ACCA7032 - Enterprise Network Security

Securing the Enterprise Network with Check Point Gaia R81.20

Practical Demonstration
SMS Deployment | Firewall Policy | Threat Prevention | Verification

Smit Brijeshkumar Patel

Enrollment: 2506590 | Level 7 | MSc Cyber Security and Digital Forensics
University of Wales Trinity Saint David - London Campus

Presented: April 2026

What I'll Cover Today

Walking through the Part 2 build, end to end

01 The Scenario
Two-site enterprise network and what we were asked to secure.

02 SMS & SmartConsole
Installing A-SMS and A-GW on Gaia R81.20, establishing SIC trust, applying licences [1].

03 Firewall Policy
19 rules covering management, web, SSH, ICMP, FTP, DHCP, App Control and a final cleanup drop [2].

04 Advanced Features
Application Control, URL Filtering, IPS, Identity Awareness [3], [4].

05 Verification
DNS, DHCP, HTTPS, SSH and rule-blocking tests from real client machines.

06 Limitations & Wrap-up
Honest review of what worked, what didn't, and what I'd do differently.

A note on the lab. Everything you'll see today was built from scratch in VirtualBox - one Gaia SMS, one Gaia gateway, two Windows clients, a domain controller, and a SmartConsole admin workstation. A few things didn't go to plan; I'll be upfront about those at the end.

The Scenario

Two sites, one Check Point gateway, one job: lock it down

What We Started With

Two sites: SWANSEA.ACCA (HQ) and LONDON.SWANSEA.ACCA (branch). Connected over a simulated WAN through the Check Point gateway.

Core services running: Active Directory and DNS on S-DC, DHCP on the same box, IIS web server (HTTPS), and two domain-joined client workstations - one per site.

The job for Part 2: drop a Gaia SMS into this design, install a SmartConsole, get the gateway under management, write a sensible firewall policy, and turn on the protections that a real enterprise would actually use [1].

Key IP Addresses

A-SMS	10.1.1.101	Security Mgmt Server
A-GW	10.1.1.1	Gateway (mgmt int.)
A-GUI	10.1.1.201	SmartConsole admin
S-DC	192.168.1.1	DC / DNS / DHCP / IIS
ClientS1	192.168.1.10	Swansea client
L-CD	192.168.2.1	London branch device
ClientL1	192.168.2.10	London client

Note: *S-DC handles DNS, DHCP, IIS and the domain controller role. That's a deliberate lab simplification - in a real deployment those would sit on separate hardened hosts [5].*

Question 1 - Gaia Appliances and the SMS

Modifying the topology and bringing the management plane online (30%)

What I Built

A-SMS Check Point Gaia R81.20 Security Management Server. 10.1.1.101 [1].

A-GW Gaia R81.20 Security Gateway. eth0 = 10.1.1.1 (management), with three more interfaces wired for the WAN side.

A-GUI Windows 10 admin workstation at 10.1.1.201, running SmartConsole R81.20.

Pieces between them: SIC trust, certificate exchange, licences applied through SmartUpdate.

Why It Matters

Without a Security Management Server, every gateway has to be configured by hand and there's no central place to write or push policy. The SMS is what lets us treat the network as one system - one rulebase, one log stream, one set of objects shared across sites [1].

In other words, the SMS is the foundation everything else in this presentation sits on. If A-SMS doesn't trust A-GW, there is no policy to push.

1. Install & configure A-GW, A-SMS, A-GUI • **2. License the SMS** • **3. Connect Swansea network to A-SMS**

A-SMS - Gaia Portal Login

Security Management Server up and reachable on 10.1.1.101

What's on screen

Gaia web portal of A-SMS, accessed from the admin workstation at https://10.1.1.101.

Build: Check Point Security Management R81.20, kernel 3.10.0-1160.15.2cpx86_64, build 634, 64-bit, on Open Server [1].

Right pane shows the management blades available for activation - Firewall, IPSec VPN, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Threat Emulation and Threat Extraction. We come back to several of these in Q3 [3].

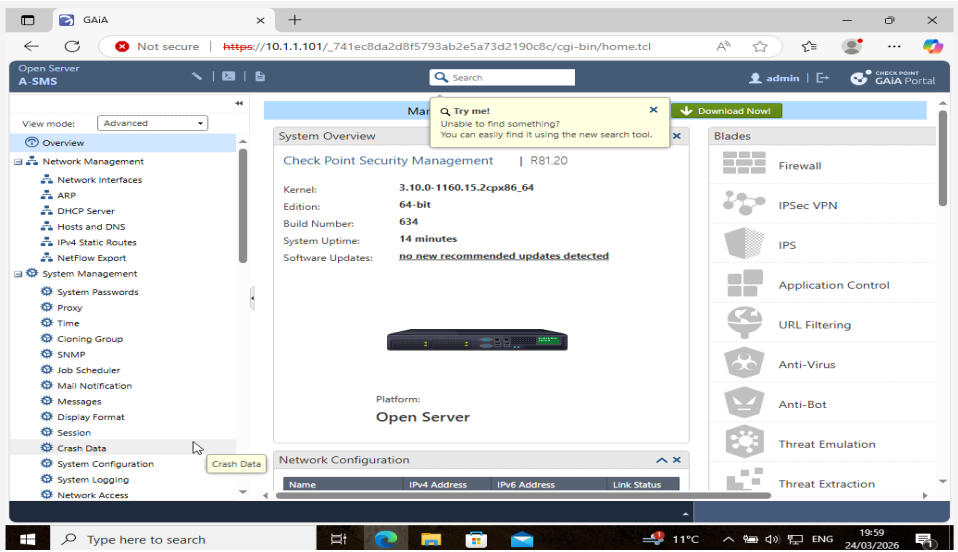


Figure 1 - A-SMS Gaia portal showing R81.20 system info

A-GW - Network Interfaces

Gateway interfaces configured for management and WAN traffic

Interface plan

eth0	10.1.1.1 / 24	Management (same subnet as A-SMS)
eth1	192.168.1.254 / 24	Inside (Swansea LAN)
eth2	20.0.0.1 / 30	WAN to London (point-to-point)
eth3	10.0.5.15 / 24	VirtualBox NAT (internet access)
lo	127.0.0.1	Loopback

Why this wiring: eth0 shares a subnet with A-SMS so SIC negotiation works without routing tricks. eth1 is the Swansea LAN side — traffic from ClientS1 and S-DC exits here. eth2 is the /30 WAN link to L-CD in London. eth3 (10.0.5.15) is the VirtualBox NAT — this is why IPS signature updates failed; A-GW couldn't route back out through NAT to reach Check Point's update servers.

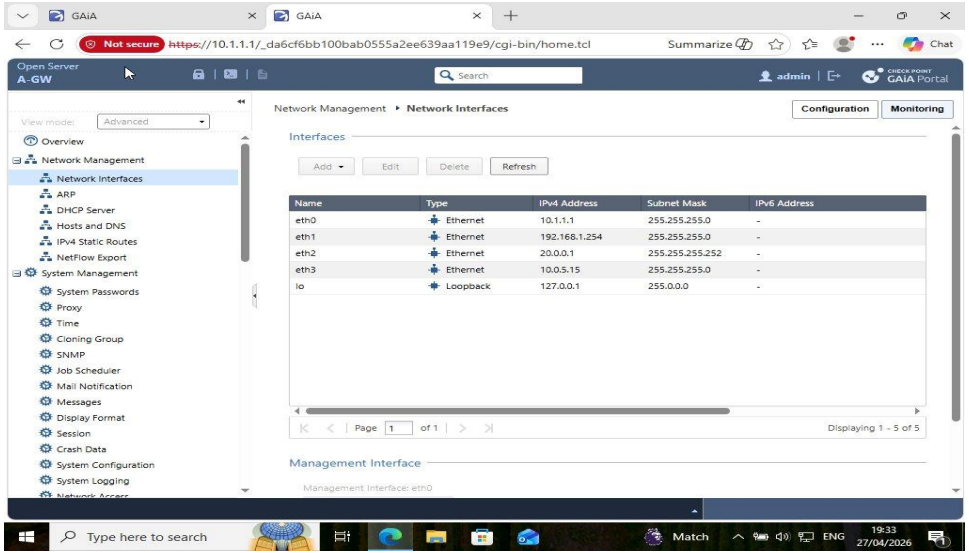


Figure 2 - A-GW Gaia portal: configured network interfaces

SmartConsole R81.20 - Connecting to A-SMS

From A-GUI to A-SMS as the 'Smitpatel' admin user

The connection in plain English

SmartConsole is the GUI we use to talk to the SMS. Without it, every change goes through Gaia CLI [1].

Login target: 10.1.1.101 (A-SMS).

User: Smitpatel - created during the SMS first-time wizard.

Build: R81.20.9700.633.

Once authenticated, SmartConsole pulls down the existing object database, policies and logs from A-SMS. Anything I change here gets staged as a 'session' and only goes live when I publish it - a useful safety net while learning.

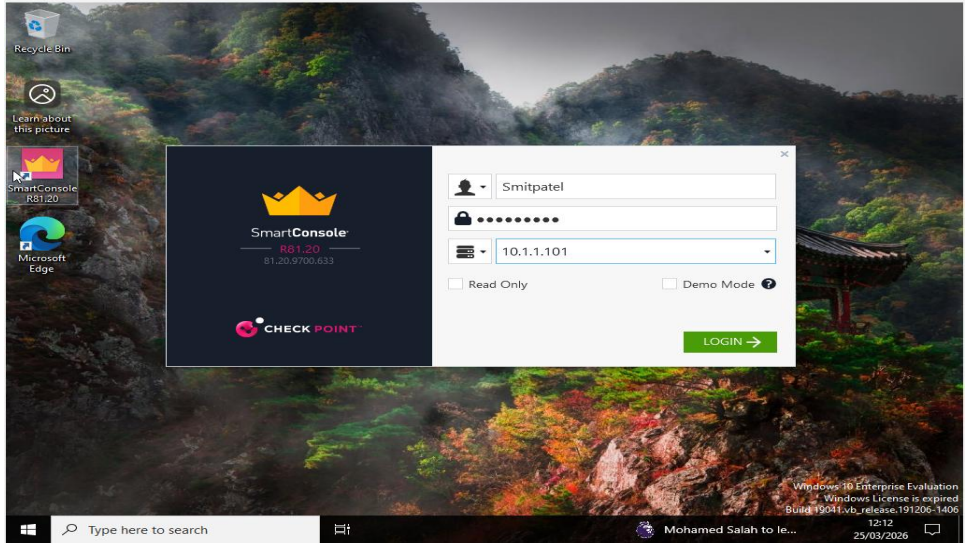


Figure 3 - SmartConsole login dialog connecting to A-SMS at 10.1.1.101

Gateways & Servers - SIC Trust Established

Both A-GW and A-SMS visible, healthy, and managed

What this view confirms

- **A-GW** `10.1.1.1`

  Status OK, R81.20, CPU 12%

- **A-SMS** `10.1.1.101`

  Status OK, R81.20, CPU 17%

SIC trust (Secure Internal Communication) is the bit that took the longest. The gateway and the SMS exchange certificates over an activation key, and from that point every command between them is encrypted and authenticated [1].

If SIC is broken, the gateway shows up but you can't push policy. 'Trust established' on both is the green light to start writing rules.

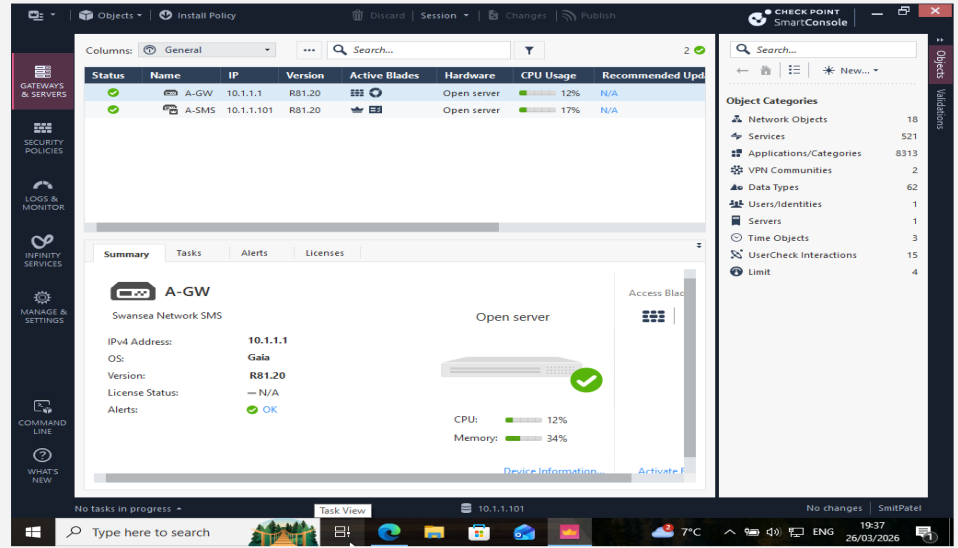


Figure 4 - SmartConsole Gateways & Servers: A-GW and A-SMS healthy

Licensing the Management Server

Applied through SmartUpdate, status verified in SmartConsole

A-SMS

Lab evaluation licence applied via SmartUpdate. Tied to the SMS IP (10.1.1.101) and the host fingerprint - it won't work if either changes [1].

A-GW

Gateway licence attached after SIC was up. License Status surfaces in the gateway summary tab - useful at a glance during incidents.

Expiration

Expiry date checked in the licence properties pane. Documented in the report appendix so the next person picking this up isn't caught out.

Why I'm spending a slide on this

Licences are the silent failure point in Check Point deployments. A gateway can be up, SIC can be fine, the policy can be installed - and then traffic still doesn't flow correctly six weeks later because a blade licence quietly expired [1]. Documenting status and expiry up front is one of those small things that saves real grief later.

Question 2 - Writing the Firewall Policy

19 rules built around a default-deny posture (30%)

Default deny

If the policy doesn't explicitly allow it, the cleanup rule drops it. No 'Any-Any-Allow' anywhere [2].

Specific over generic

Where I could name a host, I named it. Allow_Admin_SSH targets the workstation, not 'any internal'.

Symmetric thinking

Every allow has a matching question: who initiates this, why, and what could it be misused for if the source is wrong?

Logging on by default

Drop rules log so I can see what's being attempted. Allow rules log so I can audit [6].

Real-world thinking

Treated as if this were a small enterprise where Swansea staff need to browse the web, hit the internal IIS server, and resolve internal DNS - while a separate admin needs SSH to the management plane. Telnet, FTP, ICMP from outside, and unsolicited inbound traffic are all dropped. SSH is allowed only from the admin workstation, not from a regular client - one of the more useful tests later [6].

Network Objects in SmartConsole

Defining who and where, before defining what they can do

Why objects come first

A rulebase that uses raw IP addresses ages badly. As soon as someone re-IPs a subnet, every rule that touched it has to be rewritten by hand. Defining named objects first means rules read in plain English and changing an IP is a one-place edit [2].

Networks

Swansea_LAN 192.168.1.0/24
London_LAN 192.168.2.0/24
Hosts: S-DC, ClientS1, ClientL1, L-CD, Admin_Workstation

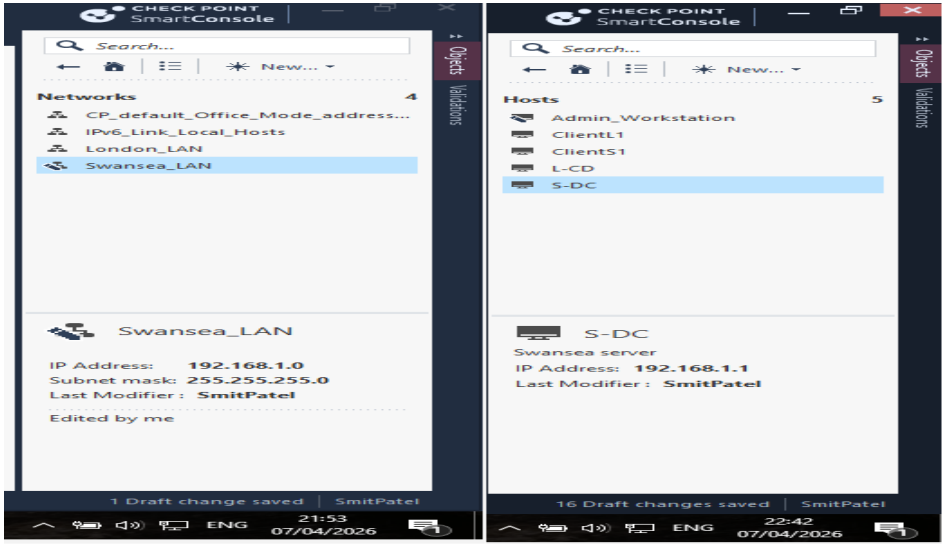


Figure 5 - Network and Host objects in SmartConsole's object explorer

Firewall Rules 1-8 - Management and Web Traffic

First half of the policy: who reaches what, on which ports

What these rules say

1. `Allow_Management_Access`
   Admin -> Any (any service)
2. `Allow_GW_to_AD`
   A-GW -> S-DC
3. `Allow_SMS_to_AD`
   A-SMS -> S-DC
4. `Allow_Internal_DNS`
   LANs -> S-DC (DNS)
5. `Allow_HTTPS_to_webServer`
   Any -> S-DC (HTTPS)
6. **`Block_HTTP_to_webServer`**
   Any -> S-DC (HTTP) - DROP
7. `Allow_Outbound_Web`
   LANs -> Any (HTTP/HTTPS)
8. `Allow_Admin_SSH`
   Admin -> Any (SSH)

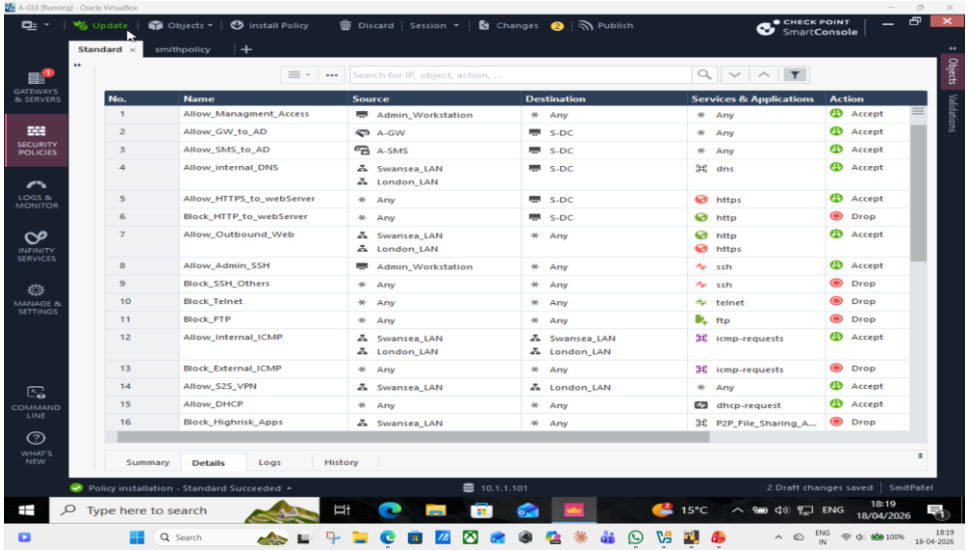


Figure 6 - SmartConsole Security Policy: rules 1-16 (rules 1-8 highlighted)

Firewall Rules 9-15 - Service Lockdown and ICMP

Second half: explicit drops for the noisy stuff

Where the policy bites

9 **Block_SSH_Others**
Any -> Any (SSH) - DROP

10 **Block_Telnet**
Any -> Any (telnet) - DROP

11 **Block_FTP**
Any -> Any (FTP) - DROP

12 Allow_Internal_ICMP
LAN <-> LAN (icmp)

13 **Block_External_ICMP**
Any -> Any (icmp) - DROP

14 Allow_S2S_VPN
Swansea_LAN -> London_LAN

15 Allow_DHCP
Any -> Any (dhcp-request)

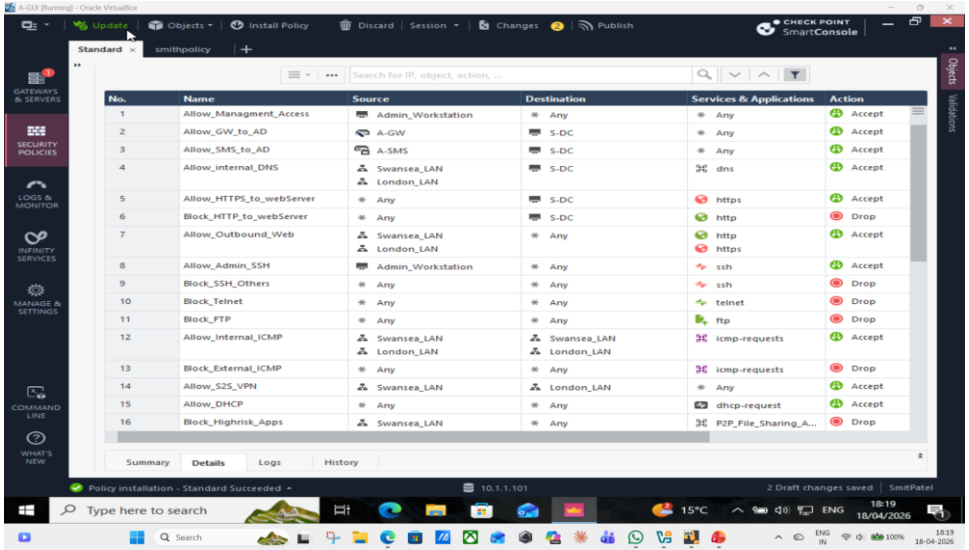


Figure 7 - SmartConsole Security Policy showing rules 9-15

Rules 16-19 - App Control, URL Filtering, Cleanup Drop

Layer 7 protections and the last line of the policy

What gets blocked here

16 **`Block_Highrisk_Apps`**

Swansea_LAN, London_LAN -> Any (P2P File Sharing, Anonymizer, Remote Admin) - DROP

17 **`Block_Dangerous_URL`**

Any -> Any (Phishing, Malware, Spyware, Gambling, Hacking) - DROP

18 **`Block_SocialMedia_Standard`**

Standard_Users_Role -> Any (Social Networking) - DROP

19 **`Cleanup_Drop_ALL`**

Any -> Any -> Any - DROP (catch-all)

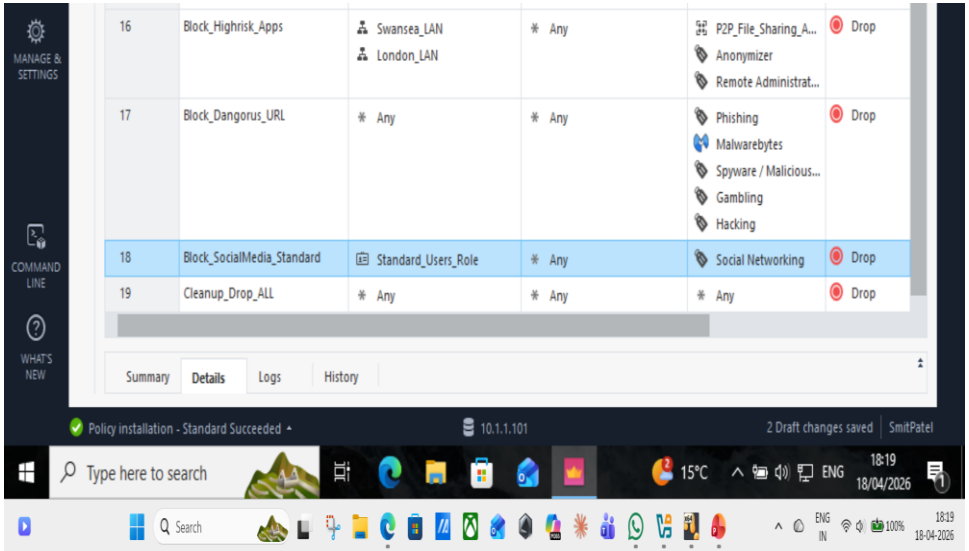


Figure 8 - SmartConsole rules 16-19 with App Control and URL categories

Why These Rules, Specifically

Mapping each rule to a real business or security need

Management isolation

Admin SSH from one workstation only. Stops a compromised user box from pivoting to the SMS or gateway [6].

DNS lock-down

Clients only resolve through S-DC. Stops DNS exfiltration and matches AD's split-horizon DNS [5].

External ICMP dropped

Reduces network reconnaissance. Internal ICMP stays for admin troubleshooting.

No HTTP, only HTTPS

Internal IIS serves over HTTPS. Blocking port 80 to S-DC removes a downgrade target.

Telnet & FTP killed

Cleartext credentials in 2026 are inexcusable. SCP for any actual file transfer needs.

P2P & anonymisers

Both common malware C2 channels and a classic data-loss vector. Off by default is the right call [3].

Question 3 - Threat Prevention (IPS)

Custom IPS profile, signatures pulled, traffic inspected at L4-L7 (20%)

What's enabled

On A-GW > Threat Prevention tab:

- IPS blade with a Custom Threat Prevention profile (Optimised baseline) [3].
- SandBlast modules (Threat Emulation, Extraction, Zero Phishing) off in this lab.
- Anti-Bot and Anti-Virus visible but not activated for the demo.

What IPS does here: inspects traffic against Check Point's signature feed for known exploits and protocol abuse, and either logs or drops based on the profile [4].

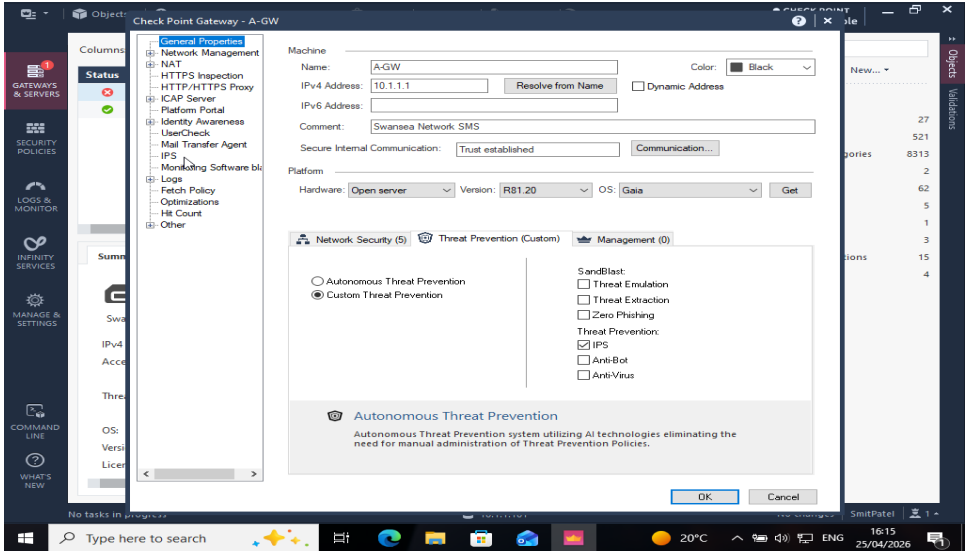


Figure 9 - A-GW Threat Prevention: Custom profile with IPS enabled

Network Security Blades - The Full Set

Application Control, URL Filtering, Identity Awareness, Content Awareness

Blade-by-blade summary

- **Firewall** — Stateful filter carrying the 19-rule policy [2].
- **Application Control** — 8000+ apps recognised at L7. Powers the P2P / anonymiser drops [3].
- **URL Filtering** — Category-based web filter feeding Block_Dangerous_URL.
- **Identity Awareness** — AD-based source identity. Backs Standard_Users_Role rule [4].
- **Content Awareness** — Data-type recognition for DLP-style controls. Visible, kept minimal here.
- **Monitoring** — Performance and traffic visibility for the lab walkthrough.

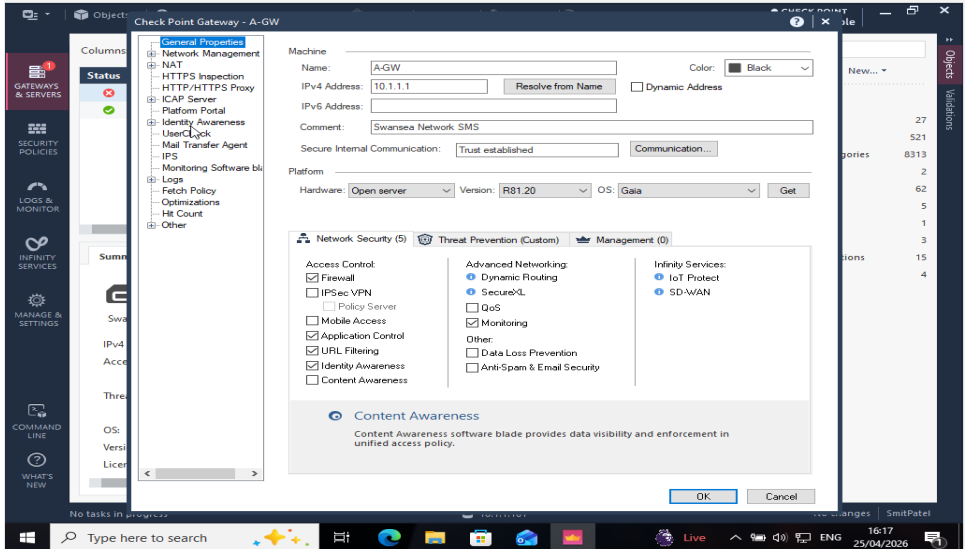
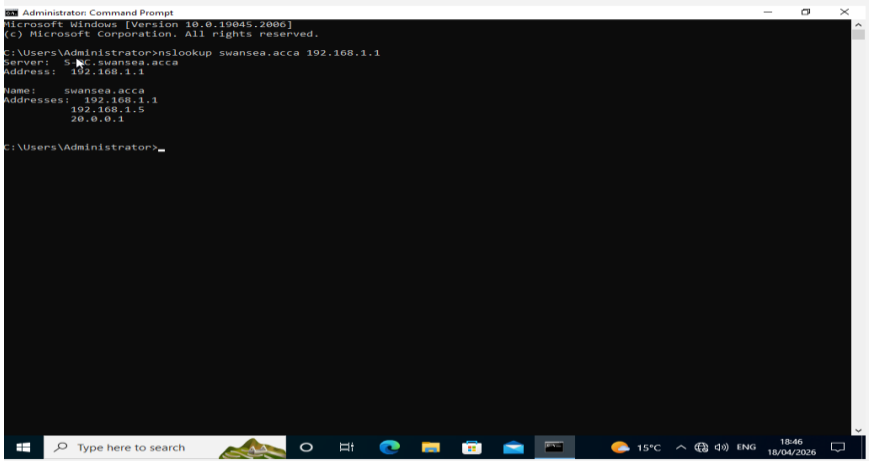


Figure 10 - A-GW Network Security blade set in General Properties

Verification - DNS Resolution and Connectivity

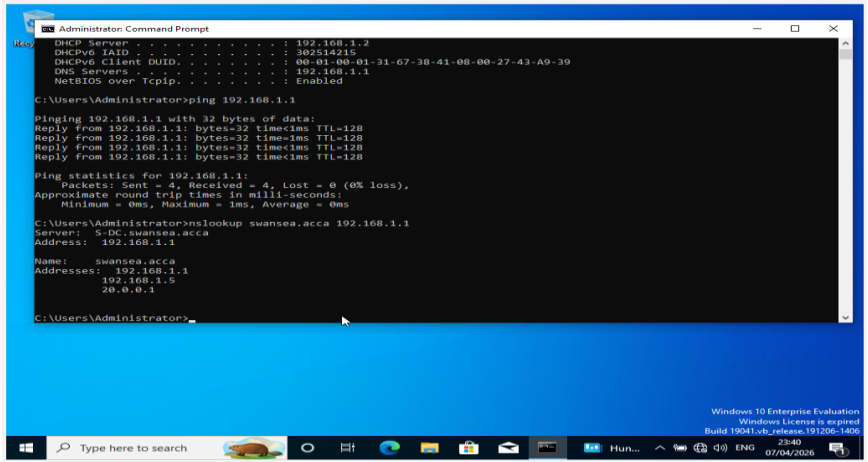
Allow-rules doing their job from the client side



`nslookup swansea.acca`

DNS resolves through S-DC at 192.168.1.1. Returns the expected internal records (192.168.1.1, 192.168.1.5, 20.0.0.1). Rule 4 (Allow_Internal_DNS) confirmed [6].

Figure 11 - nslookup against internal DNS



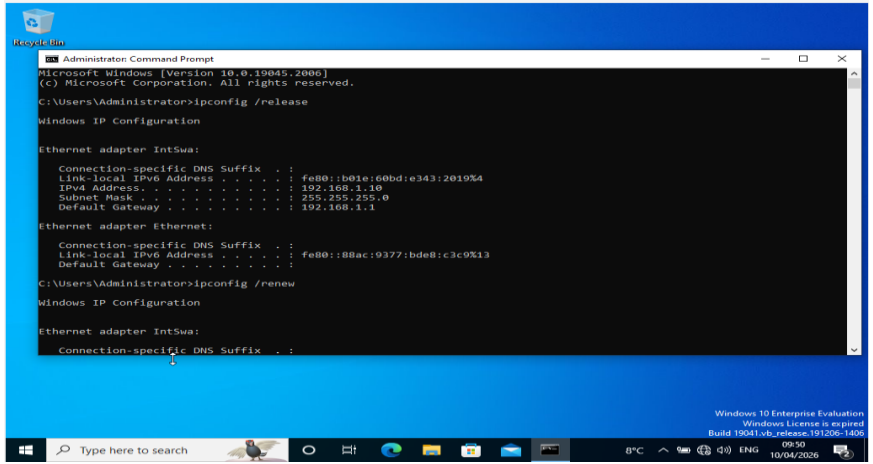
`ping 192.168.1.1`

4/4 replies, sub-1ms RTT, 0% packet loss. Rule 12 (Allow_Internal_ICMP) holds. The DHCP info above the ping shows the client also picked up its lease cleanly.

Figure 12 - ping showing intra-LAN ICMP allowed

Verification - DHCP /release and /renew

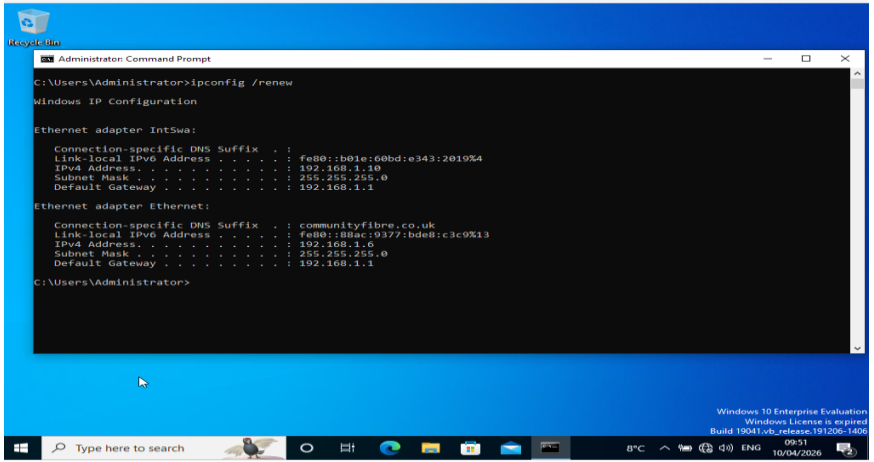
Rule 15 (Allow_DHCP) traced end-to-end on ClientS1



Step 1 - ipconfig /release

Client gives up its current lease on the IntSwa adapter (was 192.168.1.10, mask 255.255.255.0, gateway 192.168.1.1). Interface drops back to a link-local IPv6 address only - the release went through.

Figure 13 - ipconfig /release on ClientS1



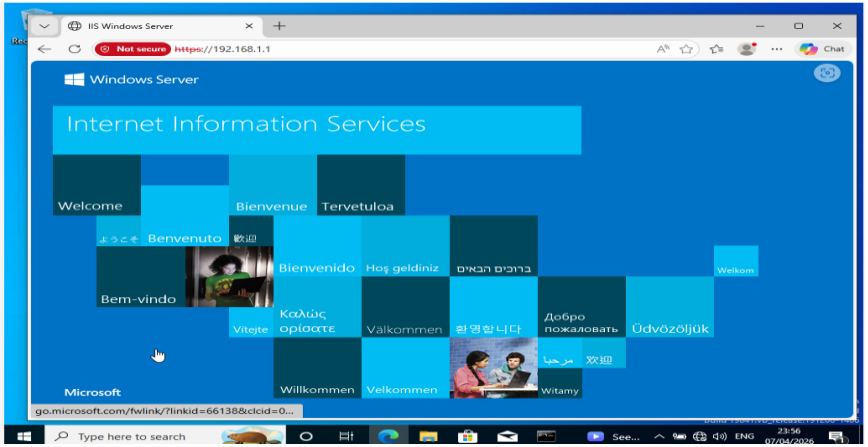
Step 2 - ipconfig /renew

Client broadcasts DHCPDISCOVER, S-DC's DHCP service answers, and the same 192.168.1.10 address is leased back. Rule 15 (Allow_DHCP, dhcp-request service) lets the broadcast/unicast exchange traverse the gateway [6].

Figure 14 - ipconfig /renew restores the lease

Verification - HTTPS Allowed, HTTP Blocked

Rule 5 and Rule 6 - same target, different protocol, different outcomes

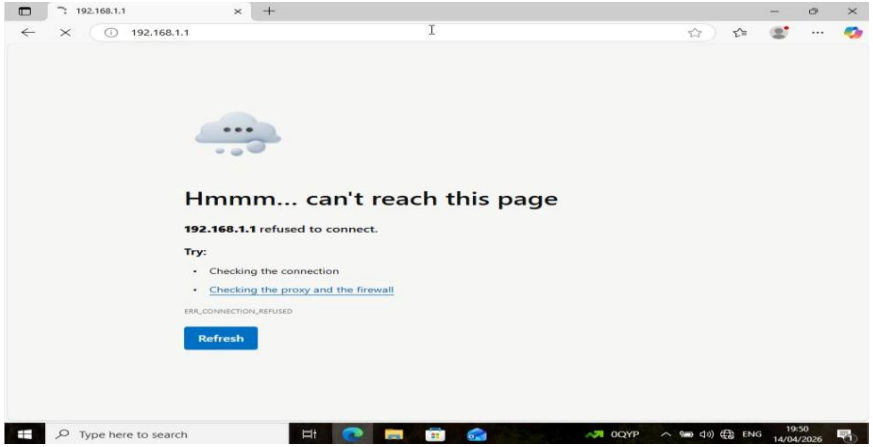


https://192.168.1.1

ALLOWED

IIS welcome page renders. Rule 5 (Allow_HTTPS_to_webServer) lets the TLS handshake reach S-DC on port 443. DNS, gateway routing and the IIS binding all work.

Figure 15 - HTTPS to S-DC permitted by Rule 5



http://192.168.1.1

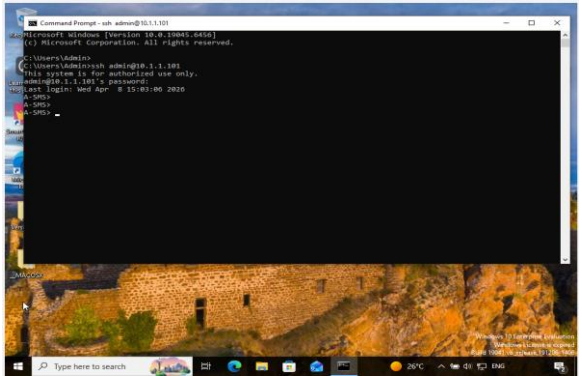
REFUSED

ERR_CONNECTION_REFUSED. Rule 6 (Block_HTTP_to_webServer) drops the SYN before it gets to port 80 - browser never sees a server response [6].

Figure 16 - HTTP to S-DC dropped by Rule 6

Verification - SSH and FTP

Same protocol, different sources, different outcomes

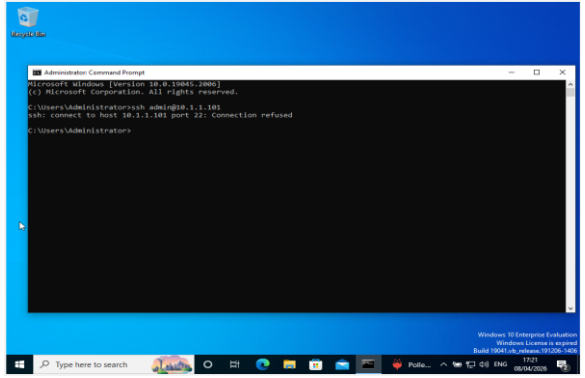


SSH from Admin (A-GUI)

ALLOWED

Login successful. Rule 8 (Allow_Admin_SSH) lets the admin workstation through to A-SMS on port 22.

Figure 17 - SSH from admin: allowed

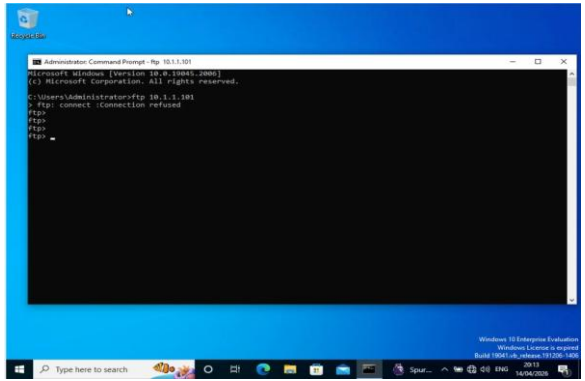


SSH from ClientS1

REFUSED

'Connection refused' on port 22. Rule 9 (Block_SSH_Others) drops everything that isn't the admin workstation [6].

Figure 18 - SSH from client: refused



FTP from ClientS1

REFUSED

'ftp: connect : Connection refused' on port 21. Rule 11 (Block_FTP) drops the connection - no cleartext file transfer leaving the LAN.

Figure 19 - FTP from client: refused

What Didn't Go to Plan

Honest review of the rough edges and what I'd do differently

IPS signature update failed

A-GW runs behind a VirtualBox NAT (10.0.5.x) and couldn't reach its upstream gateway on the host network. The cpview update job timed out. Workaround: 'ignore errors and continue'. Real fix: bridged adapter or a host-only network with proper routing [3].

Identity Awareness LDAP didn't bind

AD LDAP connection failed for the same lab routing reason - A-GW couldn't reach S-DC on 389/636 reliably. Standard_Users_Role still works because identity is sourced via Identity Collector for the demo, but I'd want a clean LDAP bind in production [4].

Same-subnet traffic doesn't traverse A-GW

ClientS1 to S-DC is intra-subnet, so the firewall doesn't see it. The rules that show up in logs are the ones crossing zones (LAN to gateway, LAN out to WAN). Tested cross-subnet behaviour to compensate.

Self-signed certificate noise

Browser warnings on Gaia portal and IIS are expected - documented but not replaced. In a real environment a small internal CA solves it cleanly [5].

Conclusion and Recommendations

Key Findings

Working Gaia R81.20 management plane built on the Part 1 topology - SMS, gateway, SmartConsole, SIC trust, licensing.

19-rule firewall policy with default-deny posture, identity-aware blocking, Layer 7 controls via App Control and URL Filtering.

Verified end-to-end from real client machines: DNS, DHCP, HTTPS allow / HTTP block, SSH source-based decision, FTP block.

IPS and Identity Awareness configured but constrained by lab routing - both work in principle and would be straightforward to fix on a real network.

Recommendations

Replace VirtualBox NAT with bridged or host-only routing so IPS signature feeds and AD LDAP bind work cleanly [3], [4].

Replace self-signed certs with an internal CA on Gaia portal and IIS - removes browser warnings and prevents a real downgrade vector [5].

Enable Anti-Bot, Anti-Virus and Threat Emulation once licences allow - the policy framework is already in place.

Schedule monthly licence and signature health checks; document expiry dates in the operations runbook [1].

Thank You | Q & A

References

[1] Check Point Software Technologies, R81.20 Security Management Administration Guide. Tel Aviv, Israel: Check Point Software Technologies Ltd., 2023.

[2] Check Point Software Technologies, "Quantum Security Gateway Best Practices for Access Control Policy," sk108600, 2024. [Online]. Available: https://support.checkpoint.com

[3] Check Point Software Technologies, R81.20 Threat Prevention Administration Guide. Tel Aviv, Israel: Check Point Software Technologies Ltd., 2023.

[4] Check Point Software Technologies, R81.20 Identity Awareness Administration Guide. Tel Aviv, Israel: Check Point Software Technologies Ltd., 2023.

[5] K. Scarfone and P. Hoffman, "Guidelines on Firewalls and Firewall Policy," NIST Special Publication 800-41 Rev. 1, National Institute of Standards and Technology, Gaithersburg, MD, 2009.

[6] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. London, U.K.: Pearson, 2017.

[7] R. Bejtlich, The Practice of Network Security Monitoring: Understanding Incident Detection and Response. San Francisco, CA: No Starch Press, 2013.

[8] M. Lucas, Networking for System Administrators. Detroit, MI: Tilted Windmill Press, 2015.