητα των εταιρικών δικτύων.

Η συγκριτική αξιολόγηση με τις παραδοσιακές μεθόδους ανέδειξε ότι η προτεινόμενη αρχιτεκτονική μειώνει την πολυπλοκότητα διαχείρισης, βελτιώνει την τεκμηρίωση και διασφαλίζει την επαναληψιμότητα των διαδικασιών διαμόρφωσης. Η βασική ερευνητική συμβολή της εργασίας έγκειται στην τεκμηρίωση ότι η επίτευξη ικανοποιητικού επιπέδου ασφάλειας δεν προϋποθέτει απαραίτητα την υιοθέτηση ακριβών εμπορικών λύσεων επόμενης γενιάς (Next Generation Firewalls – NGFWs). Αντιθέτως, ο ορθός αρχιτεκτονικός σχεδιασμός, σε συνδυασμό με τη χρήση αξιόπιστων εργαλείων ανοιχτού λογισμικού όπως το pfSense, το Suricata και το pfBlockerNG, καθώς και η εφαρμογή δομημένων διαδικασιών διαχείρισης πολιτικών ασφάλειας, μπορούν να συμβάλουν στη δημιουργία ενός αποτελεσματικού πλαισίου προστασίας.

Επιπλέον, η προτεινόμενη προσέγγιση συνδέεται με βασικές αρχές διαχείρισης ασφάλειας πληροφοριών που περιγράφονται στο πρότυπο ISO/IEC 27001. Η δομημένη διαχείριση πολιτικών firewall, η καταγραφή αλλαγών και η μείωση των σφαλμάτων διαμόρφωσης συμβάλλουν στη βελτίωση πρακτικών που σχετίζονται με τη διαχείριση λειτουργιών ασφάλειας και τη διαχείριση δικτυακής ασφάλειας, όπως περιγράφονται στο πρότυπο (ISO, 2022). Με τον τρόπο αυτό, η προτεινόμενη αρχιτεκτονική μπορεί να υποστηρίξει SMEs στη συστηματικότερη εφαρμογή πολιτικών ασφάλειας και στη βελτίωση της συνολικής ωριμότητας της διαχείρισης κυβερνοασφάλειας.

8.2 Προτάσεις για Μελλοντική Έρευνα

Παρότι τα αποτελέσματα της εργασίας είναι ενθαρρυντικά, υπάρχουν σαφή περιθώρια για περαιτέρω έρευνα και τεχνική εξέλιξη της προτεινόμενης προσέγγισης.

Για την πλήρη αυτοματοποίηση της διαδικασίας (end-to-end automation) και την επίλυση του προβλήματος της χειροκίνητης εισαγωγής του αρχείου ρυθμίσεων (zero-touch provisioning), η μελλοντική έρευνα μπορεί να εστιάσει στην ενσωμάτωση προγραμματιστικών διεπαφών. Η αξιοποίηση πακέτων όπως το "FauxAPI" για το pfSense ή η μεταφορά του μοντέλου σε παραπλήσιες πλατφόρμες όπως το OPNsense, το οποίο υποστηρίζει εγγενώς REST API, θα επέτρεπε τη δυναμική εφαρμογή των πολιτικών απευθείας από το script, εξαλείφοντας πλήρως την αλληλεπίδραση με το γραφικό περιβάλλον. Επιπλέον, το προτεινόμενο πρότυπο θα μπορούσε να επεκταθεί για να υποστηρίζει τη διαχείριση κανόνων Network Address Translation (NAT) και VPN.

Μια εξίσου κρίσιμη διάσταση που χρίζει μελλοντικής μελέτης είναι η διασφάλιση της ακεραιότητας του ίδιου του αρχείου Excel. Εφόσον το αρχείο λειτουργεί ως η μοναδική πηγή αλήθειας, η προστασία του καθίσταται εξίσου σημαντική με αυτήν του τείχους προστασίας. Η διασφάλιση αυτή πρέπει να επιτευχθεί μέσω αυστηρών μηχανισμών ελέγχου πρόσβασης στο σύστημα αρχείων και ισχυρής κρυπτογράφησης του εγγράφου, αποτρέποντας μη εξουσιοδοτημένες αλλαγές που θα μπορούσαν να μεταφερθούν αυτόματα στην περίμετρο του δικτύου.

Μια φυσική εξέλιξη για την οριστική επίλυση των παραπάνω περιορισμών είναι η αντικατάσταση του στατικού προτύπου Excel από μια κεντρική, εσωτερική διαδικτυακή εφαρμογή (Web-based Policy Portal). Η ανάπτυξη μιας τέτοιας πλατφόρμας (π.χ. μέσω πλαισίων όπως Django ή Flask) θα επέτρεπε την ενσωμάτωση ελέγχου πρόσβασης βάσει ρόλων (Role-Based Access Control - RBAC) και τη χρήση σχεσιακής βάσης δεδομένων για την τήρηση πλήρους ιστορικού αλλαγών (audit trail).

Τέλος, ιδιαίτερο ερευνητικό ενδιαφέρον παρουσιάζει η ενσωμάτωση μηχανισμών Μηχανικής Μάθησης και Τεχνητής Νοημοσύνης (AI/ML). Η αξιοποίηση Μεγάλων Γλωσσικών Μοντέλων (LLMs) για την αυτοματοποιημένη ανάλυση των αρχείων καταγραφής (logs) του Suricata IDS, θα μπορούσε να οδηγήσει σε ένα σύστημα που όχι απλώς ανιχνεύει απειλές, αλλά προτείνει

δυναμικά νέους κανόνες αποκλεισμού στο σύστημα διαχείρισης, μετατρέποντας την υποδομή σε ένα πλήρως αυτο-αποκαθιστώμενο δίκτυο (self-healing network).

Με βάση τα παραπάνω, η εργασία δείχνει ότι η ημι-αυτοματοποίηση της διαχείρισης πολιτικών firewall με χρήση εργαλείων ανοιχτού λογισμικού και δομημένων διαδικασιών μπορεί να αποτελέσει μια ρεαλιστική και οικονομικά βιώσιμη προσέγγιση για την ενίσχυση της κυβερνοασφάλειας στις SMEs.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Access Control List (ACL): Σύνολο κανόνων που καθορίζουν ποια δικτυακή κίνηση επιτρέπεται ή απορρίπτεται βάσει συγκεκριμένων κριτηρίων (διεύθυνση IP, θύρα, πρωτόκολλο).

Cybersecurity: Το σύνολο των τεχνολογιών, διαδικασιών και πρακτικών που στοχεύουν στην προστασία συστημάτων, δικτύων και δεδομένων από ψηφιακές επιθέσεις.

Firewall: Μηχανισμός ελέγχου δικτυακής κυκλοφορίας που εφαρμόζει προκαθορισμένους κανόνες ασφάλειας για την προστασία ενός πληροφοριακού συστήματος.

Intrusion Detection System (IDS): Σύστημα που παρακολουθεί τη δικτυακή ή συστημική δραστηριότητα και εντοπίζει πιθανές κακόβουλες ενέργειες ή παραβιάσεις πολιτικής ασφάλειας.

Intrusion Prevention System (IPS): Σύστημα που, εκτός από τον εντοπισμό επιθέσεων, έχει τη δυνατότητα να μπλοκάρει ή να αποτρέπει ενεργά την κακόβουλη δραστηριότητα.

Threat Intelligence: Πληροφορίες σχετικά με απειλές κυβερνοασφάλειας, οι οποίες συλλέγονται, αναλύονται και αξιοποιούνται για την πρόληψη επιθέσεων.

Virtualization: Τεχνολογία που επιτρέπει τη δημιουργία εικονικών μηχανών και την ταυτόχρονη εκτέλεση πολλαπλών λειτουργικών συστημάτων σε έναν φυσικό εξυπηρετητή.

Proxmox Virtual Environment (Proxmox VE): Πλατφόρμα εικονικοποίησης ανοικτού κώδικα που βασίζεται σε KVM και επιτρέπει τη διαχείριση εικονικών μηχανών και containers.

pfSense: Λογισμικό ανοικτού κώδικα βασισμένο σε FreeBSD που χρησιμοποιείται για την υλοποίηση firewall και δρομολογητή δικτύου.

Suricata: Σύστημα ανίχνευσης και πρόληψης εισβολών ανοικτού κώδικα, το οποίο υποστηρίζει επιθεώρηση πακέτων σε πραγματικό χρόνο.

pfBlockerNG: Επέκταση του pfSense που επιτρέπει φιλτράρισμα IP διευθύνσεων και DNS βάσει λιστών απειλών (blocklists).

VLAN (Virtual Local Area Network): Λογικός διαχωρισμός ενός φυσικού δικτύου σε επιμέρους απομονωμένα τμήματα για λόγους ασφάλειας και διαχείρισης.

Zero Trust Architecture: Μοντέλο ασφάλειας που βασίζεται στην αρχή «μηδενικής εμπιστοσύνης», όπου κάθε πρόσβαση επαληθεύεται ανεξάρτητα από τη θέση του χρήστη στο δίκτυο.

ISO/IEC 27001: Διεθνές πρότυπο που καθορίζει τις απαιτήσεις για την εγκαθίδρυση, εφαρμογή και συνεχή βελτίωση Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).

Risk Assessment: Διαδικασία αναγνώρισης, ανάλυσης και αξιολόγησης κινδύνων που απειλούν τα πληροφοριακά συστήματα ενός οργανισμού.

Access Control: Διαδικασία περιορισμού της πρόσβασης σε πληροφοριακά συστήματα και δεδομένα βάσει καθορισμένων πολιτικών και δικαιωμάτων.

Access Control List (ACL): Σύνολο κανόνων που καθορίζουν ποια δικτυακή κίνηση επιτρέπεται ή απορρίπτεται βάσει συγκεκριμένων κριτηρίων (IP, θύρα, πρωτόκολλο).

Advanced Persistent Threat (APT): Στοχευμένη και μακροχρόνια κυβερνοεπίθεση από οργανωμένο φορέα με σκοπό την απόκτηση πρόσβασης σε ευαίσθητα δεδομένα.

Anomaly Detection: Μέθοδος εντοπισμού αποκλίσεων από τη φυσιολογική συμπεριφορά ενός συστήματος με σκοπό την ανίχνευση πιθανών επιθέσεων.

Attack Surface: Το σύνολο των πιθανών σημείων εισόδου μέσω των οποίων ένας επιτιθέμενος μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.

Availability: Ιδιότητα της ασφάλειας πληροφοριών που διασφαλίζει ότι τα συστήματα και τα δεδομένα είναι προσβάσιμα όταν απαιτείται.

Backup: Διαδικασία δημιουργίας αντιγράφων ασφαλείας δεδομένων για σκοπούς αποκατάστασης σε περίπτωση απώλειας ή καταστροφής.

Blocklist: Λίστα διευθύνσεων IP ή domain names που έχουν χαρακτηριστεί ως κακόβουλες και αποκλείονται από την επικοινωνία.

Brute Force Attack: Μέθοδος επίθεσης κατά την οποία δοκιμάζονται πολλαπλοί πιθανοί συνδυασμοί κωδικών μέχρι την επιτυχή πρόσβαση.

Cloud Computing: Μοντέλο παροχής υπολογιστικών πόρων μέσω διαδικτύου, επιτρέποντας δυναμική κλιμάκωση και απομακρυσμένη πρόσβαση.

Confidentiality: Αρχή της ασφάλειας πληροφοριών που διασφαλίζει ότι η πρόσβαση στα δεδομένα επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα.

Cybersecurity: Το σύνολο τεχνολογιών και πρακτικών που στοχεύουν στην προστασία συστημάτων και δεδομένων από ψηφιακές απειλές.

Denial of Service (DoS): Επίθεση που αποσκοπεί στην εξάντληση πόρων ενός συστήματος ώστε να καθίσταται μη διαθέσιμο στους νόμιμους χρήστες.

Distributed Denial of Service (DDoS): Επίθεση άρνησης υπηρεσίας που πραγματοποιείται ταυτόχρονα από πολλαπλά συστήματα.

DNS Filtering: Τεχνική φιλτραρίσματος αιτημάτων DNS ώστε να αποτρέπεται η πρόσβαση σε κακόβουλους ή μη επιτρεπόμενους ιστότοπους.

Encryption: Διαδικασία μετατροπής δεδομένων σε μορφή που δεν μπορεί να αναγνωστεί χωρίς το κατάλληλο κλειδί αποκρυπτογράφησης.

Endpoint Security: Μέτρα ασφάλειας που εφαρμόζονται σε τελικές συσκευές (υπολογιστές, κινητά, servers).

Exploit: Κώδικας ή τεχνική που εκμεταλλεύεται ευπάθεια λογισμικού.

Firewall: Μηχανισμός ελέγχου δικτυακής κυκλοφορίας που εφαρμόζει πολιτικές ασφάλειας βάσει προκαθορισμένων κανόνων.

Forensics (Digital Forensics): Επιστημονική διαδικασία συλλογής και ανάλυσης ψηφιακών αποδεικτικών στοιχείων.

Hardening: Διαδικασία ενίσχυσης της ασφάλειας ενός συστήματος μέσω απενεργοποίησης περιττών υπηρεσιών και ρύθμισης ασφαλών παραμέτρων.

Hypervisor: Λογισμικό που επιτρέπει τη δημιουργία και διαχείριση εικονικών μηχανών σε έναν φυσικό εξυπηρετητή.

Incident Response: Διαδικασία διαχείρισης και αντιμετώπισης περιστατικών ασφάλειας.

Integrity: Ιδιότητα που διασφαλίζει ότι τα δεδομένα δεν έχουν αλλοιωθεί χωρίς εξουσιοδότηση.

Intrusion Detection System (IDS): Σύστημα που παρακολουθεί τη δραστηριότητα δικτύου και εντοπίζει πιθανές επιθέσεις.

Intrusion Prevention System (IPS): Σύστημα που εντοπίζει και αποτρέπει ενεργά κακόβουλη δραστηριότητα.

Least Privilege: Αρχή σύμφωνα με την οποία κάθε χρήστης διαθέτει μόνο τα απολύτως απαραίτητα δικαιώματα.

Log Management: Διαδικασία συλλογής, αποθήκευσης και ανάλυσης αρχείων καταγραφής.

Malware: Κακόβουλο λογισμικό που σχεδιάζεται για πρόκληση βλάβης ή μη εξουσιοδοτημένη πρόσβαση.

Multi-Factor Authentication (MFA): Μέθοδος αυθεντικοποίησης που απαιτεί περισσότερους από έναν παράγοντες επαλήθευσης.

Network Segmentation: Διαχωρισμός δικτύου σε επιμέρους τμήματα για ενίσχυση της ασφάλειας.

Patch Management: Διαδικασία εγκατάστασης ενημερώσεων ασφαλείας σε λογισμικό.

Penetration Testing: Ελεγχόμενη προσομοίωση επίθεσης για την αξιολόγηση της ασφάλειας συστήματος.

Phishing: Τεχνική εξαπάτησης με σκοπό την απόκτηση ευαίσθητων πληροφοριών.

Policy: Επίσημο σύνολο κανόνων που καθορίζει τον τρόπο λειτουργίας ενός συστήματος.

Proxmox VE: Πλατφόρμα εικονικοποίησης ανοικτού κώδικα βασισμένη σε KVM.

Risk: Πιθανότητα επέλευσης συμβάντος που μπορεί να επηρεάσει αρνητικά την ασφάλεια.

Risk Assessment: Διαδικασία αναγνώρισης και αξιολόγησης κινδύνων.

Security Information and Event Management (SIEM): Σύστημα συλλογής και ανάλυσης συμβάντων ασφάλειας.

Suricata: Σύστημα ανίχνευσης και πρόληψης εισβολών ανοικτού κώδικα.

Threat Intelligence: Πληροφορίες για υφιστάμενες και αναδυόμενες κυβερνοαπειλές.

VLAN: Λογικός διαχωρισμός φυσικού δικτύου σε απομονωμένα τμήματα.

Virtual Machine (VM): Λογικό υπολογιστικό σύστημα που λειτουργεί μέσα σε φυσικό εξυπηρετητή.

Virtualization: Τεχνολογία που επιτρέπει τη δημιουργία εικονικών υπολογιστικών περιβαλλόντων.

Vulnerability: Αδυναμία ή ελάττωμα που μπορεί να εκμεταλλευτεί επιτιθέμενος.

Zero Trust Architecture: Μοντέλο ασφάλειας που βασίζεται στη συνεχή επαλήθευση κάθε πρόσβασης.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Al-Shaer, E. and Hamed, H., 2004. Modeling and management of firewall policies. *IEEE Transactions on Network and Service Management*.

Anderson, R., 2020. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd ed. Indianapolis: Wiley.

Axelsson, S., 2000. *Intrusion Detection Systems: A Survey and Taxonomy*. Technical Report No. 99-15. Chalmers University of Technology.

Bace, R. and Mell, P., 2001. *Intrusion Detection Systems*. NIST Special Publication 800-31. Gaithersburg, MD: National Institute of Standards and Technology.

Barabási, A.-L., 2016. *Network Science*. Cambridge: Cambridge University Press.

Bass, L., Clements, P. and Kazman, R., 2013. *Software Architecture in Practice*. 3rd ed. Boston: Addison-Wesley Professional.

Behl, A. and Behl, K., 2017. *Cyberwar: The Next Threat to National Security and What to Do About It*. Oxford: Oxford University Press.

Bishop, M., 2018. *Computer Security: Art and Science*. 2nd ed. Boston: Addison-Wesley.

Buczak, A.L. and Guven, E., 2016. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 18(2), pp.1153–1176.

Center for Internet Security (CIS), 2023. *CIS Critical Security Controls v8*. Available at: https://www.cisecurity.org/controls (Accessed: 15 January 2026).

Chandola, V., Banerjee, A. and Kumar, V., 2009. Anomaly Detection: A Survey. *ACM Computing Surveys*, 41(3), pp.1–58.

Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2012. *Computer Security Incident Handling Guide* (SP 800-61 Rev.2). Gaithersburg, MD: NIST.

Cisco Systems, 2023. *Threat Intelligence Overview*. Available at: https://www.cisco.com/site/us/en/products/security/threat-intelligence.html (Accessed: 15 January 2026).

Cloud Security Alliance (CSA), 2022. *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. Available at: https://cloudsecurityalliance.org/artifacts/security-guidance-v4 (Accessed: 15 January 2026).

Conti, M., Dehghantanha, A., Franke, K. and Watson, S., 2018. Internet of Things Security and Forensics: Challenges and Opportunities. *Future Generation Computer Systems*, 78, pp.544–546.

ENISA, 2023. *ENISA Threat Landscape Report*. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends (Accessed: 15 January 2026).

European Commission, 2022. *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union.

European Union Agency for Cybersecurity (ENISA), 2022. *Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*. Available at: https://www.enisa.europa.eu/publications (Accessed: 15 January 2026).

Garfinkel, S.L., 2010. Digital Forensics Research: The Next 10 Years. *Digital Investigation*, 7, pp.S64–S73.

Gazoni, E. and Clark, C., 2023. *openpyxl - A Python library to read/write Excel 2010 xlsx/xlsm files*. Available at: https://openpyxl.readthedocs.io/ (Accessed: 15 January 2026).

Howard, M. and LeBlanc, D., 2003. *Writing Secure Code*. 2nd ed. Redmond: Microsoft Press.

Humble, J. and Farley, D., 2010. *Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation*. Boston: Addison-Wesley Professional.

IETF, 2008. *The Secure Shell (SSH) Protocol Architecture (RFC 4251)*. Available at: https://datatracker.ietf.org/doc/html/rfc4251 (Accessed: 15 January 2026).

International Organization for Standardization (ISO), 2018. *ISO/IEC 27001:2018 – Information technology — Security techniques — Information security management systems — Requirements*. Geneva: ISO.

International Organization for Standardization (ISO), 2018. *ISO/IEC 27005:2018 – Information technology — Security techniques — Information security risk management*. Geneva: ISO.

ISO/IEC, 2022. *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls*. Geneva: International Organization for Standardization.

Jajodia, S., Liu, P., Swarup, V. and Wang, C., 2010. *Cyber Situational Awareness: Issues and Research*. New York: Springer.

Kim, G., Lee, S. and Kim, S., 2014. A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection. *Expert Systems with Applications*, 41(4), pp.1690–1700.

Kizza, J.M., 2020. *Guide to Computer Network Security*. 5th ed. Cham: Springer.

McHugh, J., 2001. Intrusion and Intrusion Detection. *International Journal of Information Security*, 1(1), pp.14–35.

Mell, P. and Grance, T., 2011. *The NIST Definition of Cloud Computing (SP 800-145)*. Gaithersburg, MD: NIST.

Microsoft, 2023. *Microsoft Security Documentation*. Available at: https://learn.microsoft.com/en-us/security/ (Accessed: 15 January 2026).

MITRE, 2024. *MITRE ATT&CK® Framework*. Available at: https://attack.mitre.org/ (Accessed: 15 January 2026).

National Institute of Standards and Technology (NIST), 2009. *Guidelines on Firewalls and Firewall Policy (SP 800-41 Rev.1)*. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf (Accessed: 15 January 2026).

National Institute of Standards and Technology (NIST), 2012. *Guide for Conducting Risk Assessments (SP 800-30 Rev.1)*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology (NIST), 2014. *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*. Gaithersburg, MD: NIST.

National Institute of Standards and Technology (NIST), 2020. *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev.5)*. Gaithersburg, MD: NIST.

Netgate, 2024. *pfSense Documentation*. Available at: https://docs.netgate.com/pfsense/en/latest/ (Accessed: 15 January 2026).

Open Information Security Foundation (OISF), 2024. *Suricata User Guide*. Available at: https://docs.suricata.io/ (Accessed: 15 January 2026).

OWASP Foundation, 2021. *OWASP Top 10 – The Ten Most Critical Web Application Security Risks*. Available at: https://owasp.org/www-project-top-ten/ (Accessed: 15 January 2026).

Patel, K.C., et al., [n.d.]. *A Review paper on pfsense – an Open source firewall introducing with different capabilities & customization*.

Paxson, V., 1999. Bro: A System for Detecting Network Intruders in Real-Time. *Computer Networks*, 31(23–24), pp.2435–2463.

pfBlockerNG Development Team, 2024. *pfBlockerNG Documentation*. Available at: https://docs.netgate.com/pfsense/en/latest/packages/pfblocker.html (Accessed: 15 January 2026).

Ponemon Institute, 2023. *Cost of a Data Breach Report 2023*. Available at: https://www.ibm.com/reports/data-breach (Accessed: 15 January 2026).

Praptodiyono, S., et al., 2023. Development of hybrid intrusion detection system based on Suricata with pfSense method for high reduction of DDoS attacks on IPv6 networks. *Eastern-European Journal of Enterprise Technologies*, 5(9), p. 125.

Proxmox Server Solutions GmbH, 2024. *Proxmox Virtual Environment Documentation*. Available at: https://pve.proxmox.com/wiki/Documentation (Accessed: 15 January 2026).

Python Software Foundation, 2023. *Python 3.10.x Documentation (xml.etree.ElementTree)*. Available at: https://docs.python.org/3/library/xml.etree.elementtree.html (Accessed: 15 January 2026).

Raharjo, D. H. K. and Nurmala, A., 2022. Performance Evaluation of Intrusion Detection System Performance for Traffic Anomaly Detection Based on Active IP Reputation Rules. *2022 3rd International Conference on Electrical Engineering and Informatics (ICon EEI)*, IEEE, pp. 248-253.

Rescorla, E., 2018. *The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446)*. Internet Engineering Task Force (IETF). Available at: https://datatracker.ietf.org/doc/html/rfc8446 (Accessed: 15 January 2026).

RFC Editor, 2016. *HTTP/1.1: Semantics and Content (RFC 7231)*. Available at: https://datatracker.ietf.org/doc/html/rfc7231 (Accessed: 15 January 2026).

Rose, S., Borchert, O., Mitchell, S. and Connelly, S., 2020. *Zero Trust Architecture (SP 800-207)*. Gaithersburg, MD: NIST.

SANS Institute, 2023. *Incident Handler's Handbook*. Available at: https://www.sans.org/white-papers/33901/ (Accessed: 15 January 2026).

Scarfone, K. and Mell, P., 2007. *Guide to Intrusion Detection and Prevention Systems (IDPS) (SP 800-94)*. Gaithersburg, MD: NIST.

Shirey, R., 2007. *Internet Security Glossary, Version 2 (RFC 4949)*. Internet Engineering Task Force (IETF). Available at: https://datatracker.ietf.org/doc/html/rfc4949 (Accessed: 15 January 2026).

Sommer, R. and Paxson, V., 2010. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *IEEE Symposium on Security and Privacy*, pp.305–316.

Stallings, W., 2018. *Network Security Essentials: Applications and Standards*. 6th ed. Boston: Pearson.

Symantec, 2019. *Internet Security Threat Report*. Available at: https://www.broadcom.com/company/newsroom/press-releases (Accessed: 15 January 2026).

Verizon, 2023. *2023 Data Breach Investigations Report (DBIR)*. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 15 January 2026).

Whitman, M.E. and Mattord, H.J., 2021. *Principles of Information Security*. 6th ed. Boston: Cengage Learning.

Wool, A., 2004. A quantitative study of firewall configuration errors. *IEEE Computer*.

Yuan, L. et al., 2006. Fireman: A toolkit for firewall modeling and analysis. *IEEE Symposium on Security and Privacy*.