

Enterprise Network Security

(Implementation)

Name: Kcval Mahc□día Motivaías

Student Id: 251574C

Module: 6CC670C2

Lecturer: Rc□ua JaQakumaí

AIM / Objectives

- To design and implement a secure enterprise network using Check Point Firewall
- To configure access control policies and network segmentation
- To test allowed and blocked traffic using real scenarios
- To monitor network activity using logs and security tools

LAB Setup

The screenshot displays the Oracle VM VirtualBox Manager interface. On the left, a list of virtual machines is shown under the 'P3Selection' folder. The 'A-GW' VM is selected and highlighted in blue. The right pane shows the 'Details' tab for the 'A-GW' VM, displaying various configuration settings.

Virtual Machines List:

- ClientS1 (x64, 10) Powered Off
- S-DC (x64, 2022) Powered Off
- L-CD (x64, 2022) Powered Off
- ClientL1 (x64, 10) Powered Off
- A-GUI (x64, 10) Powered Off
- A-SMS (x64) Powered Off
- A-GW (x64) Powered Off**

Details for A-GW:

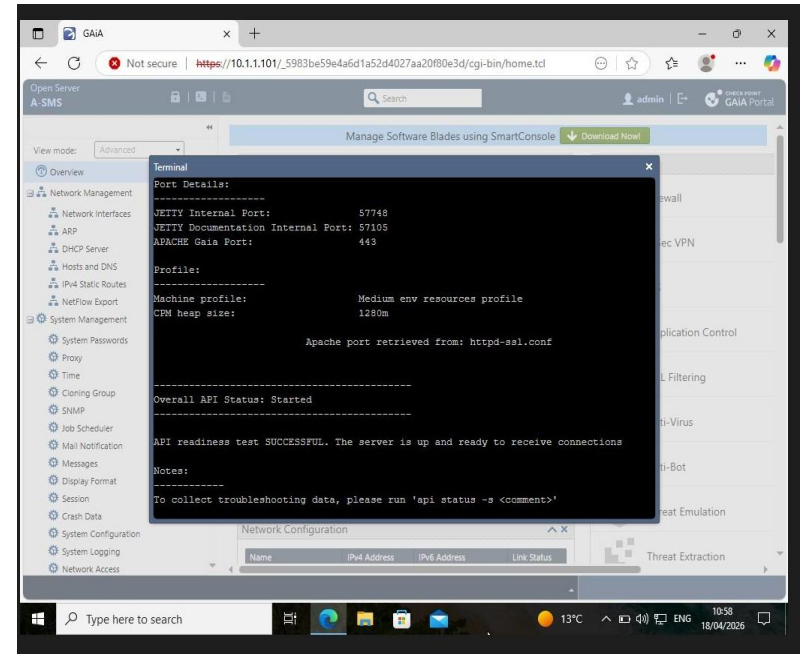
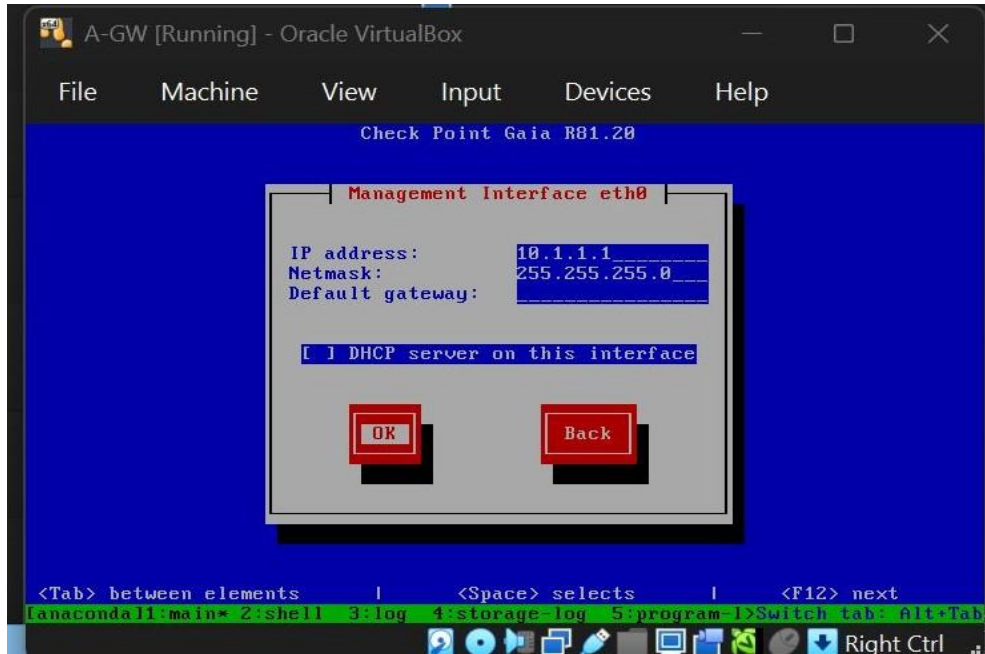
- General**
 - Name: A-GW
 - Operating System: Other/Unknown (64-bit)
- System**
 - Base Memory: 6345 MB
 - Boot Order: Hard Disk
 - Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization
- Display**
 - Video Memory: 9 MB
 - Graphics Controller: VBoxVGA
 - Remote Desktop Server: Disabled
 - Recording: Disabled
- Storage**
 - Controller: IDE
 - IDE Primary Device 0: A-GW.vdi (Normal, 40.77 GB)
 - IDE Secondary Device 0: [Optical Drive] Check_Point_R81.20_T634.iso (4.07 GB)
- Audio**
 - Host Driver: Default
 - Controller: ICH AC97
- Network**
 - Adapter 1: Intel PRO/1000 MT Desktop (Internal Network, 'IntCP')
 - Adapter 2: Intel PRO/1000 MT Desktop (Internal Network, 'IntSwa')
 - Adapter 3: Intel PRO/1000 MT Desktop (Internal Network, 'ExtLCD')
 - Adapter 4: Intel PRO/1000 MT Desktop (NAT)
- USB**
 - USB Controller: OHCI, EHCI
 - Device Filters: 0 (0 active)
- Shared folders**

System Information:

- 15°C Mostly cloudy
- Search
- 15:32 18/04/2026

Configuration

- Setting up gateway



Configuration

- WAN & LAN Setup
- Wizard Installation

The screenshot shows the Check Point GAIA Portal interface. The left sidebar contains a navigation menu with options like Overview, Network Management, and System Management. The main content area is titled 'Network Management > Network Interfaces' and shows a table of network interfaces. The 'eth3' interface is selected and highlighted in blue. Below the table, there is a 'Management Interface' section showing 'eth0' as the selected interface.

Name	Type	IPv4 Address	Subnet Mask	IPv6 Address
eth0	Ethernet	10.1.1.1	255.255.255.0	-
eth1	Ethernet	192.168.1.254	255.255.255.0	-
eth2	Ethernet	20.0.0.1	255.255.255.252	-
eth3	Ethernet	10.0.5.15	255.255.255.0	-
lo	Loopback	127.0.0.1	255.0.0.0	-

The screenshot shows the 'Check Point Gateway Installation Wizard' completion screen. The wizard has finished, and the 'Configuration Summary' is displayed. The summary includes the Gateway's Name (AGW), IPV4 (10.1.1.1), Platform (Open server), SIC (Trust established), NAT (Disabled), and Active Blades (Firewall and NAT). There is a checkbox for 'Edit Gateway properties for further configuration' which is checked. The screen also shows the 'Back', 'Finish', and 'Cancel' buttons.

Configuration Summary

- Gateway's Name: AGW
- IPV4: 10.1.1.1
- Platform: Open server
- SIC: Trust established
- NAT: Disabled
- Active Blades: Firewall and NAT

☒ Edit Gateway properties for further configuration

Managing License

- Add new license and attached to A-SMS & A-GW

The screenshot displays the Check Point SmartUpdate interface for machine 10.1.1.101. The 'Licenses & Contracts' tab is active, showing a list of licenses and contracts. Below this, the 'License And Contract Repository' table is visible, listing various licenses and their details. At the bottom, the 'Operation Status' section shows the progress of operations.

Machine List:

Machines	IPv4 Address	IPv6 Address	Operating Sy...	Vendor	Major Version	Minor Version
10.1.1.101	10.1.1.101					
A-SMS	10.1.1.101					
A-GW	10.1.1.1					

License And Contract Repository:

Attached	Machine	State	Upgrade St...	Version	IP Address	SKU	Description	Certificate ...	Na
Attached	A-GW			Software BL...	10.1.1.101	CPSG-C-8-...	Security Gateway Container for Security Gateways with 8 ...	6B626899F...	CP
Attached	A-SMS			Software BL...	10.1.1.101	CPSM-C-5 ...	Security Management container to manage up to 5 gate...	0BD70EC82...	CP
Attached	A-SMS			Software BL...	10.1.1.101	CPSB-W5 ...	Web Security blade. SSL Network Extender for unlimited ...	6B626899F...	CP
Contract...	A-SMS					CPSB-EVN...		0BD70EC82...	Co
Contract...	A-SMS					CPSB-CO...		0BD70EC82...	Co
Contract...	A-SMS					CPSB-RPRT...		0BD70EC82...	Co

Operation Status:

Operation	Status	Progress	Time

For Help, press F1

10.1.1.101 Read/Write NUM

21:30 18/04/2026

Firewall Rules

- Configured rules to allow DNS, HTTP, ICMP
- Blocked insecure services like FTP and Telnet

The screenshot displays the Check Point SmartConsole interface for configuring Firewall Rules. The left sidebar shows the navigation menu with categories like Gateways & Servers, Security Policies, Logs & Monitor, Infinity Services, Manage & Settings, Command Line, and What's New. The main area is titled 'Standard' and shows a list of rules under 'Access Control'. The 'Policy' tab is selected, showing a table of rules. Rule 6, 'Cleanup rule', is highlighted. Below the table, the 'Summary' tab for Rule 6 is shown, indicating it is a 'Drop' rule. The 'Details' tab is also visible, showing the rule's configuration, including 'Created by: System', 'Date created: 17/11/2022 01:43', 'Expiration time: Never', and 'Hit Count: 0 (0%, Zero)'. The bottom status bar shows 'No tasks in progress' and '39 Draft changes saved'.

No.	Name	Source	Destination	VPN
1	Allow_DNS	* Any	S_DC	* Any
2	Allow_HTTP	* Any	S_DC	* Any
3	Allow_Ping	* Any	* Any	* Any
4	Block_Telnet	* Any	* Any	* Any
5	Block_FTP	* Any	* Any	* Any
6	Cleanup rule	* Any	* Any	* Any

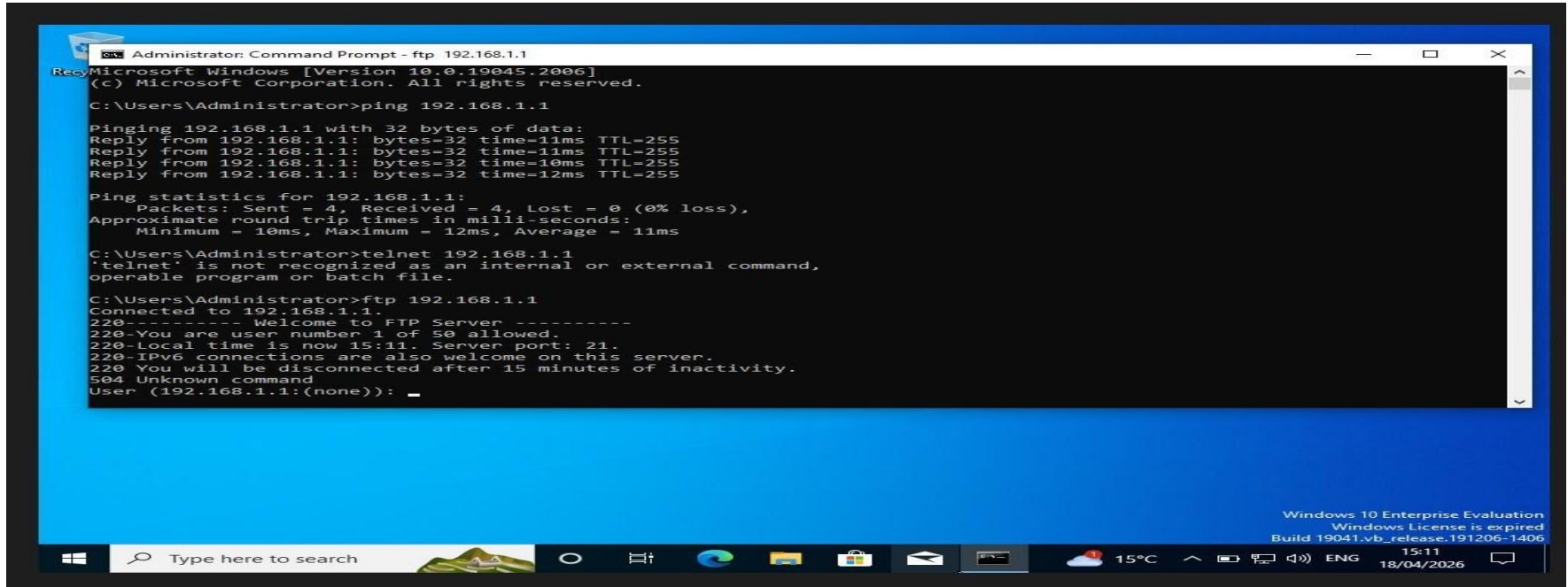
Summary Details Logs History

Cleanup rule

Created by: System
Date created: 17/11/2022 01:43
Expiration time: Never
Hit Count: 0 (0%, Zero)

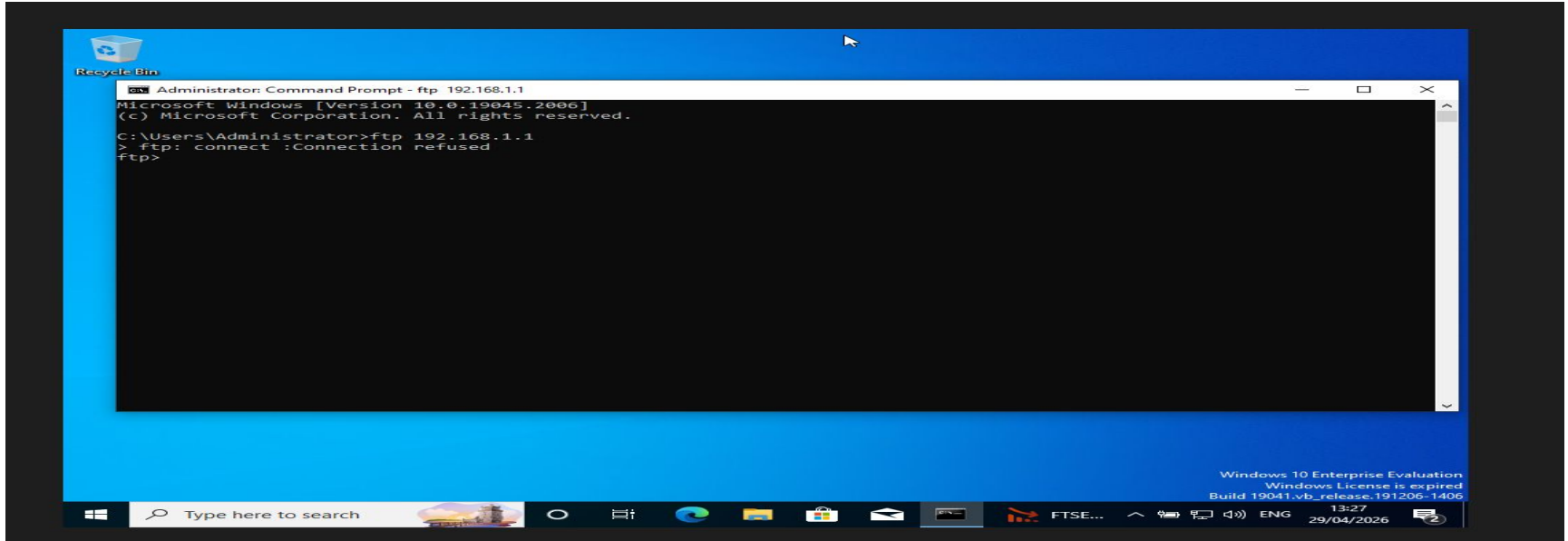
Testing

- Allow ping
- Block Telnet & FTP



Testing

- Allow ping
- Block Telnet & FTP



Logs & Monitoring

- Logs used to monitor allowed and blocked traffic
- Helps verify firewall rule behaviour in real time

The screenshot displays the Check Point SmartConsole interface. The top navigation bar includes options like 'Objects', 'Install Policy', 'Discard', 'Session', 'Changes', and 'Publish'. The left sidebar contains navigation icons for 'GATEWAYS & SERVERS', 'SECURITY POLICIES', 'LOGS & MONITOR' (which is highlighted), 'INFINITY SERVICES', 'MANAGE & SETTINGS', 'COMMAND LINE', and 'WHAT'S NEW'. The main window is titled 'fw.log' and shows a 'General Overview' of firewall logs. It features a search bar with the text 'Log File: Latest Log File' and a search icon. Below the search bar, a table displays log entries with columns for Time, Origin, Source, Source User, Destination, Service, Action, and Access Rule Name. The table shows 50 results, with the first 10 visible. The bottom section of the window shows a search interface for 'URLs' and 'Files' with a search bar and a search icon. Below the search bar, it says 'Found 0 results (1.4 sec.)'. At the bottom of the window, there is a message 'No matches found for your search'.

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Today, 14:18:41	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	6	Cleanup rule
Today, 14:18:41	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	1	Allow_DNS
Today, 14:18:36	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	6	Cleanup rule
Today, 14:18:36	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	1	Allow_DNS
Today, 14:18:25	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	6	Cleanup rule
Today, 14:18:25	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	1	Allow_DNS
Today, 14:18:17	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	6	Cleanup rule
Today, 14:18:17	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	1	Allow_DNS
Today, 14:18:14	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	6	Cleanup rule
Today, 14:18:13	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	1	Allow_DNS
Today, 14:18:13	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	6	Cleanup rule
Today, 14:18:13	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	6	Cleanup rule
Today, 14:18:13	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	1	Allow_DNS

Policies Installation

- Publish and Install to A-GW gateway

The screenshot displays the Check Point SmartConsole interface. At the top, the navigation bar includes 'Objects', 'Install Policy', 'Discard', 'Session', 'Changes', and 'Publish'. The main window is titled 'Revisions' and shows a table of installed revisions. Below the table, there is a 'Summary' tab and an 'Audit Logs' tab. The 'Summary' tab is active, showing details for the revision 'cpadmin@18/04/2026'.

The table lists the following revision:

Publish Time	Name	Publisher	Changes From Previous	Description
18/04/2026 16:26	cpadmin@18/04/2026	cpadmin	2	Changes Don...

Below the table, the 'Summary' tab is selected, showing the following information:

- cpadmin@18/04/2026**
- Changes Done By Keval
- Total of 2 changes were published by cpadmin on 18/04/2026 16:26.
- No Tags

At the bottom of the interface, a status bar indicates 'Policy installation - Standard Succeeded'. The Windows taskbar at the very bottom shows the time as 15:28 on 18/04/2026.

Implimentation

In this task, the design and implementation of a secure enterprise network environment were done using the Check Point Firewall. Several virtual machines were set up in Oracle VirtualBox, in which the interfaces eth0 and eth1 were used to establish communication from WAN and LAN. The first step was setting up the gateway, after which Secure Internal Communication (SIC) between the Management Server (A-SMS) and Gateway (A-GW) was established. Rules for DNS, HTTP, and ICMP were defined to permit them while FTP and Telnet were denied in the Firewall. This was tested using ping and web browsing, and logging was done to check the allowed and blocked traffic.

Conclusion

The project successfully demonstrated the implementation of a secure network using firewall policies and access control mechanisms. The configured rules effectively managed network traffic, and testing along with log monitoring confirmed correct functionality. This practical implementation provided a strong understanding of enterprise-level network security and firewall management.