

Enterprise Network Security

Applied Network Security: Securing the Enterprise with Check Point GAIA

Module: ACCA7032 – Enterprise Network Security

Programme: MSc Cybersecurity and Digital Forensics

Student ID: 2503493

April 2026 | Vaishnavi Patel

What We'll Cover Today

01 Network Topology Overview

Two sites, VMs and the security architecture

02 Installing Check Point GAIA Appliances

A-SMS & A-GW: OS install, FTCW, IP addressing

03 SmartConsole Setup & Licensing

R81.20 login, gateway/SMS objects, licence verification

04 Connectivity – SMS ↔ Swansea

SIC and management connectivity between appliances

05 Firewall Policy & Rules

10 access-control rules: HTTPS, DNS, SSH, P2P, cleanup

06 Additional Security Features

IPS blade, threat prevention, network objects & identity

07 Summary & Justification

Why these choices matter for enterprise security

Network Topology Overview

Two-site enterprise: SWANSEA.ACCA and LONDON.SWANSEA.ACCA connected via site-to-site VPN, secured by Check Point GAIA appliances [1].

Swansea Site – SWANSEA.ACCA

192.168.1.x

A-GW (Security Gateway) – 10.1.1.1

A-SMS (Mgmt Server) – 10.1.1.101

A-GUI (SmartConsole) – 10.1.1.201

S-DC – 192.168.1.1 (DNS, AD, DHCP, IIS)

ClientS1 – 192.168.1.10

London Site – LONDON.SWANSEA.ACCA

192.168.2.x • VPN S2S to Swansea

L-CD – 192.168.2.1 / 20.0.0.2

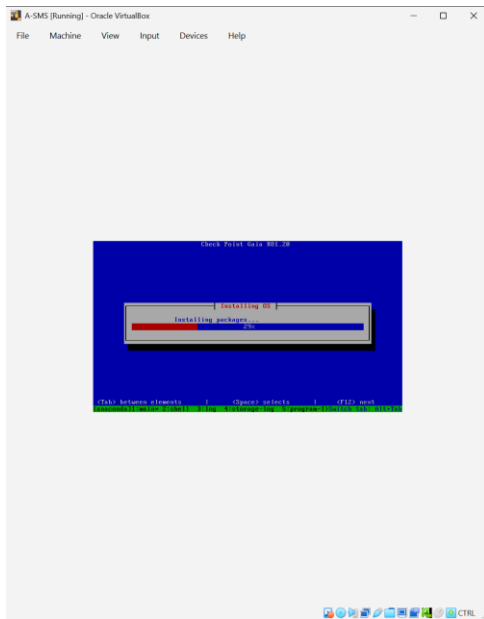
ClientL1 – 192.168.2.10

Core Services

DNS • Active Directory • DHCP • IIS • VPN • Firewall

Installing Check Point GAIA R81.20

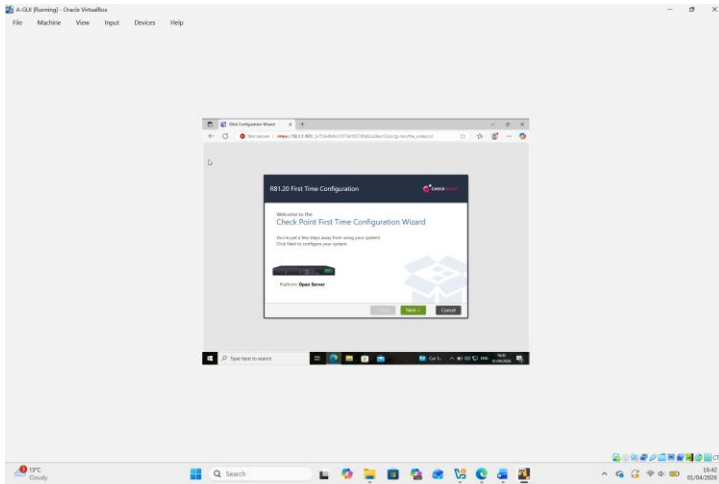
A-SMS (Security Management Server) — OS installation via VirtualBox



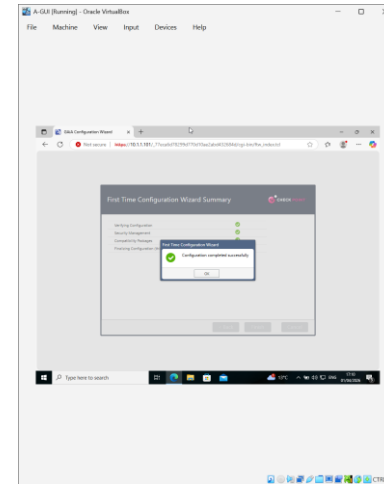
Installation Steps [2]

1. VirtualBox VM: 4GB RAM, 2 vCPUs, 60GB disk
2. Check Point Gaia R81.20 ISO attached and booted
3. Installation type: Security Management Server
4. Packages installing... (29% progress shown)
5. Post-install: system reboot, web portal accessible

First Time Configuration Wizard (FTCW)



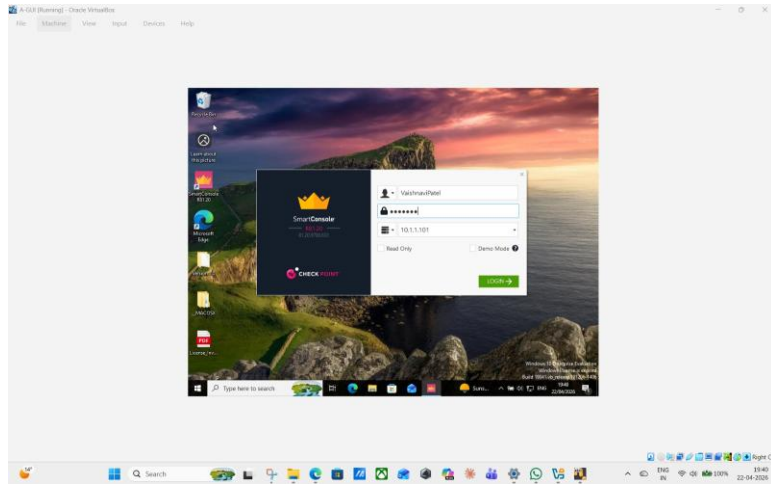
FTCW Welcome – A-SMS IP: 10.1.1.101



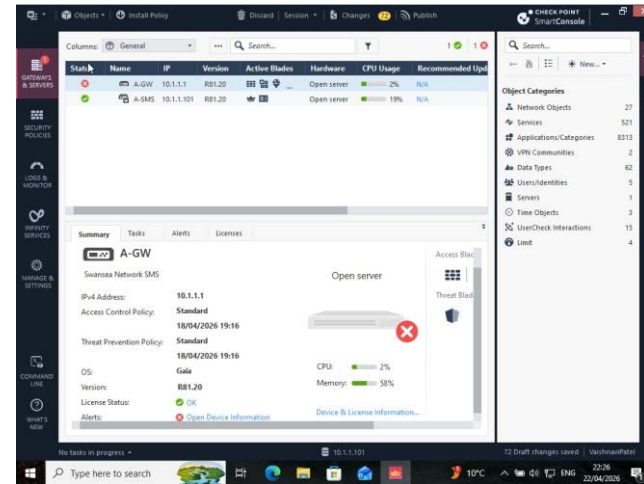
Configuration completed successfully ✓

Key steps: Network interface IP → Hostname → DNS → SIC activation key (Chkp!234) → Product selection (Security Management) → Finalize. Both A-SMS and A-GW completed FTCW successfully [2].

SmartConsole R81.20 – Login & Gateway Objects



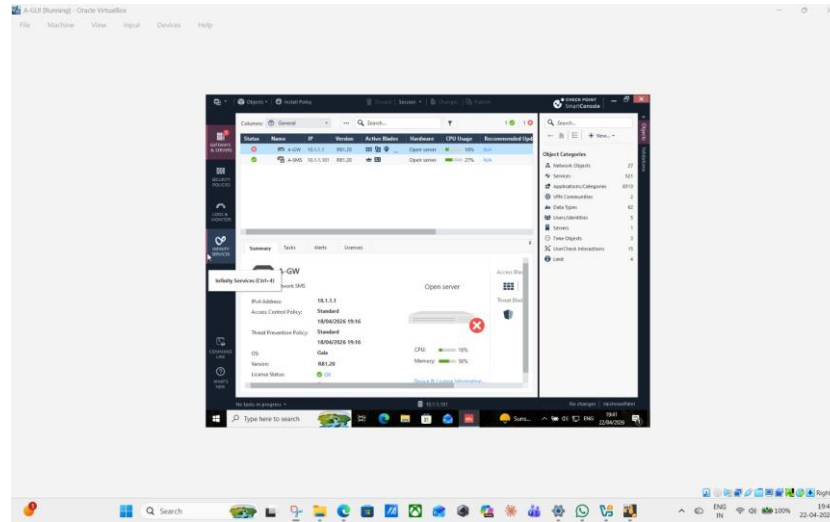
SmartConsole login – VaishnaviPatel, 10.1.1.101



A-GW: 10.1.1.1, R81.20, Licence OK

Both A-GW (10.1.1.1) and A-SMS (10.1.1.101) in Gateways & Servers view. Licence OK. SIC established via shared activation key [1][2].

Licensing the Check Point SMS & Gateway

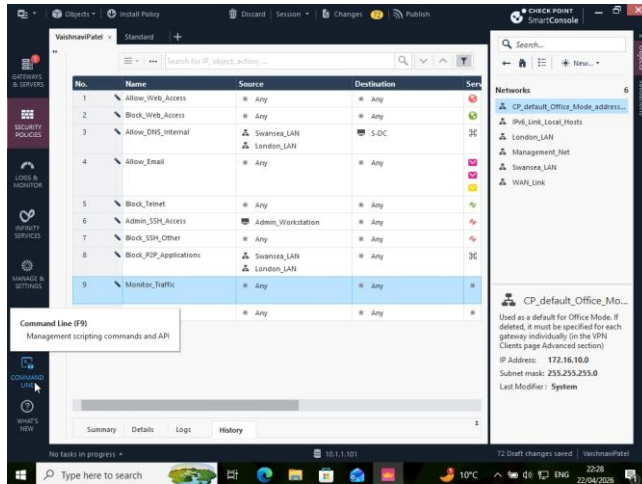


SmartConsole – A-GW Licence Status: OK, Access Control Policy: Standard, 18/04/2026

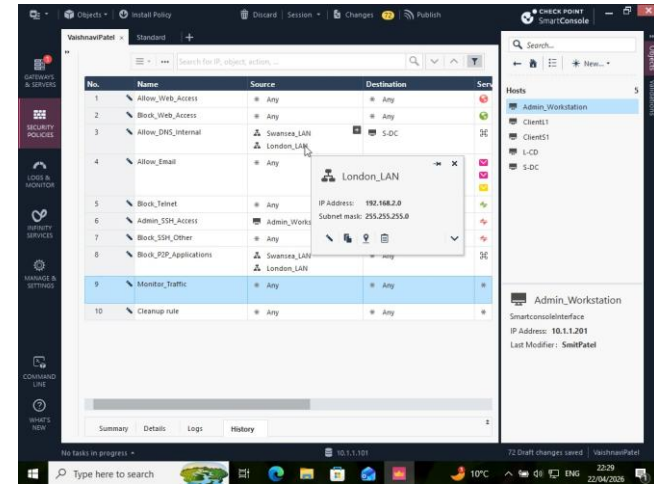
Licence applied per Check Point portal guidelines [1]. **A-GW Licence: OK ✓ A-SMS Licence: OK ✓**

Policies deployed: Access Control (Standard), Threat Prevention (Standard), both dated 18/04/2026.

Network Objects & Identity Configuration



Networks: Swansea_LAN, London_LAN, Management_Net

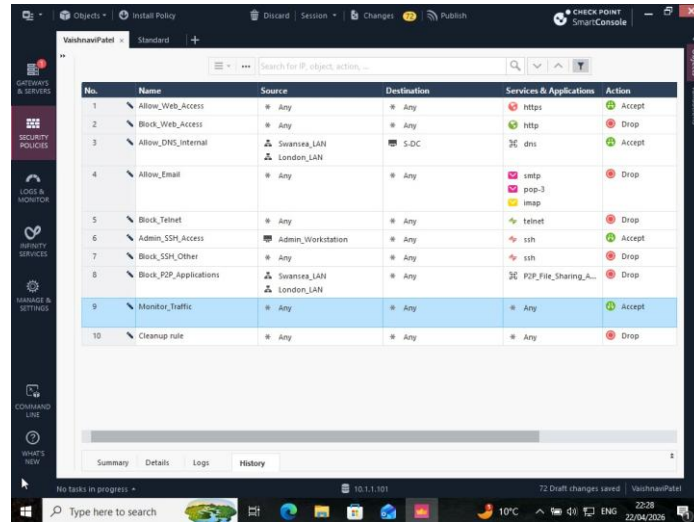


London_LAN (192.168.2.0/24) + Admin_Workstation

Network objects: Swansea_LAN, London_LAN.

Hosts: Admin_Workstation, ClientL1, ClientS1, L-CD, S-DC [1].

Firewall Policy – Access Control Rules



No.	Name	Source	Destination	Services & Applications	Action
1	Allow_Web_Access	* Any	* Any	https	Accept
2	Block_Web_Access	* Any	* Any	http	Drop
3	Allow_DNS_Internal	Swamesa_LAN London_LAN	5-DC	dns	Accept
4	Allow_Email	* Any	* Any	smtp-pop-3 imap	Drop
5	Block_Telnet	* Any	* Any	telnet	Drop
6	Admin_SSH_Access	Admin_Workstation	* Any	ssh	Accept
7	Block_SSH_Other	* Any	* Any	ssh	Drop
8	Block_P2P_Applications	Swamesa_LAN London_LAN	* Any	P2P_File_Sharing_A...	Drop
9	Monitor_Traffic	* Any	* Any	* Any	Accept
10	Cleanup rule	* Any	* Any	* Any	Drop

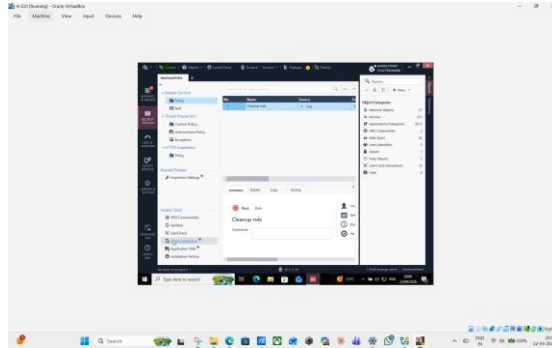
SmartConsole – VaishnaviPatel, 72 draft changes, 22/04/2026

10 rules: HTTPS allowed, HTTP blocked, DNS from internal LANs, SSH to Admin WS only, Telnet/P2P blocked, cleanup drops unmatched [3][4].

Rule Justification – Why Each Rule Exists

1	Allow_Web_Access	Permits users to browse websites, but only over HTTPS (secure/encrypted), plain HTTP is blocked.
2	Block_Web_Access	Blocks all plain HTTP (unencrypted) web traffic, forcing users to only use secure HTTPS connections.
3	Allow_DNS_Internal	Allows devices inside the network to translate website names (like google.com) into IP addresses but only using the internal DNS server (S-DC).
4	Allow_Email (Drop)	SMTP/POP3/IMAP dropped. No mail server – reduces attack surface. [4]
5	Block_Telnet	Telnet sends credentials in plaintext. Blocked globally. [3]
6	Admin_SSH_Access	SSH only from Admin_Workstation (10.1.1.201). Least privilege. [4]
7	Block_SSH_Other	All other SSH dropped. Prevents lateral movement. [4]
8	Block_P2P_Apps	P2P blocked – mitigates exfiltration and malware vectors. [3]
9	Monitor_Traffic	Accept + log for any/any. Full visibility before cleanup. [1]
10	Cleanup Rule	Implicit deny-all. Unmatched traffic dropped – defence in depth. [4]

Additional Security Features – Threat Prevention



IPS Blade [5]

Intrusion Prevention System enabled. Signature-based detection of exploits.

Anti-Virus / Anti-Bot [6]

Real-time file inspection and C&C callback detection.

Threat Prevention Policy [5]

Standard policy applied 18/04/2026. Custom layer available.

HTTPS Inspection [3]

Encrypted traffic inspection. Prevents hidden payloads in TLS.

Identity Awareness [7]

UserCheck configured. Rules tied to AD user/group identity.

Summary – What Was Delivered

Check Point GAIA Appliances Deployed

Installed A-SMS (10.1.1.101) and A-GW (10.1.1.1) on VirtualBox VMs, Gaia R81.20. Completed FTCW, assigned correct IPs.

SmartConsole Configured & Licences Applied

SmartConsole R81.20 on A-GUI (10.1.1.201). Registered objects, verified licence OK, confirmed SIC trust.

10 Firewall Rules Defined & Justified

HTTPS allow, HTTP block, internal DNS, email drop, Telnet drop, SSH restricted, P2P block, monitoring, cleanup.

Additional Security Features Enabled

IPS, Anti-Virus/Anti-Bot activated. Threat Prevention applied. HTTPS Inspection. Identity Awareness configured.

References

IEEE Citation Format

[1] Check Point, "R81.20 Security Management Administration Guide," 2023.

[2] Check Point, "R81.20 Gaia Administration Guide," 2023.

[3] W. Stallings, Network Security Essentials, 6th ed. Pearson, 2017.

[4] NIST, "Guidelines on Firewalls and Firewall Policy," SP 800-41 Rev. 1, 2009.

[5] Check Point, "IPS Administration Guide R81.20," 2023.

[6] Check Point, "Threat Prevention Administration Guide R81.20," 2023.

[7] Check Point, "Identity Awareness Administration Guide R81.20," 2023.

Thank You

Questions & Answers

Module: ACCA7032 Enterprise Network Security

Student: Vaishnavi Patel | 2503493

Lecturer: Renuga Jayakumar

MSc Cybersecurity and Digital Forensics | University of Wales Trinity Saint David | April 2026