REPORT
pfSense IDS Traffic Monitoring and EternalBlue Detection

v1.0.0

Author:

Eldon Gabriel

January 13, 2026

TABLE OF CONTENTS

Disclaimer: This report documents my personal work completed as part of an MCSI lab exercise. It reflects my independent understanding and configuration of pfSense in a controlled lab environment. No MCSI video content, lab materials, or proprietary instructions are included or shared. All information presented follows MCSI disclosure and academic integrity policies.

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	01/13/2026	Eldon G.	Initial draft.

EXECUTIVE SUMMARY

This report documents the deployment of a pfSense firewall with Intrusion Detection System (IDS) capabilities to monitor and detect malicious network activity within a virtual laboratory environment. The objective of this study was to configure pfSense with the Snort IDS package and validate its ability to detect abnormal traffic generated during the exploitation of the Windows 7 EternalBlue (MS17-010) vulnerability.

During the engagement, network connectivity issues were encountered owing to firewall rule restrictions and an IP address conflict. These issues were identified, remediated, and validated. Once resolved, a successful EternalBlue exploit was launched from a Kali Linux system against a vulnerable Windows 7 host, resulting in system-level access and corresponding IDS alerts on the pfSense.

1.0 LAB ENVIRONMENT AND ARCHITECTURE

1.1 Virtual Machines

The virtual network consists of three systems operating on the same subnet:

- **pfSense Firewall**
    - **Role:** Firewall, router, and IDS sensor
    - **IDS Package:** Snort
    - **Gateway IP:** 10.1.1.1
- **Windows 7**
    - **Role:** Vulnerable target system
    - **Final IP Address:** 10.1.1.101
    - **Vulnerability:** MS17-010 (EternalBlue)
- **Kali Linux**
    - **Role:** Attacking system
    - **Tools Used:** Nmap, Metasploit Framework
    - **IP Address:** 10.1.1.5

2.0 PFSENSE AND IDS CONFIGURATION

2.1 pfSense Deployment

pfSense was installed as a virtual machine and configured to manage the traffic of the virtual network. All the systems were placed on the same subnet to ensure traffic visibility.

2.2 Snort IDS Installation

The Snort package was installed using the pfSense package manager and configured to monitor LAN traffic. Default rules were enabled to detect suspicious and malicious network activities. Alerts were configured to be viewed through the pfSense web console.

3.0 TECHNICAL ENGAGEMENT AND TROUBLESHOOTING

3.1 Phase I: Initial Blockage and Diagnosis

An initial Nmap scan from Kali Linux showed TCP Port 445 on the Windows 7 host as **Filtered**, preventing exploitation attempts.

Observed Issues:

- Port 445 is not reachable
- No exploit traffic reaching the target

Analysis:

- Snort alerts showed `http_inspect` warnings, such as *TOO MANY PIPELINED REQUESTS*. These were identified as false positives and were unrelated to the blocked SMB traffic.
- The pfSense firewall settings blocked RFC 1918 and Bogon networks by default.

3.2 Phase II: Network Remediation

To restore connectivity, the following corrective actions were implemented:

- **Firewall Configuration**
  - Disable “Block private networks” and “Block bogon networks” on the relevant interface
  - Added an explicit **Pass** rule on the LAN interface to allow traffic from the Kali VM to the Windows 7 system
- **IP Address Conflict Resolution**
  - Discovered the Windows 7 system was assigned the same IP address as the pfSense gateway (10.1.1.1)
  - Reassigned the Windows 7 system to **10.1.1.101**

- A follow-up Nmap scan showed Port 445 changed from a *Filtered* state, where the firewall was dropping packets, to an *Open* state, where the SMB service was actively responding.

3.3 Phase III: Exploitation and Access

With the network connectivity restored, the EternalBlue exploit was executed using Metasploit.

- **Exploit Module:** `ms17_010_eternalblue`
- **Target:** 10.1.1.101
- **Payload:** `windows/x64/meterpreter/reverse_tcp`
- **Result:** Successful Meterpreter session established

pfSense Snort generated alerts indicating abnormal SMB-related traffic during exploitation, confirming IDS functionality.

4.0 EVIDENCE OF COMPROMISE

The following evidence confirmed successful system-level access.

- **User Context:**
  `getuid` returned `NT AUTHORITY\SYSTEM`
- **System Verification:**
  `sysinfo` confirmed a vulnerable Windows 7 build
- **Credential Access:**
  `hashdump` successfully extracted local SAM hashes

5.0 VALIDATION RESULTS

The following objectives were successfully validated.

- pfSense is installed and monitoring network traffic
- Snort IDS is configured and generating alerts
- The pfSense web console is accessible
- Windows 7 EternalBlue vulnerability successfully exploited
- Abnormal exploit-related traffic is visible in Snort alerts

---

6.0 REMEDIATION RECOMMENDATIONS

- **Patching:**
  Apply the MS17-010 security updates to eliminate the EternalBlue vulnerability.
- **Firewall Hardening:**
  Avoid broad “allow all” firewall rules. While an allow rule was required to complete the lab, this approach is not suitable for production environments.
- **IDS Tuning:**
  The Snort rule sets were reviewed to reduce false positives while maintaining effective detection.

7.0 CONCLUSION

7.1 Key Takeaways

This exercise demonstrated how a firewall and IDS work together to monitor networks. The pfSense firewall controlled access, whereas the Snort IDS detected abnormal traffic during the EternalBlue exploit. Security tools can block attacks but may also block testing if misconfigured. Default firewall settings and IP conflicts prevented system access.

After fixing these issues, the exploit worked and generated IDS alerts successfully. The main value was learning to troubleshoot firewall rules, network addressing, and IDS alerts while verifying that the monitoring tools worked correctly.

7.2 Security Implications and Recommendations

The successful attack on the Windows 7 system shows the danger of not updating old operating systems. EternalBlue can take over the entire system and spread to other parts, making it a serious threat in business settings.

Technical Recommendations:

- Apply MS17-010 patches to all Windows systems or decommission unsupported operating systems.
- Restrict SMB access using firewall rules and limit it to the required hosts only.
- Maintain IDS signatures and tune the rules to reduce false positives while preserving the detection capability.
- Regularly audit firewall rules and interface settings to prevent unintended traffic blocking or exposures.

Procedural Recommendations are as follows

- Routine vulnerability scanning should be implemented to identify exploitable services.
- Enforce change management for firewall and network configuration updates.
- Document network addressing to prevent IP conflicts.

Best Practices and Framework Alignment:

- Aligns with **NIST SP 800-53** controls for vulnerability management, network monitoring, and access control.
- Supports **NIST CSF** functions: *Protect* and *Detect*.
- This is consistent with the **ISO/IEC 27001** requirements for system hardening and security monitoring.

Compliance Relevance:

- Relevant to **PCI-DSS** requirements for network segmentation, intrusion detection, and vulnerability management in environments that handle payment data.