

Applied Network Security Implementation

Rishabh Choudhary

Student ID: 2434332

Enterprise Network Security - ACCA7032

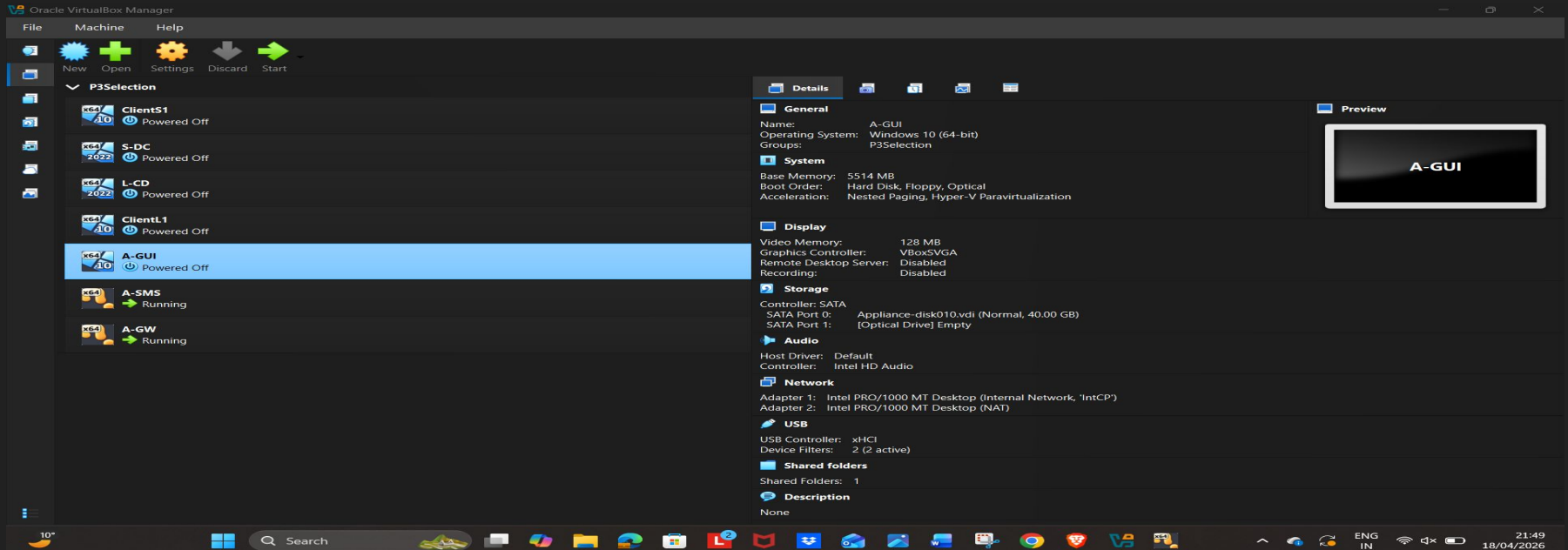


AIM / Objectives

- For creating a secure network for an organization using Check Point Firewall
- For setting access control rules and network segmentation
- For testing permitted and restricted traffic through scenarios
- For analyzing network activities with the help of log analysis

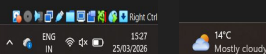
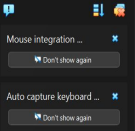
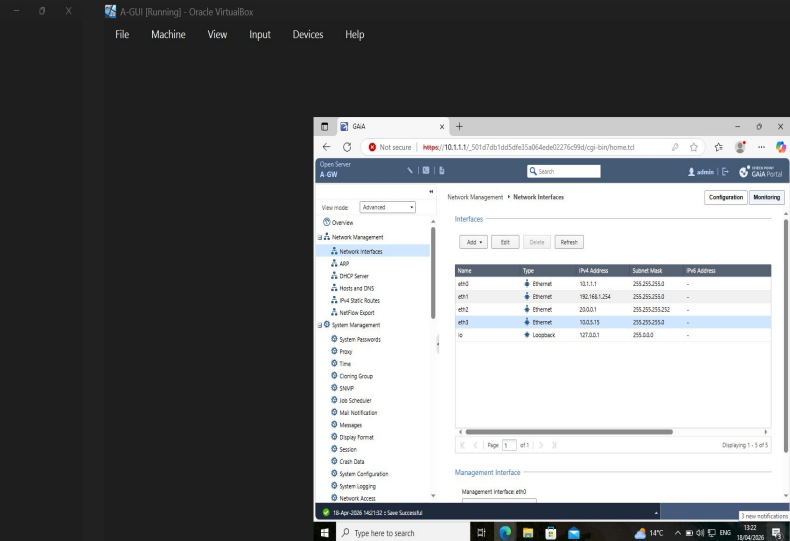
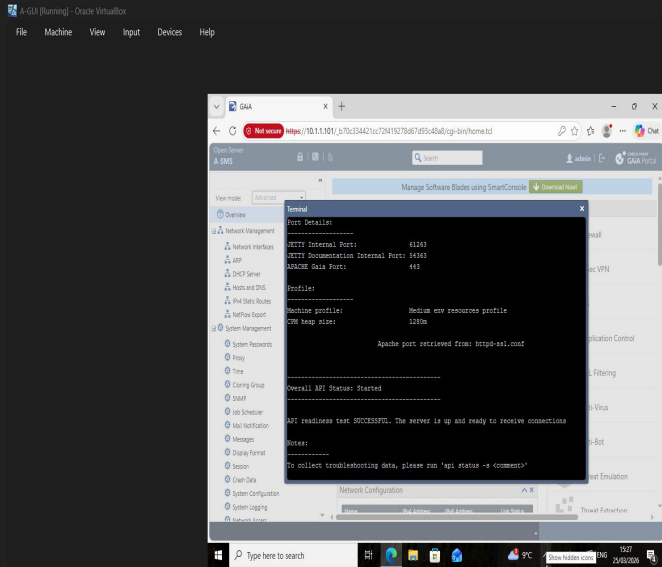
Lab Setup

- Virtual machines configured using VirtualBox
- Network adapters used to simulate real enterprise network



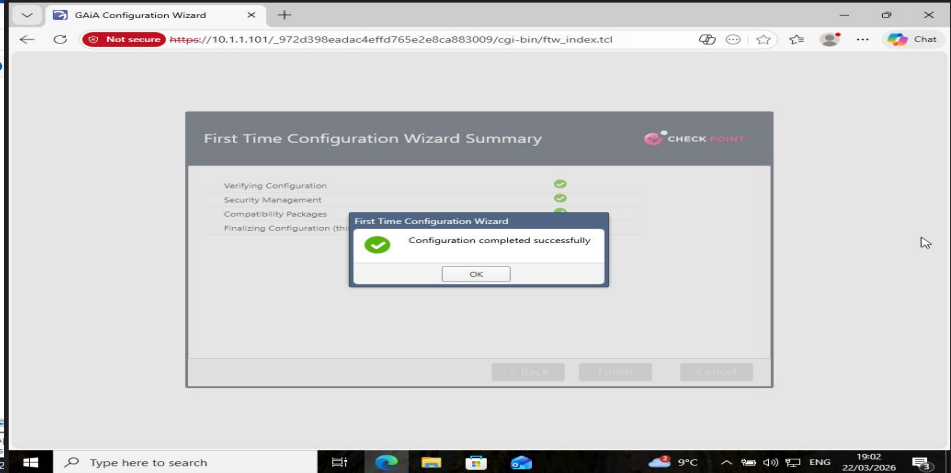
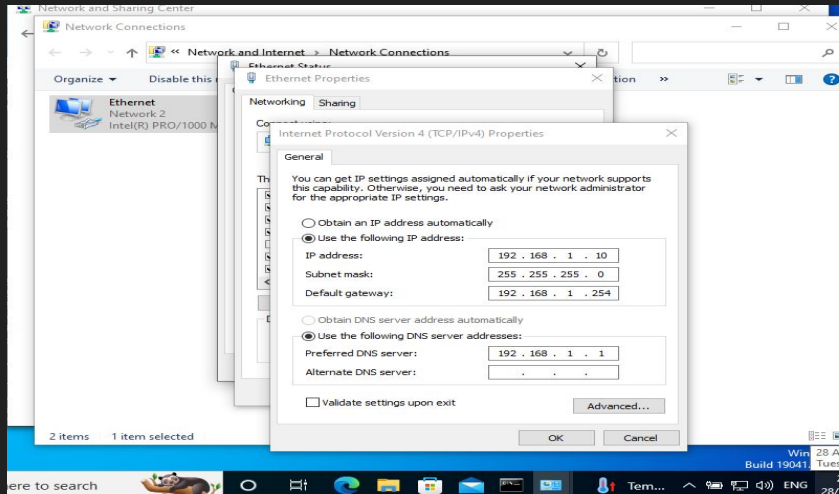
Initial Configuration

- eth0 used as external interface (WAN) for internet access
- eth1 used as internal interface (LAN) to connect lab machines securely



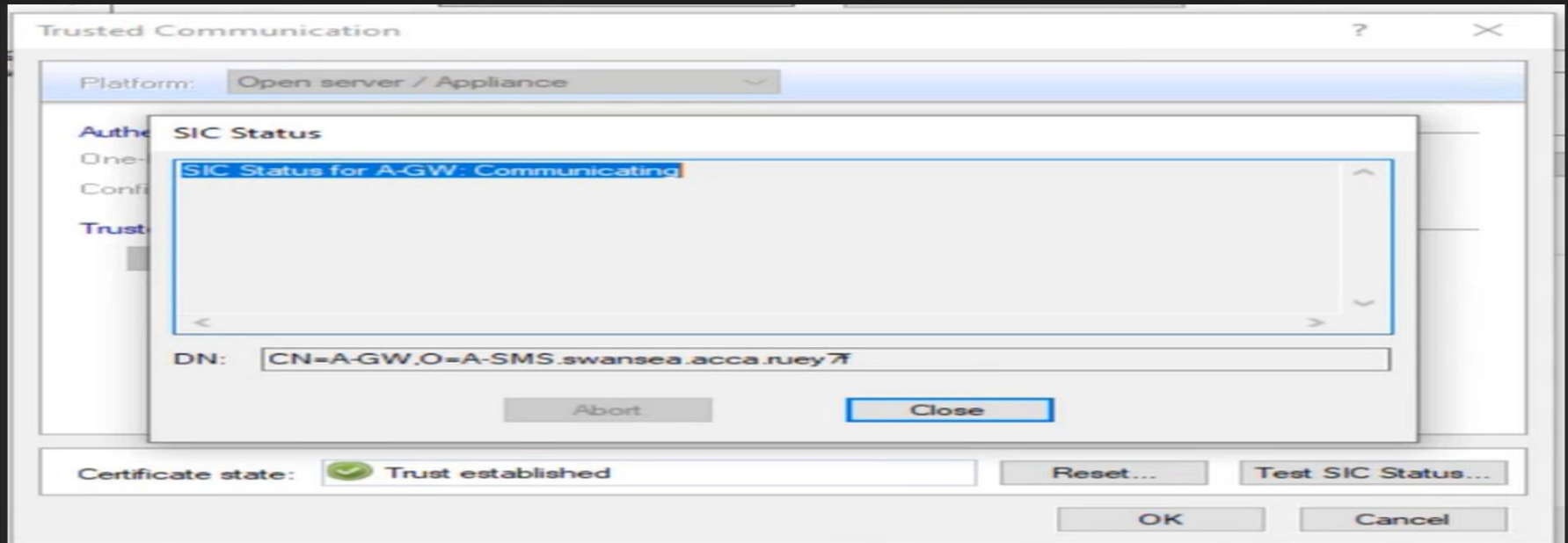
Initial Configuration

- Gateway configuration completed successfully
- Network and system setup verified
- Client machine configured with static IP, gateway, and DNS for network communication



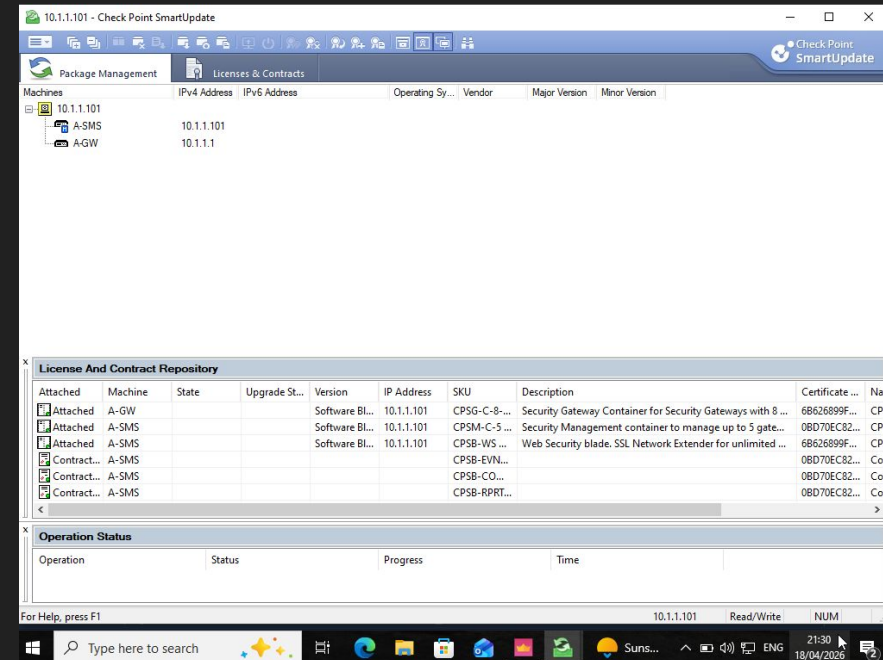
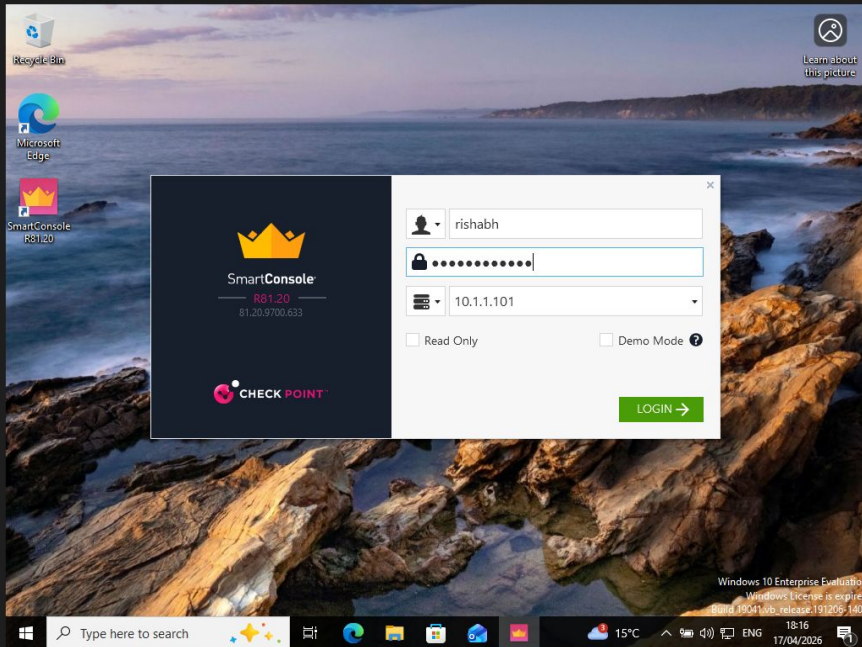
SIC Connection

- Secure Internal Communication established between A-SMS and A-GW
- Status “Communicating” confirms successful connection



SmartConsole

- SmartConsole used to manage firewall policies and objects
- Provides centralized control of security configuration



Object & Group Creation

- Created network objects and Students_Group
- Used for role-based access control

A-GUI [Running] - Oracle VirtualBox

File Machine View Input Devices Help

The screenshot displays the Check Point SmartConsole interface. On the left, the 'Object Explorer' pane shows a tree structure with categories like Network Objects, Services, and Users/Identities. The main pane shows a table of network objects. A 'Network Group' dialog box is open, titled 'Students_Group', with a search bar and a table containing one entry: 'Client_S1' with IP address '192.168.1.10'. The dialog also has 'Add Tag', 'OK', and 'Cancel' buttons.

Name	IPV4 address	Mask	IPV6 address	Mask 6	NAT Property
Client_S1	192.168.1.10				None
CP_default_Office_Mode_addresses_pool	172.16.10.0	255.255.255.0			Hide behind:

Name	IP Address	Mask	Comments
Client_S1	192.168.1.10		

Firewall Rules

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

The screenshot displays the Check Point SmartConsole interface for configuring Firewall Rules. The left sidebar contains navigation options: Gateways & Servers, Security Policies (selected), Logs & Monitor, Infinity Services, Manage & Settings, Command Line, and What's New. The main window shows a table of firewall rules under the 'Standard' tab. The table has columns for No., Name, Source, Destination, VPN, and Services & Applications. Rule 2, 'Allow_DNS', is highlighted. Below the table, the 'Summary' tab for Rule 2 is active, showing an 'Accept' action, the rule name 'Allow_DNS', a comments field, and metadata including 'Created by: rishabh', 'Date created: 12/04/2026 21:07', 'Expiration time: Never', and 'Hit Count: 1K (20%, Medium)'. The bottom status bar indicates 'No tasks in progress' and 'No changes'.

No.	Name	Source	Destination	VPN	Services & Applications
1	Students_Web_Only	Students_Group	* Any	* Any	http, https
2	Allow_DNS	* Any	S_DC	* Any	dns
3	Allow_Ping	Students_Group	* Any	* Any	icmp-requests
4	Block_Students_Server	Students_Group	S_DC	* Any	icmp-requests
5	Block_Telnet	* Any	* Any	* Any	telnet
6	Block_FTP	* Any	* Any	* Any	ftp-port
7	Cleanup rule	* Any	* Any	* Any	* Any

Summary | Details | Logs | History

Accept | Rule 2

Allow_DNS

Comments:

Created by: rishabh
Date created: 12/04/2026 21:07
Expiration time: Never
Hit Count: 1K (20%, Medium)

Addition
Ticket Nt
Ticket Re

No tasks in progress | 10.1.1.101 | No changes | rishabh

Type here to search | 0HD6 | ENG | 11:57 29/04/2026

Firewall Rules

Actions:

- Green - Accept
- Red - Drop

The screenshot shows the Check Point SmartConsole interface for configuring Firewall Rules. The left sidebar contains navigation options: Gateways & Servers, Security Policies (selected), Logs & Monitor, Infinity Services, Manage & Settings, Command Line, and What's New. The top navigation bar includes buttons for Objects, Install Policy, Discard, Session, Changes, and Publish, along with the Check Point SmartConsole logo. The main area displays a table of Firewall Rules under the 'Standard' tab. The table has columns for No., PN, Services & Applications, Action, Track, and Install On. Below the table, there are tabs for Summary, Details, Logs, and History. The 'Summary' tab is active, showing details for the selected rule 'Students_Web_Only', including its action (Accept), creation date (15/04/2026 16:19), and expiration time (Never).

No.	PN	Services & Applications	Action	Track	Install On
1	* Any	http https	Accept	Log	* Policy...
2	* Any	dns	Accept	Log	* Policy...
3	* Any	icmp-requests	Accept	Log	* Policy...
4	* Any	icmp-requests	Drop	Log	* Policy...
5	* Any	telnet	Drop	Log	* Policy...
6	* Any	ftp-port	Drop	Log	* Policy...
7	* Any	* Any	Drop	Log	* Policy...

Summary | Details | Logs | History

Students_Web_Only

Created by: rishabh
Date created: 15/04/2026 16:19
Expiration time: Never

Policies Installation

- Firewall policy installed on gateway to enforce rules

The screenshot shows the Check Point SmartConsole interface. The left sidebar contains navigation options: 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 draft changes under the 'Access Control' section. A 'Publish' dialog box is open, prompting the user to provide a session name and description before publishing the changes.

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

SmartConsole

Click 'Publish' to make these changes available to all.

You are required to provide a session name before you can publish your changes:

Session name:

Description:

Total draft changes: 36

[Show Changes](#)

The screenshot shows the 'Revisions' window in Check Point SmartConsole. It displays a table of revisions installed during the selected policy installation. The table includes columns for Publish Time, Name, Publisher, Changes From Previous, and Description. Below the table, there is a 'Summary' section showing the user 'rishabh@17/04/2026' and the total number of changes published.

Publish Time	Name	Publisher	Changes From Previous	Description
17/04/2026 20:46	rishabh@17/04/2026	rishabh	8	

Summary

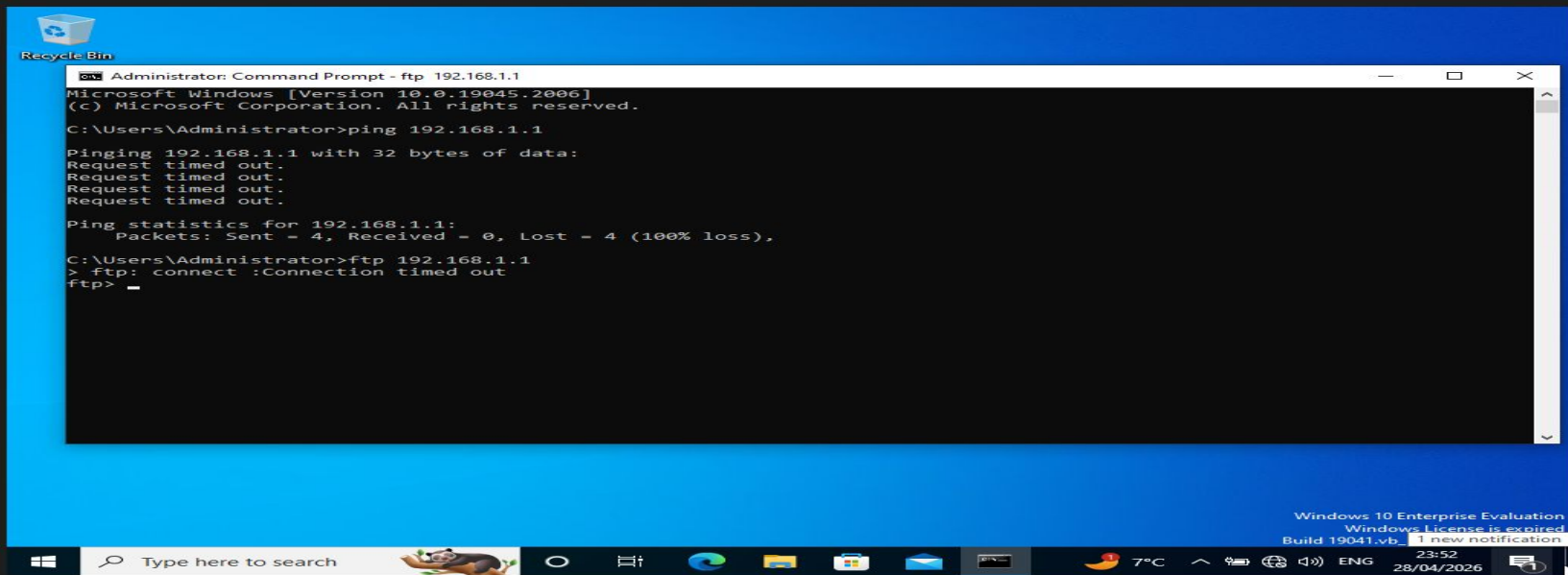
rishabh@17/04/2026
(No Description)

Total of 8 changes were published by rishabh on 17/04/2026 20:46.

No Tags

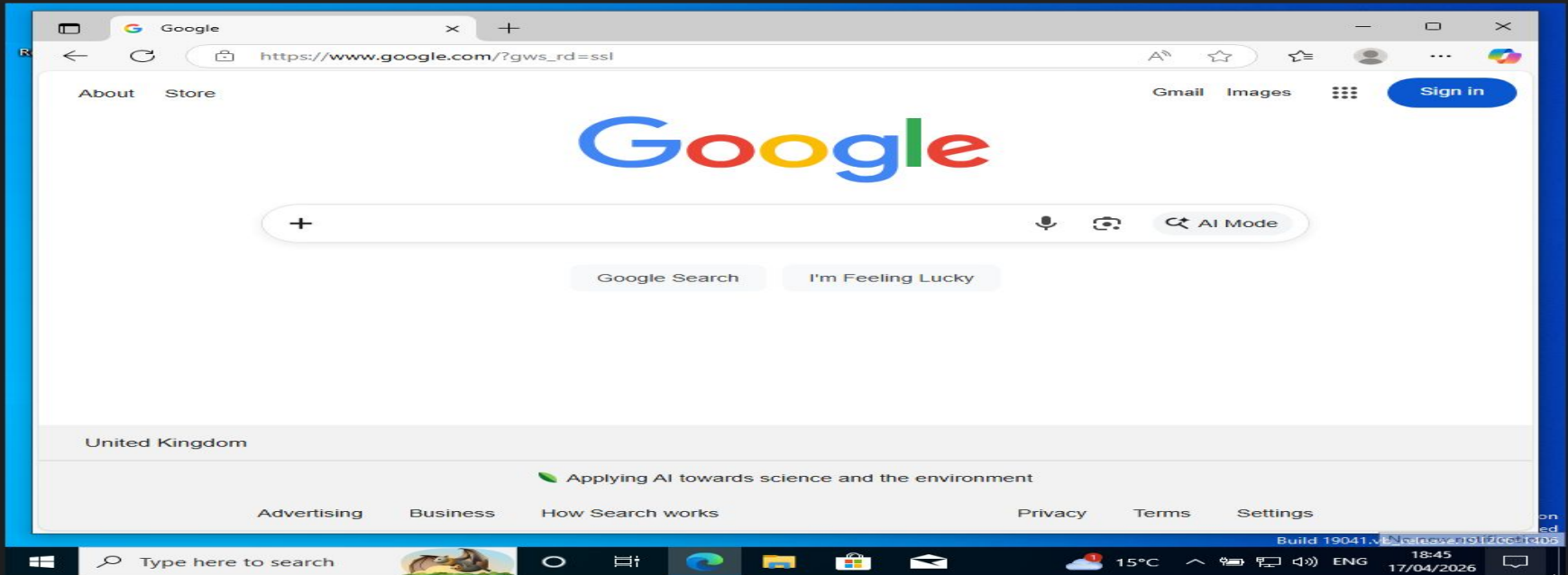
Ping Testing

- ICMP ping test performed from client machine
- Used to verify connectivity and rule behavior
- Ping blocked based on firewall rule (ICMP restriction)



HTTP Testing

- HTTP/HTTPS traffic tested using browser
- Successful access confirms rule enforcement



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' (highlighted), 'INFINITY SERVICES', 'MANAGE & SETTINGS', 'COMMAND LINE', and 'WHAT'S NEW'. The main window is titled 'fw.log' and shows a table of firewall logs. Below the table is a search section with tabs for 'URLs' and 'Files', and a search bar with the text 'Current Connection'. The search results show 'Found 0 results (1.9 sec.)' and a message 'No matches found for your search'.

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...
Today, 15:20:22	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	7	Cleanup rule
Today, 15:20:21	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	2	Allow_DNS
Today, 15:20:20	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	7	Cleanup rule
Today, 15:20:09	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	7	Cleanup rule
Today, 15:20:08	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	2	Allow_DNS
Today, 15:20:07	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	7	Cleanup rule
Today, 15:20:06	A-GW	10.1.1.201		10.1.1.255	nbdatalogram (UDP/138)	7	Cleanup rule
Today, 15:19:56	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	7	Cleanup rule
Today, 15:19:55	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	7	Cleanup rule
Today, 15:19:54	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	2	Allow_DNS
Today, 15:19:47	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	7	Cleanup rule
Today, 15:19:46	A-GW	10.1.1.201		8.8.8.8	domain-udp (UDP/53)	7	Cleanup rule
Today, 15:19:45	A-GW	10.1.1.201		S_DC (192.168.1.1)	domain-udp (UDP/53)	2	Allow_DNS

Showing first 50 results (5.3 sec.) out of at least 50 results

URLs Files

Current Connection Enter search query (Ctrl+F)

Found 0 results (1.9 sec.)

No matches found for your search

29 April 2026 Wednesday 13:27 29/04/2026

Implementation

- DNS, HTTP, and ICMP traffic rules configured in firewall
- Insecure protocols such as FTP, Telnet disabled
- User groups created (Students Group)
- Role-based access control implemented
- IPS activated for threats detection and prevention
- Order of firewall rules ensures appropriate traffic filtering (top-down approach)
- Verification of rules through testing

Scenario:

- Students allowed to use HTTP/HTTPS protocol
- Students restricted from connecting to servers
- Extended access permitted to staff (future scope)
- Alike university security framework
- Guarantees controlled and safe communication

Learning Outcomes & Conclusion

- Hands-on experience gained for Check-Point firewall
- Learned the process of filter rule traffic
- Rule order is crucial, learned about the cleanup rule
- Group network segregation skills acquired
- Monitoring and analysis of traffic learned

Conclusion:

- Secure network environment implemented successfully
- Traffic control with firewall rules successfully implemented
- Successful testing and monitoring showed proper configuration
- Acquired practical knowledge for enterprise security