

Securing the Enterprise Network

Check Point SmartConsole configuration, policy evidence and improved topology

Hari Barot | 2520160

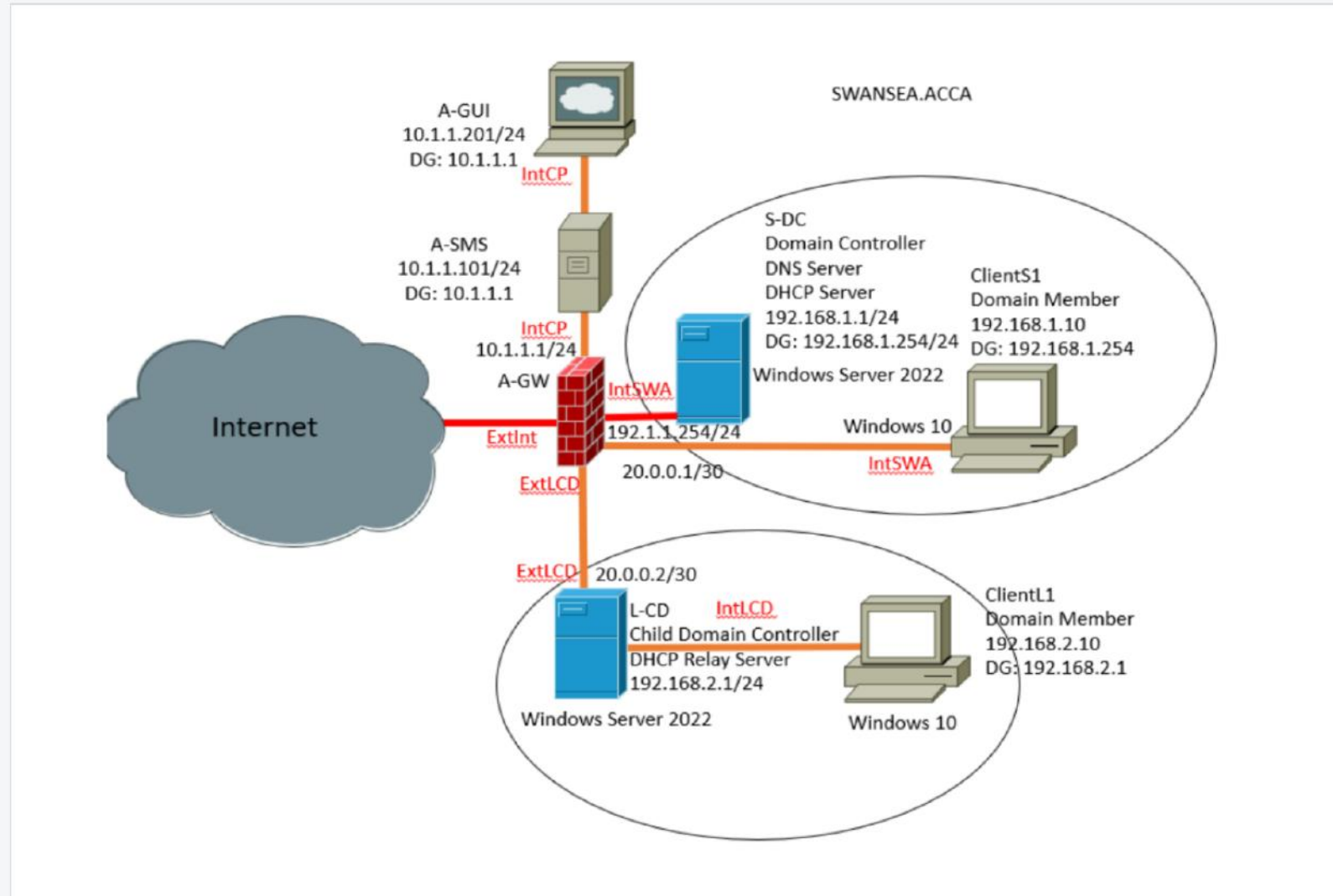
University of Wales Trinity Saint David

The evidence demonstrates a working centrally managed firewall

By the end of this report, the reader should understand how the configured gateway, management server, policy rules and monitoring evidence combine into a defensible enterprise security design.

1	Topology	Baseline architecture and the secured modified design
2	Management plane	A-GW and A-SMS status, Gaia version and licensing evidence
3	Access control	Management, SSH, FTP and ICMP policy intent
4	Deployment	Published policy and successful installation on A-GW
5	Assurance	Logs, network objects, host objects and identified control gaps

Baseline topology connects management and two domain networks



BASELINE OBSERVATIONS

- A-SMS centralizes policy management; A-GUI is the administrator workstation.
- A-GW provides the control point between the Internet and the internal networks.
- Parent and child domain networks are separated, but the design lacks a dedicated DMZ and explicit remote-access zone.
- The management subnet is security-critical and should permit only named administration flows.

A-GW and A-SMS are operational and centrally managed

The screenshot displays the Check Point SmartConsole interface. At the top, a table lists the licenses for A-GW and A-SMS. Below this, the configuration page for A-GW is shown, including details like IP address, access control policy, OS, version, and license status. The status bar at the bottom indicates that the policy installation was successful.

Status	Name	IP	Version	SKU	Account ID	Support Level	Support Expiration
✓	A-GW	10.1.1.1	R81.20	✓ OK			
✓	A-SMS	10.1.1.101	R81.20	✓ OK			

A-GW Configuration Details:

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

Access Blades: Firewall, Monitoring

System Health: CPU: 7%, Memory: 39%

Status Bar: Policy installation - Standard Succeeded

HEALTHY MANAGEMENT PLANE

The gateway and management server report green status.

- A-GW 10.1.1.1 and A-SMS 10.1.1.101 both show green status.
- A-GW runs Gaia R81.20; the capture shows 7% CPU and 39% memory use.
- License status is OK, and the status bar confirms a successful Standard policy installation.

SKU, account, support level and expiry are not visible. Record them separately for a complete licensing audit.

The initial rule permits management services and drops other traffic

No.	Destination	VPN	Services & Applications	Action	Track	Install On
1	A-GW	* Any	https http	Accept	Log	* Policy...
2	* Any	* Any	* Any	Drop	None	* Policy...

Summary | Details | Logs | History

Accept | Rule 1

Allow Management Allow

Comments:

Created by: hari2520160
 Date created: 09/08/2026 14:48
 Expiration time: Never
 Hit Count: 0 (0%, Zero)

Policy installation - Standard Succeeded

DEFAULT-DENY FOUNDATION

One logged allow rule sits above a catch-all drop rule.

- Rule 1 accepts HTTPS and HTTP to A-GW and records the connection in logs.
- Rule 2 drops Any-to-Any traffic, providing a clear default-deny boundary.
- The structure is easy to audit because the permitted exception precedes the cleanup control.

HTTP is clear text. Retain HTTPS only unless a documented legacy requirement exists.

Management access is constrained to A-GUI and A-GW

The screenshot displays the Check Point SmartConsole interface. The left sidebar contains navigation options: Gateways & Servers, Security Policies (selected), Logs & Events, Integration & Services, Manage & Settings, Command Line, and Whats New. The main pane shows a table of rules under the 'Standard' tab. Rule 1, 'Allow Management Allow', is selected. Below the table, the 'Summary' tab is active, showing details for Rule 1, including its name, comments, and creation information.

No.	Name	Source	Destination	VPN	Services & Applications
1	Allow Management Allow	A-GUI	A-GW	* Any	https http
2	Cleanup rule	* Any	* Any	* Any	* Any

Summary Details for Rule 1:

- Accept** | Rule 1
- Allow Management Allow**
- Comments:** [Empty text box]
- Created by:** hari2520160
- Date created:** 09/08/2026 14:48
- Expiration time:** Never
- Hit Count:** 0 (0%, Zero)
- Actions:** Addition, Ticket Nt, Ticket Re

At the bottom, a status bar indicates 'Policy installation - Standard Succeeded' and 'No changes'.

HOST-SPECIFIC ADMINISTRATION

The rule binds the admin workstation to the gateway.

- The source is A-GUI and the destination is A-GW, limiting who may administer the gateway.
- The selected rule exposes only HTTP and HTTPS rather than a broad service set.
- The rule has no expiry. Privileged access should have an owner, change reference and periodic review date.

Use HTTPS with MFA and strong administrator roles; remove HTTP from the permitted service list.

Logs prove that the HTTPS management rule is being used

fw.log

Queries | All Time | Log File: Latest Log File | Enter search query (Ctrl+F)

Found 49 results (1.3 sec.)

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:34	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:32	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:53:11	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...

URLs | Files

Current Connection | Enter search query (Ctrl+F)

Found 0 results (1.1 sec.)

No matches found for your search

Policy installation - Standard Succeeded

10.1.1.101 | No changes | hari2520160

CONFIGURATION BECOMES EVIDENCE

The log links A-GUI, A-GW, TCP/443 and the allow rule.

- The view reports 49 results and repeated HTTPS sessions from A-GUI 10.1.1.201.
- The destination is A-GW 10.1.1.1 and the service is HTTPS TCP/443.
- The Access Rule Name column associates traffic with the management allow rule.

Create saved filters and alerts for failed, unusual or out-of-hours administrator connections.

Successful installation activates the policy on A-GW

Standard Policy Rules:

No.	Destination	VPN	Services & Applications	Action	Track	Install On
1	* Any	* Any	telnet	Accept	None	* Policy...
2	A-GW	* Any	https, http	Accept	Log	* Policy...
3	* Any	* Any	* Any	Drop	None	* Policy...

Recent Tasks:

- Policy installation - Standard: Installation succeeded on A-GW (09-Aug-26 16:04:59 by hari2520160)
- Policy installation - Standard: Installation succeeded on A-GW (09-Aug-26 14:58:31 by hari2520160)
- Policy installation - Standard: Installation succeeded on A-GW (09-Aug-26 14:53:06 by hari2520160)
- Policy installation - Standard: Installation succeeded on A-GW (09-Aug-26 14:49:56 by hari2520160)

Policy Details:

- Created by: hari2520160
- Date created: 09/08/2026 14:56
- Expiration time: Never
- Hit Count: 0 (0%, Zero)

Status: Policy installation - Standard Succeeded

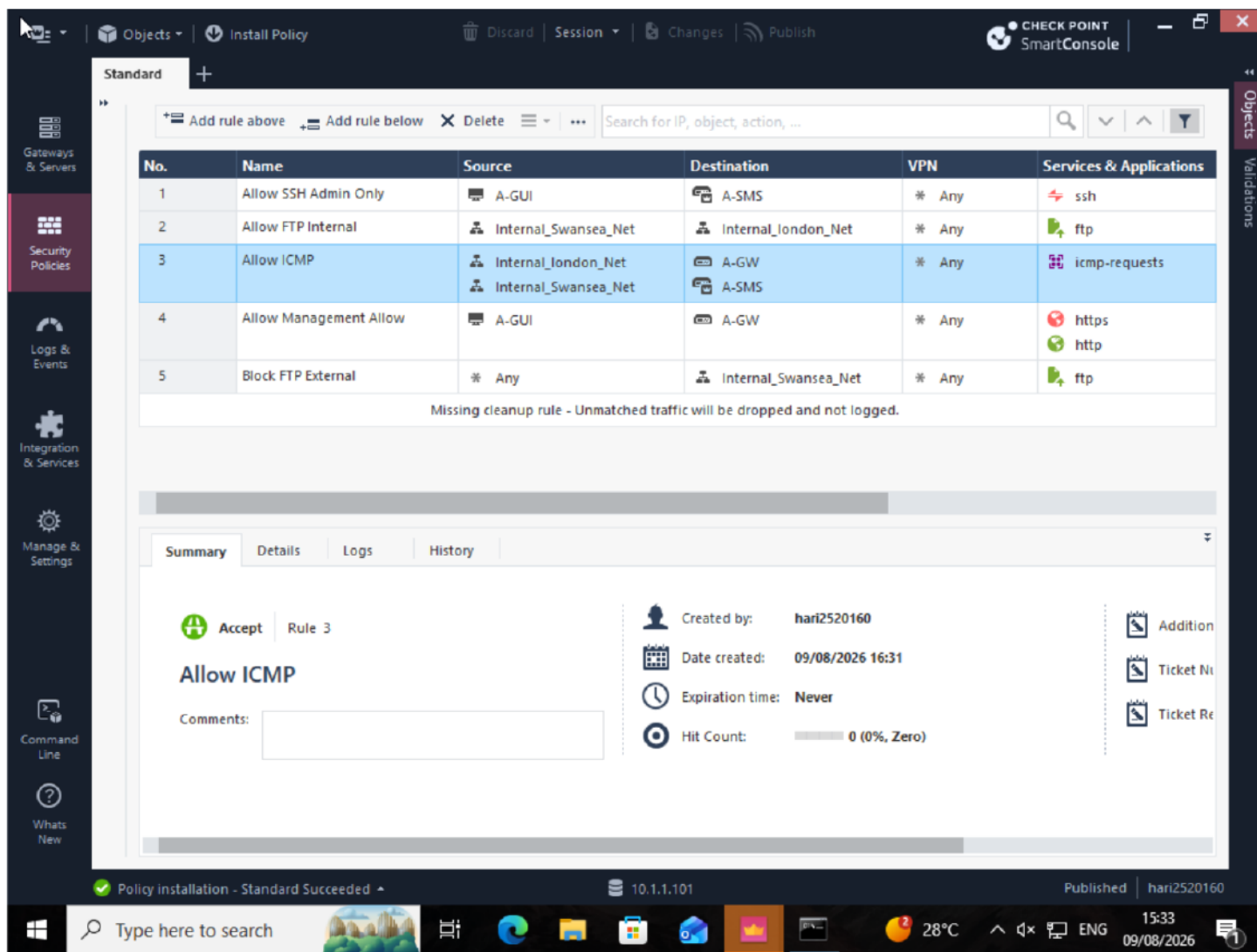
DEPLOYMENT EVIDENCE

The recent-task history records multiple successful installs.

- The Recent Tasks panel shows repeated successful Standard policy installations on A-GW.
- A visible Telnet rule accepts Any traffic and has no tracking, weakening the otherwise restrictive design.
- Publishing and installing after approved changes creates an auditable configuration lifecycle.

Remove Telnet, replace it with SSH, and enable logging before production use.

SSH, FTP, ICMP and management rules define operational boundaries



Standard

Search for IP, object, action, ...

No.	Name	Source	Destination	VPN	Services & Applications
1	Allow SSH Admin Only	A-GUI	A-SMS	* Any	ssh
2	Allow FTP Internal	Internal_Swansea_Net	Internal_London_Net	* Any	ftp
3	Allow ICMP	Internal_London_Net Internal_Swansea_Net	A-GW A-SMS	* Any	icmp-requests
4	Allow Management Allow	A-GUI	A-GW	* Any	https http
5	Block FTP External	* Any	Internal_Swansea_Net	* Any	ftp

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

Summary Details Logs History

Accept Rule 3

Allow ICMP

Comments:

Created by: hari2520160

Date created: 09/08/2026 16:31

Expiration time: Never

Hit Count: 0 (0%, Zero)

Policy installation - Standard Succeeded

10.1.1.101 Published hari2520160

OBJECT-BASED POLICY

Named sources, destinations and services replace broad Any rules.

- The rule names express five intentions: admin-only SSH, internal FTP, ICMP, management access and external FTP blocking.
- Internal_Swansea_Net and Internal_London_Net make the policy easier to maintain than individual addresses.
- ICMP is restricted to internal network objects and management destinations for diagnostics.

SmartConsole warns that the cleanup rule is missing. Add an explicit drop-and-log cleanup rule.

The revised rule set installs successfully after policy changes

Standard

Search for IP, object, action, ...

No.	Name	Source	Destination	VPN	Services & Applications
1	Allow SSH Admin Only	A-GUI	A-SMS	* Any	ssh
2	Allow FTP Internal	Internal_Swansea_Net	Internal_London_Net	* Any	ftp
3	Allow ICMP	Internal_London_Net Internal_Swansea_Net	A-GW A-SMS Internal_Swansea_Net	* Any	icmp-requests https http ftp

All tasks

Policy installation - Standard

- Installation succeeded on A-GW
09-Aug-26 16:33:34 by hari2520160
- Policy installation - Standard
Installation succeeded on A-GW
09-Aug-26 16:28:25 by hari2520160
- Policy installation - Standard
Installation succeeded on A-GW
09-Aug-26 16:04:59 by hari2520160
- Policy installation - Standard
Installation succeeded on A-GW
09-Aug-26 14:58:31 by hari2520160

Created by: hari2520160
Date created: 09/08/2026 16:31
Expiration time: Never
Hit Count: 0 (0%, Zero)

Policy installation - Standard Succeeded

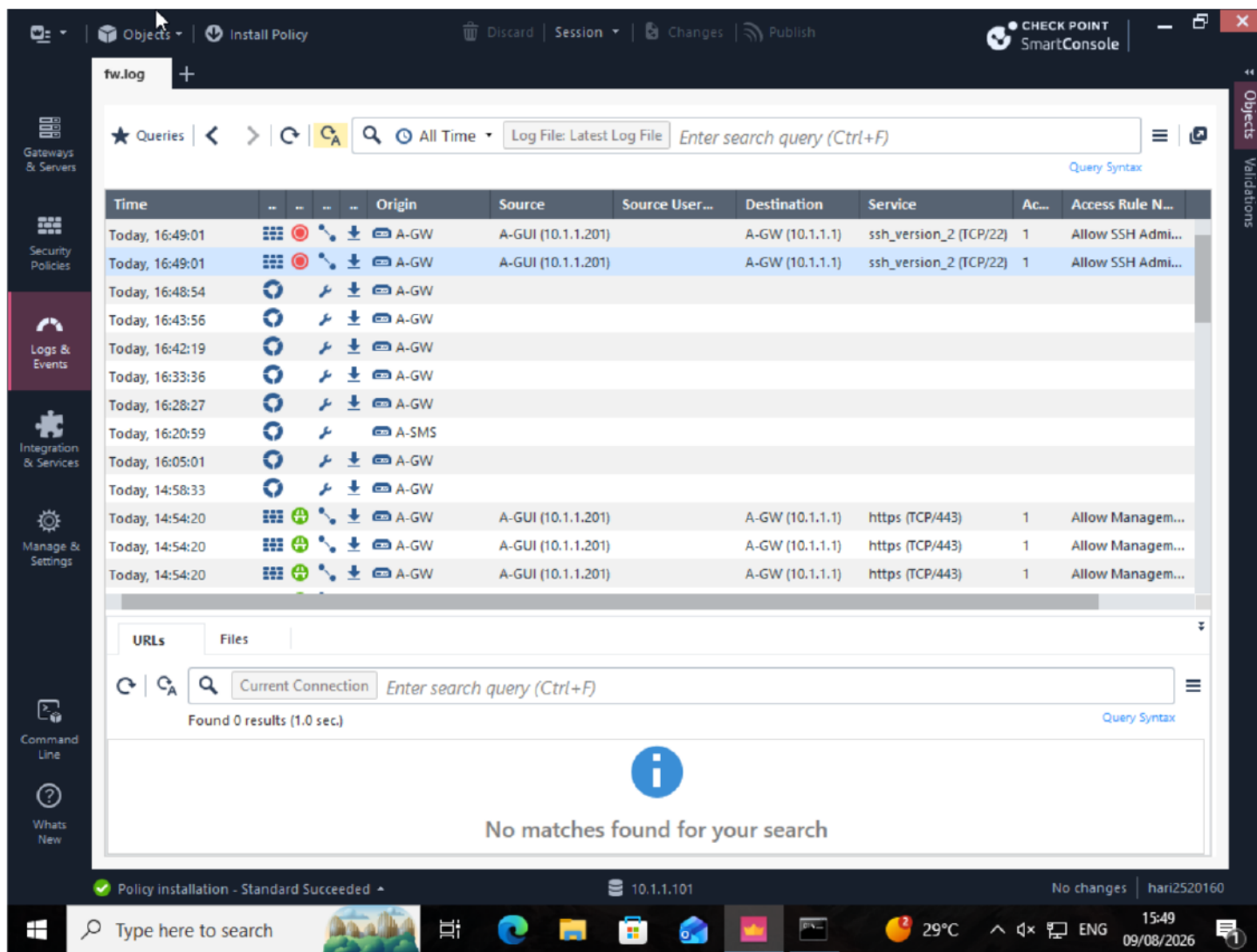
GATEWAY ACCEPTANCE

A-GW accepts the updated Standard policy package.

- The 16:33:34 task confirms successful installation after the multi-rule policy was prepared.
- The green task state demonstrates that the gateway accepted the package without an installation error.
- For formal assurance, record the policy, gateway, administrator, time and related change ticket.

Successful installation proves deployment, but functional testing and log review are still required.

Traffic logs validate SSH and HTTPS activity



Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Today, 16:49:01	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	ssh_version_2 (TCP/22)	1	Allow SSH Admi...
Today, 16:49:01	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	ssh_version_2 (TCP/22)	1	Allow SSH Admi...
Today, 16:48:54	A-GW						
Today, 16:43:56	A-GW						
Today, 16:42:19	A-GW						
Today, 16:33:36	A-GW						
Today, 16:28:27	A-GW						
Today, 16:20:59	A-SMS						
Today, 16:05:01	A-GW						
Today, 14:58:33	A-GW						
Today, 14:54:20	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:54:20	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...
Today, 14:54:20	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	1	Allow Managem...

Below the table, there is a search bar with the text "Found 0 results (1.0 sec)" and a message "No matches found for your search".

RUNTIME VERIFICATION

TCP/22 and TCP/443 events are visible in the same evidence set.

- SSH version 2 traffic uses TCP/22 from A-GUI 10.1.1.201 to A-GW 10.1.1.1.
- The log also retains HTTPS management events, supporting end-to-end policy verification.
- The visible rule name associates the SSH events with the admin SSH control.

The policy view targets SSH at A-SMS, while this log targets A-GW. Reconcile the intended destination and objects.

Reusable network objects support segment-based policy

The screenshot displays the Check Point SmartConsole interface. The main window shows a list of security policy rules under the 'Standard' tab. The rules are as follows:

No.	Name	Source	Destination	VPN	Service
1	Allow SSH Admin Only	A-GUI	A-GW	* Any	SSH
2	Allow FTP Internal	Internal_Swansea_Net	Internal_London_Net	* Any	FTP
3	Allow ICMP	Internal_London_Net Internal_Swansea_Net	A-GW A-SMS	* Any	ICMP
4	Allow Management Allow	A-GUI	A-GW	* Any	Management
5	Block FTP External	* Any	Internal_Swansea_Net	* Any	FTP

Below the rules, a message states: "Missing cleanup rule - Unmatched traffic will be dropped and not logged."

The lower pane shows the 'Logs' tab for the selected rule. It displays a log entry for today at 16:49:01, showing traffic from A-GUI (10.1.1.201) to A-GW (10.1.1.1) on the SSH service.

On the right, a sidebar shows the 'Networks' list with 4 objects. The selected object is 'CP_default_Office_Mode_address...', which is configured with IP Address 172.16.10.0 and Subnet mask 255.255.255.0. The last modifier is 'System'.

MAINTAINABLE SEGMENTATION

The rule base references named Swansea and London networks.

- Internal_London_Net and Internal_Swansea_Net appear as reusable network objects.
- The selected Office Mode object is configured as 172.16.10.0 with mask 255.255.255.0.
- The lower pane shows a current-rule log, connecting object-based policy to observed traffic.

The secured topology also assigns 172.16.10.0/24 to the DMZ. Resolve this overlap before deployment.

Host objects anchor least-privilege administration

The screenshot displays the Check Point SmartConsole interface. The main window shows a security policy rule with the following details:

No.	Name	Source	Destination	VPN	Service
1	Allow SSH Admin Only	A-GUI	A-GW	* Any	SSH
2	Allow FTP Internal	Internal_Swansea_Net	Internal_london_Net	* Any	FTP
3	Allow ICMP	Internal_london_Net Internal_Swansea_Net	A-GW A-SMS	* Any	ICMP
4	Allow Management Allow	A-GUI	A-GW	* Any	Management
5	Block FTP External	* Any	Internal_Swansea_Net	* Any	FTP

Below the rule table, a message states: "Missing cleanup rule - Unmatched traffic will be dropped and not logged."

The bottom section shows the "Logs" tab with a search query "All Time" and "Log File: Latest Log File". It displays "Found 1 results (1.0 sec.)" with the following log entry:

Time	Origin	Source	Source User...	Destination	Service
Today, 16:49:01	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	ssh

The right-hand pane shows the "Objects" section with a search bar and a list of hosts: A-GUI, ClientL1, ClientS1, L-CD, and S-DC. The "A-GUI" host object is selected, showing its details: IP Address: 10.1.1.201, Last Modifier: hari2520160.

IDENTITY BY OBJECT

A-GUI is a defined host at 10.1.1.201.

- The inventory contains A-GUI, ClientL1, ClientS1, L-CD and S-DC host objects.
- A-GUI resolves to 10.1.1.201, supporting a precise source condition for administration rules.
- Named hosts improve auditability, but each object should include an owner, purpose and review date.

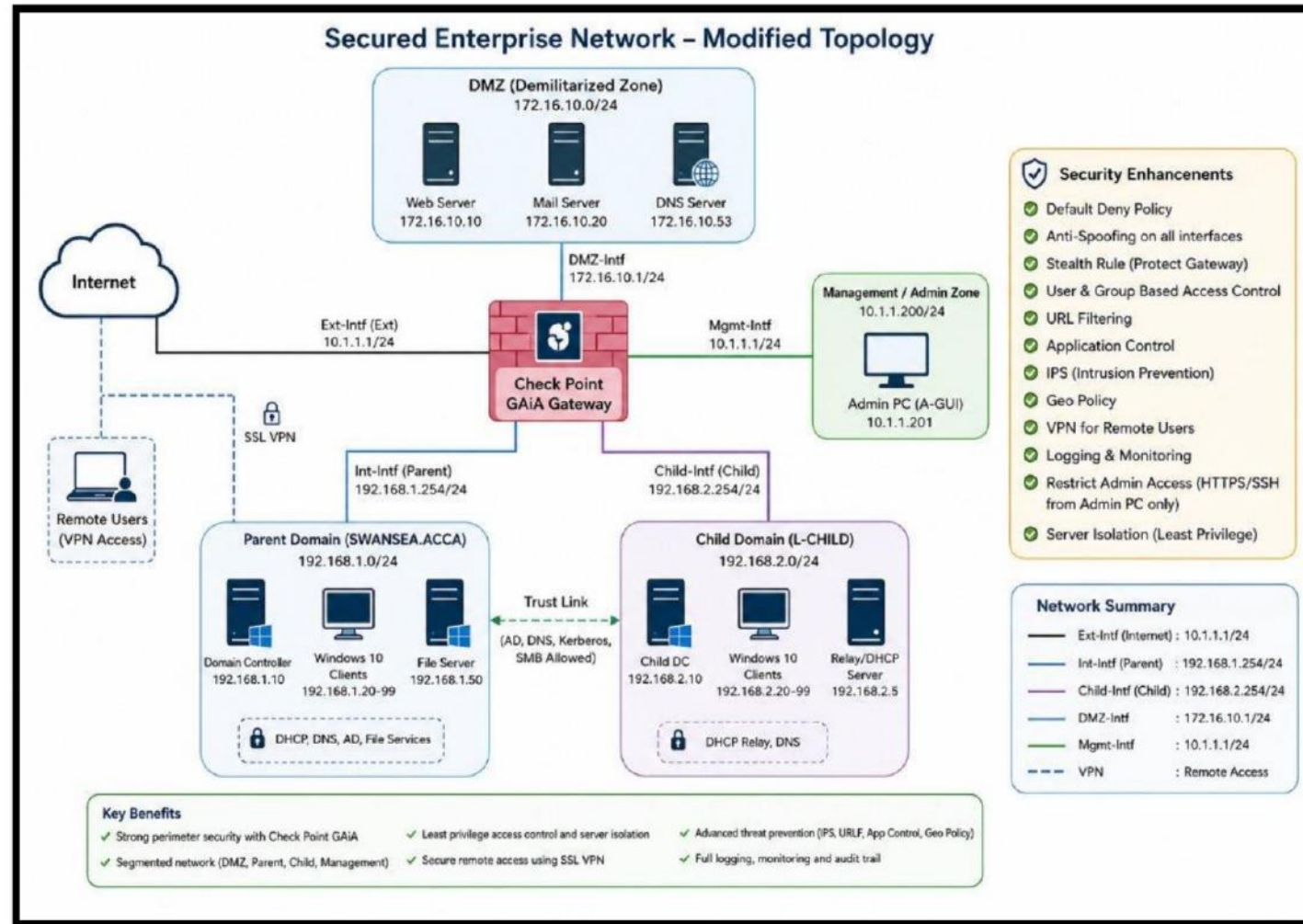
Remove stale objects promptly and use groups only where membership has a clear security purpose.

The rule base is functional, but production hardening is still required

POLICY INTENT	VISIBLE SCOPE	SECURITY VALUE	RECOMMENDED REFINEMENT
SSH administration	A-GUI to A-SMS; SSH	Encrypted remote administration	Confirm whether A-SMS or A-GW is the approved destination; log every session.
Internal FTP	Swansea to London; FTP	Limits file transfer to named networks	Prefer SFTP or FTPS because standard FTP exposes credentials and data.
ICMP diagnostics	Internal networks to A-GW/A-SMS	Supports controlled troubleshooting	Allow only required ICMP types; log or rate-limit abnormal volumes.
Gateway management	A-GUI to A-GW; HTTP/HTTPS	Restricts administration to one host	Remove HTTP; require HTTPS, MFA, least privilege and periodic review.
External FTP block	Any to Swansea network; FTP	Explicitly rejects an unwanted path	Set Drop with Log and retain an explicit final cleanup drop-and-log rule.

Priority corrections: remove Telnet/HTTP, add an explicit logged cleanup rule, reconcile the SSH destination, and eliminate the 172.16.10.0/24 address overlap.

The modified topology applies defence in depth across six zones



DESIGN LOGIC

- A-GW becomes the enforcement point between Internet, management, DMZ, parent, child and VPN paths.
- The management zone limits SmartConsole access to the authorized A-GUI host.
- A DMZ isolates public services; internal segmentation reduces lateral movement.
- Remote users enter through SSL VPN and can be governed by identity and least privilege.

Addressing check: allocate a unique DMZ subnet because 172.16.10.0/24 is already shown as the Office Mode pool.

Defence in depth turns the topology into an enforceable control system

PREVENT

Reduce attack paths

- Default-deny access policy and gateway stealth rule
- Anti-spoofing on every routed interface
- IPS, Anti-Bot, Anti-Virus, URL filtering and application control

CONTROL

Constrain privileged access

- Dedicated management zone and A-GUI-only administration
- MFA, role-based access and least-privilege server rules
- Encrypted HTTPS, SSH and VPN services; remove clear-text protocols

DETECT

See and investigate activity

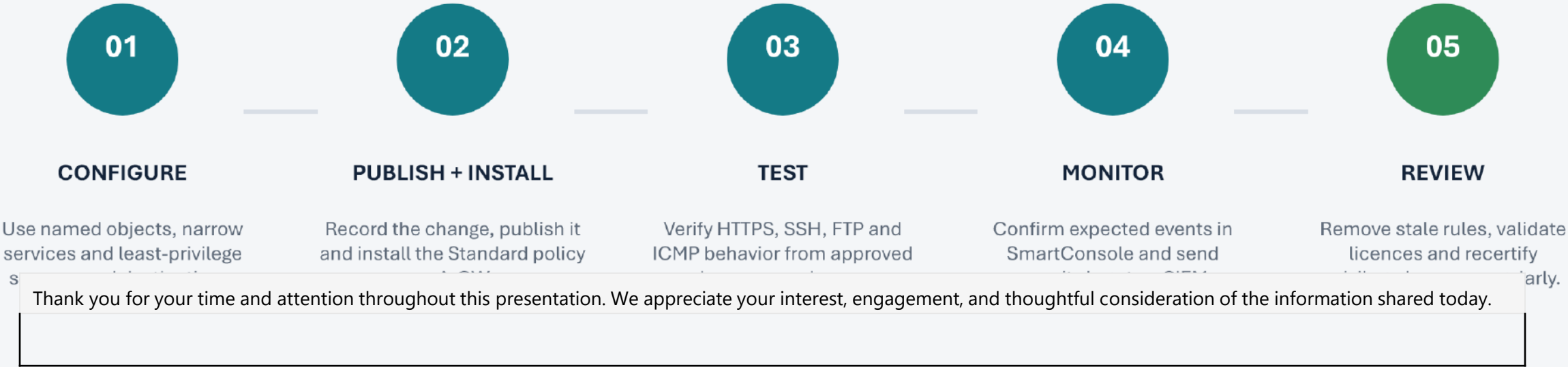
- Log allowed and denied traffic with useful rule names
- Forward firewall, Windows and application logs to a SIEM
- Alert on failed admin access, malware indicators and unusual east-west traffic

SUSTAIN

Keep controls effective

- Patch gateways, servers, endpoints and SmartConsole regularly
- Document licences, support entitlement, expiry and policy review
- Test restores, policy rollback, incident response and rule recertification

Assurance requires a repeatable configure-test-monitor-review cycle



The screenshots demonstrate configure, install and monitor stages. Formal testing records and scheduled review complete the assurance chain.

CONCLUSION

The design is demonstrably functional and has a clear path to production readiness

- SmartConsole shows healthy A-GW and A-SMS status, valid gateway licensing and successful policy installation.
- The rule base uses named hosts, networks and services to constrain management, SSH, FTP and ICMP traffic.
- Logs provide operational evidence for HTTPS and SSH sessions and connect observed traffic to access rules.
- The secured topology adds segmentation, a management zone, DMZ, VPN access and layered threat prevention.

Before production sign-off: remove Telnet and HTTP, add a logged cleanup rule, reconcile the SSH destination, resolve the Office Mode/DMZ subnet overlap, and document licence support details.