

Part 2 - Securing the Enterprise Network

Check Point SmartConsole, firewall policy and secured topology

Demonstration Link: [Recording 2026-08-11 225806.mp4](#)

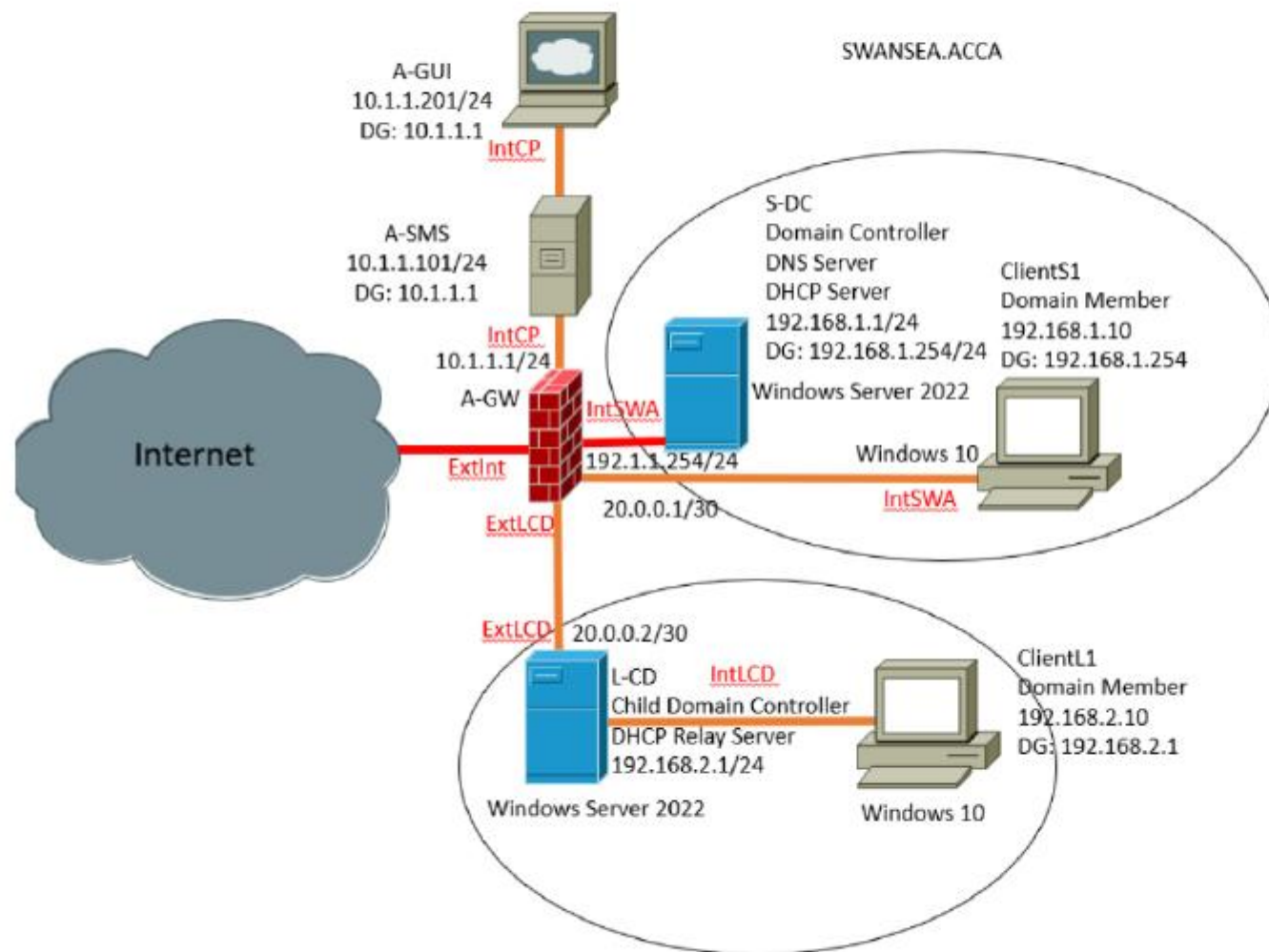
Harsh Valand

Student ID: 2437861

University of Wales Trinity Saint David

Academic evidence report | August 2026

Part 2 Securing Enterprise Network



Network context

The lab places A-GW at the perimeter and uses A-SMS and A-GUI for central policy administration.

- Management segment: 10.1.1.0/24.
- Swansea parent domain: 192.168.1.0/24.
- Child domain: 192.168.2.0/24.
- Routed transit between parent and child infrastructure: 20.0.0.0/30.
- Task 3 introduces stronger trust boundaries, a DMZ, remote-access controls and central monitoring.

Figure 1. Existing topology reproduced in full; no image content has been cropped.

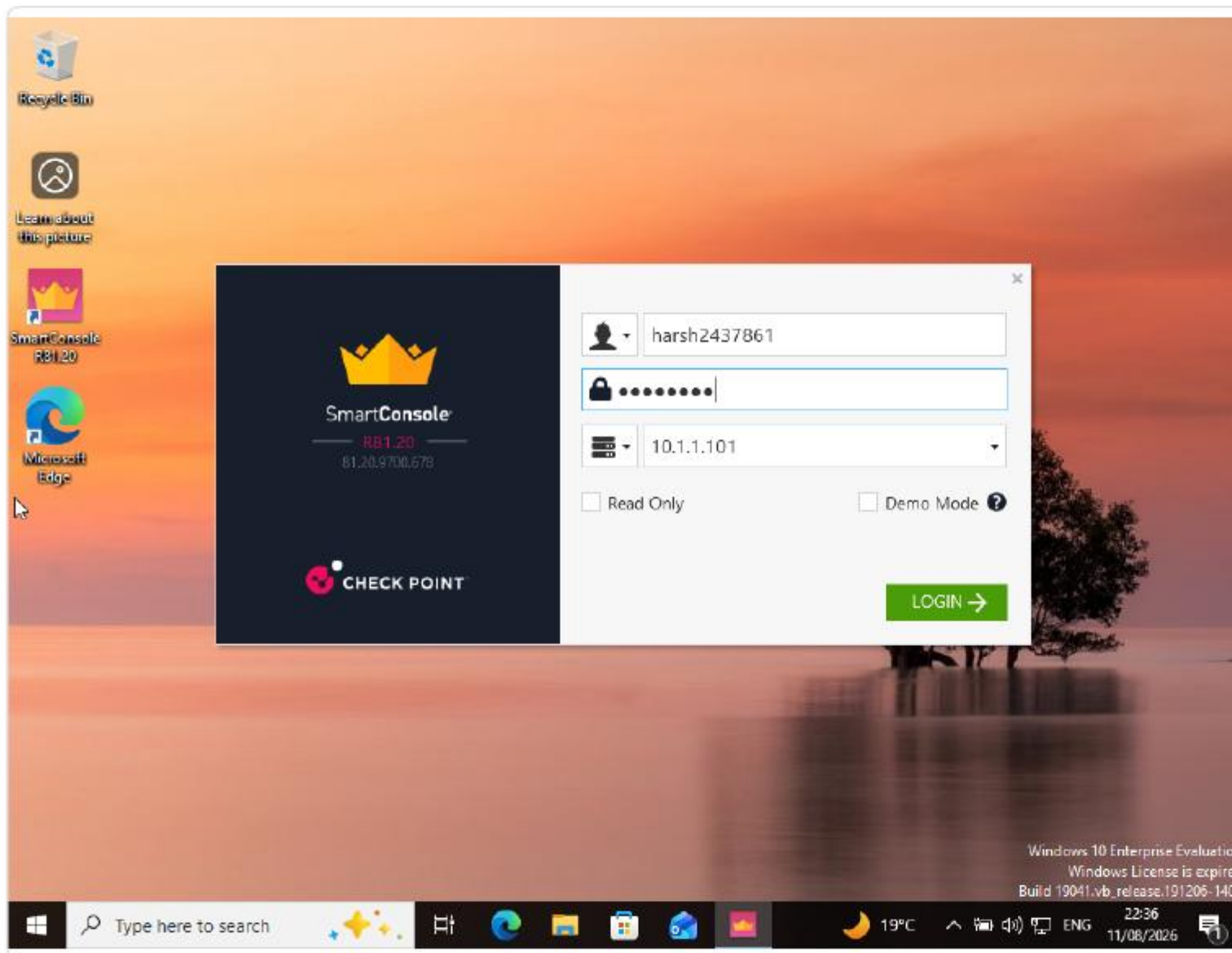


Figure 2. SmartConsole R81.20 login to the management server at 10.1.1.101. The screenshot is shown in full.

Interpretation

The login screen confirms the intended management endpoint and administrator workflow.

- Use named administrator accounts rather than shared credentials.
- Protect login with MFA, strong password policy and a restricted management network.
- Keep SmartConsole and Gaia management services patched to a supported release.

The screenshot displays the Check Point SmartConsole interface. The top navigation bar includes 'Objects', 'Install Policy', 'Discard', 'Session', 'Changes', and 'Publish'. The main content area shows a table of objects with columns: Status, Name, IP, Version, Active Blades, Hardware, CPU Usage, Recommended Updates, and Recommend. Two objects are listed: A-GW (IP: 10.1.1.1, Version: R81.20) and A-SMS (IP: 10.1.1.101, Version: R81.20). Below the table, the 'Summary' tab for the A-GW object is selected, showing details such as IPv4 Address (10.1.1.1), Access Control Policy (Standard), OS (Gaia), Version (R81.20), License Status (OK), and Alerts (OK). The 'Open server' status is indicated by a green checkmark. The bottom status bar shows 'No tasks in progress', the IP address '10.1.1.101', and the user 'Harsh2437861'.

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommend
✓	A-GW	10.1.1.1	R81.20	6	Open server	31%	N/A	N/A
✓	A-SMS	10.1.1.101	R81.20	1	Open server	6%	N/A	N/A

A-GW Summary:

- IPv4 Address: 10.1.1.1
- Access Control Policy: Standard
- OS: Gaia
- Version: R81.20
- License Status: OK
- Alerts: OK

Access Blades: Open server (6 blades)

Resource Usage: CPU: 31%, Memory: 39%

Buttons: Device & License Information..., Activate Blades...

Interpretation

A-GW is visible to SmartConsole with green operational, license and alert indicators.

- IPv4 address shown: 10.1.1.1; platform: Gaia; version: R81.20.
- The footer records Standard policy installation as succeeded, supporting A-SMS-to-A-GW connectivity.
- Continue monitoring CPU, memory, alerts and blade state after every policy change.

Figure 3. A-GW object summary and policy-installation success state. The screenshot is shown in full.

The screenshot shows the Check Point SmartConsole interface. The top navigation bar includes 'Objects', 'Install Policy', 'Discard', 'Session', 'Changes', and 'Publish'. The main content area displays a table of objects and a detailed summary for the A-SMS object.

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommend
✓	A-GW	10.1.1.1	R81.20	🔄	Open server	32%	N/A	N/A
✓	A-SMS	10.1.1.101	R81.20	👑	Open server	5%	N/A	N/A

The A-SMS object summary shows the following details:

- IPv4 Address:** 10.1.1.101
- OS:** Gaia
- Version:** R81.20
- License Status:** ✓ OK
- Alerts:** ✓ OK
- Open server** status with a green checkmark.
- CPU:** 5% (green bar)
- Memory:** 98% (red bar)
- Management Blades:** 👑 (Admin) and 📄 (Blades)
- Links:** Device & License Information..., Activate Blades...

The bottom status bar shows 'No tasks in progress', '10.1.1.101', 'No changes', and 'Harsh2437861'. The Windows taskbar at the bottom shows the date and time as 09/08/2025, 16:35.

Interpretation

A-SMS is shown as an open server on Gaia R81.20 with green license and alert indicators.

- IPv4 address shown: 10.1.1.101.
- The high memory reading visible in this capture should be investigated before production deployment.
- Restrict A-SMS administration to approved A-GUI hosts and back up the management database regularly.

Figure 5. A-SMS object summary in SmartConsole. The screenshot is shown in full.

The screenshot displays the Check Point SmartUpdate console. The 'Licenses & Contracts' tab is active, showing a list of machines and their associated licenses and contracts. Below this, the 'License And Contract Repository' table provides detailed information for each machine.

Attached	Machine	State	Upgrade St...	Version	IP Address	SKU	Description	Certificate ...	Name	Type	Expiration ...
Attached	A-GW			Software Bl...	10.1.1.101	CPSG-C-8-...	Security Ga...	68626899F...	CPSG-C-8-...	central	21Sep2026
Attached	A-SMS			Software Bl...	10.1.1.101	CPSM-C-5-...	Security M...	08D70EC82...	CPSM-C-5-...	local	never
Contract...	A-GW					CPSB-AV-E...		68626899F...	Contract H...	contract	17Sep2026
Contract...	A-GW					CPSB-APC...		68626899F...	Contract FI...	contract	17Sep2026
Contract...	A-GW					CPSB-ASP...		68626899F...	Contract 9...	contract	17Sep2026
Contract...	A-GW					CPSB-DLP...		68626899F...	Contract 8...	contract	17Sep2026
Contract...	A-GW					CPSB-TEX...		68626899F...	Contract A...	contract	17Sep2026

The 'Operation Status' section at the bottom is currently empty, showing columns for Operation, Status, Progress, and Time.

Interpretation

The repository lists installed products and contract information for the managed Check Point systems.

- Record SKU, enabled blades, support entitlement and expiration date for each appliance.
- Confirm that contracts cover signature, software and threat-prevention updates.
- Set renewal alerts before expiry to prevent protection or support gaps.

Figure 6. SmartUpdate license and contract repository for A-GW and A-SMS. The screenshot is shown in full.

Standard +

Search for IP, object, action, ...

No.	Name	Source	Destination	VPN	Services & Applicat...	Action
1	Block FTP	* Any	Internet swansea net	* Any	ftp	Drop
2	Allow HTTP	* Any	A-GW	* Any	http https	Accept
3	Allow Management	Internet London Net	A-GW	* Any	icmp-requests	Accept
4	Block telnet	Internet London Net	Internet swansea net	* Any	telnet	Drop
5	Allow SSH	A-GUI	Internet swansea net A-GW	* Any	ssh ssh_version_2	Accept

Missing cleanup rule - Unmatched traffic will be dropped and not logged.

Summary Details Logs History

Drop Rule 5

Allow SSH

Comments:

Created by: System

Date created: 17/11/2022 01:43

Expiration time: Never

Hit Count: 0 (0%, Zero)

Policy Installation - Standard Succeeded

10.1.1.101 No changes harsh2437861

22:59 11/08/2026

Interpretation

The rule base demonstrates explicit allow/drop decisions and logging for the selected services.

- Block Telnet because it transmits credentials and data without encryption.
- Prefer HTTPS over HTTP and SFTP/FTPS over standard FTP.
- Limit ICMP and SSH by source, destination and operational purpose; finish with a logged clean-up drop.

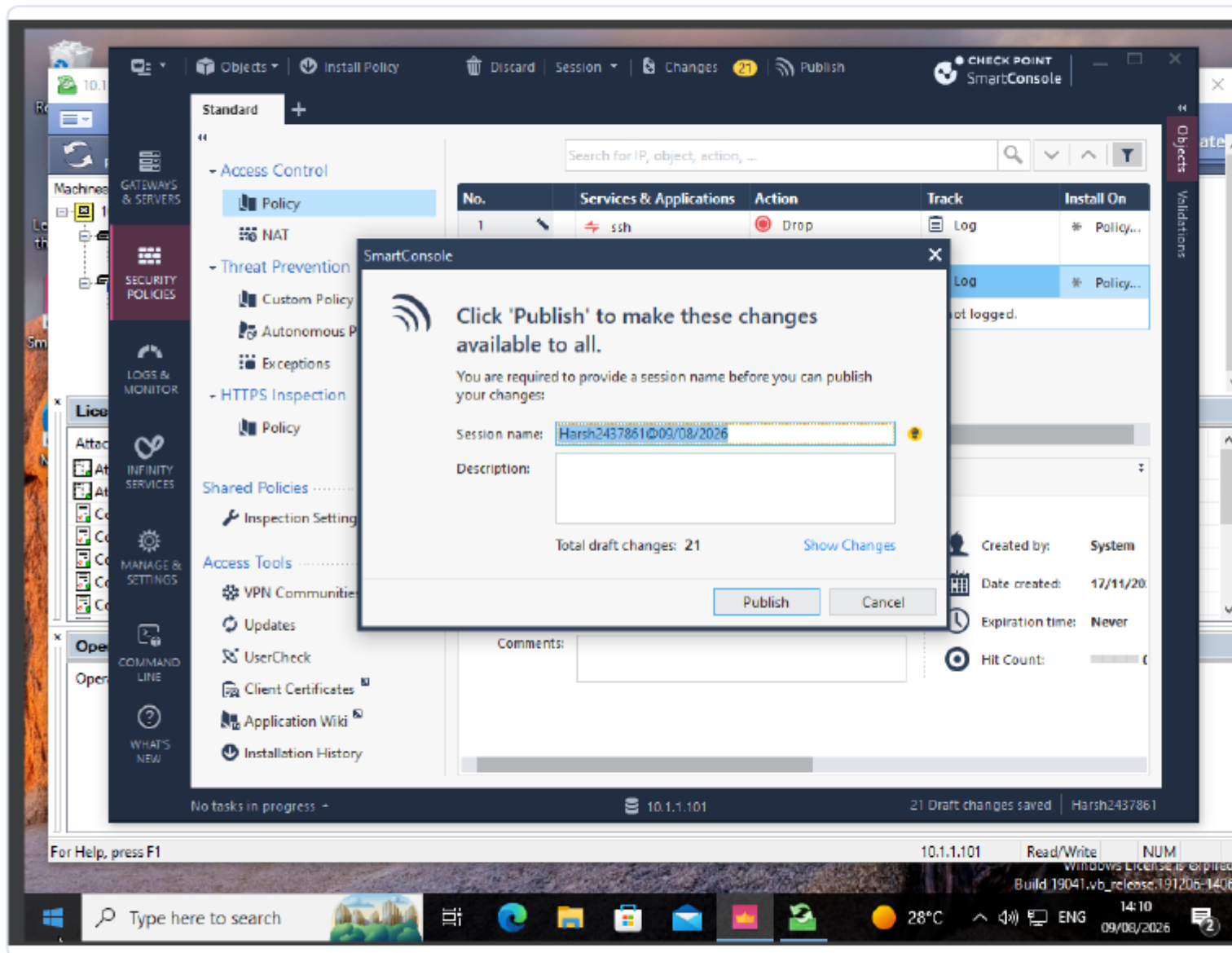
Figure 7. Ordered access-control rules for Telnet, HTTP, ICMP, FTP and SSH with tracking enabled. The screenshot is shown in full.

Protocol explanations

Protocol	Operational purpose	Security treatment
ICMP	Diagnostics and error reporting, including ping.	Permit only where monitoring or troubleshooting requires it; log unusual patterns.
FTP	Traditional file transfer using separate control and data channels.	Prefer SFTP or FTPS because standard FTP does not protect credentials or content.
HTTP / HTTPS	Web application traffic over TCP 80 / 443.	Redirect to HTTPS, inspect where authorised and restrict destinations by business need.
SSH	Encrypted remote login and command execution, normally TCP 22.	Allow only from named administration hosts; use key-based access and MFA where available.
Telnet	Legacy remote terminal protocol that transmits data in clear text.	Block and log; use SSH instead.

Policy design principles

- Apply specific source, destination and service objects; avoid broad Any rules; place explicit administrative rules before general rules; enable tracking; finish with a logged clean-up drop rule.

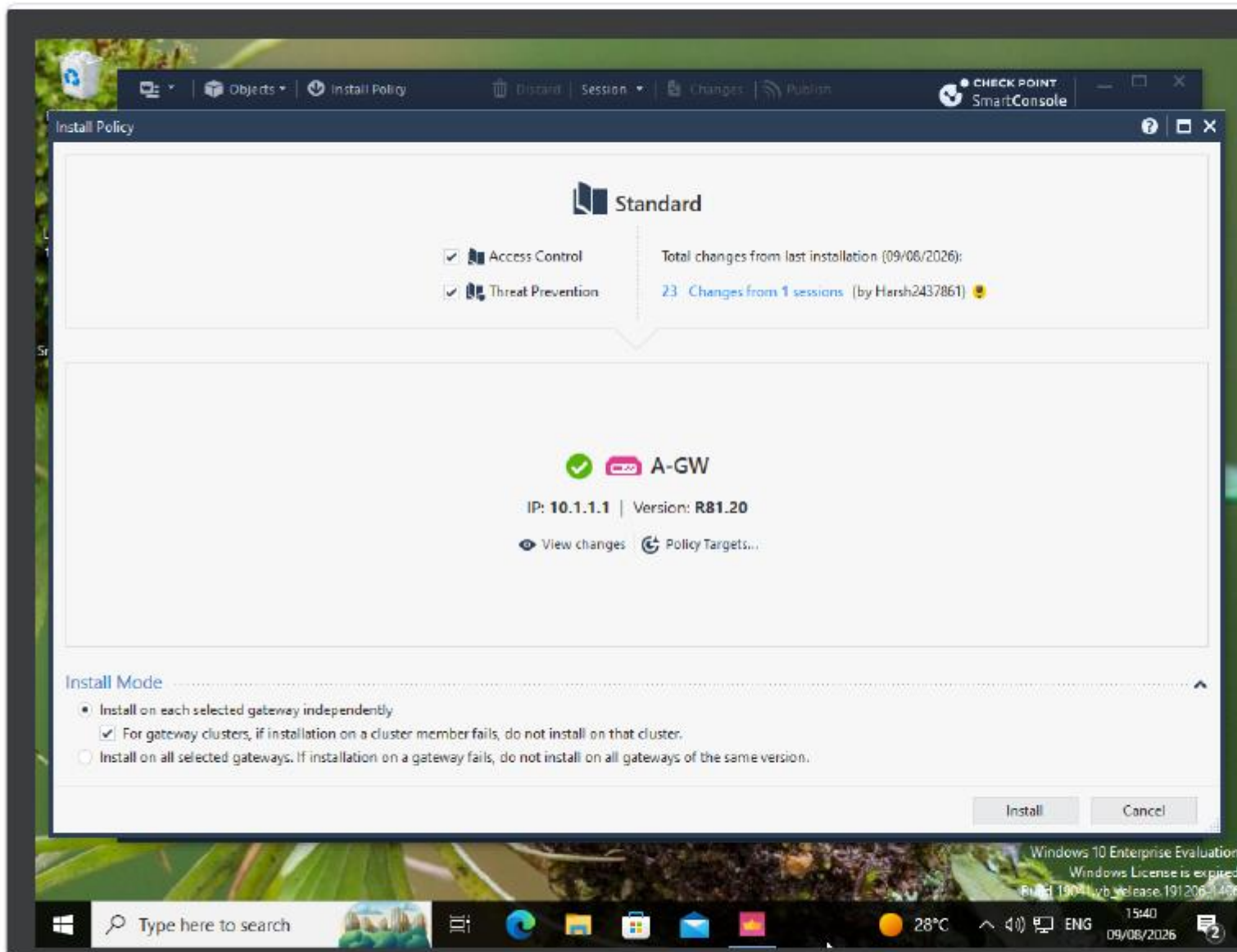


Interpretation

Publishing writes the session changes to the management database so they can be reviewed and installed.

- Use a meaningful session name and change description.
- Apply peer review and an approved change reference for production policy changes.
- Publishing does not enforce policy on A-GW until installation completes.

Figure 8. SmartConsole publish dialogue for the active policy session. The screenshot is shown in full.



Interpretation

The installation view associates the policy package with A-GW and shows Access Control and Threat Prevention changes.

- Confirm the correct package and gateway target before installation.
- Monitor validation warnings and installation status; Figure 3 records a successful Standard policy installation.
- Retain the prior policy version and a rollback plan for higher-risk changes.

Figure 9. Standard policy installation workflow targeting A-GW. The screenshot is shown in full.

The screenshot shows the SmartConsole interface with the following data:

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...
5:43	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	ssh_version_2 (TCP/22)	5	Allow SSH	Standard
5:38	A-GW							
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard
2:53	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP	Standard

The bottom section shows a search for 'Current Connection' with 0 results.

Interpretation

Mixed actions show that the policy both permits authorised flows and blocks prohibited traffic.

- Investigate repeated drops, unexpected administration attempts and unusual service patterns.
- Correlate gateway events with Windows, DNS, authentication and endpoint telemetry in a SIEM.
- Tune alerts without disabling the underlying log evidence.

Figure 11. SmartConsole log view containing both accepted and dropped events. The screenshot is shown in full.

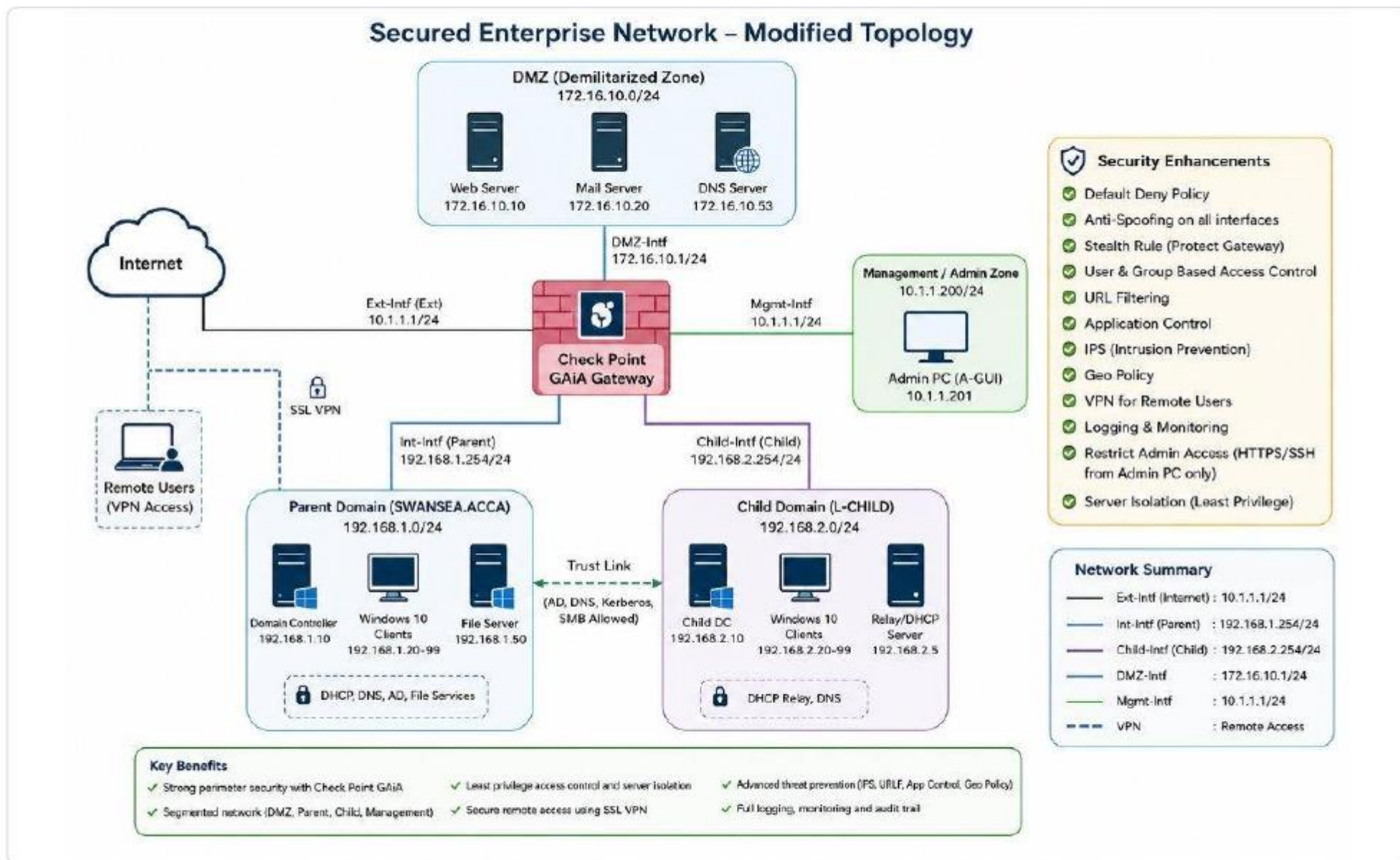


Figure 14. Secured enterprise topology from the reference work, reproduced in full without cropping.

The modified design converts a largely trusted lab network into explicit security zones.

Task 3 augments the original topology with layered prevention, controlled administration, safer remote access and central monitoring. The changes retain the parent and child domain services while reducing direct exposure and lateral movement.

Original exposure	Security improvement introduced
Broad perimeter trust	Default-deny enforcement, a gateway stealth rule and anti-spoofing on every interface
Public and internal services share trust	A dedicated DMZ for web, mail and DNS services, separated from domain systems
Administrative access is insufficiently bounded	A management zone, named administrators, MFA and HTTPS/SSH from approved hosts only
Limited detection and response	IPS, Anti-Virus, Anti-Bot, URL filtering, Application Control and centralised logging/SIEM
Remote access is not explicitly protected	SSL VPN with MFA, device checks and least-privilege authorisation

Implementation principle

- Each routed interface must use a unique subnet, and every allowed flow should have a documented business purpose, explicit objects and enabled logging.

Segmentation and perimeter

- A-GW separates Internet, management, parent-domain, child-domain and DMZ trust zones.
- The DMZ isolates public web, mail and DNS services from internal domain systems.
- Default deny, a gateway stealth rule and interface anti-spoofing reduce unauthorised access and address-forgery attacks.

Threat prevention and access

- IPS, Anti-Virus, Anti-Bot, URL filtering and Application Control provide layered inspection beyond port-based filtering.
- User/group-based policy and least privilege limit server and administrative access to approved identities and devices.
- SSL VPN supports remote users; MFA and device posture checks should protect remote and administrator authentication.

Monitoring and resilience

- Log accept and drop events, centralise them in SmartConsole or a SIEM, and alert on repeated denials, malware indicators and administrative changes.
- Maintain backups, policy versions, tested recovery procedures, endpoint protection and a documented patching programme.
- Review licenses and contracts before expiry so security blades and updates remain available.

Validation note

- The supplied secured-topology figure labels both external and management interfaces as 10.1.1.1/24. Before implementation, assign unique non-overlapping subnets and addresses to every routed gateway interface.
- After correction, validate routing, NAT, DNS, anti-spoofing definitions and the rule base with authorised connectivity tests and log review.

Outcome: stronger access control, reduced lateral movement, protected public services and auditable security operations.

IMPLEMENTATION EVIDENCE COMPLETE

Thank you

Questions and discussion

Thank you for always being approachable, answering questions with patience, and providing valuable guidance whenever it was needed. Your support has given me confidence and motivation to achieve my best. I am truly grateful for everything you have done and greatly appreciate the effort you invest in your students' success.

Documented outcome

Centralised management, explicit firewall controls, successful policy publication and installation, operational logging, and a segmented secured topology are presented as one auditable implementation story.

Harsh Valand

Student ID: 2437861 | University of Wales Trinity Saint David