

Part 2 - Securing the Enterprise Network

Check Point SmartConsole, firewall policy and secured topology

https://uowtsd-my.sharepoint.com/:f:/g/personal/2529430_student_uwtsd_ac_uk/IgD1Jh2uCS1PQbWvKEpKh17vAQRqeZBsN4vyzIS7FQ6sUWs

Dhrumil Acharya

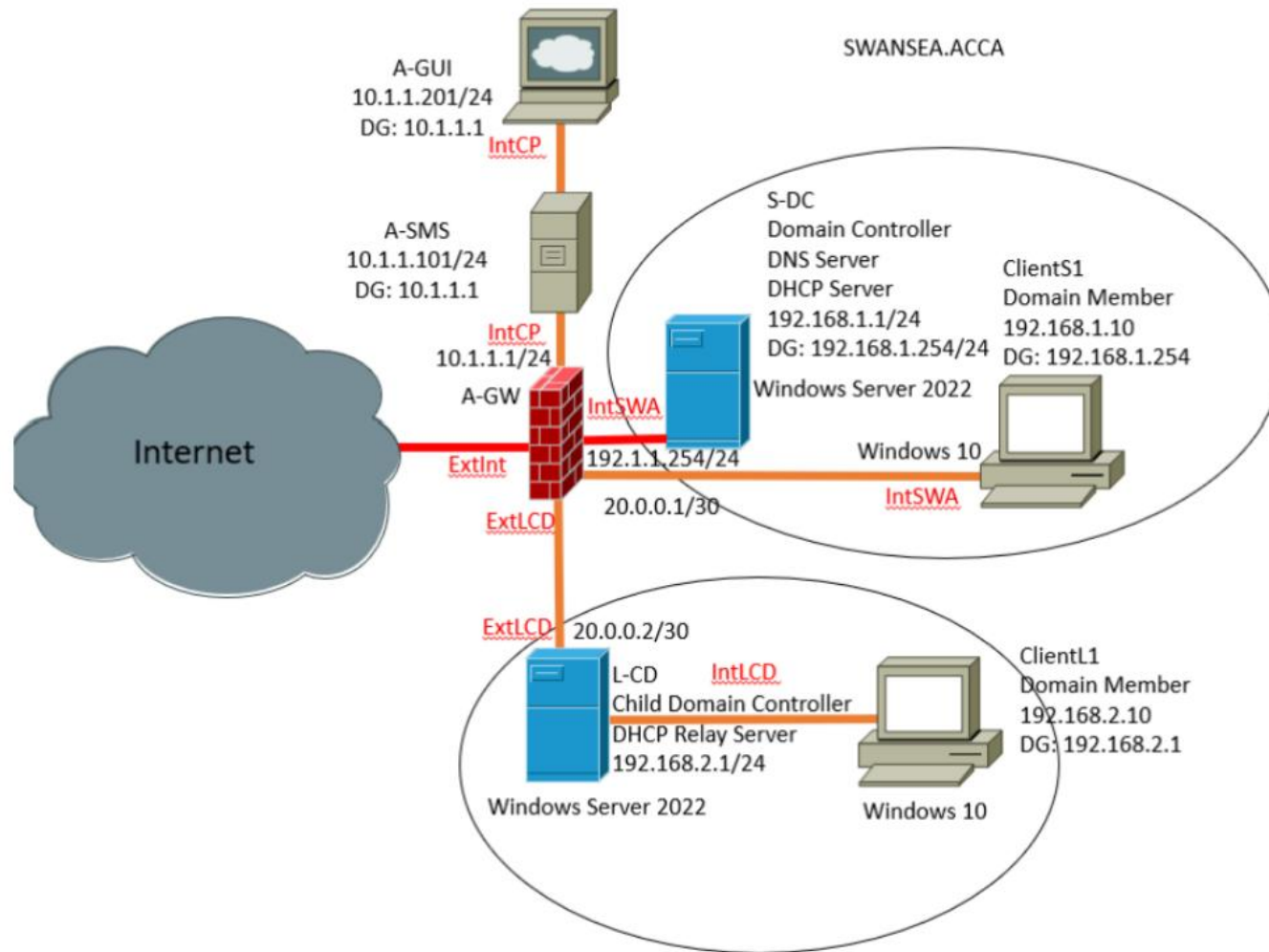
Student ID: 2529430

University of Wales Trinity Saint David

Academic evidence report | August 2026

Existing enterprise topology

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.

Purpose

Task 1 adds a Check Point Security Management Server (SMS) with Gaia OS and uses SmartConsole on A-GUI to administer gateway policy, monitor events and manage updates. The evidence below confirms login, gateway and SMS health, management properties, licensing and connectivity.

Component	Address / segment	Role
A-GUI	10.1.1.201/24	SmartConsole administration workstation
A-SMS	10.1.1.101/24	Security Management Server
A-GW	10.1.1.1/24	Check Point Gaia security gateway
S-DC / ClientS1	192.168.1.0/24	Parent domain services and client network
L-CD / ClientL1	192.168.2.0/24	Child domain services and client network

Assessment focus

- Green gateway/SMS, license and alert indicators support operational connectivity; the successful installation status provides additional evidence that A-SMS can manage A-GW.
- Production management should use named administrators, MFA, least privilege, encrypted administration and restricted management-source networks.

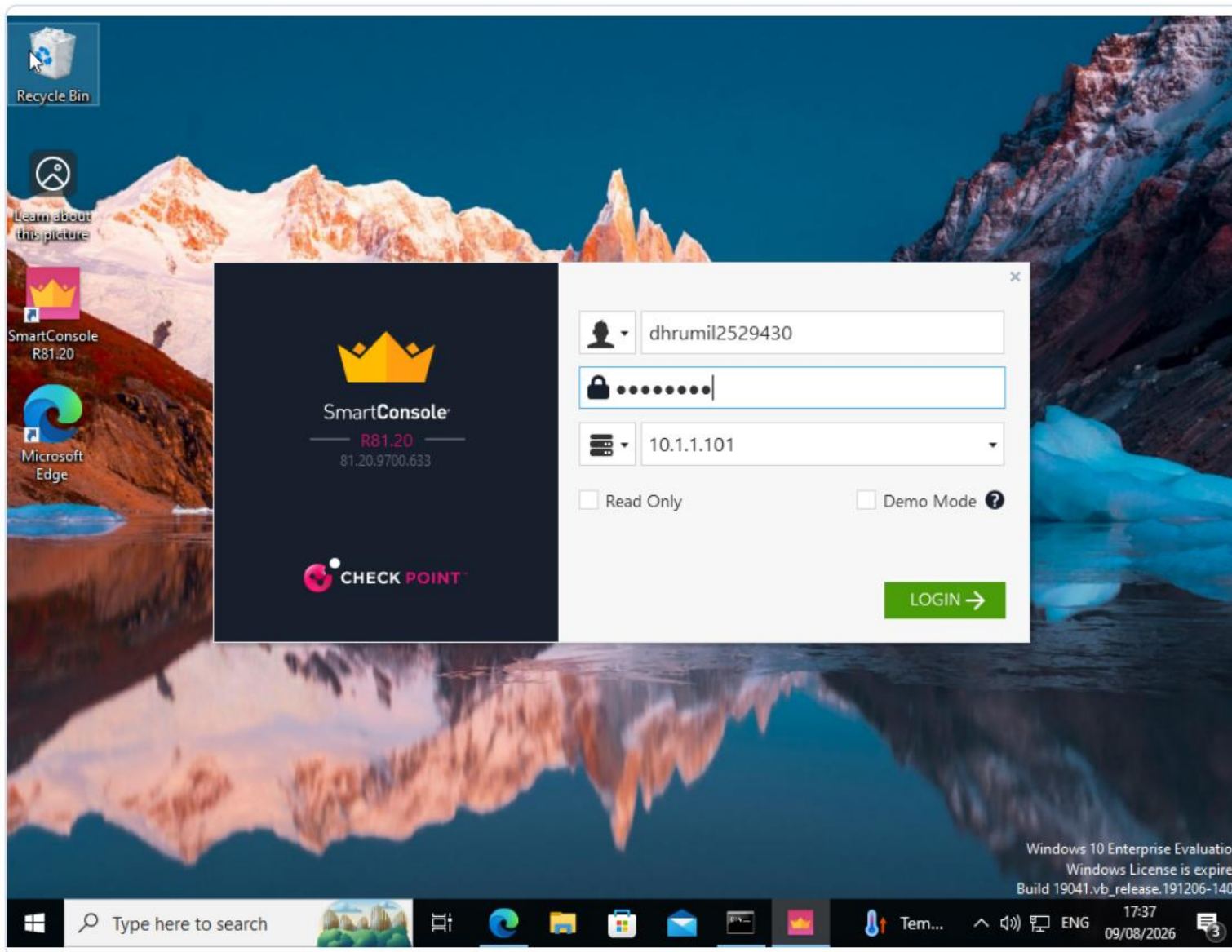


Figure 2. SmartConsole R81.20 login to the management server at 10.1.1.101. The screenshot is shown in full.

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. At the top, a navigation bar includes 'Objects', 'Install Policy', 'Discard', 'Session', 'Changes', and 'Publish'. A dropdown menu for 'Install Policy' shows the shortcut 'Install Policy (Ctrl+Shift+Enter)'. Below this is a table of objects:

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo	Com
✓	A-GW	10.1.1.1	R81.20	Firewall	Open server	20%	N/A	N/A	
✓	A-SMS	10.1.1.101	R81.20	Monitoring	Open server	50%	N/A	N/A	

Below the table, the 'Summary' tab for the 'A-GW' object is shown. It includes the following details:

- IPv4 Address:** 10.1.1.1
- Access Control Policy:** Standard
- OS:** Gaia
- Version:** R81.20
- License Status:** ✓ OK
- Alerts:** ✓ OK
- CPU:** 20%
- Memory:** 26%

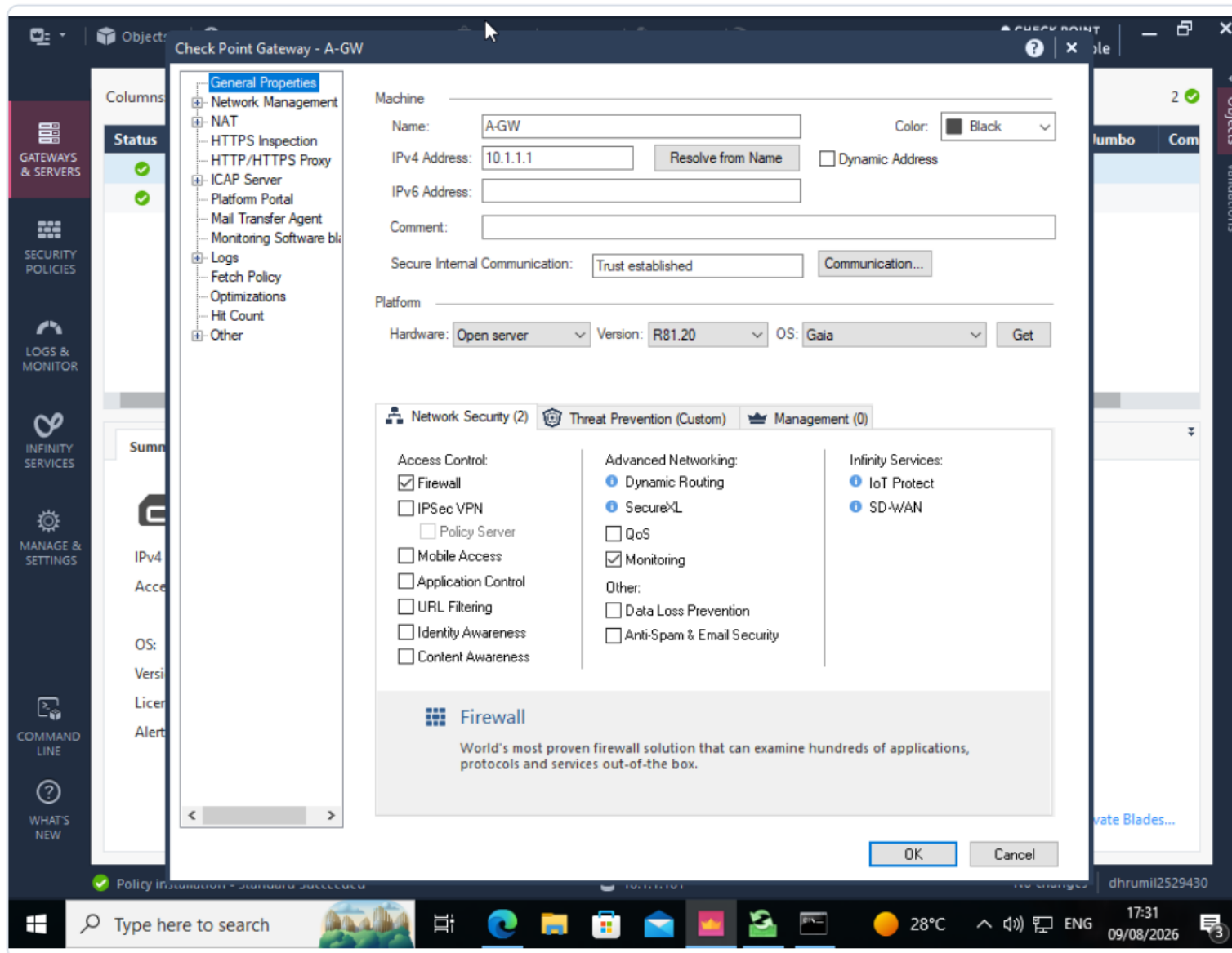
On the right, 'Access Blades' are listed: Firewall and Monitoring. A green checkmark icon is visible next to the 'Open server' status. At the bottom, a status bar indicates 'Policy installation - Standard Succeeded'.

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.



Interpretation

Gateway properties define identity, address, platform, version and active software blades.

- The management object must match the gateway's real interface and SIC configuration.
- Enable anti-spoofing on every interface and classify each interface by its actual topology.
- Activate IPS and other licensed threat-prevention blades only with tuned policy and monitoring.

Figure 4. A-GW general properties with the Firewall blade enabled. The screenshot is shown in full.

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

A-SMS Summary

- IPv4 Address: 10.1.1.101
- OS: Gaia
- Version: R81.20
- License Status: ✓ OK
- Alerts: ✓ OK

Management Blades

- Open server
- CPU: 5%
- Memory: 98%

[Device & License Information...](#) [Activate Blades...](#)

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 interface. The top navigation bar includes 'Package Management' and 'Licenses & Contracts'. The main window shows a tree view of machines under '10.1.1.101', including 'A-GW' and 'A-SMS'. Below this, a table titled 'License And Contract Repository' lists details for each machine, including attached licenses, contracts, and their expiration dates. The bottom section shows the 'Operation Status' table, which is currently empty.

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...	6B626899F...	CPSG-C-8-...	central	21Sep2026
Attached	A-SMS			Software Bl...	10.1.1.101	CPSM-C-5 ...	Security M...	0BD70EC82...	CPSM-C-5 ...	local	never
Contract...	A-GW					CPSB-AV-E...		6B626899F...	Contract H...	contract	17Sep2026
Contract...	A-GW					CPSB-APC...		6B626899F...	Contract FI...	contract	17Sep2026
Contract...	A-GW					CPSB-ASP...		6B626899F...	Contract 9...	contract	17Sep2026
Contract...	A-GW					CPSB-DLP...		6B626899F...	Contract 8...	contract	17Sep2026
Contract...	A-GW					CPSB-TEX...		6B626899F...	Contract A...	contract	17Sep2026

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.

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.

The screenshot displays the Check Point SmartConsole interface. The top navigation bar includes 'Objects', 'Install Policy', 'Discard', 'Session', 'Changes', and 'Publish'. The left sidebar contains icons for Gateways & Servers, Security Policies, Logs & Monitor, Infinity Services, Manage & Settings, Command Line, and What's New.

The main area shows a table of network objects with the following columns: Status, Name, IP, Version, Active Blades, Hardware, CPU Usage, and Recommended Upd. The table contains two rows:

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Upd
✓	A-GW	10.1.1.1	R81.20	6	Open server	20%	N/A
✓	A-SMS	10.1.1.101	R81.20	1	Open server	11%	N/A

Below the table, the 'Summary' tab for object 'A-GW' is expanded, 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). It also displays resource usage for CPU (20%) and Memory (26%).

The right sidebar shows a list of networks under the 'Networks' section, including 'CP_default_Office_Mode_address...', 'Internal London Net', 'Internal Swansea net', and 'IPv6_Link_Local_Hosts'.

The bottom status bar indicates 'Policy installation - Standard Succeeded' and shows the current session information.

Interpretation

Network objects make subnet definitions reusable and reduce manual addressing errors in the rule base.

- Use accurate masks and non-overlapping ranges for management, parent, child and DMZ networks.
- Group objects by function only where the same security treatment is justified.
- Document owners and review unused objects to avoid stale policy references.

Figure 7. Network object catalogue used by the access-control policy. The screenshot is shown in full.

The screenshot displays the Check Point SmartConsole interface. The top navigation bar includes 'Objects', 'Install Policy', 'Discard', 'Session', 'Changes', and 'Publish'. The left sidebar contains navigation icons for Gateways & Servers, Security Policies, Logs & Monitor, Infinity Services, Manage & Settings, Command Line, and What's New.

The main content area shows a table of Host objects:

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Upd
✓	A-GW	10.1.1.1	R81.20	6	Open server	20%	N/A
✓	A-SMS	10.1.1.101	R81.20	1	Open server	11%	N/A

Below the table, the 'Summary' tab for 'A-GW' is selected, showing details:

- IPv4 Address: 10.1.1.1
- Access Control Policy: Standard
- OS: Gaia
- Version: R81.20
- License Status: ✓ OK
- Alerts: ✓ OK
- CPU: 20%
- Memory: 26%

The right sidebar shows a list of Hosts: A-GUI, ClientL1, ClientS1 (selected), L-CD, and S-DC. Below this, details for 'ClientS1' are shown, including IP Address: 192.168.1.10 and Last Modifier: dhrumil2529430.

The bottom status bar indicates 'Policy installation - Standard Succeeded' and shows the current session details: 10.1.1.101, No changes, dhrumil2529430.

Interpretation

Named hosts let rules target specific systems rather than broad network ranges or Any.

- Restrict administrative services to A-GUI or another dedicated jump host.
- Keep domain controllers and ordinary clients in distinct access-control roles.
- Synchronise object addresses with DHCP reservations, DNS and change records.

Figure 8. Host objects including A-GUI, Client1, ClientS1, L-CD and S-DC. The screenshot is shown in full.

Standard +

Search for IP, object, action, ...

No.	Name	Source	Destination	VPN	Services & Applicat...	Action	Track	Insta
1	Block telnet	* Any	* Any	* Any	telnet	Drop	Log	*
2	Allow HTTP	* Any	A-GW	* Any	http https	Accept	Log	*
3	Allow ICMP	Internal...	A-GW A-SMS	* Any	icmp-requests	Accept	Log	*
4	Allow FTP	Internal...	Internal Lo...	* Any	ftp	Accept	Log	*
5	Allow ssh	A-GUI	A-GW	* Any	ssh ssh_version_2	Drop	Log	*

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

Summary Details Logs History

Accept Rule 2

Allow HTTP

Comments:

Created by: dhrumil2529430

Date created: 09/08/2026 18:18

Expiration time: Never

Hit Count: 0 (0%, Zero)

Policy installation - Standard Succeeded

10.1.1.101 No changes dhrumil2529430

Type here to search

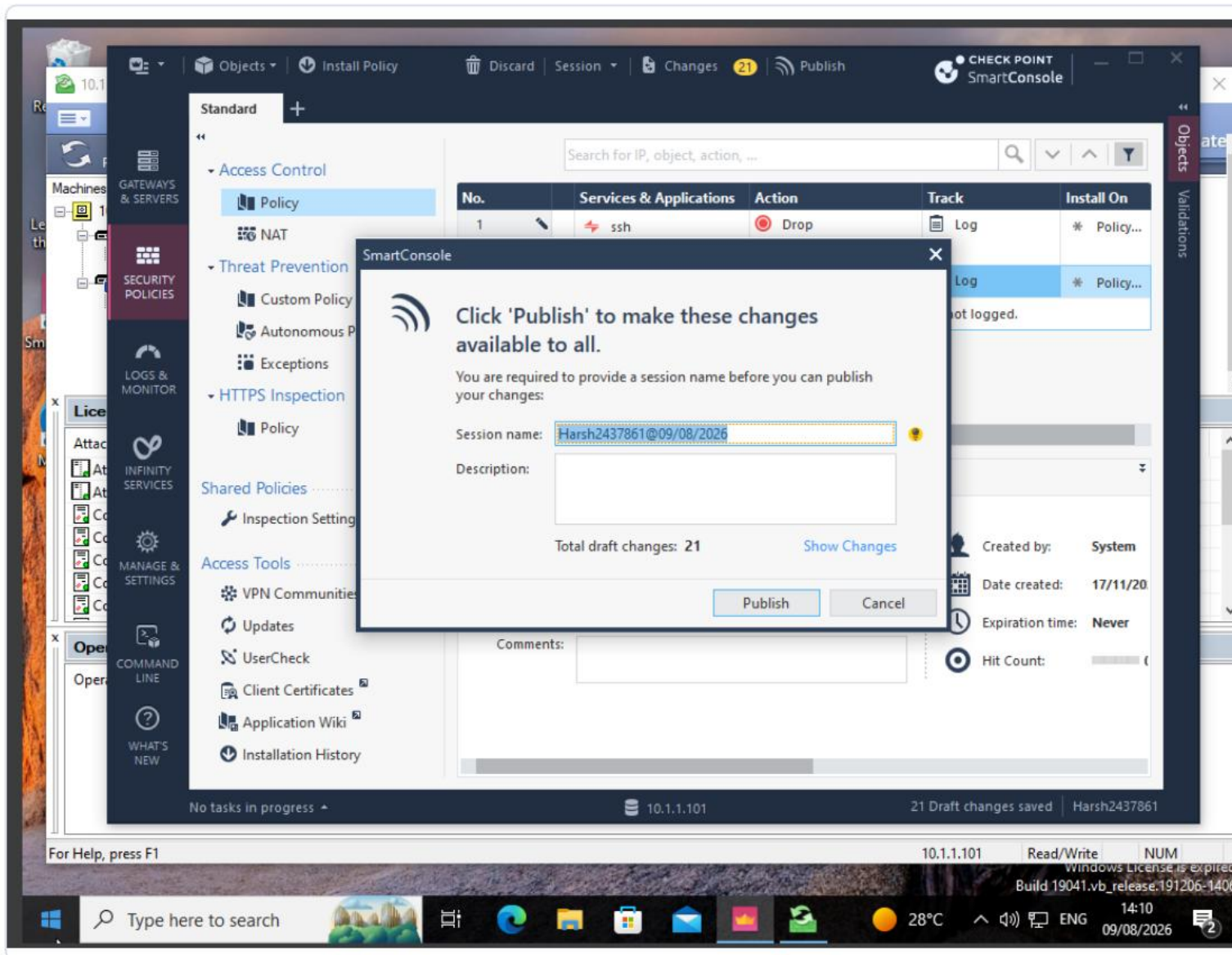
28°C 17:33 09/08/2026

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

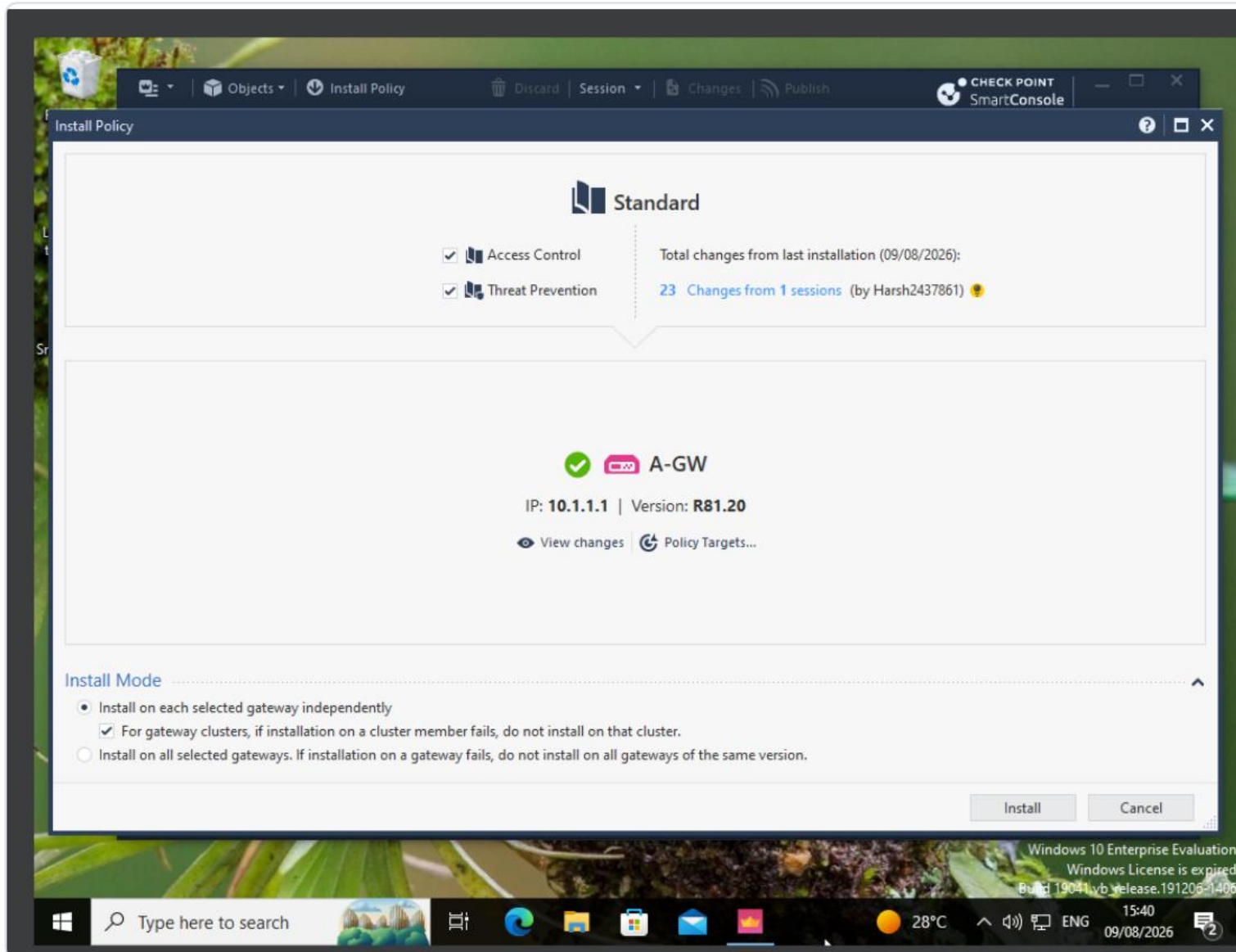


Interpretation

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 10. 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 11. Standard policy installation workflow targeting A-GW. The screenshot is shown in full.

Log File: Latest Log File Enter search query (Ctrl+F)

Found 47 results (1.1 sec.)

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)		A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP

Found 0 results (1.1 sec.)

No matches found for your search

Policy installation - Standard Succeeded

10.1.1.101 No changes dhrumil2529430

Interpretation

Accepted events confirm that traffic matched an allow rule and that tracking is enabled.

- Validate source, destination, service, rule number and action rather than relying only on the green icon.
- Use focused queries to prove each authorised test case.
- Retain logs according to security, legal and capacity requirements.

Figure 12. SmartConsole log view showing accepted test connections. The screenshot is shown in full.

Log File: Latest Log File Enter search query (Ctrl+F)

Found 47 results (1.1 sec.)

Time	Origin	Source	Destination	Service	Ac...	Access Rule N...
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:09	A-GW	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:08	A-GW	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:08	A-GW	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:08	A-GW	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:30:00	A-GW	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	https (TCP/443)	2	Allow HTTP
Today, 18:28:13	A-GW	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	ssh_version_2 (TCP/22)	5	Allow ssh
Today, 18:28:12	A-GW	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	ssh_version_2 (TCP/22)	5	Allow ssh
Today, 18:27:29	A-GW	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	ssh_version_2 (TCP/22)	5	Allow ssh
Today, 18:25:11	A-SMS	A-GUI (10.1.1.201)	A-GW (10.1.1.1)	ssh_version_2 (TCP/22)	5	Allow ssh

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 dhrumil2529430

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

Modified secured enterprise topology

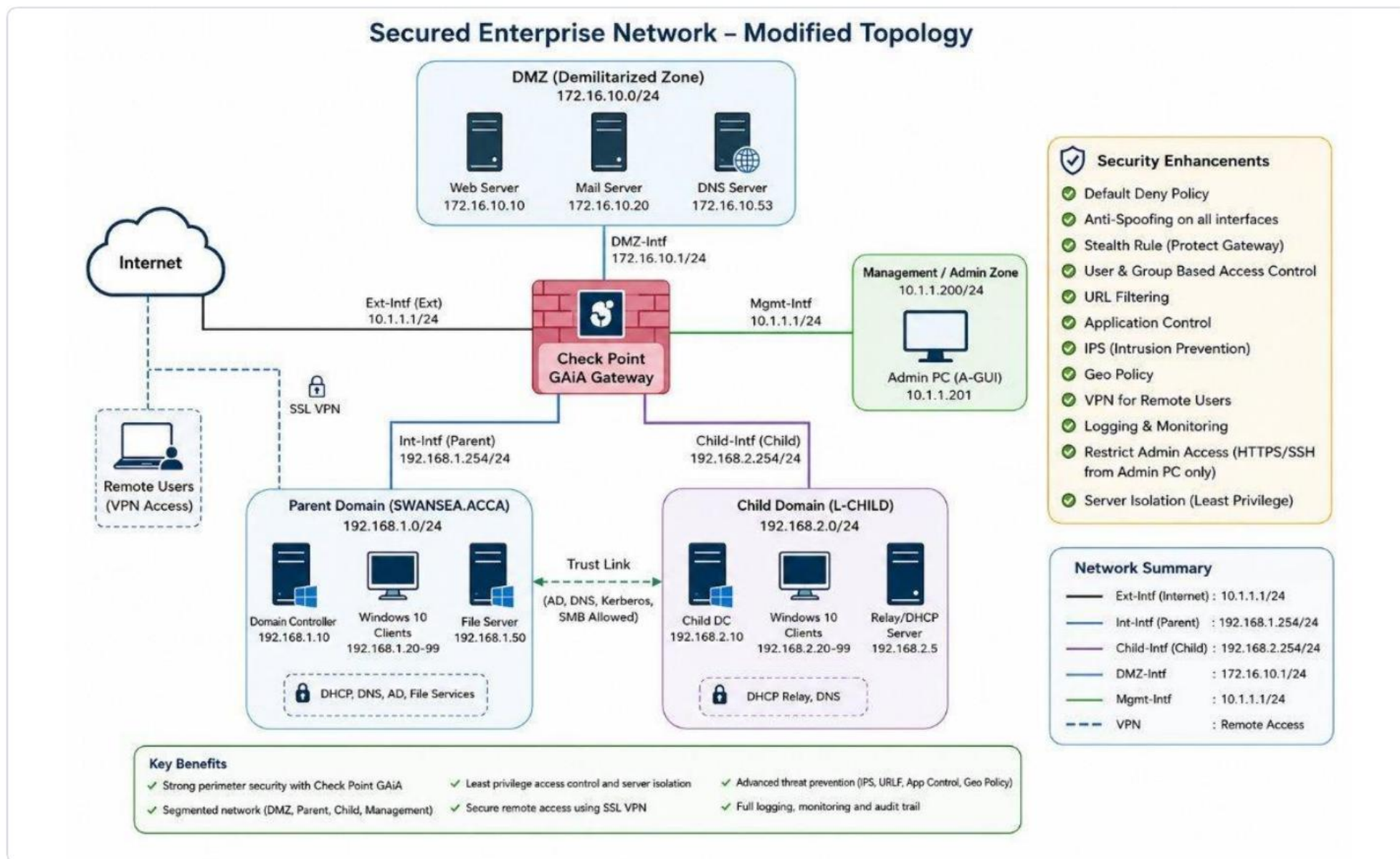


Figure 14. Secured enterprise topology from the reference work, reproduced in full without cropping.

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.

The documented implementation meets the intended report flow.

SmartConsole connects to A-SMS, both A-SMS and A-GW report healthy management and licensing indicators, and the rule base is expressed through reusable objects with tracked allow and deny decisions. Publishing, policy installation and log evidence demonstrate the operational policy lifecycle.

01**Central management**

A-GUI uses SmartConsole to manage A-SMS and A-GW from the dedicated management segment.

02**Controlled services**

Telnet is blocked; HTTP, ICMP, FTP and SSH are treated explicitly and should be narrowed to business need.

03**Auditable lifecycle**

Changes are published, installed to A-GW and verified through status and monitoring logs.

04**Defence in depth**

DMZ segmentation, threat-prevention blades, VPN, least privilege and central logging strengthen the original design.

Thank you for listening and participating in today's presentation. We hope the insights and findings presented have been informative, valuable, and helpful for your future learning and development.

Recommended final verification

Correct the duplicate interface addressing shown in the supplied Task 3 figure, then retest routing, access, threat prevention, logging and backup recovery against the approved policy.