

Ikbar Muhammad Mumtaz

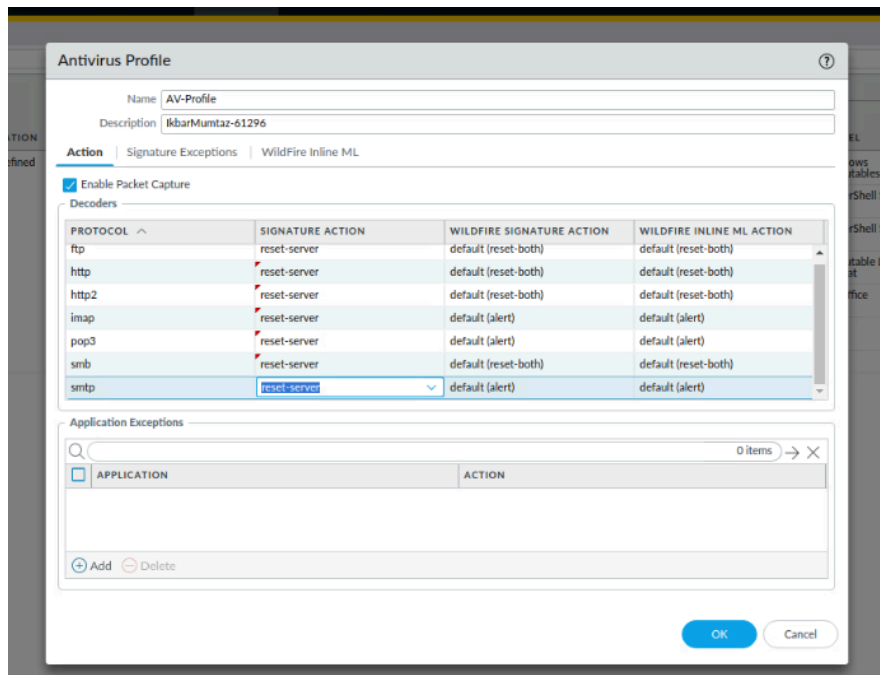
00000061296

IF 673: Cybersecurity: Firewall Configuration and Management

1. Soal 1: Early Prevention Sub-CLO0714 + Sub-CLO0721, and Bobot / Weight (25%+20%)

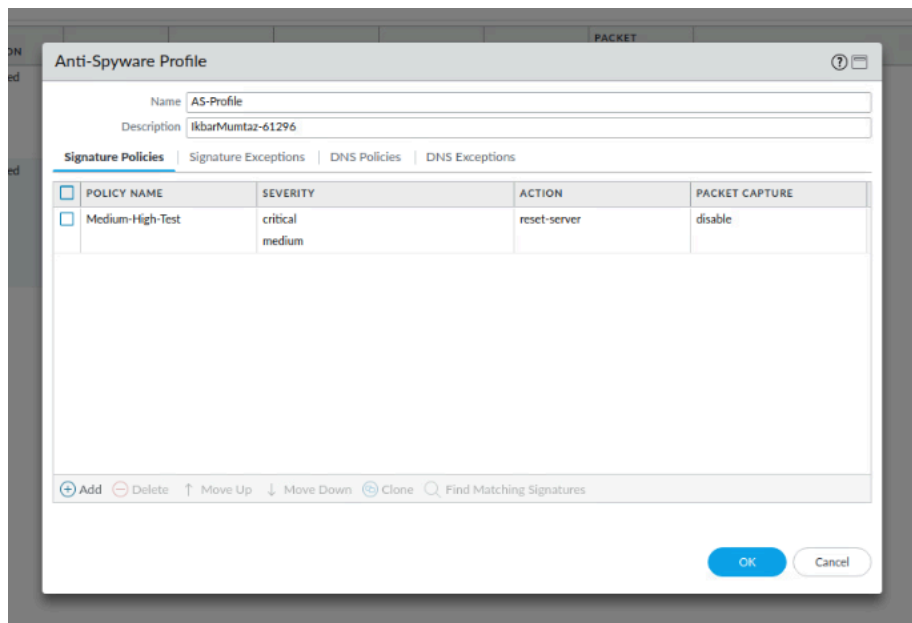
1) Antivirus Profile

Konfigurasi profil antivirus di perangkat Palo Alto bertujuan untuk melindungi jaringan dari ancaman malware dengan menetapkan tindakan spesifik untuk berbagai tingkat ancaman. Langkah pertama adalah masuk ke antarmuka web Palo Alto dan navigasi ke Objects > Security Profiles > Antivirus. Di sini, Anda dapat menambahkan profil baru dengan mengklik Add dan memberi nama profil tersebut, misalnya, "AV-Profile". Selanjutnya, Anda perlu mengkonfigurasi pengaturan profil ini dengan menetapkan tindakan pada level ancaman sedang hingga kritis menjadi Block. Tujuannya adalah untuk memastikan bahwa semua ancaman dengan tingkat keparahan sedang dan tinggi akan diblokir secara otomatis oleh sistem keamanan, sehingga meningkatkan perlindungan terhadap potensi serangan malware yang dapat merusak atau mengganggu jaringan.



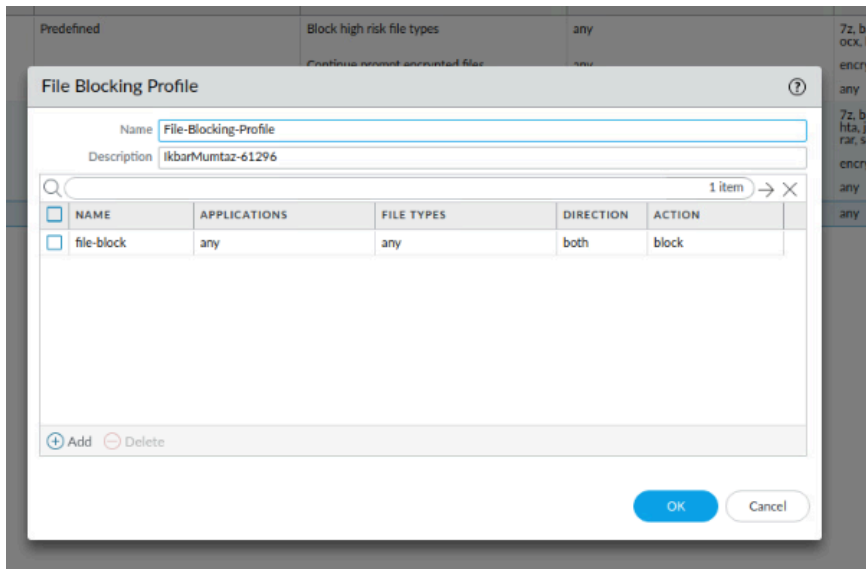
## 2) Anti-Spyware Profile

Saat ini kita akan mengkonfigurasi Anti-spyware, Konfigurasi profil anti-spyware pada perangkat Palo Alto bertujuan untuk melindungi jaringan dari ancaman spyware dengan menetapkan tindakan spesifik untuk berbagai tingkat ancaman. Langkah pertama adalah masuk ke antarmuka web Palo Alto dan navigasi ke Objects > Security Profiles > Anti-Spyware. Di sini, Anda dapat menambahkan profil baru dengan mengklik Add dan memberi nama profil tersebut, misalnya, "AntiSpyware-Profile". Selanjutnya, Anda perlu mengkonfigurasi pengaturan profil ini dengan menetapkan tindakan pada level ancaman sedang hingga kritis menjadi reset-both atau tindakan serupa yang efektif memblokir ancaman tersebut. Tujuannya adalah untuk memastikan bahwa semua ancaman dengan tingkat keparahan sedang dan tinggi akan ditangani secara otomatis oleh sistem keamanan, sehingga meningkatkan perlindungan terhadap potensi serangan spyware yang dapat merusak atau mengganggu jaringan.



### 3) File Blocking Profile

Konfigurasi profil file blocking pada perangkat Palo Alto bertujuan untuk melindungi jaringan dari file-file berbahaya dengan menetapkan aturan spesifik untuk memblokir tipe file tertentu. Langkah pertama adalah masuk ke antarmuka web Palo Alto dan navigasi ke Objects > Security Profiles > File Blocking. Di sini, Anda dapat menambahkan profil baru dengan mengklik Add dan memberi nama profil tersebut, misalnya, "FileBlocking-Profile". Selanjutnya, tambahkan aturan untuk memblokir tipe file berbahaya yang umum, seperti exe, dll, dan js, dengan menetapkan tindakan menjadi Block. Tujuannya adalah untuk memastikan bahwa file-file dengan potensi ancaman tinggi ini diblokir secara otomatis oleh sistem keamanan, sehingga meningkatkan perlindungan terhadap malware dan serangan yang dapat mengganggu atau merusak jaringan.



### 4) URL Filtering Profile

Konfigurasi profil URL filtering pada perangkat Palo Alto bertujuan untuk melindungi jaringan dari akses ke situs web berbahaya dengan menetapkan aturan spesifik untuk memblokir kategori URL tertentu. Langkah pertama adalah masuk ke antarmuka web Palo Alto dan navigasi ke Objects > Security Profiles > URL Filtering. Di sini, Anda dapat menambahkan profil baru dengan mengklik Add dan memberi nama profil tersebut, misalnya, "URLFiltering-Profile". Selanjutnya, tambahkan kategori URL yang ingin diblokir, seperti malware, phishing, atau high-risk, dengan menetapkan tindakan menjadi Block. Tujuannya adalah untuk memastikan bahwa akses ke situs web berisiko tinggi ini diblokir secara otomatis oleh sistem keamanan, sehingga meningkatkan perlindungan terhadap ancaman online yang dapat merusak atau mengganggu jaringan.

**URL Filtering Profile**

Name: URLfiltering-Profile  
Description: IkbarMumtaz-61296

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

77 items

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
Pre-defined Categories		
<input type="checkbox"/> abortion	block	block
<input type="checkbox"/> abused-drugs	block	block
<input type="checkbox"/> adult	block	block
<input checked="" type="checkbox"/> alcohol-and-tobacco	allow	allow
<input type="checkbox"/> artificial-intelligence	allow	allow
<input type="checkbox"/> auctions	allow	allow

\* Indicates a custom URL category. + Indicates external dynamic list

[Check URL Category](#)

OK Cancel

### 5) Egress Policy (Inside to Outside)

Konfigurasi kebijakan egress (Inside to Outside) pada perangkat Palo Alto bertujuan untuk mengontrol dan mengamankan lalu lintas yang keluar dari jaringan internal ke jaringan eksternal. Langkah pertama adalah masuk ke antarmuka web Palo Alto dan navigasi ke Policies > Security, kemudian klik Add untuk membuat kebijakan baru. Pada tab General, beri nama kebijakan tersebut, misalnya, "Inside-to-Outside". Pada tab Source, pilih zona asal (Inside) dan subnet atau alamat IP asal. Pada tab Destination, pilih zona tujuan (Outside). Pada tab Actions, pilih profil keamanan yang telah dibuat: Antivirus Profile (AV-Profile), Anti-Spyware Profile (AntiSpyware-Profile), Vulnerability Protection Profile (Vulnerability-Profile), File Blocking Profile (FileBlocking-Profile), dan URL Filtering Profile (URLFiltering-Profile). Tujuannya adalah untuk memastikan bahwa lalu lintas yang keluar dari jaringan internal ke jaringan eksternal diawasi dan dilindungi oleh berbagai lapisan keamanan, sehingga meningkatkan perlindungan terhadap ancaman dan serangan dari luar.

**Security Policy Rule**

General | Source | Destination | Application | Service/URL Category | **Actions** | Usage

**Action Setting**

Action: **Allow**  
☐ Send ICMP Unreachable

**Profile Setting**

Profile Type: Profiles  
Antivirus: AV-Profile  
Vulnerability Protection: None  
Anti-Spyware: AS-Profile  
URL Filtering: URLfiltering-Profile  
File Blocking: File-Blocking-Profile  
Data Filtering: None  
WildFire Analysis: None

**Log Setting**

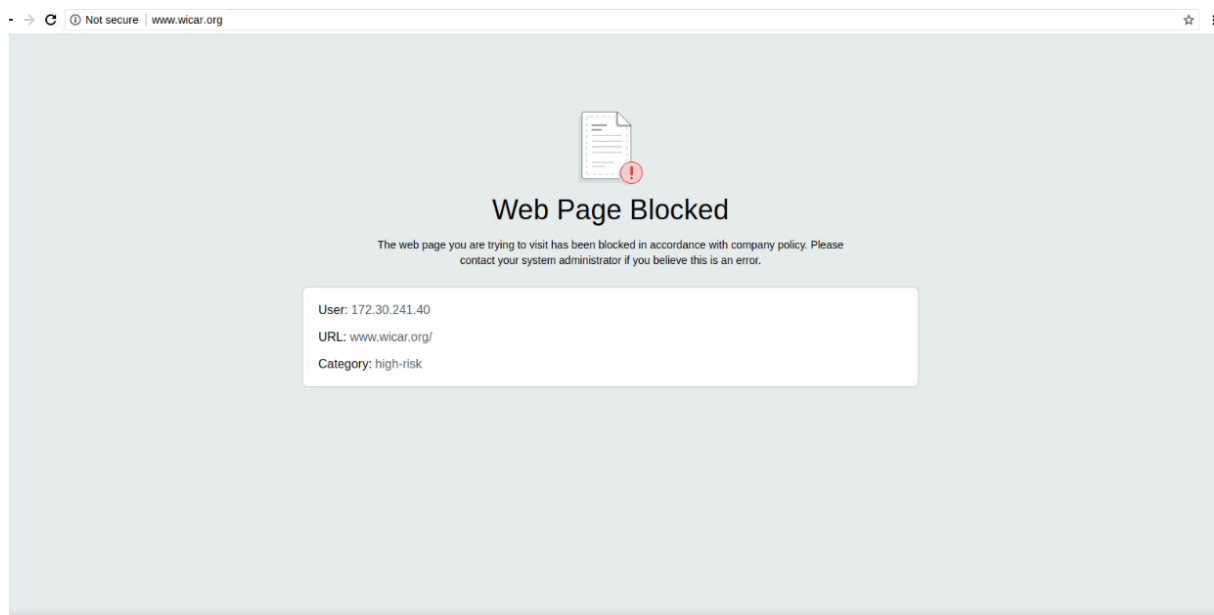
☐ Log at Session Start  
☒ Log at Session End  
Log Forwarding: None

**Other Settings**

Schedule: None  
QoS Marking: None  
☐ Disable Server Response Inspection

OK Cancel

## 6) Hasil website yang terblokir

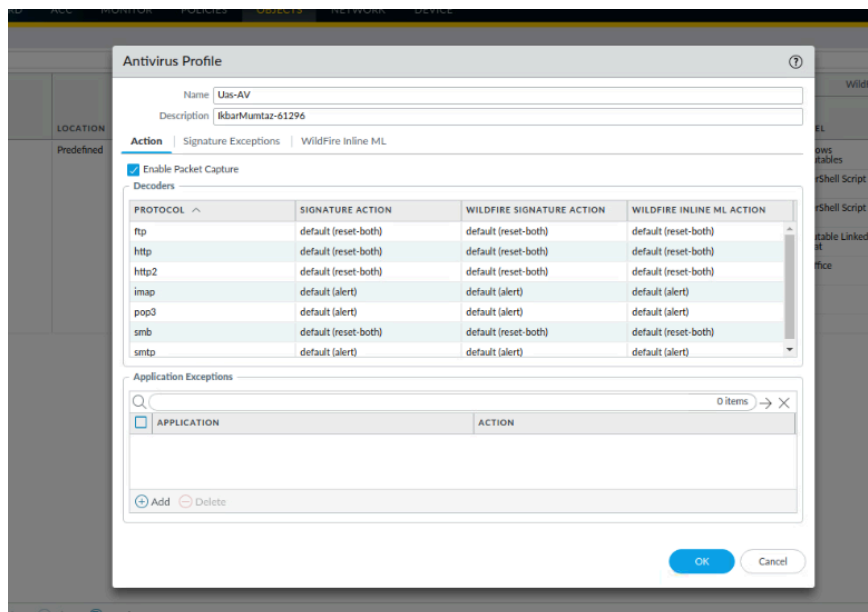


## 2. Soal 2: Malware Protection Sub-CLO0722 + Sub-CLO0724, Bobot / Weight (15%+20%)

Membuat 2 buah sertifikat: trusted-ca dan untrusted-ca.

<input type="checkbox"/>	trusted-ca	CN = trusted-ca	CN = trusted-ca	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	May 31 03:42:11 2025 GMT	valid
<input type="checkbox"/>	untrusted-ca	CN = untrusted-ca	CN = untrusted-ca	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	May 31 03:43:32 2025 GMT	valid

lalu membuat Antivirus, Spyware, Vulnerability Protection, serta Firewall Analysis Profile untuk mengidentifikasi Traffic.



PACKET

Anti-Spyware Profile

?

Name

Uas-A5

Description

IkbarMumtaz-61296

Signature Policies

Signature Exceptions

DNS Policies

DNS Exceptions

<input type="checkbox"/>	POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	crit-high	critical high	reset-server	disable
<input type="checkbox"/>	med-low	medium low	reset-server	disable

+

 Add 

-

 Delete 

↑

 Move Up 

↓

 Move Down 

⌙

 Clone 

🔍

 Find Matching Signatures

OK

Cancel

COUNT

RULE NAME

THREAT NAME

HOST TYPE

SEVERITY

ACTION

PACKET CAPTURE

Vulnerability Protection Profile

?

Name

Uas-vulne

Description

IkbarMumtaz-61296

Rules

Exceptions

<input type="checkbox"/>	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	policy-vulne	any	any	any	critical medium	reset-server	disable

+

 Add 

-

 Delete 

↑

 Move Up 

↓

 Move Down 

⌙

 Clone 

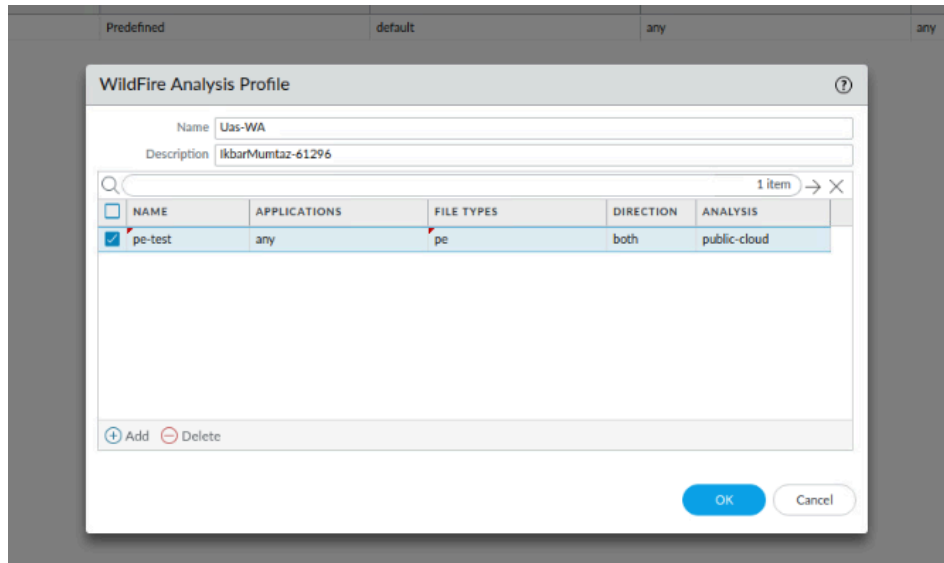
🔍

 Find Matching Signatures

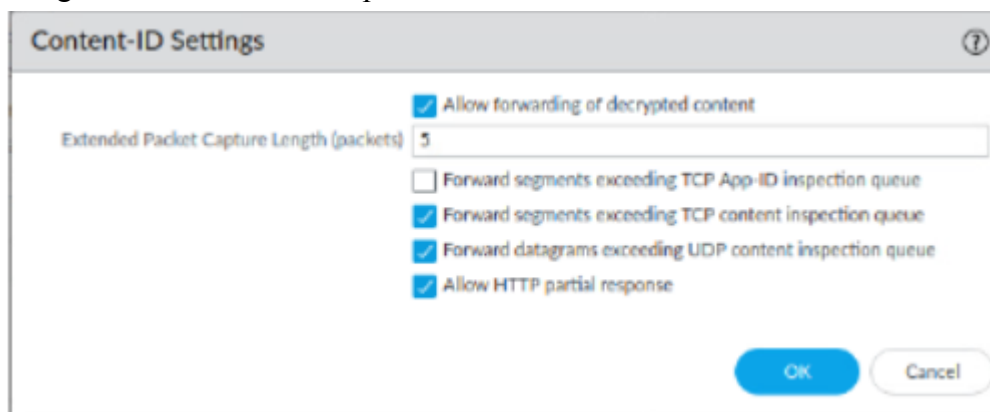
OK

Cancel

Kemudian mengidentifikasi tipe file pe (.exe) di firewall Analysis. Ketika sebuah file pe di download, firewall akan langsung melakukan identifikasi file.



Kemudian meng-allow konten yang terenkripsi untuk di deskripsi sehingga firewall dapat menganalisa konten-konten pada traffic



Setelah itu, kita membuat firewall me report grayware dan benign file. Sehingga firewall memberikan report terhadap semua file yang telah dianalisis.

WildFire Public Cloud

WildFire Private Cloud

☐ Use Proxy Settings for Private Cloud

File Size Limits

File Type	Size Limit
pe (MB)	16 (default)
apk (MB)	10 (default)
pdf (KB)	3072 (default)
ms-office (KB)	16384 (default)
jar (MB)	5 (default)
flash (MB)	5 (default)
MacOSX (MB)	10 (default)
archive (MB)	50 (default)
linux (MB)	50 (default)
script (KB)	20 (default)

☒ Report Benign Files

☒ Report Grayware Files

Terakhir, pada Security Policy, kita mengkonfigurasi traffic inside-out sehingga mengambil tindakan pada setiap traffic yang lewat berupa kumpulan profil yang telah kita buat.

Security Policy Rule ⓘ

**General** | Source | Destination | Application | Service/URL Category | Actions

Name

Rule Type

Description

Tags



**Security Policy Rule**

General | Source | Destination | Application | Service/URL Category | **Actions**

**Action Setting**

Action: **Allow**

☐ Send ICMP Unreachable

**Profile Setting**

Profile Type: **Profiles**

Antivirus: **antivirus**

Vulnerability Protection: **vulnerabilityProtection**

Anti-Spyware: **antiSpyware**

URL Filtering: **None**

File Blocking: **None**

Data Filtering: **None**

Wildfire Analysis: **wildfireAnalysis**

**Log Setting**

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: **None**

**Other Settings**

Schedule: **None**

QoS Marking: **None**

☐ Disable Server Response Inspection

OK Cancel

Test dilakukan dengan mendownload file pada  
<https://wildfire.paloaltonetworks.com/publicapi/test/pe>

Setelah menunggu beberapa saat, file pe tersebut masuk ke dalam firewall analysis. Disini kita dapat mengetahui bahwa verdict dari Analisa file yang masuk adalah malware.

**WildFire Analysis Summary** [Download PDF](#)

PCAP	Receive Time	Type	Application	Action	Rule	Rule UUID	Byt...	Severity	Categ...	URL Categ...	Verdict	URL	File Name
	2022/12/17 08:33:05	end	web-browsing	allow	Allow-Inside-Out	8ac2c...	61...		any				
	2022/12/17 08:33:15	wildfire	web-browsing	allow	Allow-Inside-Out	8ac2c...		high			malici...		wildfir...

### 3. Soal 3: User Identification Sub-CLO0723, Bobot / Weight (20%)

MONITOR POLICIES OBJECTS NETWORK DEVICE

## Zone

Name:

Log Setting:

Type:

☐ INTERFACES ^

Zone Protection

Zone Protection Profile:

☒ Enable Packet Buffer Protection

### User Identification ACL

☒ Enable User Identification

☐ INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

☐ EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

### Device-ID ACL

☐ Enable Device Identification

☐ INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Devices from these addresses/subnets will be identified.

☐ EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Devices from these addresses/subnets will not be identified.

## LDAP Server Profile

Profile Name:

☐ Administrator Use Only

### Server List

NAME	LDAP SERVER	PORT
lab-client	192.168.1.19	389

Enter the IP address or FQDN of the LDAP server

### Server Settings

Type:

Base DN:

Bind DN:

Password:

Confirm Password:

Bind Timeout:

Search Timeout:

Retry Interval:

☒ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

etup				1 item
igh Availability				
onfig Audit				
assword Profiles				
ministrators				
devin Roles				
uthentication Profile				
uthentication Sequence				
ser Identification				
ata Redistribution				
evice Quarantine				
M Information Sources				
oubleshooting				
ertificate Management				
Certificates				
Certificate Profile				
OCSF Responder				
SSL/TLS Service Profile				
SCEP				
SSL Decryption Exclusion				
SSH Service Profile				
response Pages				
g Settings				

NAME	LOCATION	SERVICES	OTHERS
ikbar-LDAP		Name: lab-client LDAP Server: 192.168.1.19 Port: 389	Type: active-directory Base: DC=lab,DC=local Bind DN: lab-user.id@lab.local SSL:

The screenshot shows the 'Group Mapping' configuration window with the 'Server Profile' tab selected. The 'Name' field is set to 'ikbar-Group-mapping'. The 'Server Profile' dropdown is set to 'ikbar-LDAP', and the 'Update Interval' is set to '[60 - 86400]'. The 'Domain Setting' section has an empty 'User Domain' field. The 'Group Objects' section has an empty 'Search Filter' and 'Object Class' set to 'group'. The 'User Objects' section has an empty 'Search Filter' and 'Object Class' set to 'person'. At the bottom, the 'Enabled' checkbox is checked, and the 'Fetch list of managed devices' checkbox is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

The screenshot shows the 'Group Mapping' configuration window with the 'Group Include List' tab selected. The 'Name' field is 'ikbar-Group-mapping'. The 'Available Groups' list is empty, and the 'Included Groups' list is also empty. An error dialog box is displayed in the center, showing a red warning icon and the text: 'Error: Failed to connect to 192.168.1.19(192.168.1.19):389Error: Failed to connect to 192.168.1.19(192.168.1.19):389'. The dialog has an 'OK' button. The background window shows 'OK' and 'Cancel' buttons at the bottom right.

Manajemen perusahaan ingin menguji kontrol pengguna jaringan dengan maksud memonitor lalu lintas secara transparan, memungkinkan identifikasi pengguna yang terlibat dalam aktivitas tersebut melalui firewall. Selain itu, mereka ingin mengintegrasikan identifikasi pengguna dari infrastruktur LDAP dengan GlobalProtect. Langkah awal adalah konfigurasi zona baru bernama "Ikbar-inside" pada antarmuka ethernet1/2 dengan tipe Layer3. Penggunaan User Identification ACL diaktifkan untuk pelacakan pengguna berdasarkan alamat IP atau subnet, sementara Device-ID ACL tidak diperlukan dalam percobaan ini. Selain itu, fitur "Enable Packet Buffer Protection" diaktifkan untuk melindungi buffer paket di Zone Protection.

Berikutnya, mereka melakukan konfigurasi profil server LDAP dengan nama "LDAP-Ikbar". Server LDAP ditambahkan dengan alamat IP 192.168.1.20 pada port 389. Dalam pengaturan server, tipe Active Directory dipilih dengan Base DN diatur ke DC=lab,DC=local dan Bind DN menggunakan lab-user.id@lab.local. Koneksi aman diaktifkan dengan SSL/TLS dan kata sandi yang relevan dipilih. Pemetaan grup juga dikonfigurasi dengan memilih profil server LDAP "LDAP-Ikbar". Filter pencarian default digunakan untuk Group Objects dan kelas objek diatur sebagai "group". Begitu juga untuk User Objects, filter pencarian kosong dan kelas objek "person" dipilih. Semua konfigurasi ini diaktifkan untuk memastikan pengelolaan yang efisien terhadap objek grup dan pengguna. Terakhir, dalam konfigurasi GlobalProtect, sertifikat SSL diperlukan untuk mengamankan komunikasi antara klien dan portal. Namun, proses ini terhenti karena sertifikat harus dibeli dari Otoritas Sertifikat (CA) yang terpercaya. Pembelian sertifikat berbayar ini penting untuk memastikan keamanan komunikasi yang konsisten dan untuk menghindari potensi masalah kepercayaan serta kerentanan keamanan yang mungkin muncul jika menggunakan sertifikat self-signed.