

# Implementing Security Monitoring and Logging

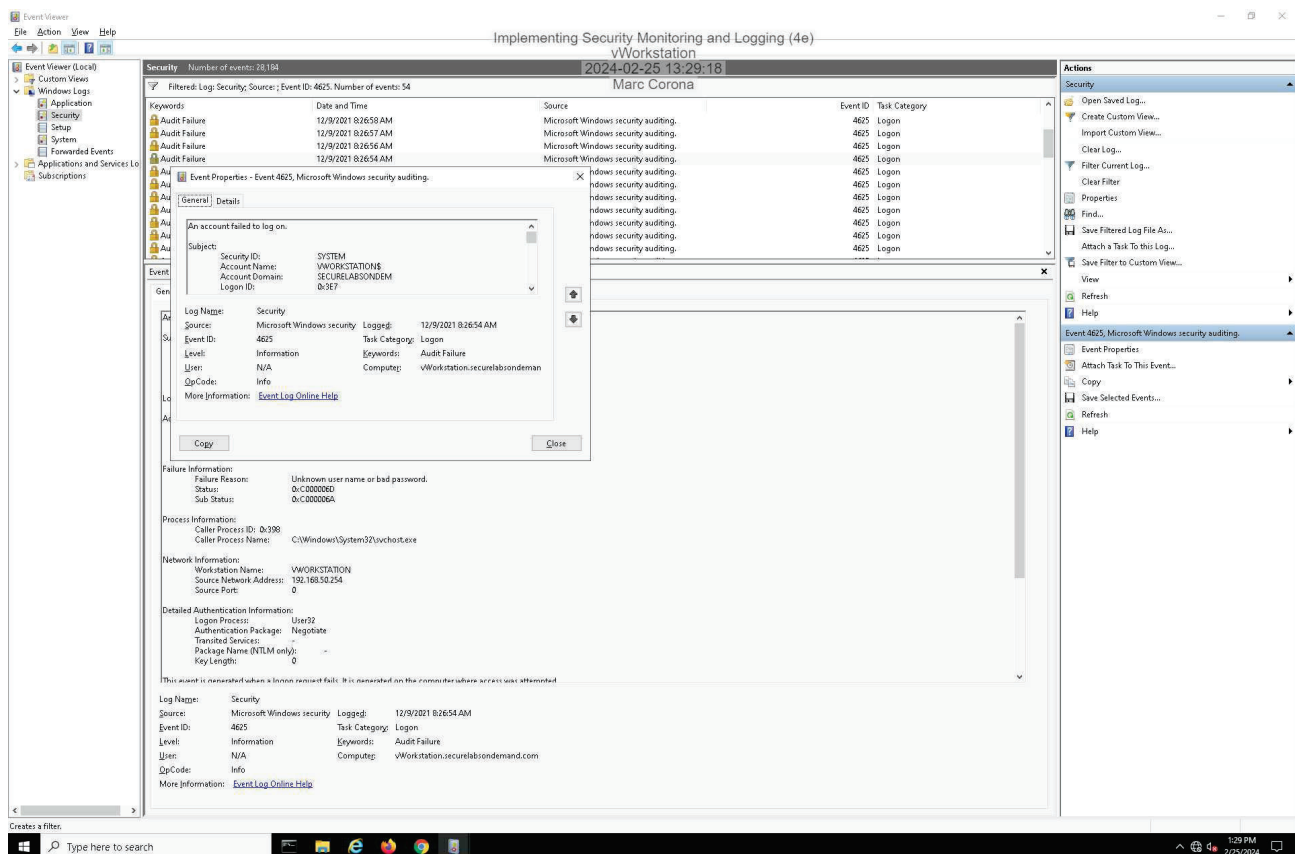
Student:

Marc Corona Mireles

## Section 1: Hands-On Demonstration

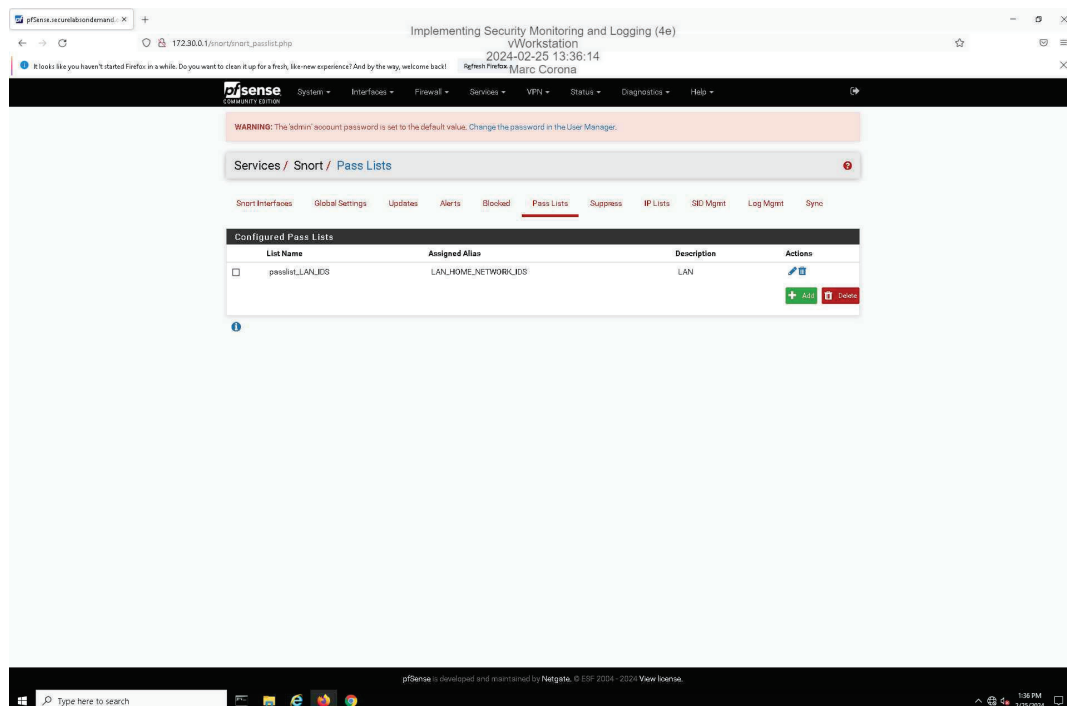
### Part 1: Identify Failed Logon Attempts on Windows Systems

8. Make a screen capture showing the **Security Event Properties** dialog box on the **vWorkstation**.

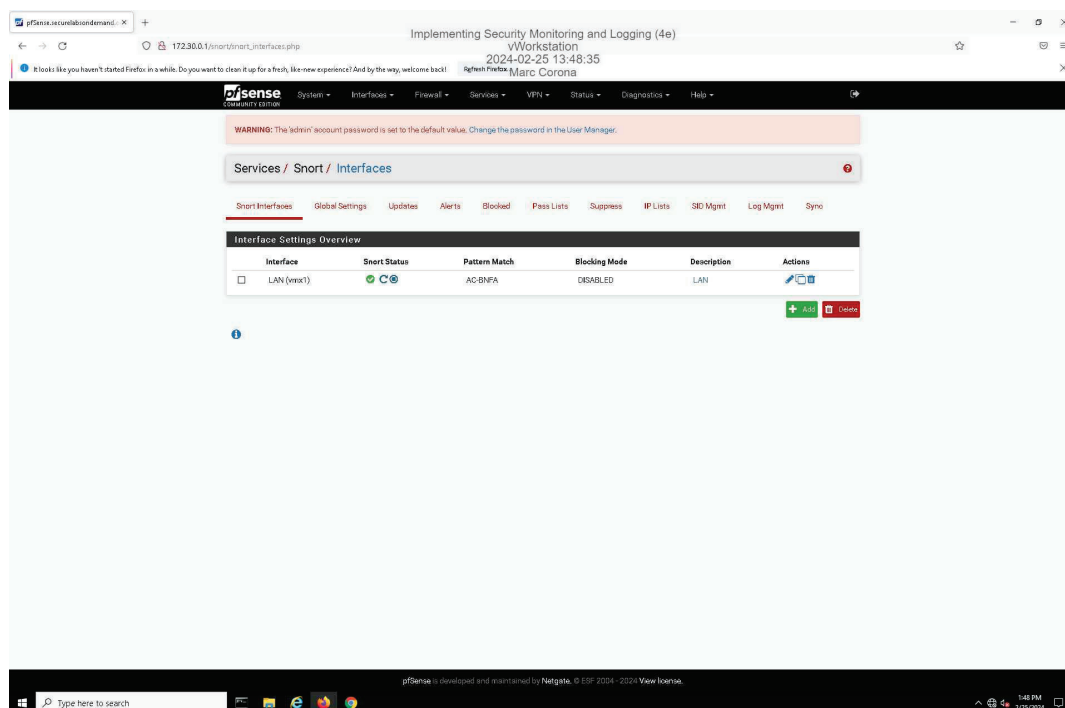


### Part 2: Monitor Network Activity with Snort

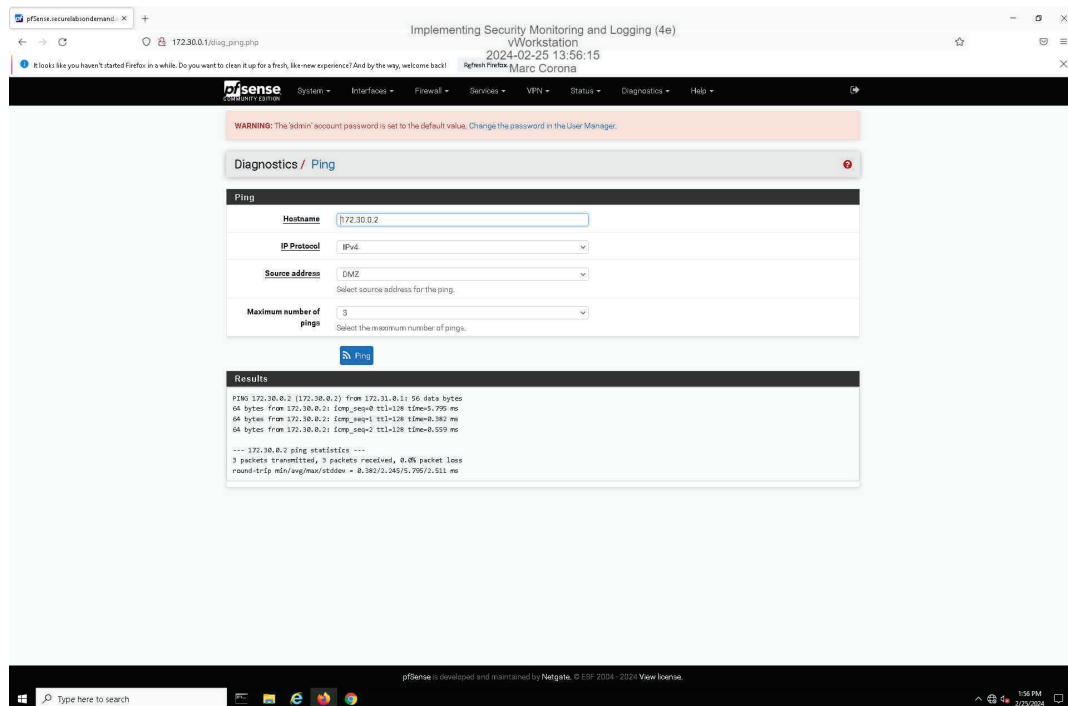
17. Make a screen capture showing the updated Pass Lists page.



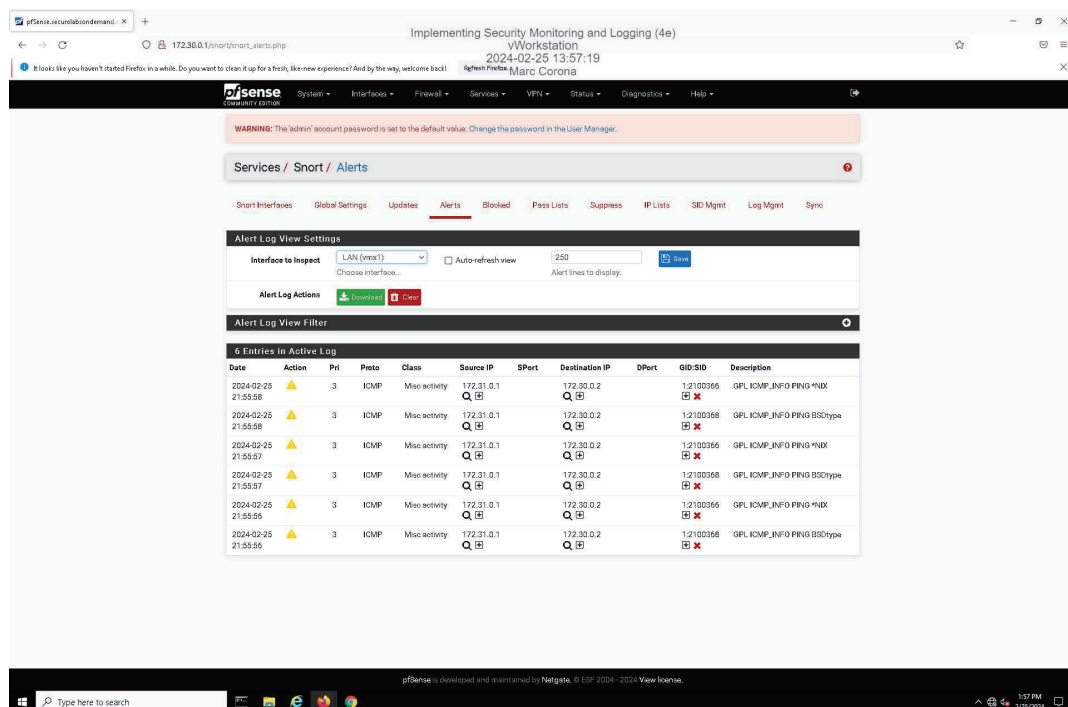
31. Make a screen capture showing the active Snort status on the LAN interface.



### 36. Make a screen capture showing the successful ping results.



### 41. Make a screen capture showing the ICMP alerts in the Snort Active Log.



---

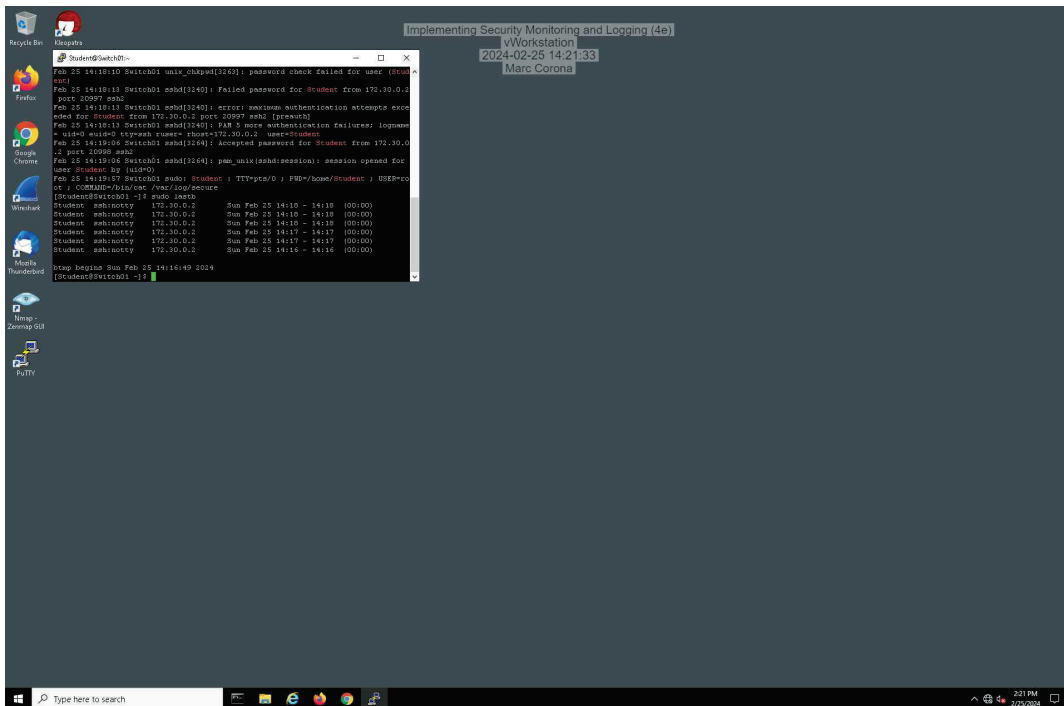
## Section 2: Applied Learning

### Part 1: Identify Failed Logon Attempts on Linux Systems

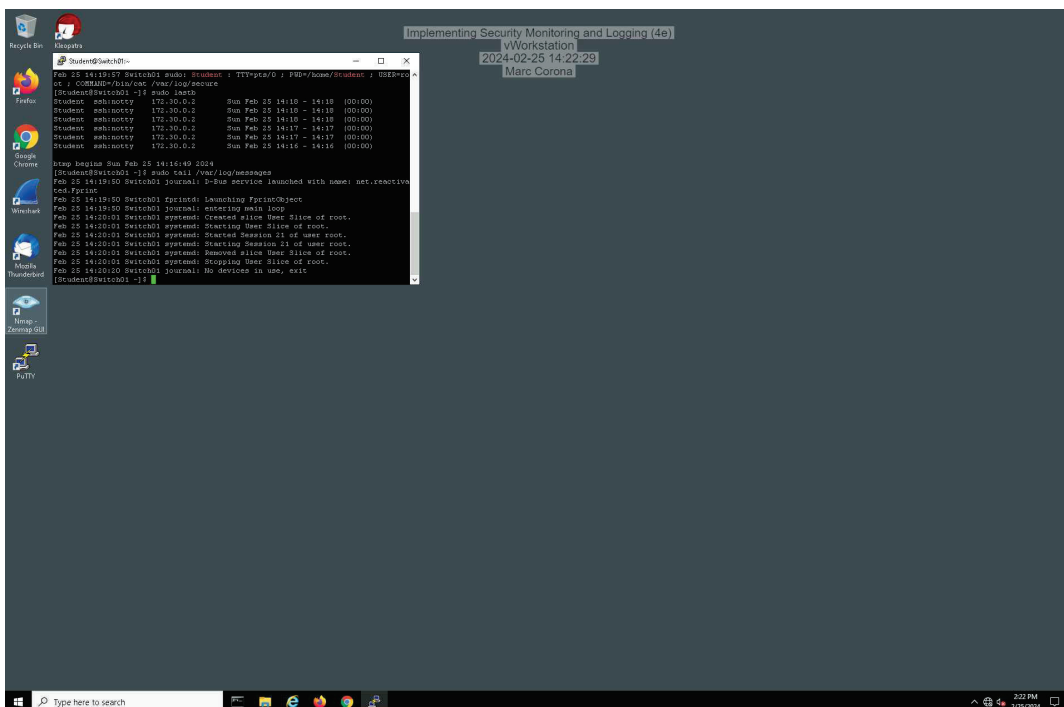
10. Make a screen capture showing the edited `rsyslog.conf` file.



## 20. Make a screen capture showing the failed login attempts.



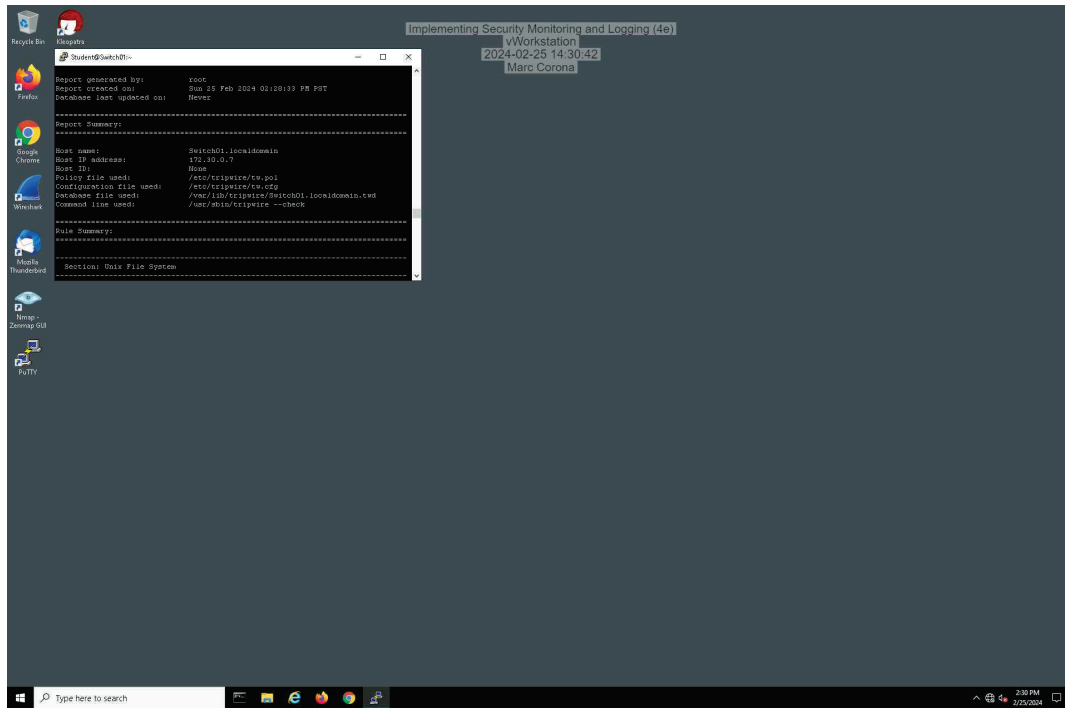
## 22. Make a screen capture showing the last 10 log messages.



## Part 2: Monitor File Integrity with Tripwire

---

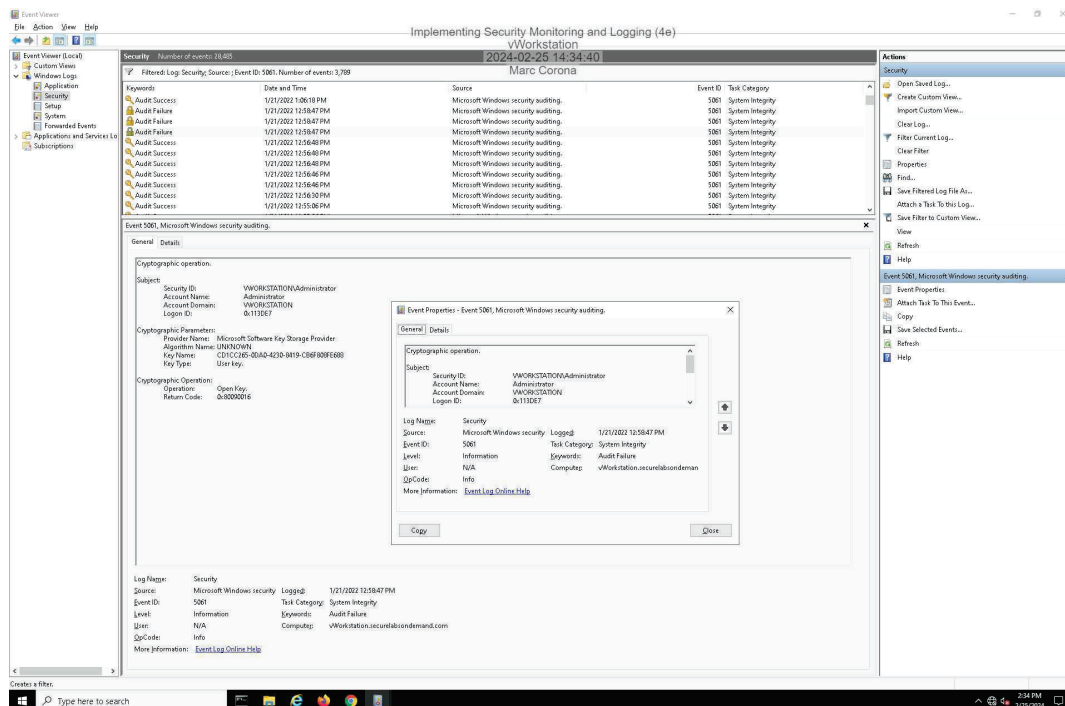
12. Make a screen capture showing the **Object Summary** section for the Tripwire report.



## Section 3: Challenge and Analysis

### Part 1: Identify Additional Event Types in the Event Viewer

Make a screen capture showing the **Security Event Properties** dialog box for an **Audit Failure** associated with **Event ID 5061**.



Provide a brief explanation of the operation that would generate a security event with Event ID 5061.

An event ID of 5061 pertains to a cryptographic operation. This event is logged when a cryptographic operation is attempted, such as the use of a cryptographic key, and involves operations like key export, key import, data encryption, data decryption, signing, and more. This event is crucial for monitoring and auditing cryptographic activities within a system to ensure security policies are followed, to identify potential unauthorized access to cryptographic keys, or to detect other security relevant activities involving cryptographic operations.

### Part 2: Configure Snort as an Intrusion Prevention System

Make a screen capture showing the **Legacy Blocking Mode** enabled on the LAN interface.

