CONFIGURE IDENTITY AWARENESS

A MINOR PROJECT REPORT

Submitted by

SUBHASHIS TRIPATHY [Reg No: RA2112703010020]

Under the Guidance of

DR. VIGNESHWARAN P

(Associate Professor, Department of Networking and Communications, School of Computing)

in partial fulfilment of the requirements for the degree

of

M.TECH INTEGRATED

COMPUTER SCIENCE ENGINEERING

with specialization in

CYBER SECURITY AND DIGITAL FORENSICS

DEPARTMENT OF NETWORKING AND COMMUNICATIONS
FACULTY OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603 203

MAY 2023

Scanned with CamScanner

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603203

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

This is certify that this project report titled "**CONFIGURE IDENTITY AWARENESS**" is the Bonafede work of "**SUBHASHIS TRIPATHY [Reg No: RA2112703010020]**" who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

02/05/2023

DR. VIGNESHWARAN P	**DR. ANNAPURANI PANAIYAPPAN.K**
GUIDE	**HEAD OF THE DEPARTMENT**
Associate Professor	Professor
Dept. Networking and Communications	Dept. Networking and Communications

Dept. of Networking and Communications
Kattankulathur
603 203
SRM IST

INTERNAL EXAMINER	**EXTERNAL EXAMINER**

Scanned with CamScanner

CONFIGURE IDENTITY AWARENESS

AIM

To Enable the Identity Awareness blade to allow further refinement of the security policies.

OBJECTIVES

Task1: Configuring the Security Policy for Identity Awareness

Task2: Defining the User Access Rule

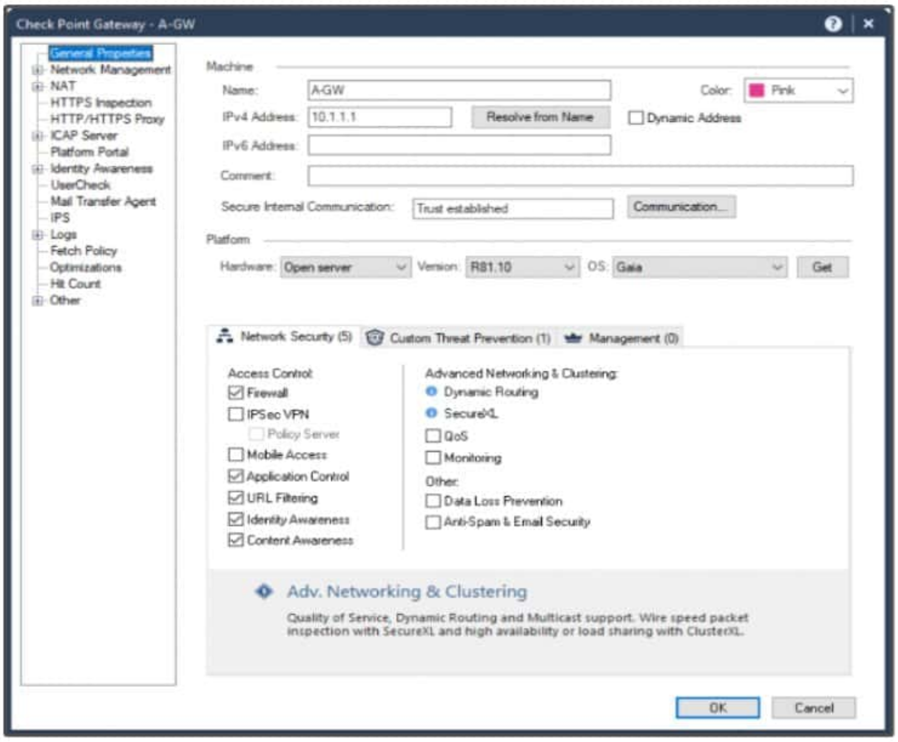
Task3: Testing the Identity Awareness Connection

Scanned with CamScanner

PROCEDURE

Configure The Security Policies For Identity Awareness

1. From the A-GUI, log into Smart Console.
2. Select **Gateways & Servers**.
3. Double-click the **A-GW** object to edit.
4. In the Network Security Section, enable **Identity Awareness**. The system displays the Identity Awareness Configuration Wizard.



Check Point Gateway - A-GW

Machine

Name: A-GW

Color: Pink

IPv4 Address: 10.1.1.1

☐ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server

Version: R81.10

OS: Gaia

Access Control

☑ Firewall

☐ IPSec VPN

☐ Policy Server

☐ Mobile Access

☑ Application Control

☑ URL Filtering

☑ Identity Awareness

☑ Content Awareness

Advanced Networking & Clustering:

● Dynamic Routing

● SecureXL

☐ QoS

☐ Monitoring

Other:

☐ Data Loss Prevention

☐ Anti-Spam & Email Security

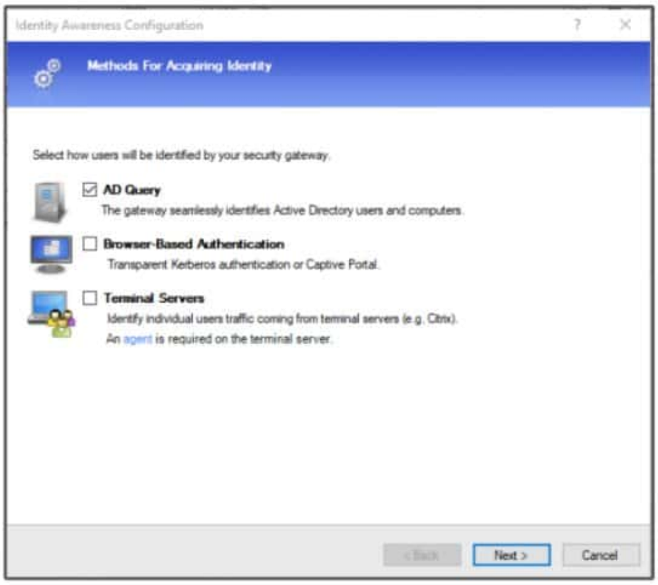
Adv. Networking & Clustering

Quality of Service, Dynamic Routing and Multicast support. Wire speed packet inspection with SecureXL and high availability or load sharing with ClusterXL.

5. Configure the Methods for Acquiring identity page as follows:

Scanned with CamScanner

AD Query:	**Enabled**
Browser-Based Authentication:	**Deselected**
Terminal Server:	**Deselected**


Identity Awareness Configuration

Methods For Acquiring Identity

Select how users will be identified by your security gateway.

☑ **AD Query**
The gateway seamlessly identifies Active Directory users and computers.

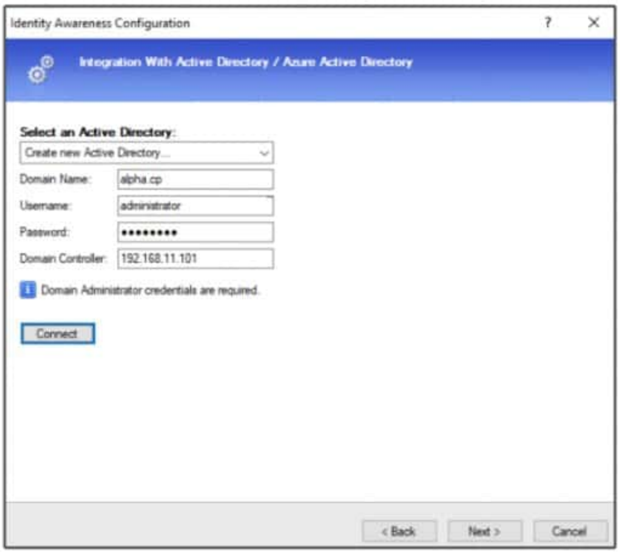
□ **Browser-Based Authentication**
Transparent Kerberos authentication or Captive Portal.

□ **Terminal Servers**
Identify individual users traffic coming from terminal servers (e.g. Citrix).
An agent is required on the terminal server.

6. Select **Next**.

7. Configure the Integration with Active Directory page as follows:

Select an Active Directory:	**Create new Domain**
Domain Name:	**alpha.cp**
Username:	**administrator**
Password:	**Chkp!234**
Domain Controller:	**192.168.11.101**


Identity Awareness Configuration

Integration With Active Directory / Azure Active Directory

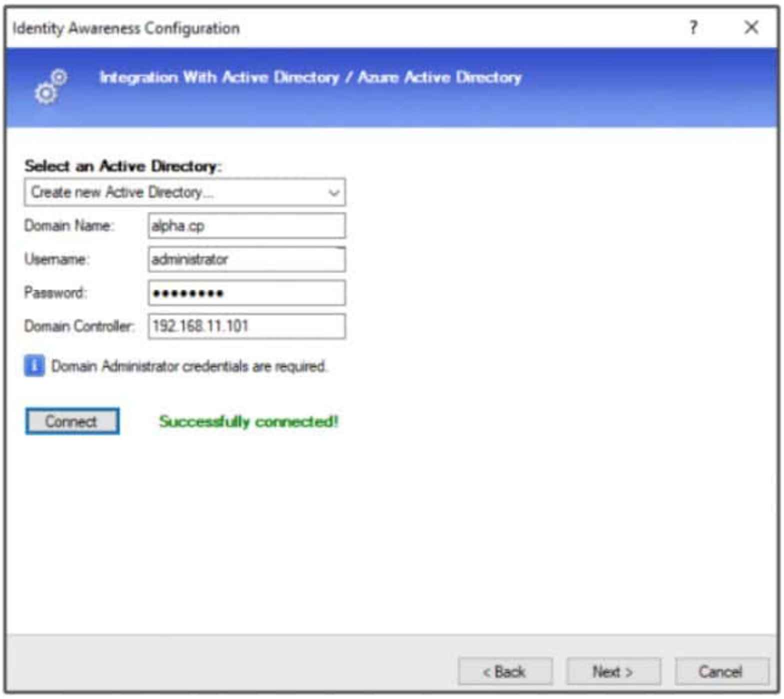
Select an Active Directory:
Create new Active Directory...

Domain Name: alpha.cp
Username: administrator
Password: ••••••••
Domain Controller: 192.168.11.101

Domain Administrator credentials are required.

8. Select Connect.

Scanned with CamScanner



Identity Awareness Configuration

Integration With Active Directory / Azure Active Directory

Select an Active Directory: Create new Active Directory...

Domain Name: alpha.cp

Username: administrator

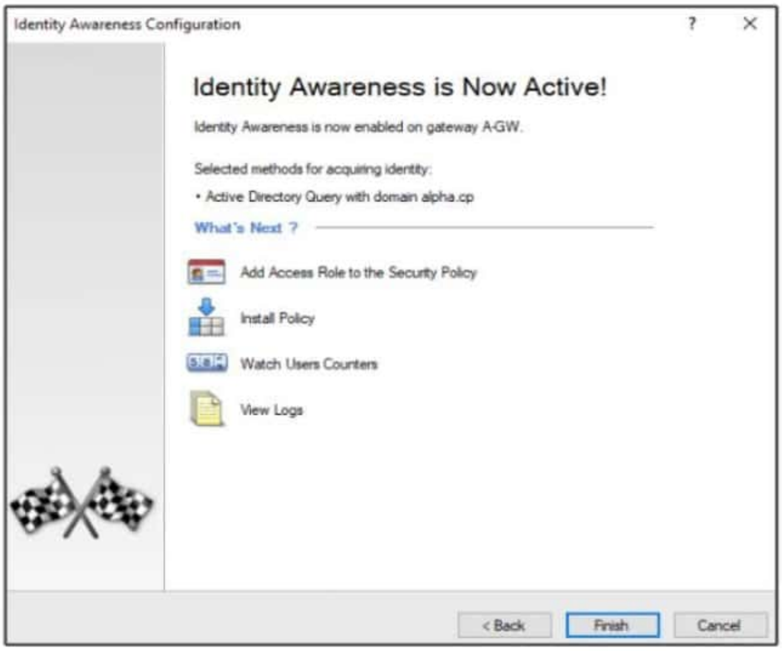
Password: •••••••••

Domain Controller: 192.168.11.101

Domain Administrator credentials are required.

Successfully connected!

9. Select **Next**, and **Finish.**



Identity Awareness Configuration

Identity Awareness is Now Active!

Identity Awareness is now enabled on gateway A-GW.

Selected methods for acquiring identity:

- Active Directory Query with domain alpha.cp

What's Next ?

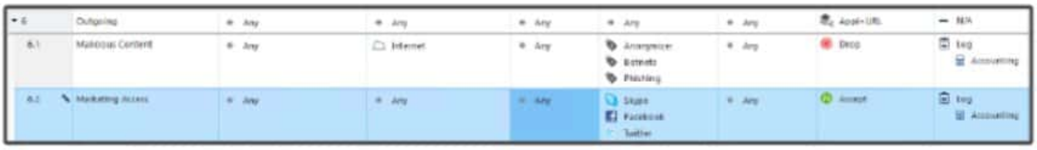
10. Select **OK**.
11. Publish the changes.

Defining the User Access Role

Scanned with CamScanner

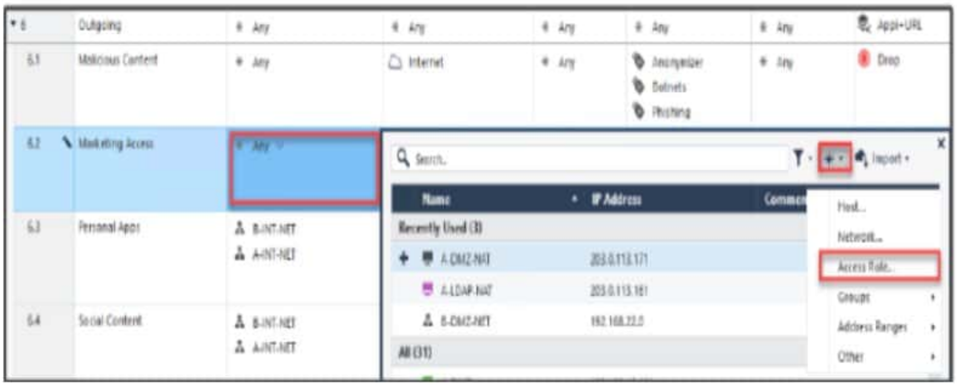
1. From the A-GUI, log in to Smart Console.
2. From the left navigation panel, select **Security Policies**.
3. Select the **Unified-Policy**.
4. Expand the Outgoing Rule.
5. Add a new rule above the Personal Apps rule
6. Configure the rule with the following Information:

Name:	**Marketing Access**
Source:	**Any**
Destination:	**Any**
Service & Applications:	**Skype** **Facebook** **Twitter**
Action:	**Accept**
Track:	**Log-accounting**



▾ 6	Outgoing	Any	Any	Any	Any	Any	Appl+URL	N/A
6.1	Malicious Content	Any	Internet	Any	Anonymizer Botnets Phishing	Any	Drop	Log Accounting
6.2	Marketing Access	Any	Any	Any	Skype Facebook Twitter	Any	Accept	Log Accounting

7. In the Source column for the Marketing Access Rule, Select the + icon.
8. Select the **New** icon.
9. Select **Access Role**.



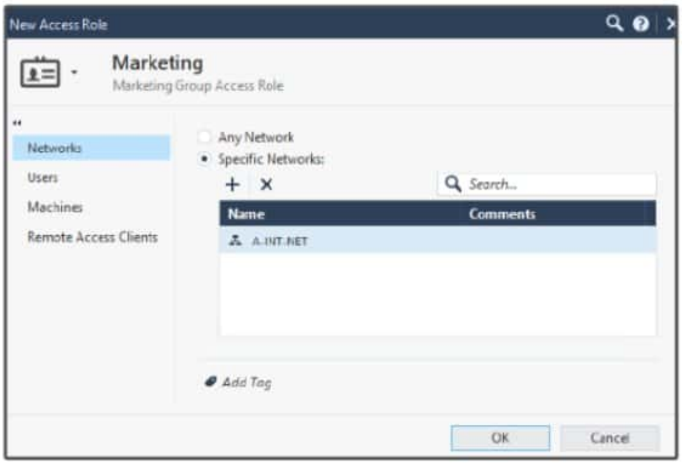
▾ 6	Outgoing	Any	Any	Any	Any	Any	Appl+URL
6.1	Malicious Content	Any	Internet	Any	Anonymizer Botnets Phishing	Any	Drop
6.2	Marketing Access	Any					
6.3	Personal Apps	B-INT-NET A-INT-NET					
6.4	Social Content	B-INT-NET A-INT-NET					

Name	IP Address	Comments
Recently Used (3)		
A-DMZ-NAT	203.0.113.171	
A-LDAP-NAT	203.0.113.181	
B-DMZ-NET	192.168.22.0	
All (31)		

10. Use the following information to configure the Access Role.

Scanned with CamScanner

Name:	**Marketing**
Comment:	**Marketing Group Access Role**
Specific Networks:	**A-INT-NET**



Marketing
Marketing Group Access Role

○ Any Network
● Specific Networks:

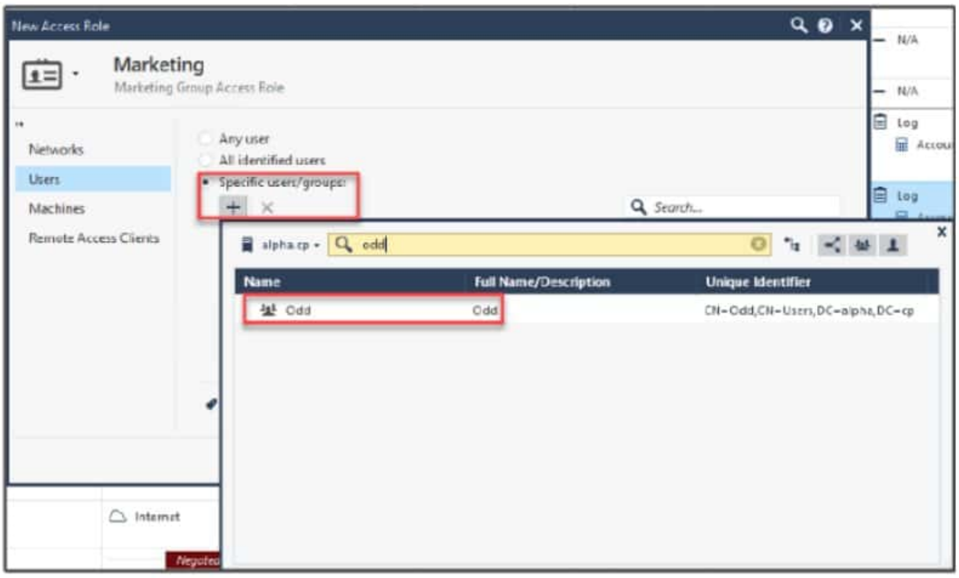
Name	Comments
A-INT-NET	

11. Navigate to **Users**.

12. Select **Specific users/groups.**

13. Select the + icon.

14. Search for and add the Odd group.



Marketing
Marketing Group Access Role

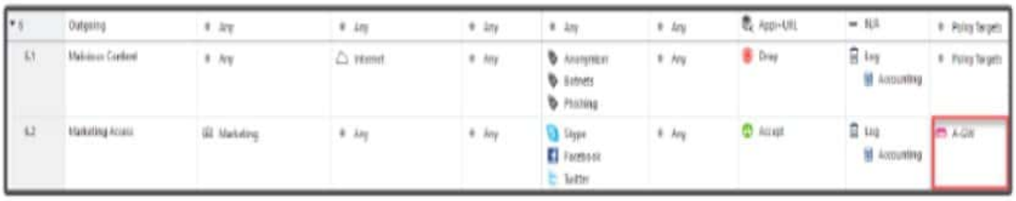
○ Any user
○ All identified users
● Specific users/groups:

odd

Name	Full Name/Description	Unique Identifier
Odd	Odd	CN=Odd,CN=Users,DC=alpha,DC=cp

15. For the Marketing Access rule, add A-GW to the Install on Column.

Scanned with CamScanner



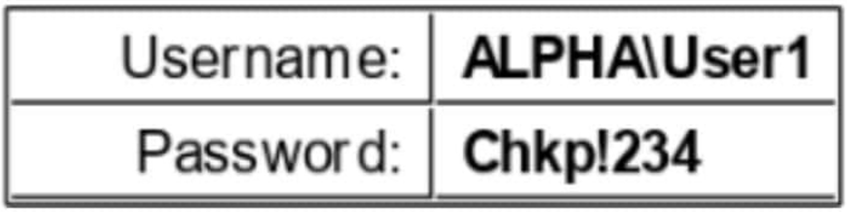
6	Outgoing	Any	Any	Any	Any	Any	Appl+URL	N/A	Policy Targets
6.1	Malicious Content	Any	Internet	Any	Anonymizer Botnets Phishing	Any	Drop	Log Accounting	Policy Targets
6.2	Marketing Access	Marketing	Any	Any	Skype Facebook Twitter	Any	Accept	Log Accounting	A-GW

16. Select **OK**.
17. Publish the changes.
18. Install the Unified-Policy security policy on the A-GW.

Testing Identity Awareness Connection

To test the Identity Awareness Connection, complete the following steps:

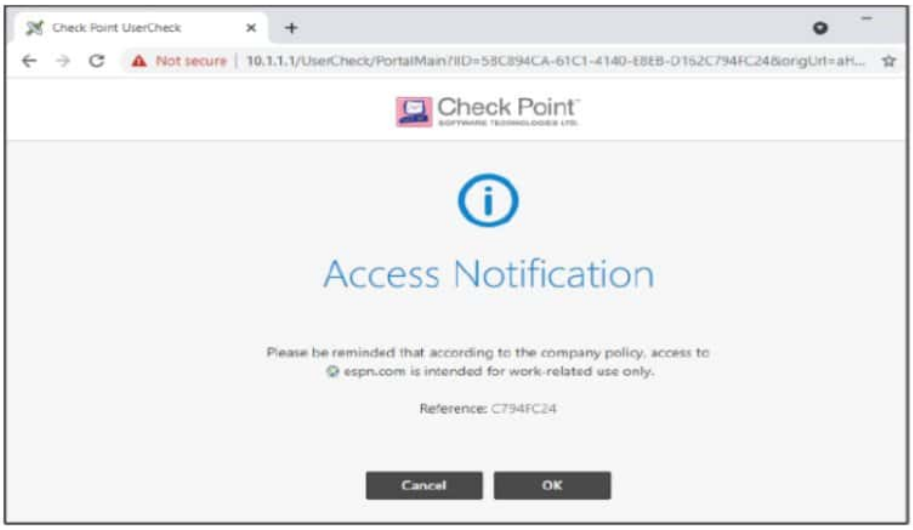
1. From the A-Host, log in with the following credentials**.**



Username:	ALPHA\User1
Password:	Chkp!234

2. Open the browser and access the following URL: **https://espn.com.**
3. On the UserCheck page, select **OK** to continue.

Scanned with CamScanner



Check Point UserCheck
Not secure | 10.1.1.1/UserCheck/PortalMain?IID=58C894CA-61C1-4140-E8EB-D152C794FC24&origUrl=aH...
Check Point
SOFTWARE TECHNOLOGIES LTD.

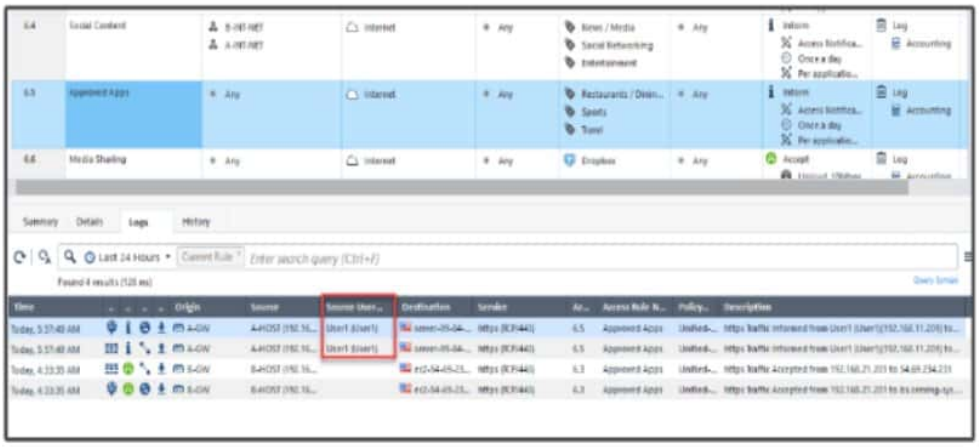
Access Notification

Please be reminded that according to the company policy, access to espn.com is intended for work-related use only.

Reference: C794FC24

Cancel OK

4. From the Security Policies menu, select the Approved Apps rule in the Unified-Policy.
5. On the bottom pane select the **Logs** tab**.**
6. Review the source and user name field.



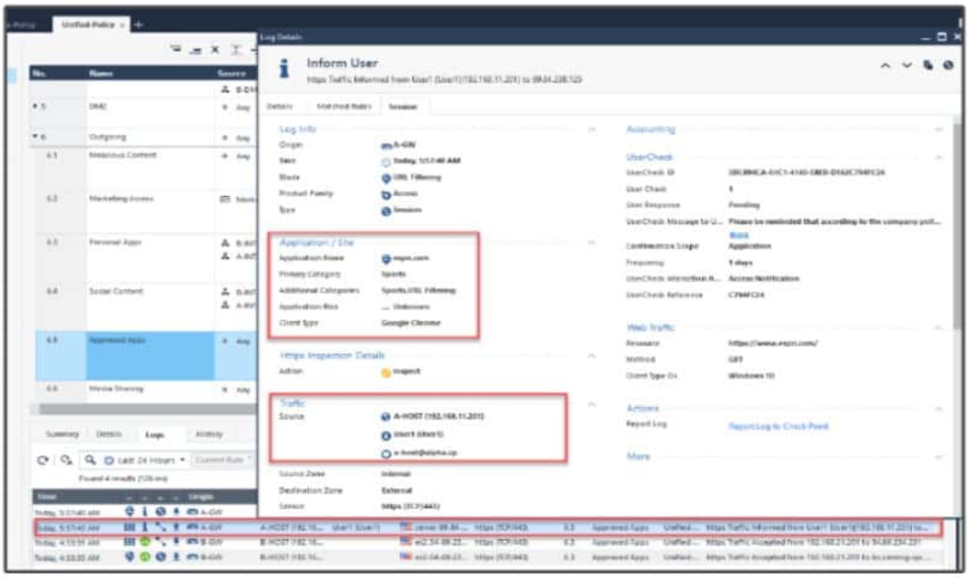
6.4	Social Content	B-INT-NET A-INT-NET	Internet	Any	News / Media Social Networking Entertainment	Any	Inform Access Notifica... Once a day Per applicatio...	Log Accounting
6.5	Approved Apps	Any	Internet	Any	Restaurants / Dinin... Sports Travel	Any	Inform Access Notifica... Once a day Per applicatio...	Log Accounting
6.6	Media Sharing	Any	Internet	Any	Dropbox	Any	Accept Upload 10Mbps	Log Accounting

Found 4 results (128 ms)

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 5:37:48 AM	A-GW	A-HOST (192.16...	User1 (User1)	server-35-04-...	https (TCP/443)	6.5	Approved Apps	Unified-...	https Traffic Informed from User1 (User1)(192.168.11.209) to...
Today, 5:37:48 AM	A-GW	A-HOST (192.16...	User1 (User1)	server-35-04-...	https (TCP/443)	6.5	Approved Apps	Unified-...	https Traffic Informed from User1 (User1)(192.168.11.209) to...
Today, 4:33:35 AM	B-GW	B-HOST (192.16...		ec2-54-69-23...	https (TCP/443)	6.3	Approved Apps	Unified-...	https Traffic Accepted from 192.168.21.201 to 54.69.234.231
Today, 4:33:35 AM	B-GW	B-HOST (192.16...		ec2-54-69-23...	https (TCP/443)	6.3	Approved Apps	Unified-...	https Traffic Accepted from 192.168.21.201 to [illegible]

7. Double-click the connection log**.**
8. In the Log Detail view, go to the **Session** tab.
9. Review the Application and the User.

Scanned with CamScanner



Inform User

https Traffic Informed from User1 (User1)(192.168.11.201) to 99.84.228.123

Log Info
Origin: A-GW
Time: Today, 5:57:40 AM
Blade: URL Filtering
Product Family: Access
Type: Session

Application / Site
Application Name: espn.com
Primary Category: Sports
Additional Categories: Sports, URL Filtering
Application Risk: Unknown
Client Type: Google Chrome

Https Inspection Details
Action: Inspect

Traffic
Source: A-HOST (192.168.11.201)
User1 (User1)
a-host@alpha.cp
Source Zone: Internal
Destination Zone: External
Service: https (TCP/443)

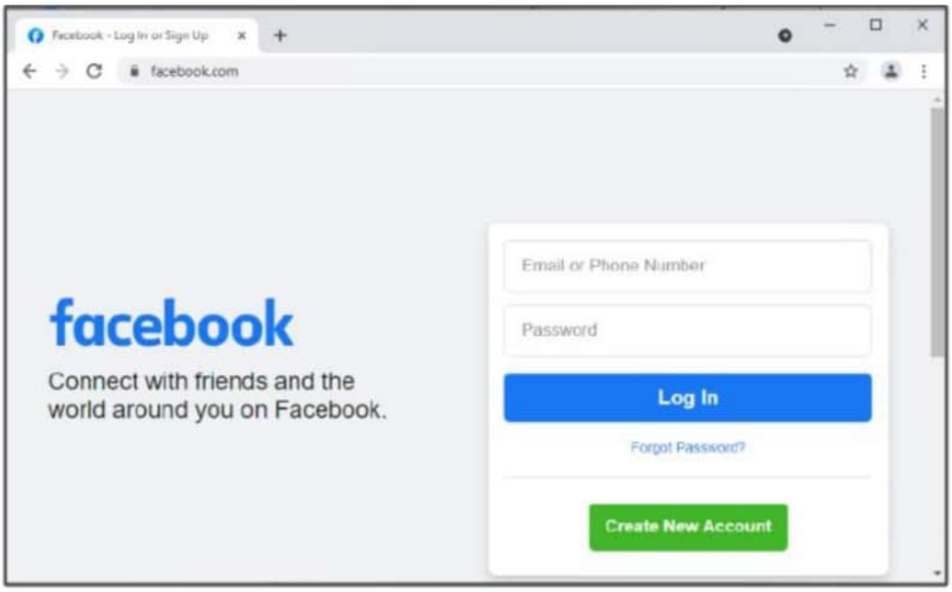
UserCheck
UserCheck ID: [illegible]
User Check: 1
User Response: Pending
UserCheck Message to U...: Please be reminded that according to the company poli... More
Confirmation Scope: Application
Frequency: 1 days
UserCheck Interaction N...: Access Notification
UserCheck Reference: C7MFC24

Web Traffic
Resource: https://www.espn.com/
Method: GET
Client Type Os: Windows 10

Actions
Report Log: Report Log to Check Point

10. Close the Log Details view.

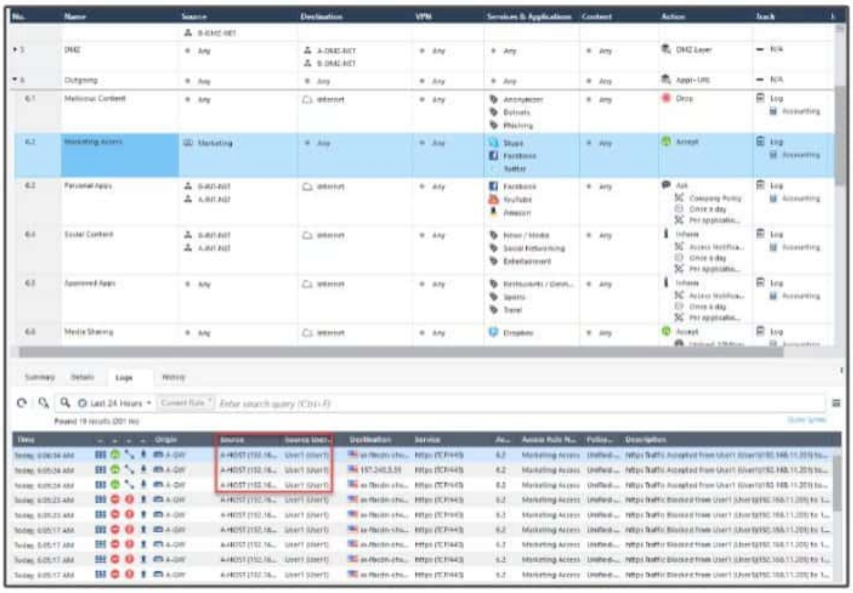
11. From the browser on A-Host, go to **https://facebook.com**.



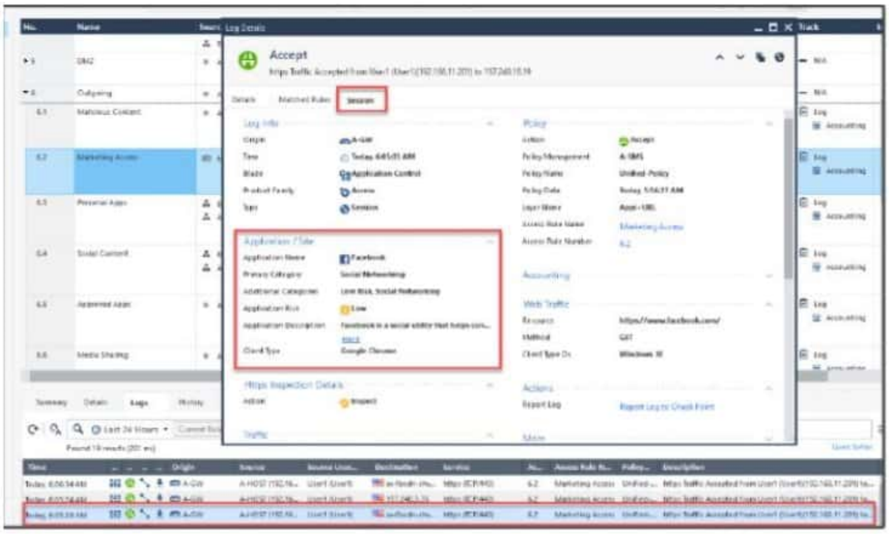
12. In SmartConsole on A-GUI, select the Marketing Access rule.

13. In the bottom pane, select the **Logs** tab.

Scanned with CamScanner



14.Locate the Facebook Session log.



Log Details

Accept

Details Matched Rules Session

Log Info

Origin A-GW

Time Today 6:05:01 AM

Blade Application Control

Product Family Access

Type Session

Application / Site

Application Name Facebook

Primary Category Social Networking

Additional Categories Low Risk, Social Networking

Application Risk Low

Application Description Facebook is a social utility that helps con...

Client Type Google Chrome

Https Inspection Details

Action Inspect

Policy

Action Accept

Policy Management A-SMS

Policy Name Unified-Policy

Layer Name Appl-URL

Access Rule Name Marketing Access

Access Rule Number 6.2

Accounting

Web Traffic

Resource https://www.facebook.com/

Method GET

Actions

Report Log Report Log to Check Point

15. Close the Log Details view.

RESULT

Successfully configured Identity Awareness.

Scanned with CamScanner