

Enterprise Firewall Implementation using Check Point SmartConsole

MSc Cyber Security Project

Student: Vanshaj Patel | **ID:** 2517969





Introduction

- A **firewall** monitors and controls traffic based on security rules, acting as a barrier between trusted and untrusted networks [1]
- This project implements a **multi-layered firewall** using Check Point SmartConsole
- Network security is critical to protecting enterprise assets from unauthorised access and cyber threats [1]

Security Features & Threat Prevention

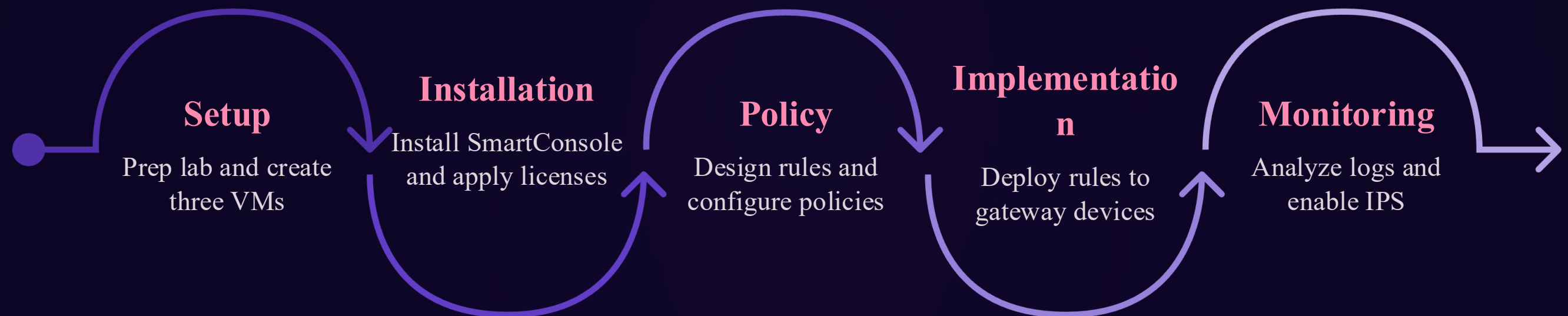
Discuss IPS and firewall capabilities

- **Intrusion Prevention System (IPS)** provides real-time threat detection and blocking [2]
- **Application Control** monitors and restricts application-level traffic
- **Threat Prevention** integrates multiple security layers for comprehensive protection [2]
- **Log Analysis** enables forensic investigation and compliance reporting

Check Point SmartConsole integrates advanced threat prevention mechanisms, combining network-level filtering with application-aware security to defend against evolving cyber threats.

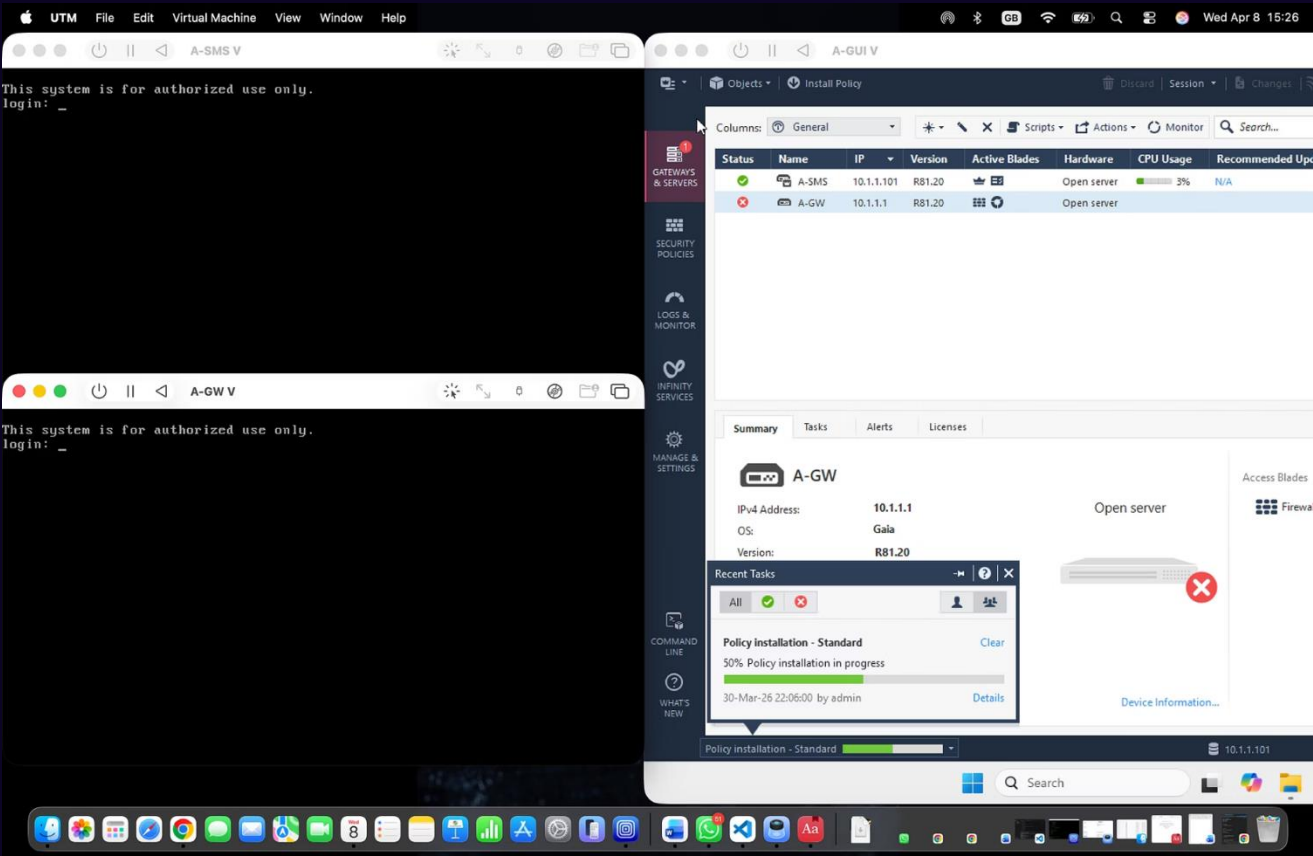


Workflow Overview



A structured five-phase methodology ensures systematic deployment and validation of the enterprise firewall.

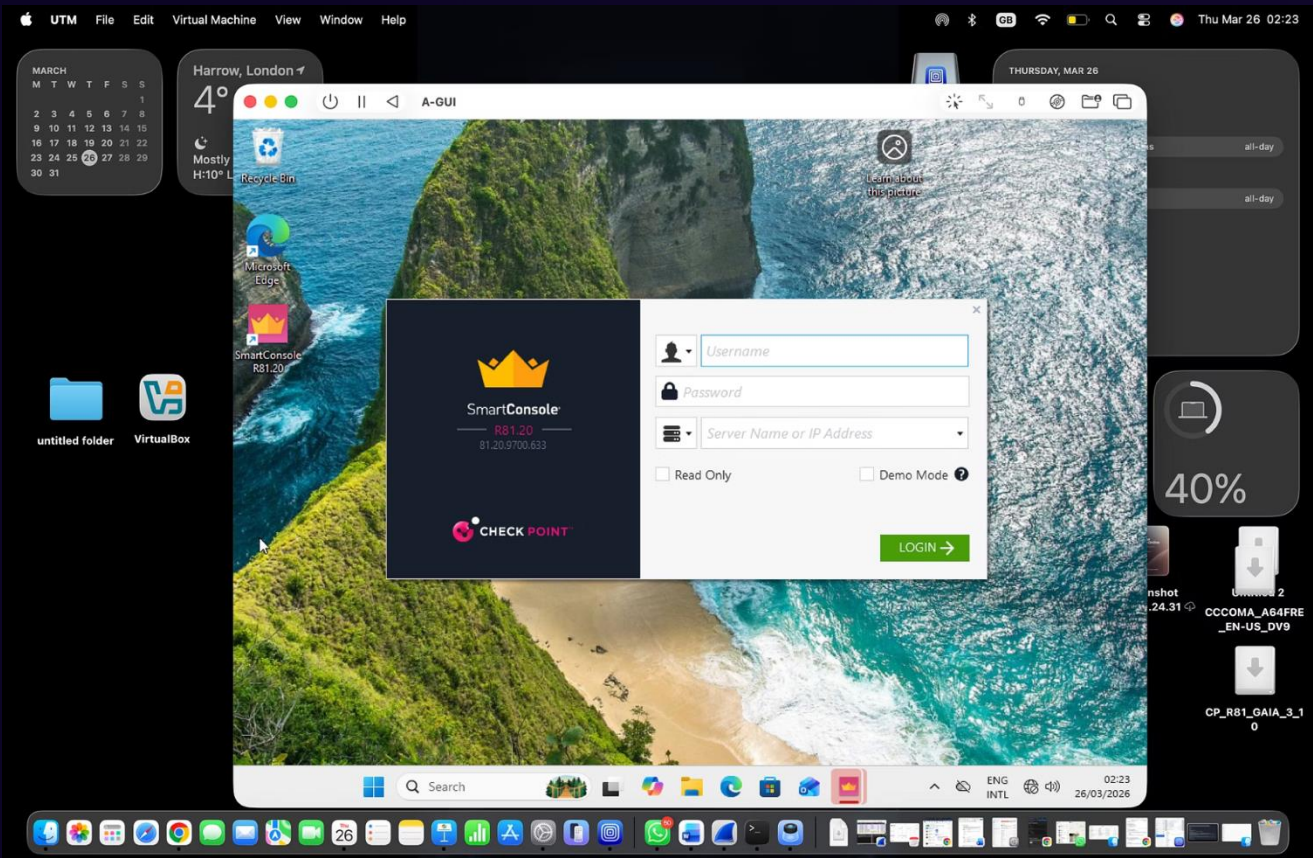
Environment Setup & SmartConsole Installation



Three Virtual Machines

- A-SMS — Security Management Server
- A-GW — Security Gateway
- A-GUI — SmartConsole Client

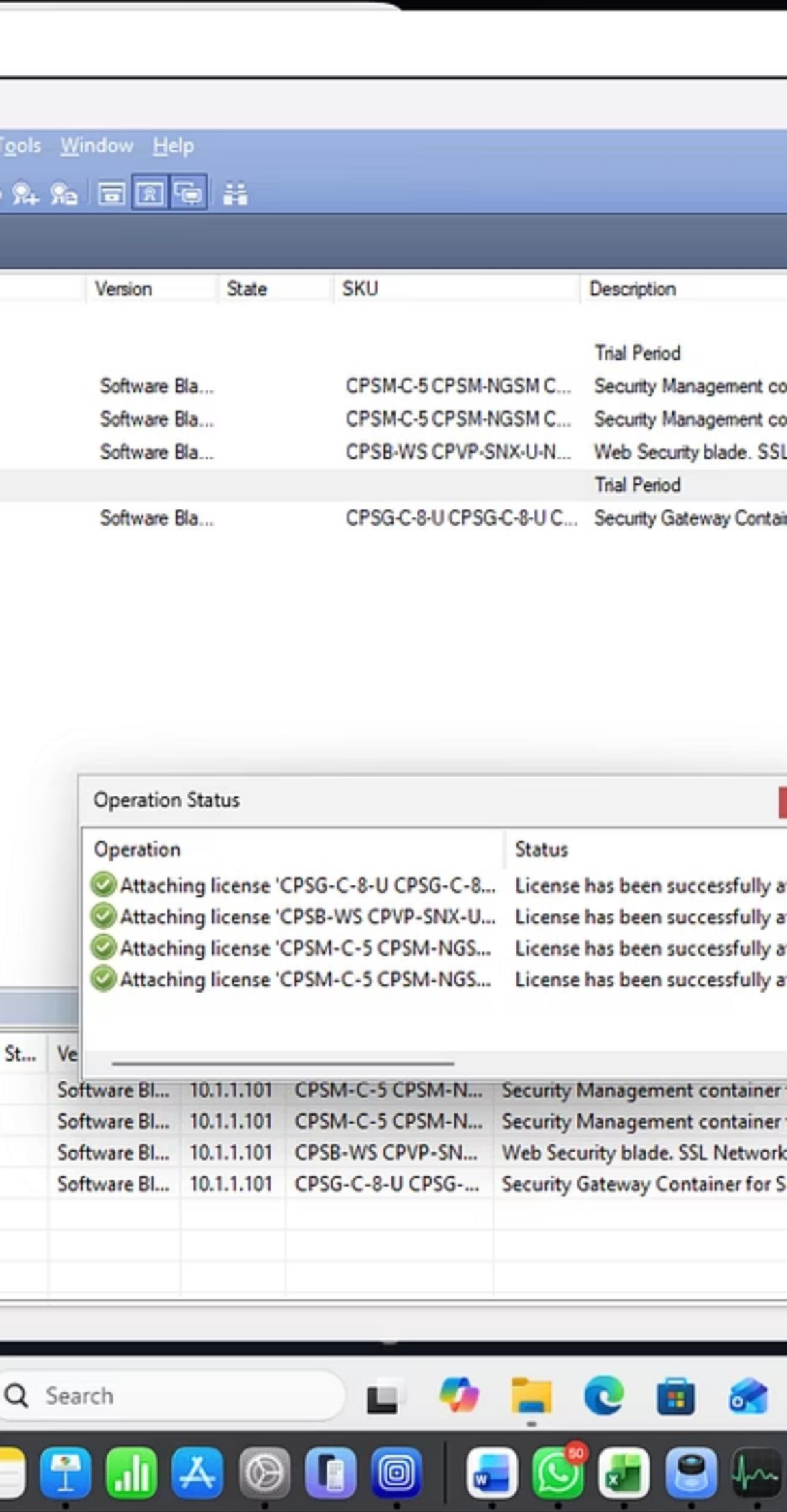
Figure 1: All three VMs operational on macOS host — *all 3 are working in mac.png*



SmartConsole Login

- Connects to A-SMS via IP and admin credentials
- Central interface for policy management and gateway configuration

Figure 2: SmartConsole login interface — *smartconsol.png*



License Installation & System Architecture

- Licence activated via SmartConsole to unlock IPS, Application Control, and Threat Prevention
- All components validated and operational before policy configuration

 **Figure 3:** Licence activation and component validation — *license.png*

A-SMS

Central management server

A-GW

Traffic inspection gateway

A-GUI

Admin console client

Policy Structure Overview

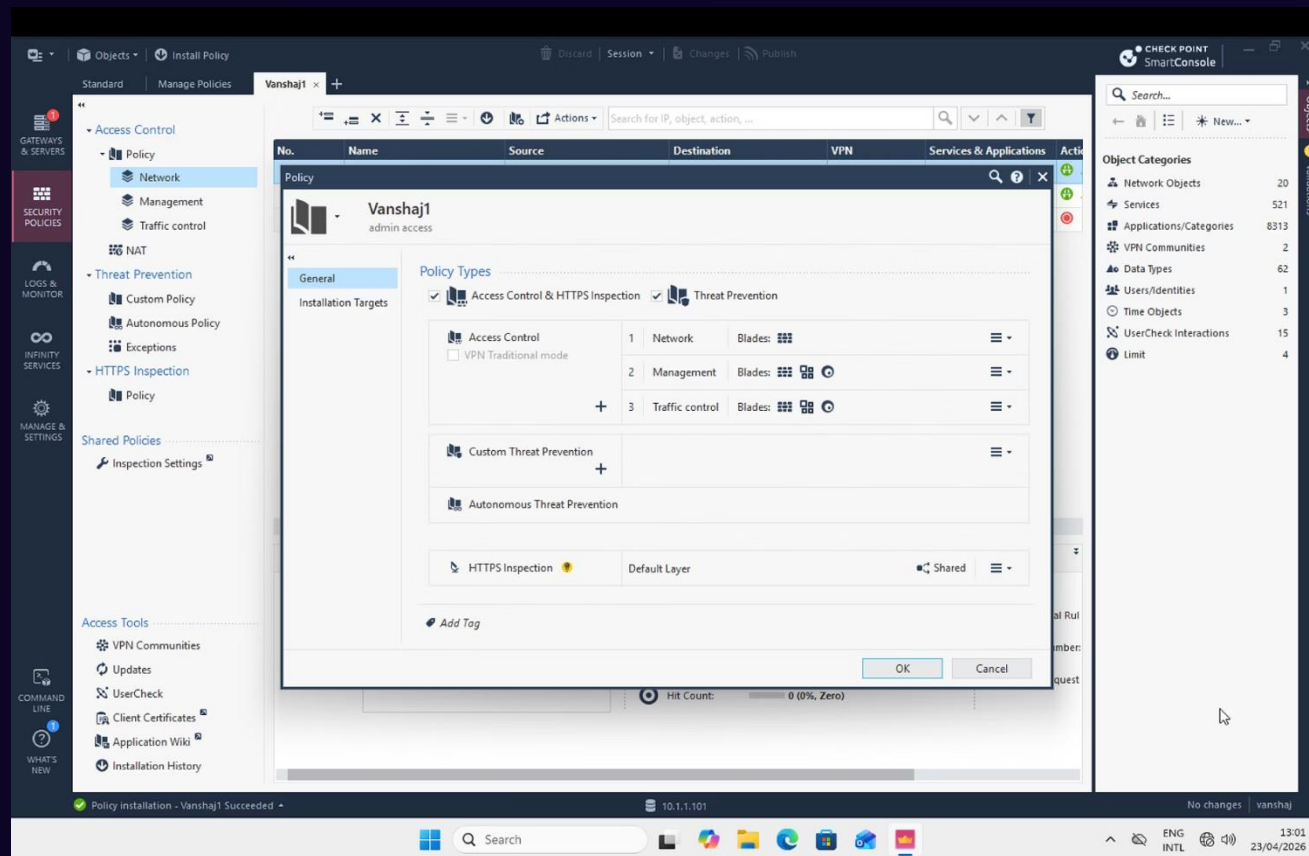


Figure 5: Custom policy structure (Vanshaj1) — Shows the tailored policy configuration for this project

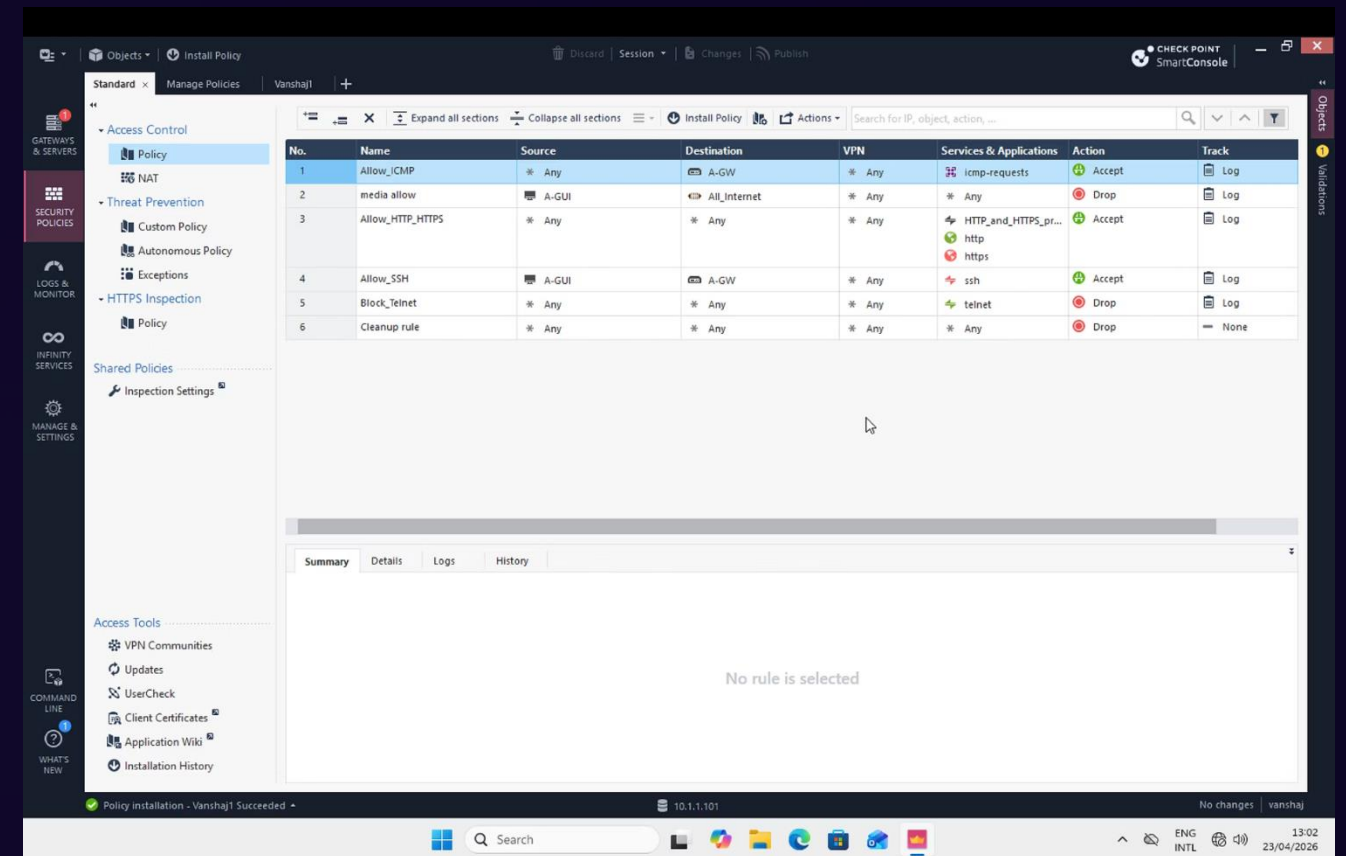


Figure 6: Standard policy overview — Demonstrates the baseline policy framework

The layered policy design separates concerns across Network, Management, and Traffic Control policies, enabling granular security control and simplified administration.

Policy Types & Network Policy Configuration

Three Policy Layers

- **Network Policy** — Controls ICMP, DNS, and general traffic
- **Management Policy** — Governs SmartConsole and SSH access
- **Traffic Control Policy** — Manages HTTP/HTTPS and Telnet rules

Network Policy Rules

- **ICMP** — Allows ping for connectivity testing
- **DNS** — Permits name resolution
- **Cleanup Rule** — Drops all unmatched traffic

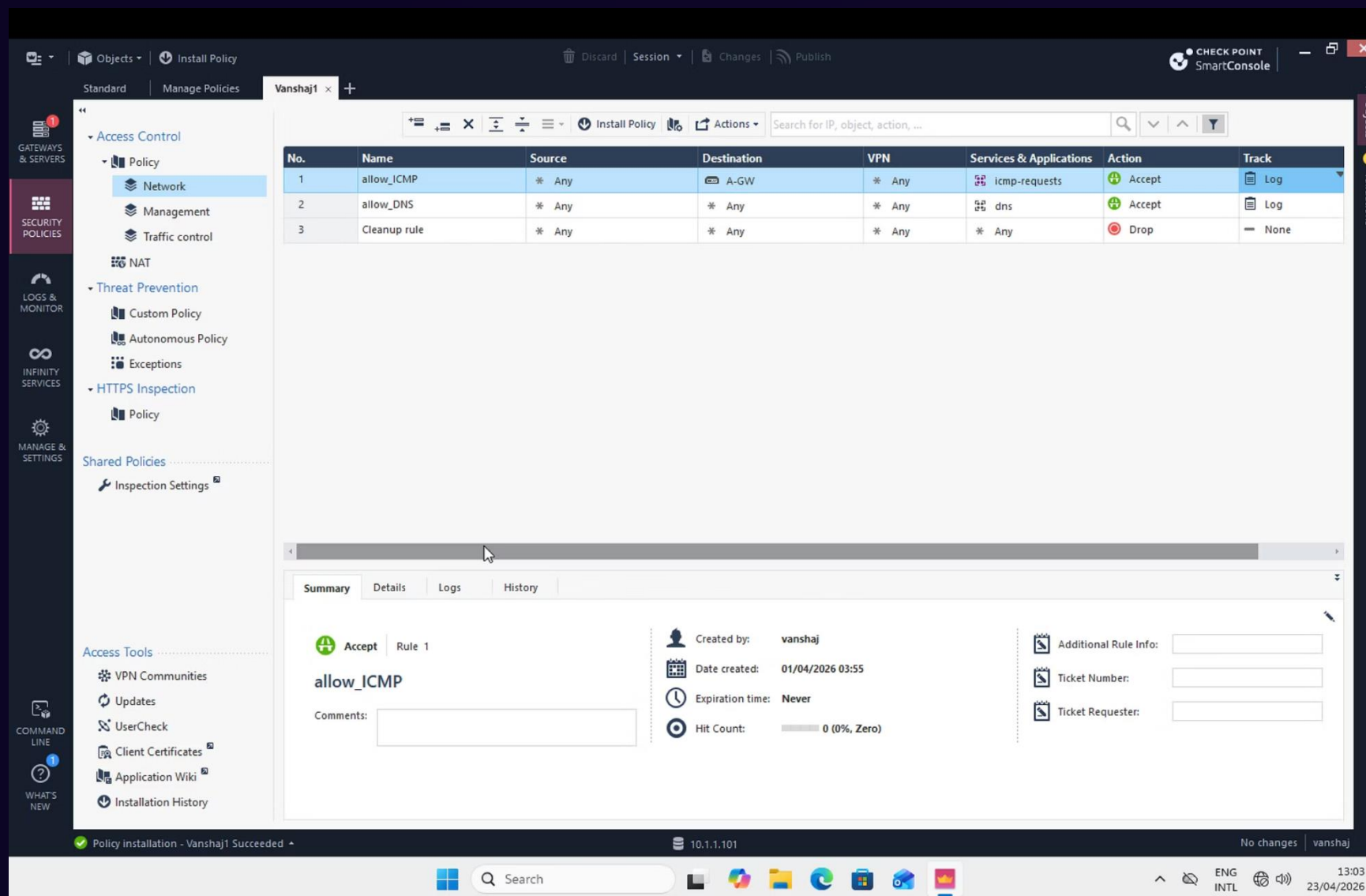
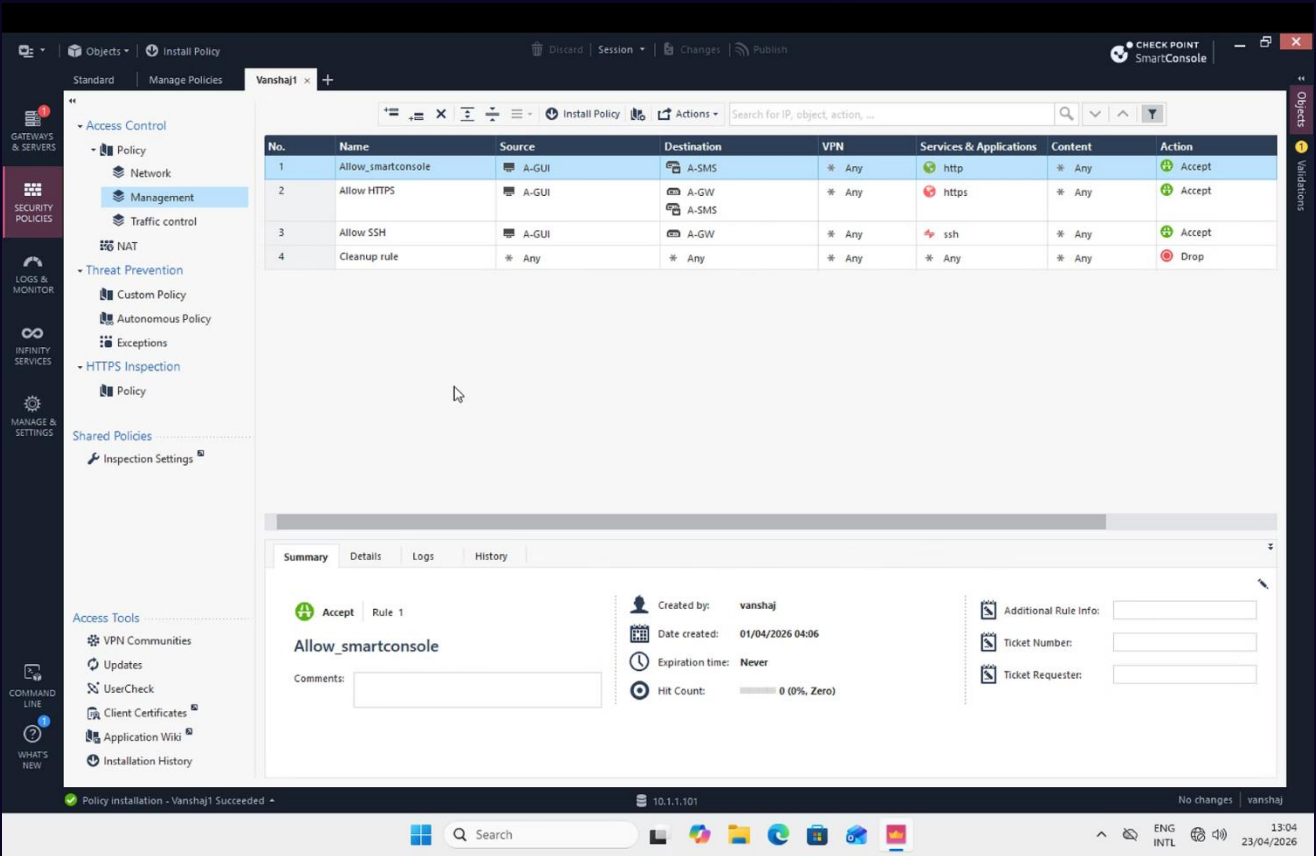


Figure 4: Network Policy rule set
— *network.png*

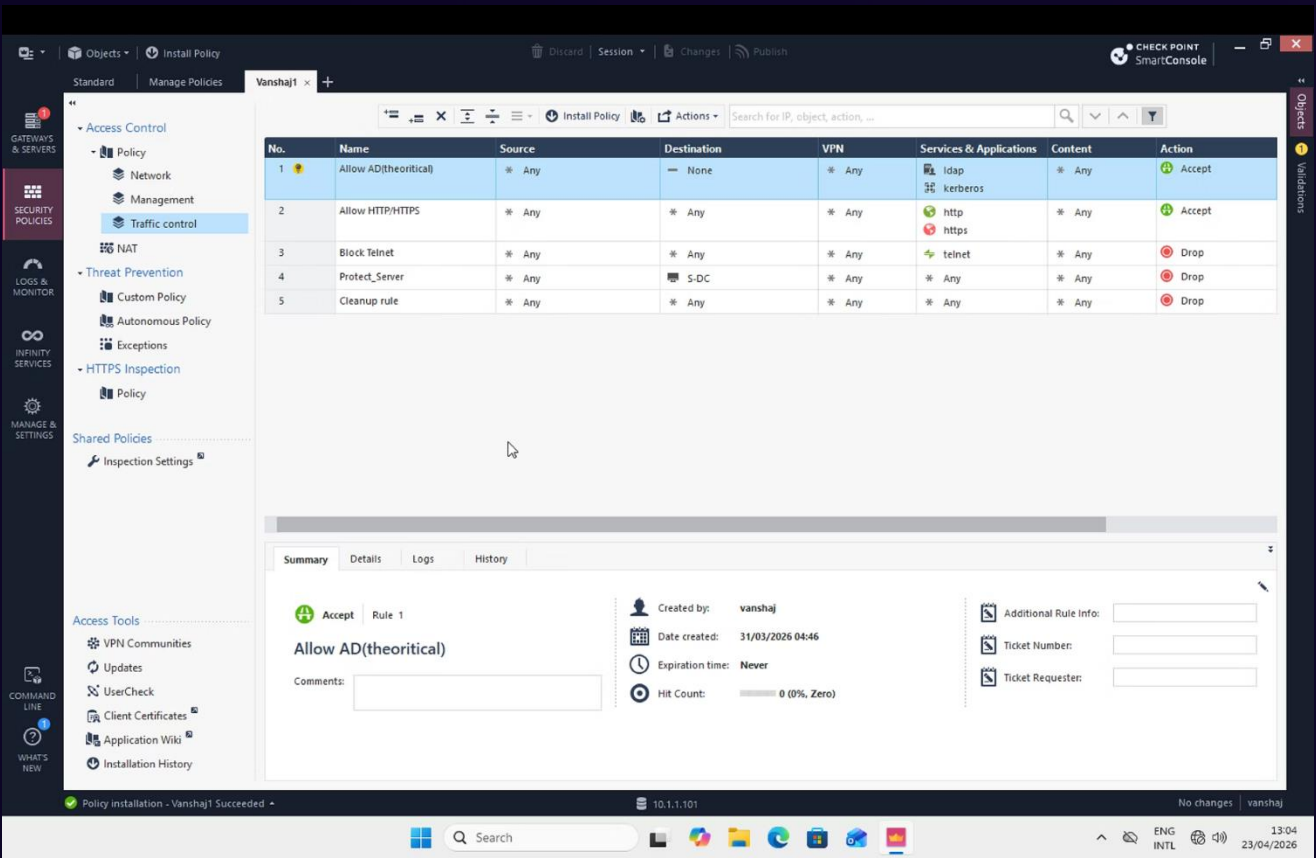
Management & Traffic Control Policies



Management Policy

- Restricts **SmartConsole** access to authorised administrators
- Permits **SSH** for secure remote management only

 **Figure 5:** Management Policy configuration — *management.png*



Traffic Control Policy

- **HTTP/HTTPS** — Allowed for web access
- **Telnet** — Blocked (insecure, unencrypted)
- **Active Directory** — LDAP/Kerberos designed but not implemented due to lab constraints

 **Figure 6:** Traffic Control Policy with AD rule — *traffic-rule.png*

Policy Installation Process

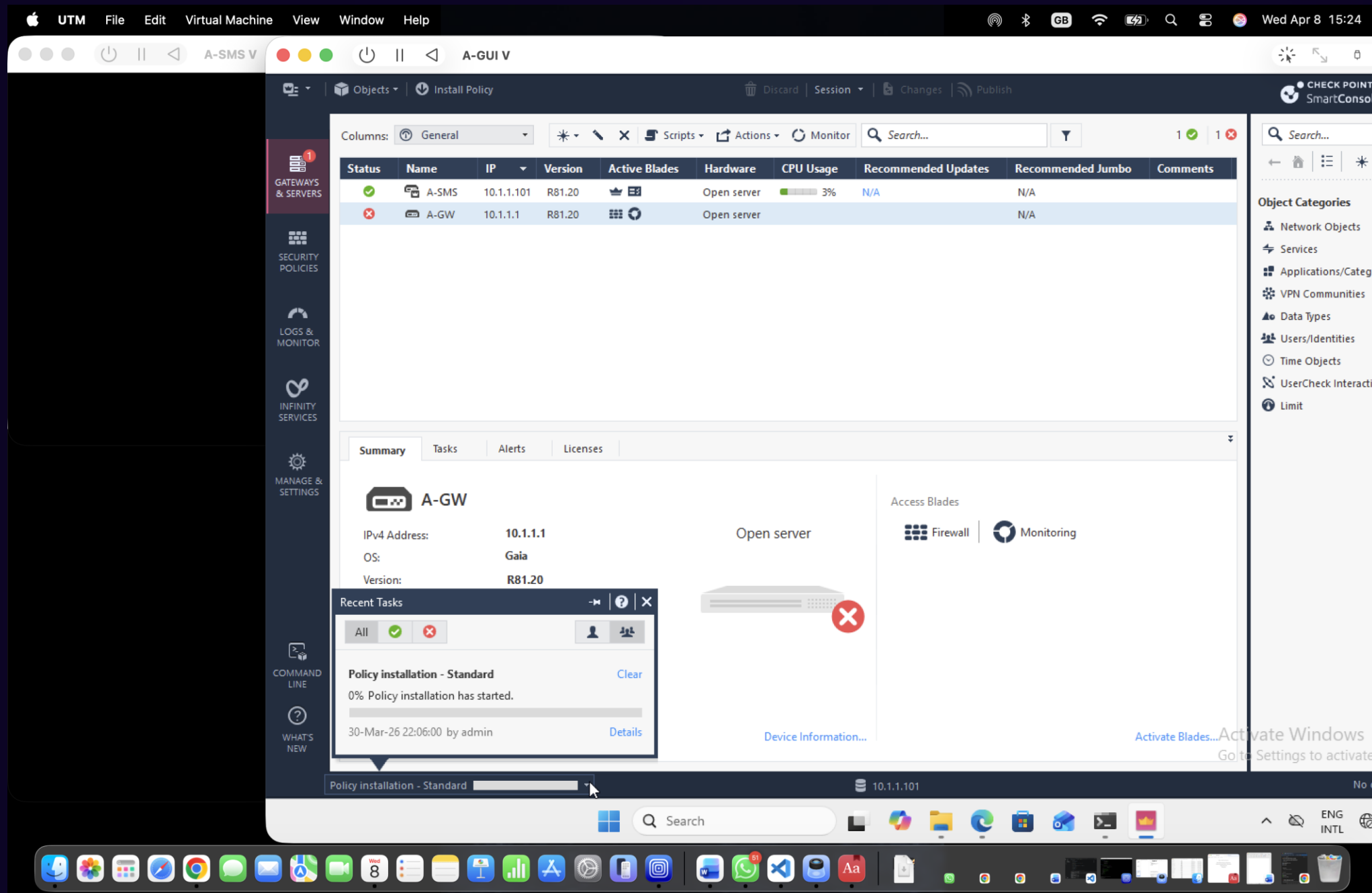


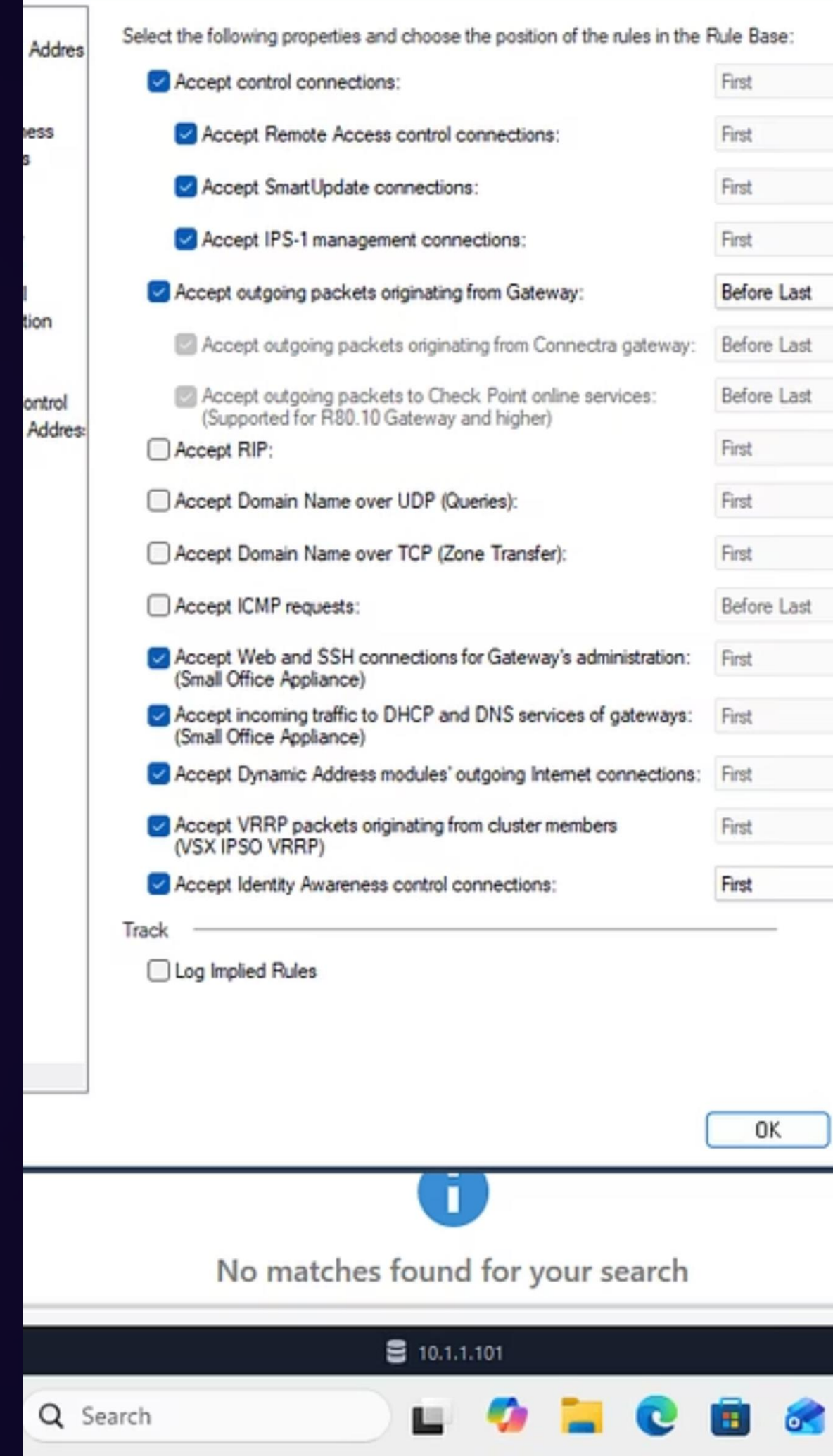
Figure 8: Policy installation progress and deployment — Demonstrates the automated policy compilation and installation workflow to the Security Gateway

Policy installation translates the configured rules into gateway-executable format, ensuring consistent enforcement across all security layers. The installation process validates syntax and deploys policies atomically to prevent partial or inconsistent rule application.

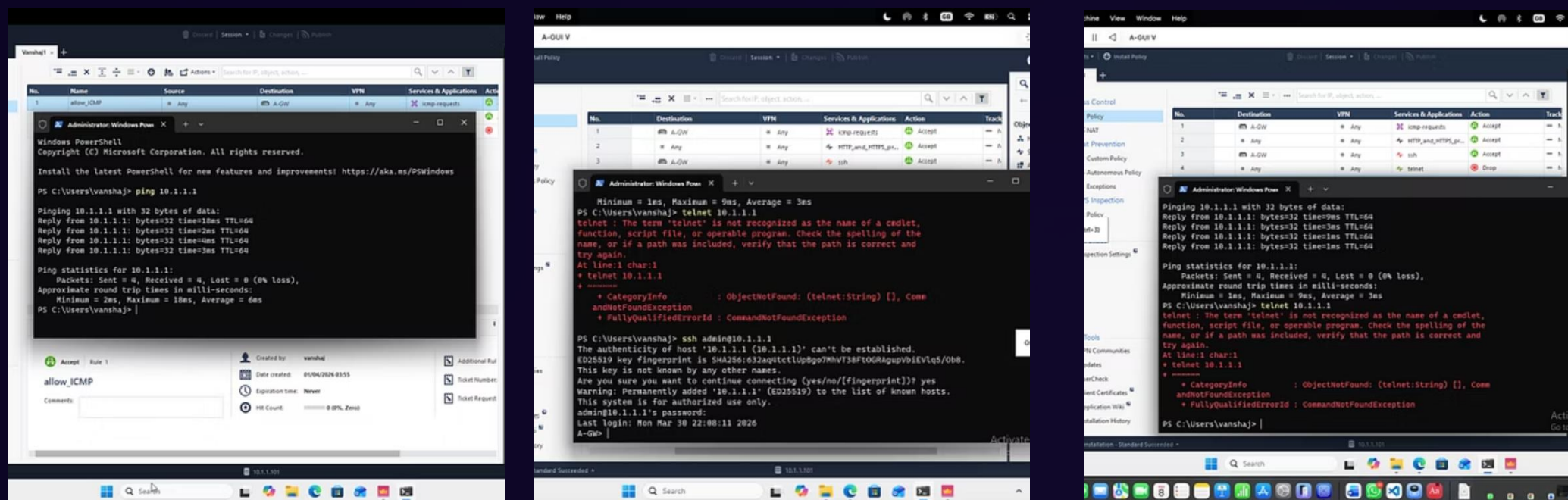
Global Properties & Default Rules

- Implied rules define default **security behaviour** for unmatched traffic
- Ensures consistent enforcement across all policy layers
- **Global Properties** define implied rules such as management access and system-level permissions
- These rules operate in the background and ensure baseline connectivity for essential services

 **Figure 7:** Global Properties and default rule configuration — *Screenshot 2026-04-24 at 12.15.33.png*



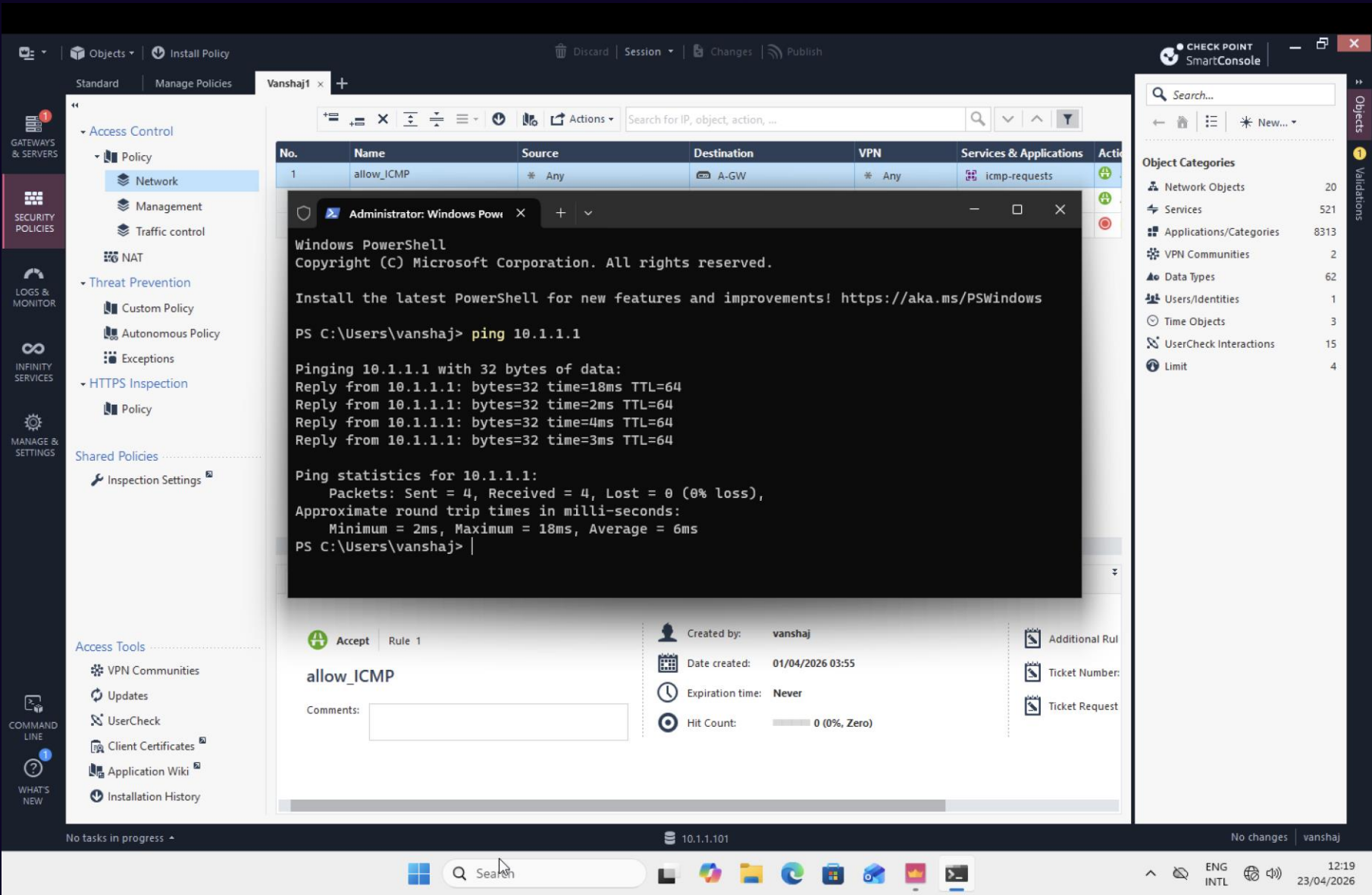
Policy Implementation — Verification Results



- **ICMP** — Ping successful; connectivity rule validated
- **SSH** — Secure remote login established
- **HTTP/HTTPS** — Web access permitted
- **Telnet** — Blocked; insecure protocol denied

i **Figures 8–11:** Implementation verification — *ICMP-implimentation.png*, *ssh.jpeg*, *http.png*, *telnet-block.png*

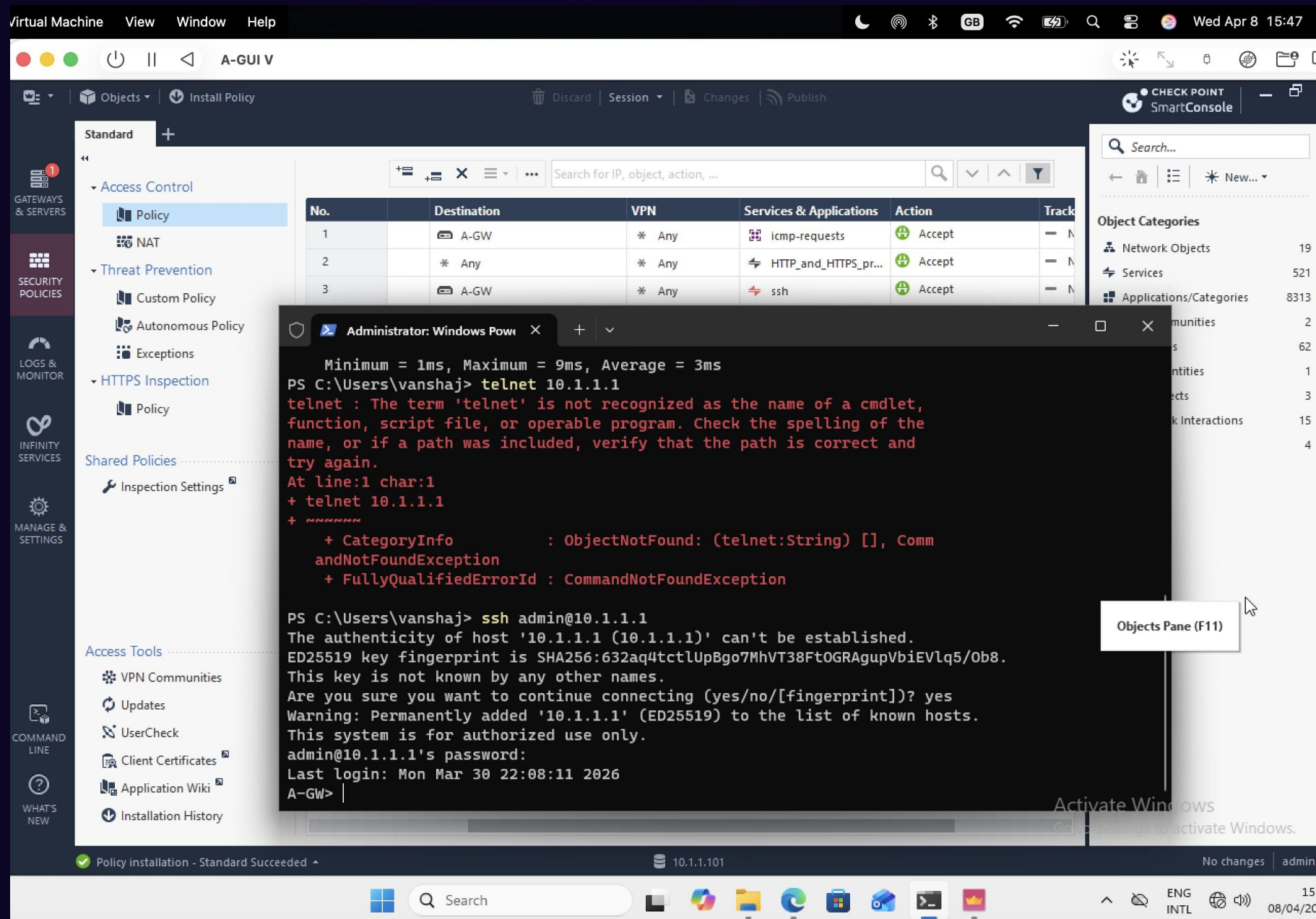
ICMP Rule Verification



This rule allows ICMP traffic to enable network connectivity testing using ping. ICMP is essential for network diagnostics and troubleshooting, allowing administrators to verify reachability between hosts.

Figure X: ICMP rule configuration — Shows the allow_ICMP rule permitting ping and network diagnostics

SSH Access Verification

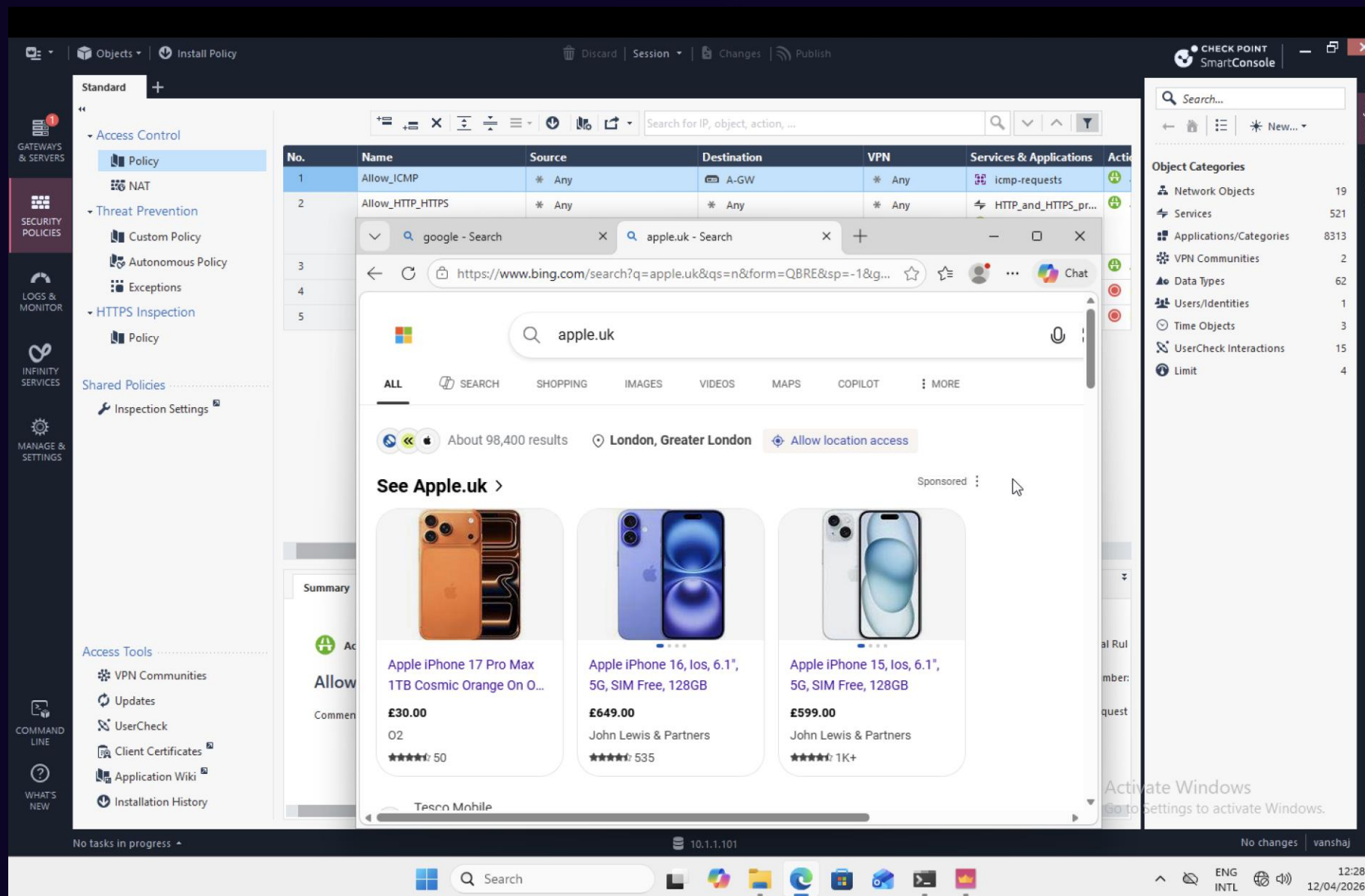


Demonstrate successful SSH secure remote access through the firewall.

This demonstrates that SSH (Secure Shell) traffic is successfully allowed through the firewall. SSH provides encrypted remote access, replacing insecure protocols like Telnet. The policy permits SSH connections while maintaining strong encryption and authentication, enabling secure administrative access to network devices.

SSH access verification — Terminal successfully establishing encrypted SSH connection through the firewall

HTTP/HTTPS Access Verification

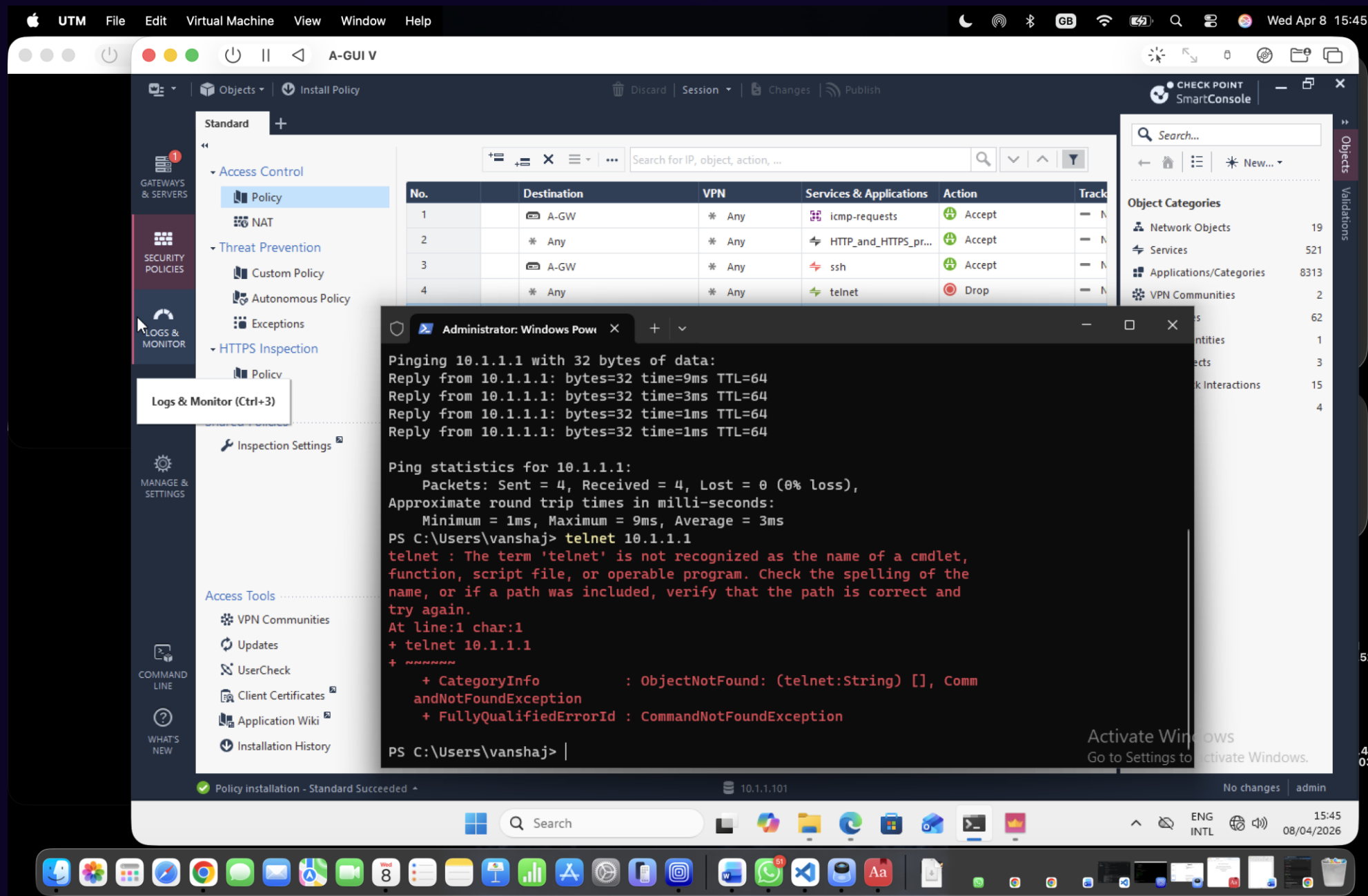


This demonstrates that HTTP/HTTPS traffic is successfully allowed through the firewall. Web access is a critical business function, and the policy permits legitimate web browsing while maintaining security controls.



Figure X: HTTP/HTTPS access verification — Browser successfully accessing web content through the firewall

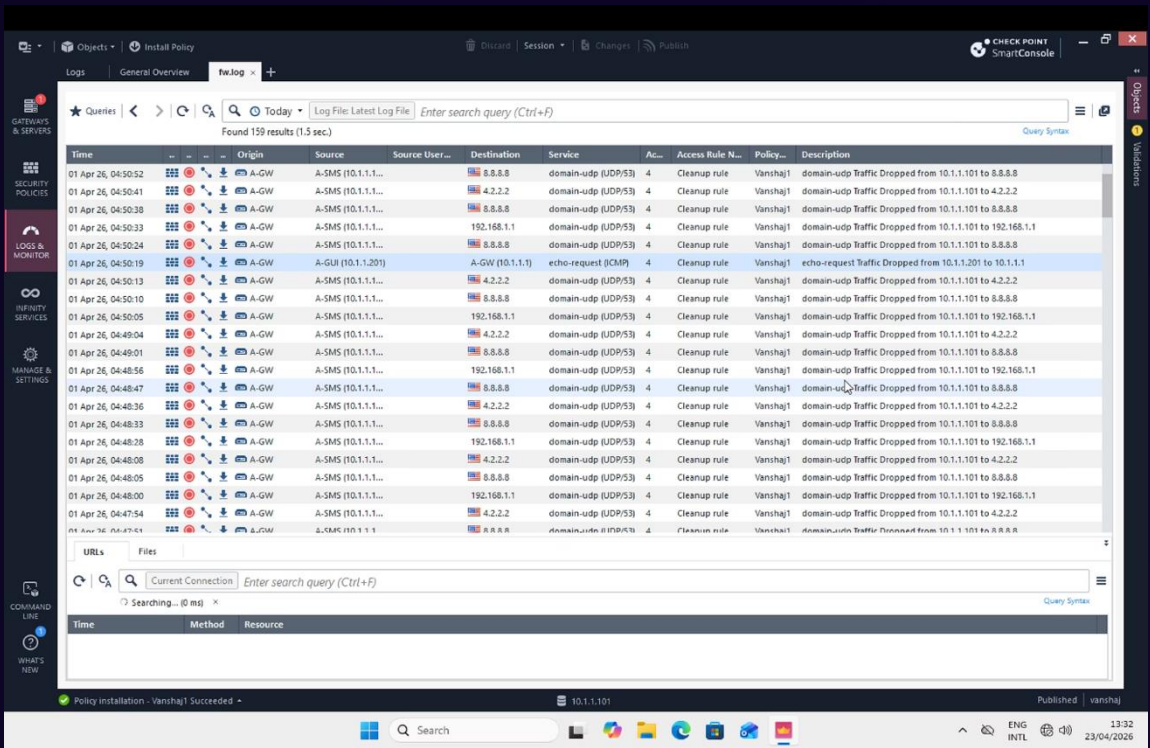
Telnet Traffic Blocked



The firewall successfully blocks insecure Telnet traffic, enforcing security policy. Telnet transmits credentials in plaintext and is considered a critical security risk. The policy explicitly denies Telnet connections, forcing users to adopt secure alternatives such as SSH.

Figure 13: Telnet traffic blocked — PowerShell error confirming firewall denial of Telnet connection attempts

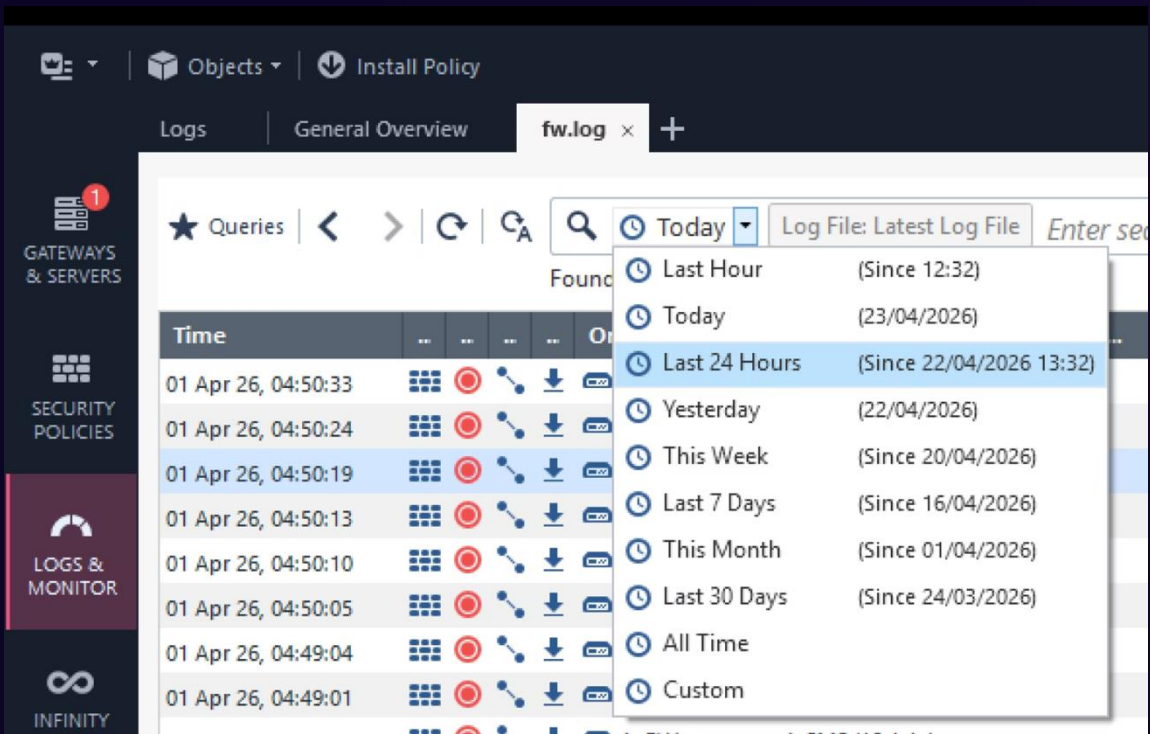
Logs, Monitoring & Threat Prevention



Log Analysis

- Real-time monitoring of **dropped** and accepted traffic with comprehensive log analysis for forensic investigation and threat detection [3]
- Rule-matching verification and ICMP log review

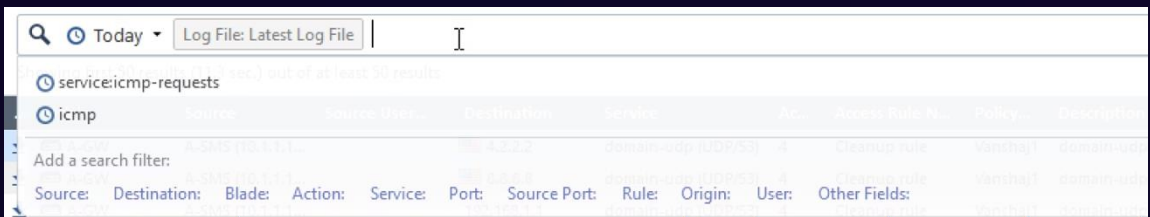
Figure 12: Real-time log view — *logs.png*



Log Filtering

- Filters isolate specific events for targeted analysis

Figure 13: Log filter interface — *filter.png*



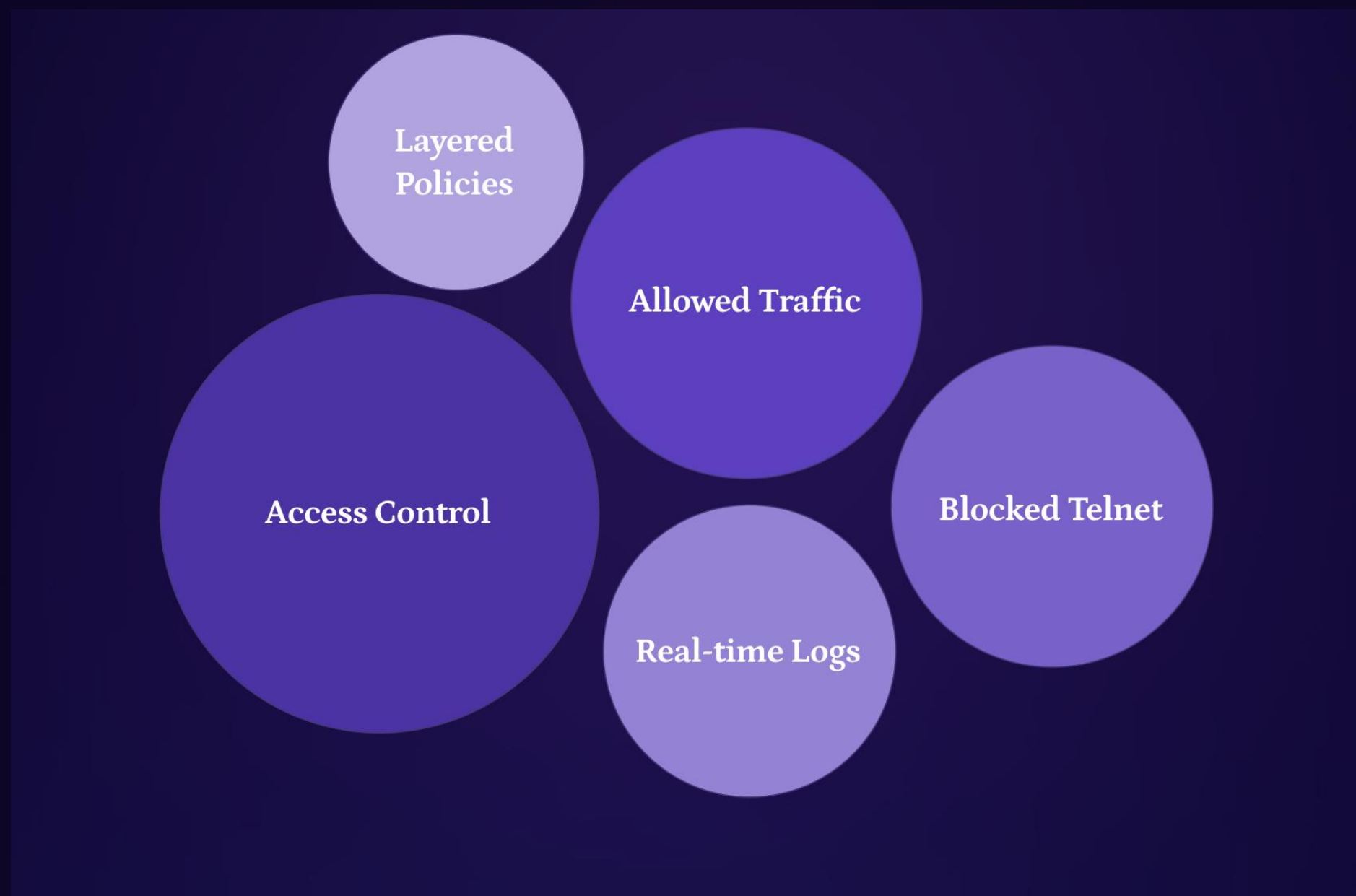
Specific Search

- Targeted queries locate individual events for forensic review

Figure 14: Specific log search — *specific-search.png*

Results & Key Outcomes

- Firewall rules successfully enforced network access control
- ICMP, SSH, and HTTP traffic were allowed as configured
- Insecure Telnet traffic was blocked by the firewall
- Logs confirmed real-time monitoring and rule enforcement
- Multi-layered policy improved security and network segmentation



References

- [1] W. Stallings, Network Security Essentials, 6th ed., Pearson, 2017.
- [2] Check Point Software Technologies, "Check Point Security Management Documentation," 2024.
- [3] NIST, "Guide to Firewall and Policy Management," 2022.

The background of the slide features a dark blue gradient. In the center, there is a faint, light blue graphic of a shield with a keyhole at the top, overlaid with a circuit board pattern of thin, wavy lines.

Thank You

Securing networks is not just implementation
— it is responsibility, precision, and continuous vigilance.

Presented by: Vanshaj Patel