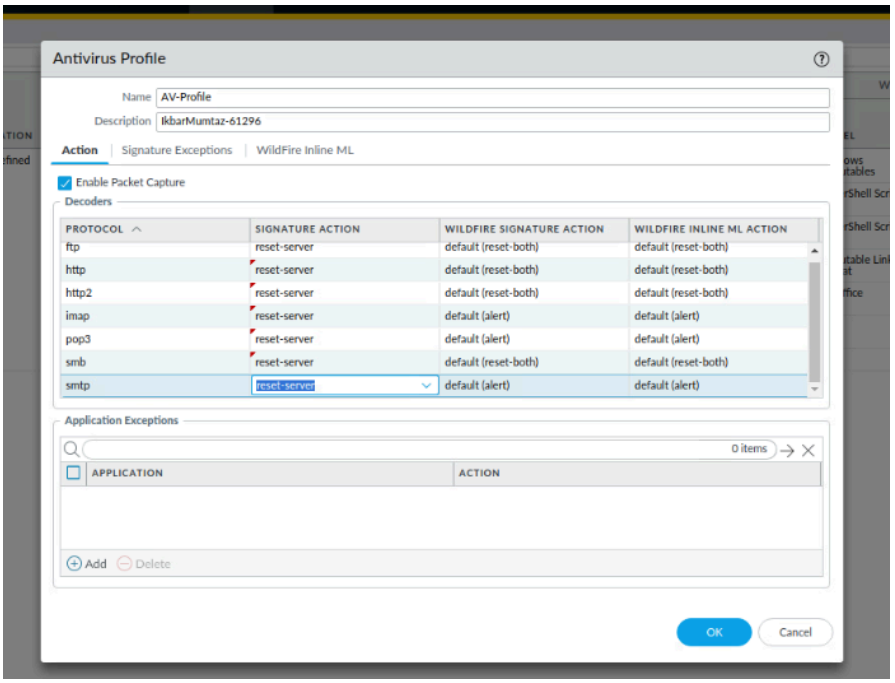
Ikbar Muhammad Mumtaz
00000061296
IF 673: Cybersecurity: Firewall Configuration and Management

---

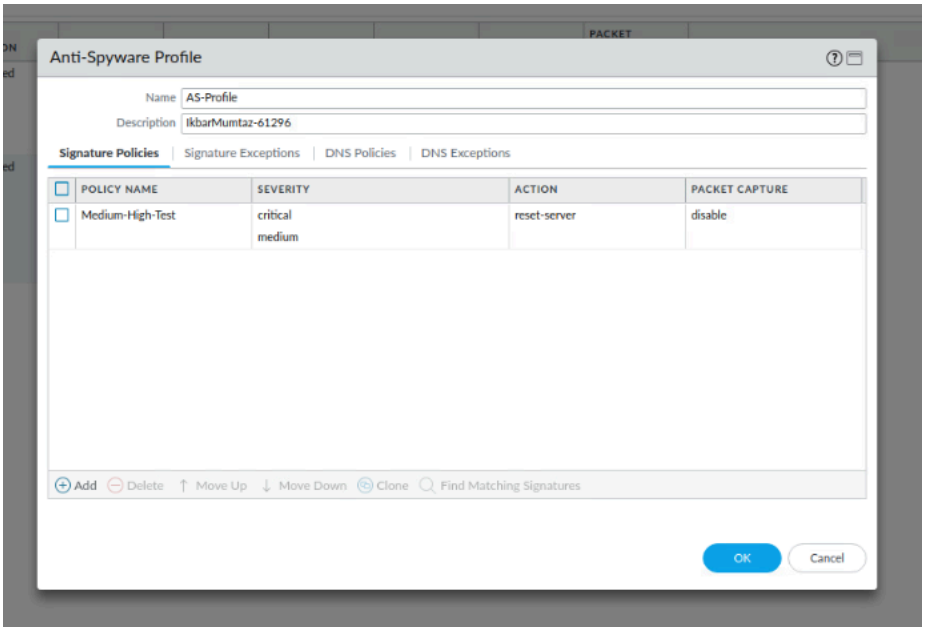
1. Soal 1: Early Prevention Sub-CLO0714 + Sub-CLO0721, and Bobot / Weight (25%+20%)
   1) Antivirus Profile

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.



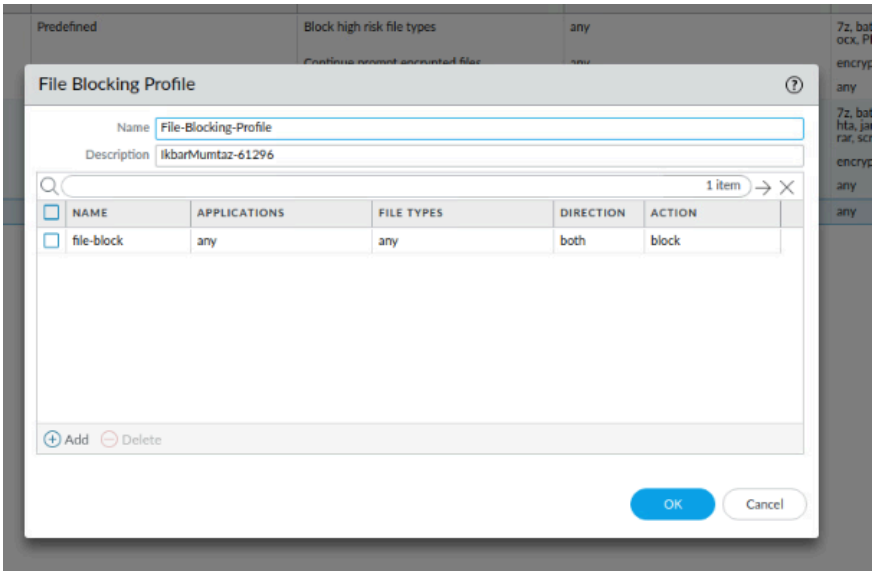
2) Anti-Spyware Profile

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.



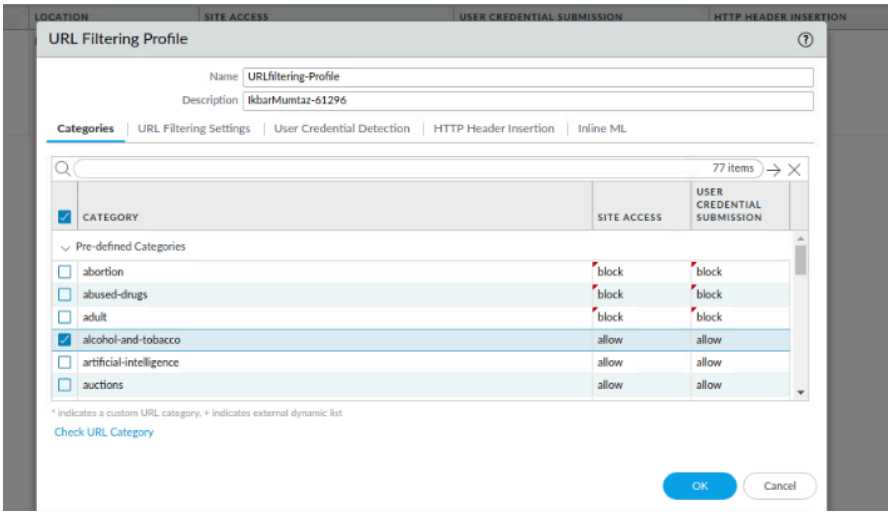
3) File Blocking Profile

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.



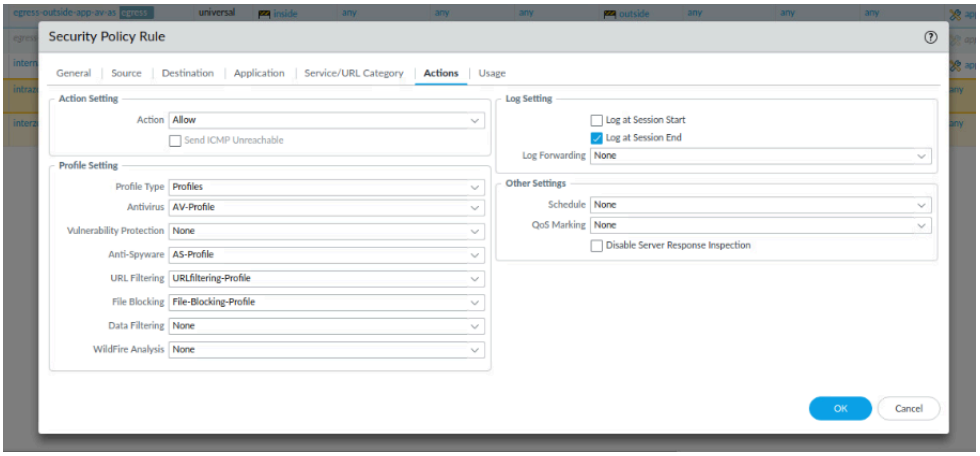
4) URL Filtering Profile

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.

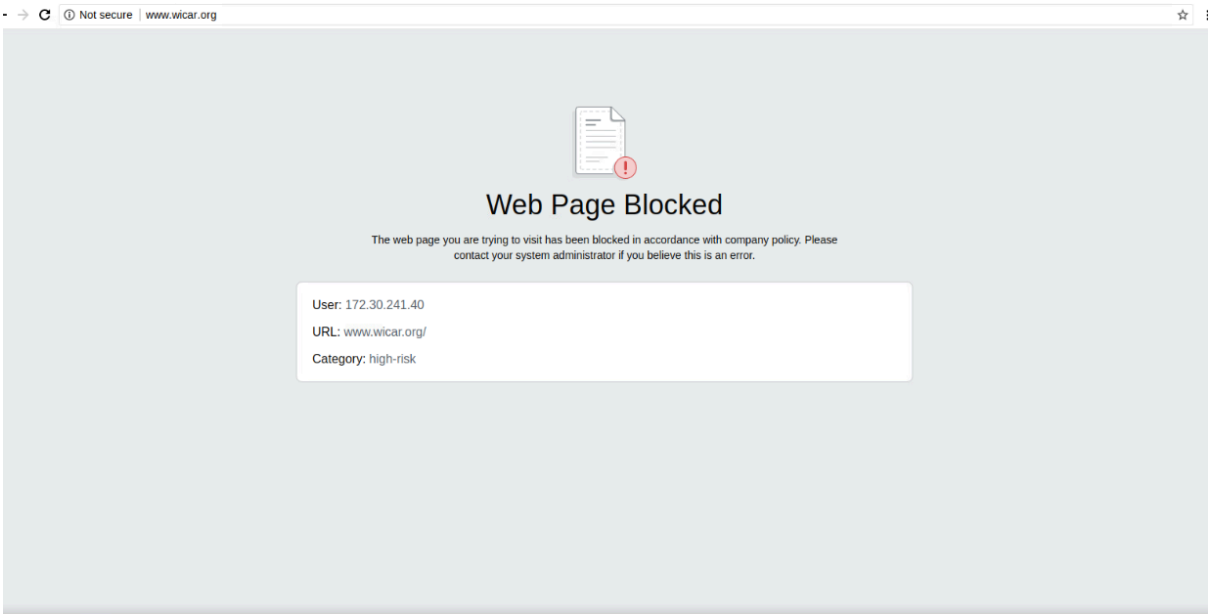


5) Egress Policy (Inside to Outside)

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.



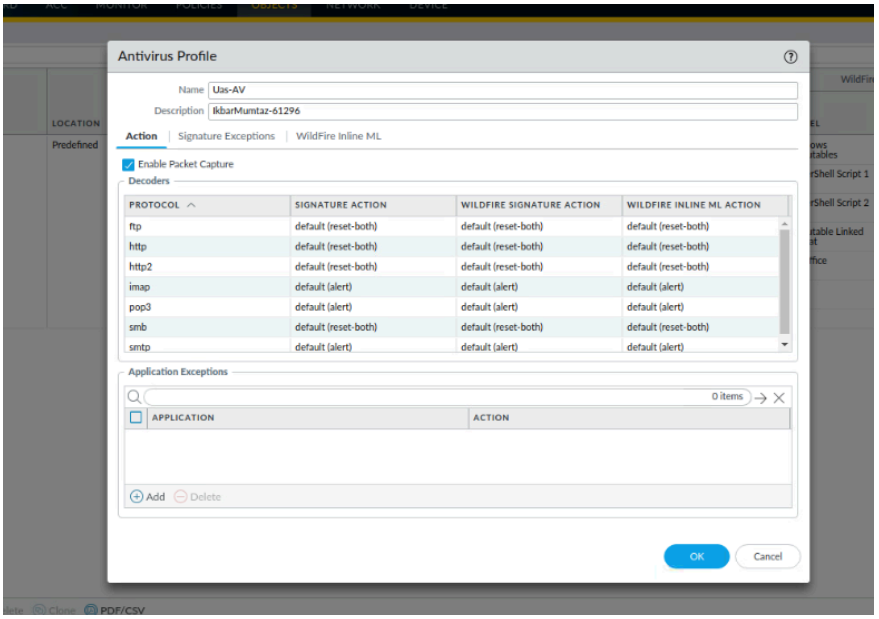
6) Hasil website yang terblokir

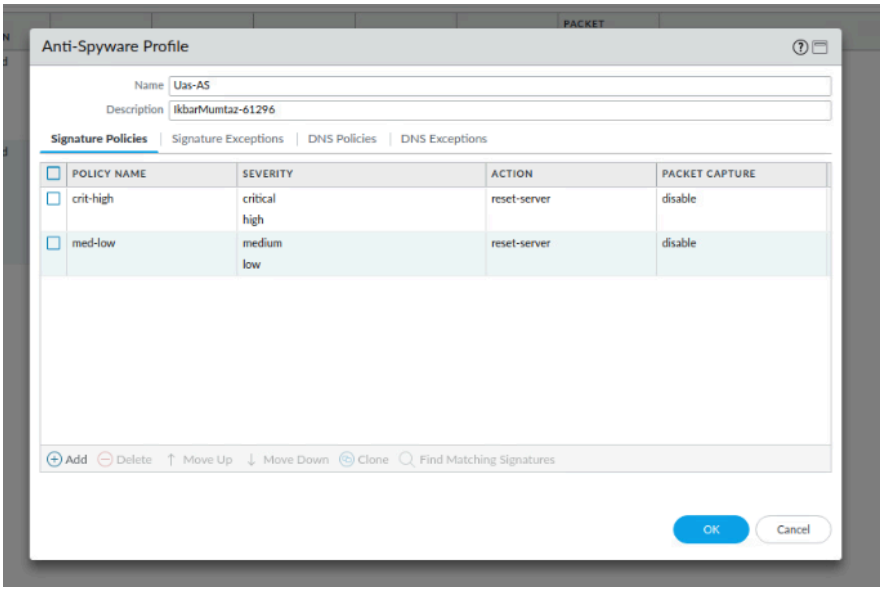


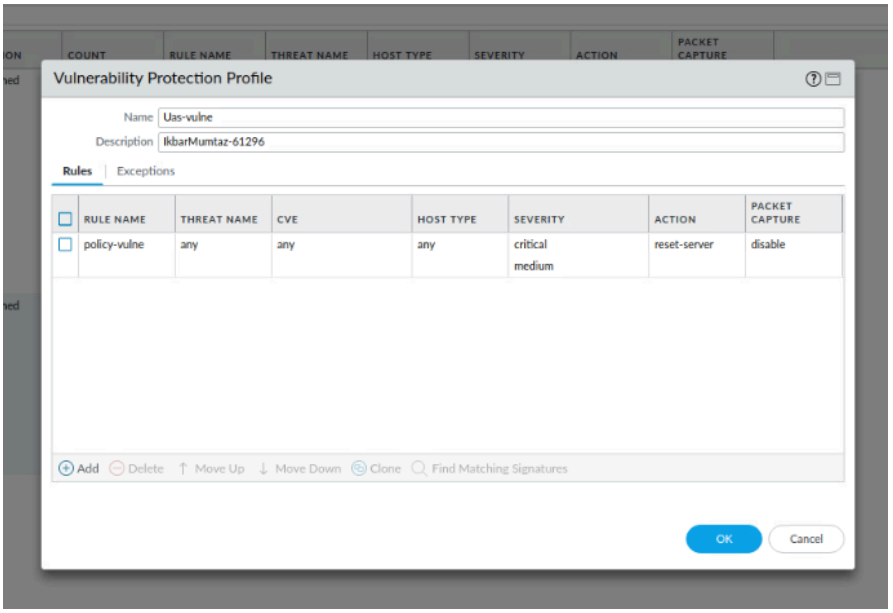
2. Soal 2: Malware Protection Sub-CLO0722 + Sub-CLO0724, Bobot / Weight (15%+20%)

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

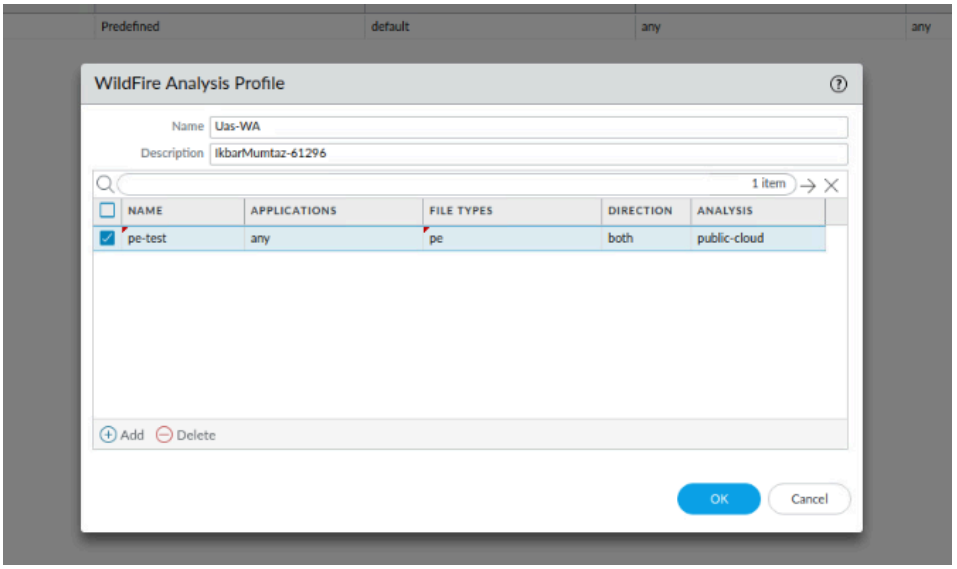
lalu membuat Antivirus, Spyware, Vulnerability Protection, serta Firewall Analysis Profile untuk mengidentifikasi Traffic.



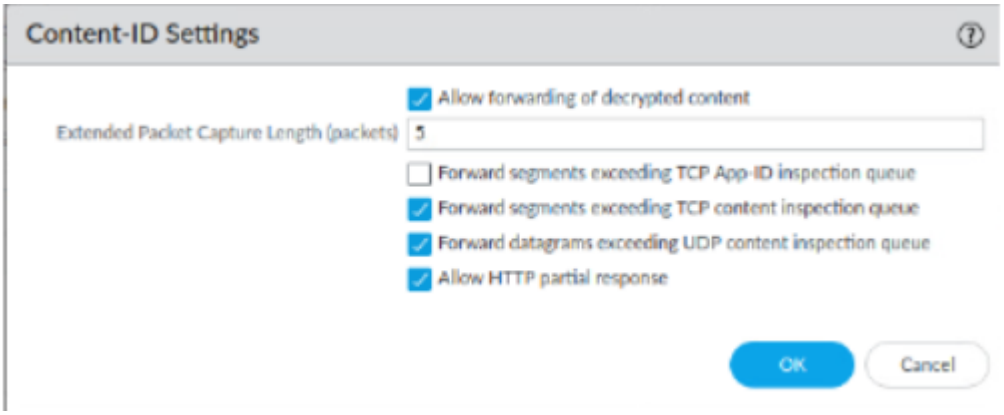

Anti-Spyware Profile
Name Uas-AS
Description IkbarMumtaz-61296
Signature Policies | Signature Exceptions | DNS Policies | DNS Exceptions
POLICY NAME | SEVERITY | ACTION | PACKET CAPTURE
crit-high | critical high | reset-server | disable
med-low | medium low | reset-server | disable
Add Delete Move Up Move Down Clone Find Matching Signatures
OK Cancel


Vulnerability Protection Profile
Name Uas-vulne
Description IkbarMumtaz-61296
Rules | Exceptions
RULE NAME | THREAT NAME | CVE | HOST TYPE | SEVERITY | ACTION | PACKET CAPTURE
policy-vulne | any | any | any | critical medium | reset-server | disable
Add Delete Move Up Move Down Clone Find Matching Signatures
OK Cancel

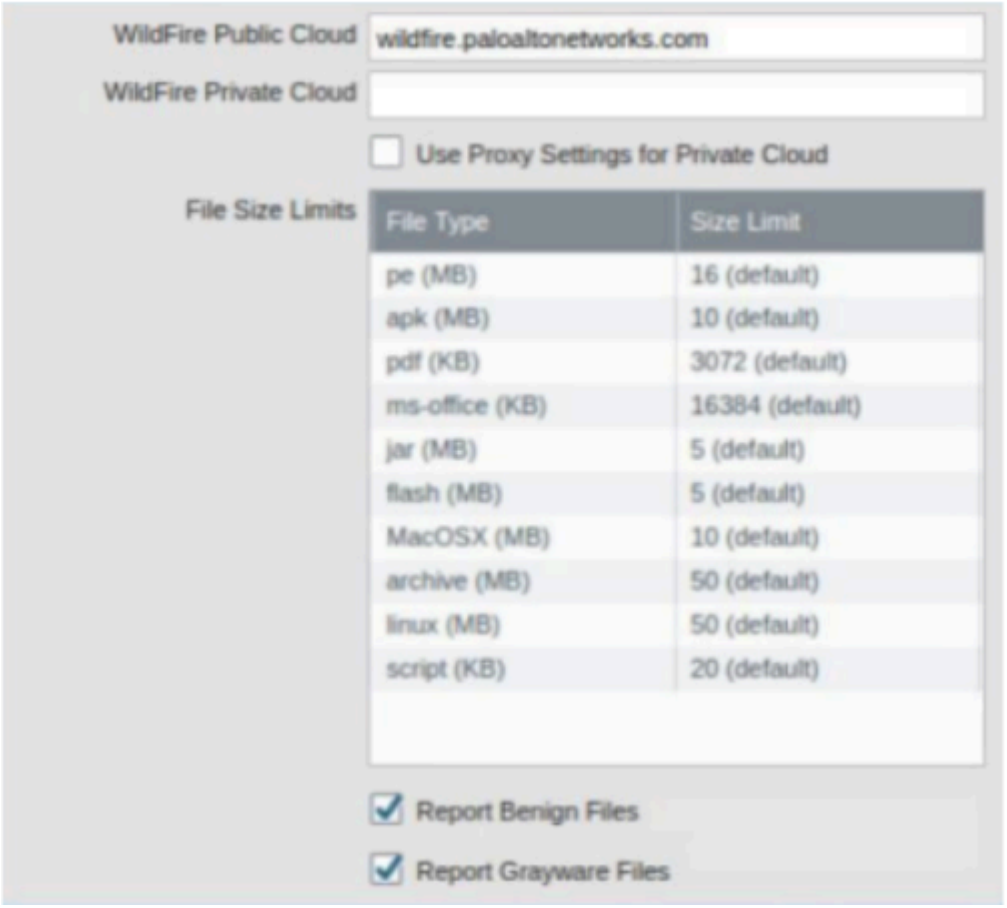
Kemudian mengidentifikasi tipe file pe (.exe) di firewall Analysis. Ketika sebuah file pe di download, firewall akan langsung melakukan identifikasi file.



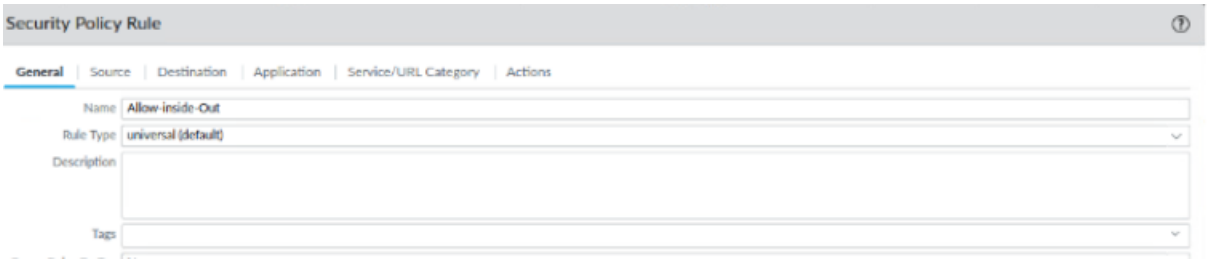
Kemudian meng-allow konten yang terenkripsi untuk di deskripsi sehingga firewall dapat menganalisa konten-konten pada traffic

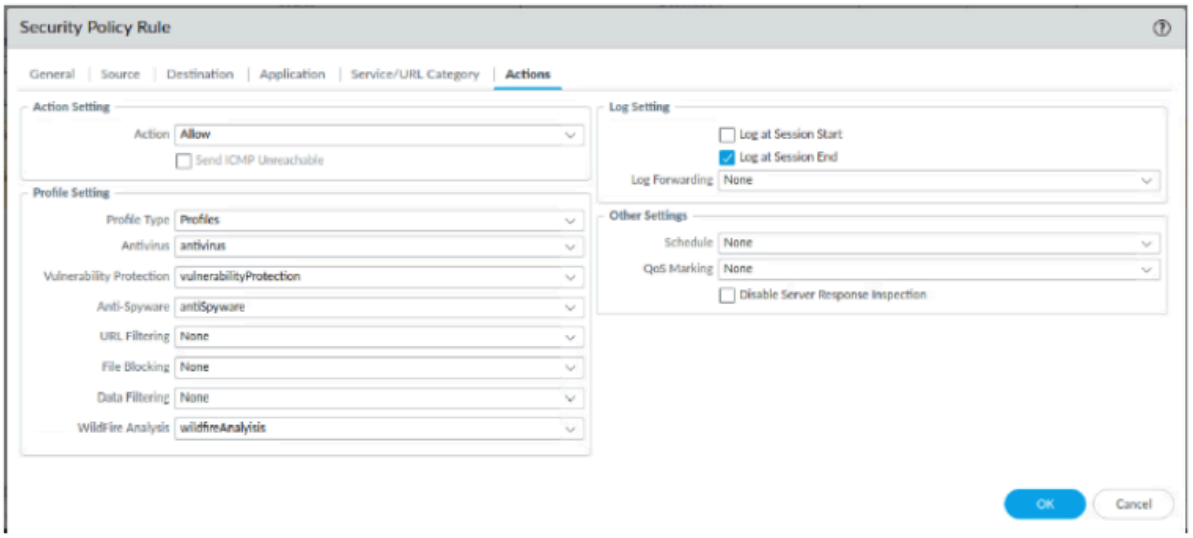


Setelah itu, kita membuat firewall me report grayware dan benign file. Sehingga firewall memberikan report terhadap semua file yang telah dianalisis.



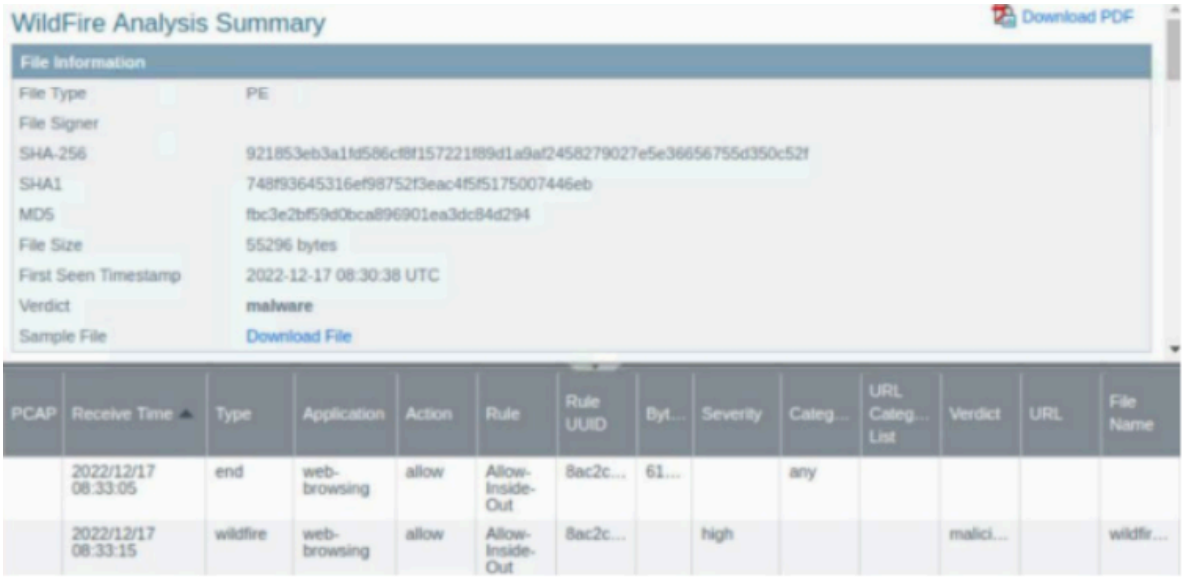
Terakhir, pada Security Policy, kita mengkonfigurasi traffic inside-out sehingga mengambil tindakan pada setiap traffic yang lewat berupa kumpulan profil yang telah kita buat.



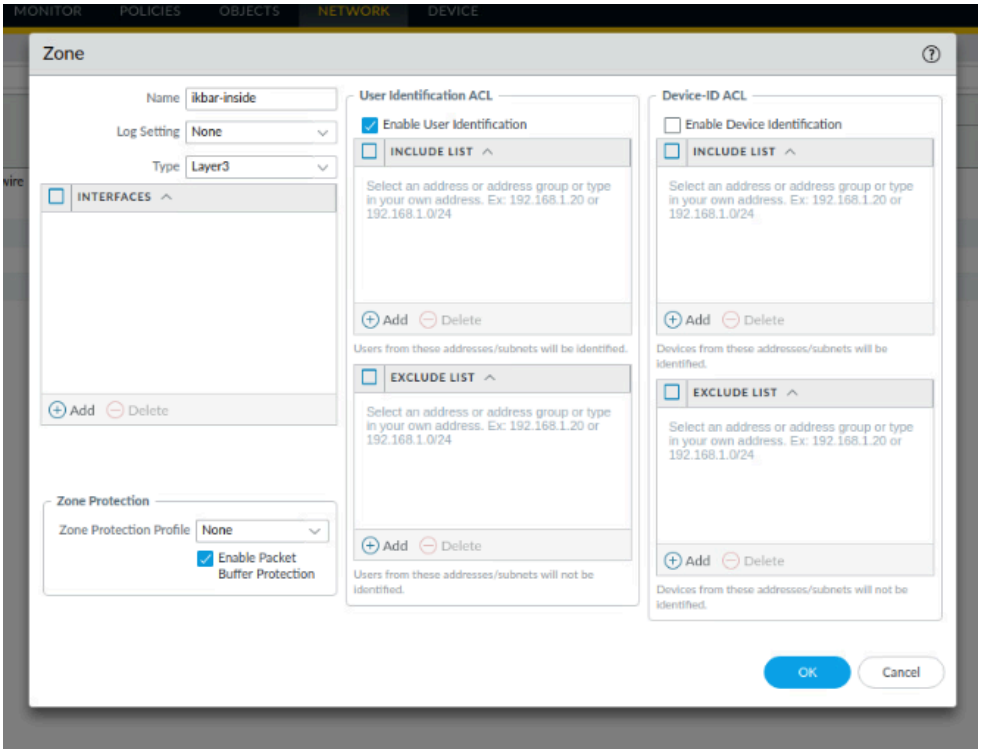


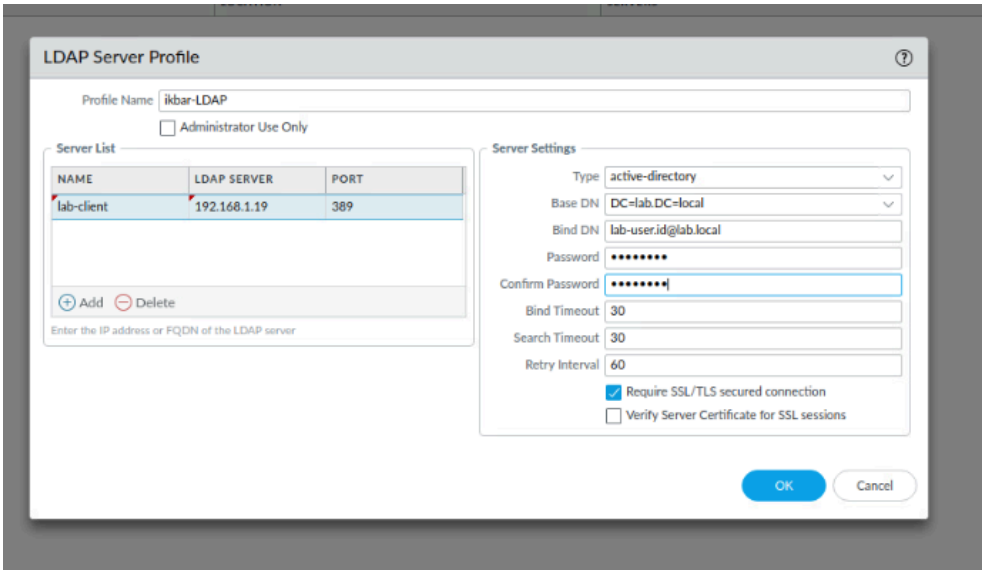
Test dilakukan dengan mendownload file pada
https://wildfire.paloaltonetworks.com/publicapi/test/pe

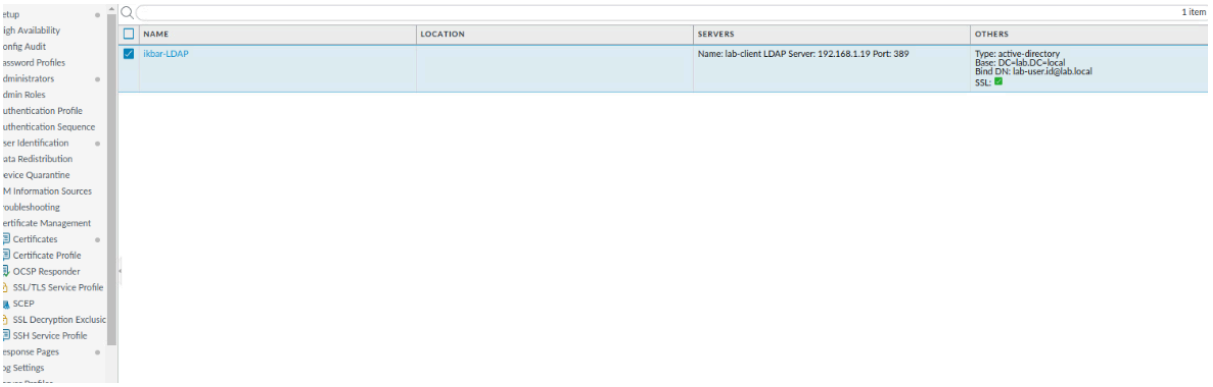
Setelah menunggu beberapa saat, file pe tersebut masuk ke dalam firewall analysis. Disini kita dapat mengetahui bahwa verdict dari Analisa file yang masuk adalah malware.

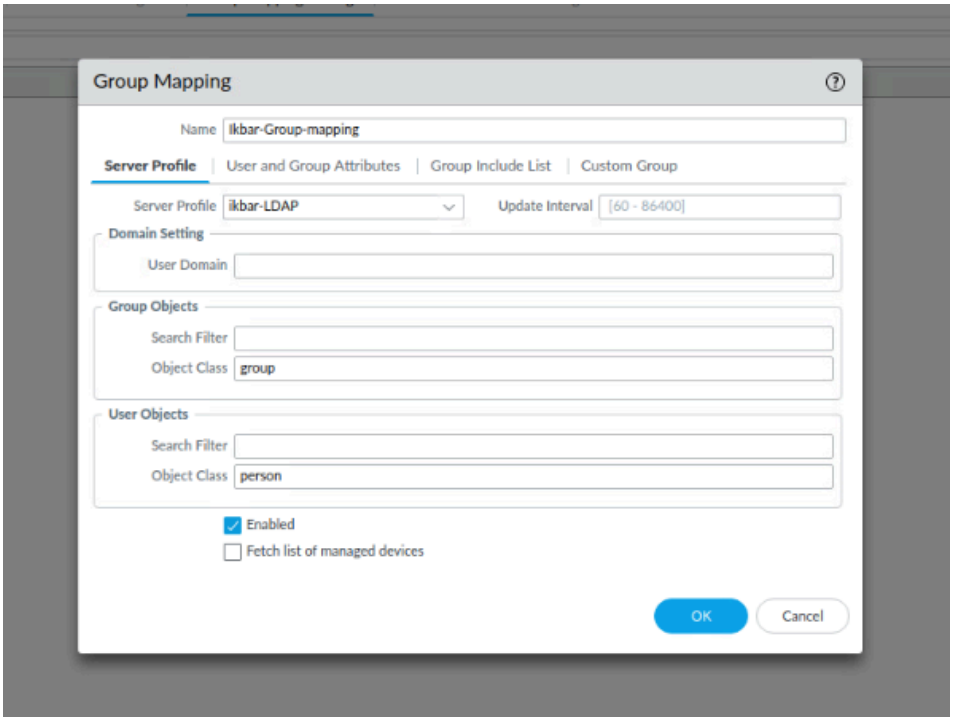


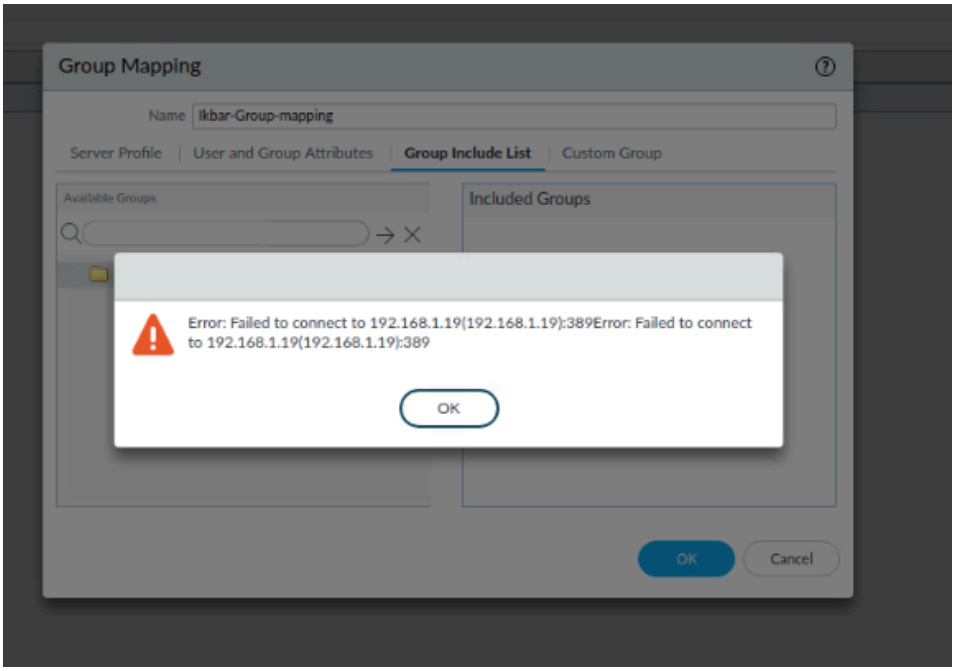
3. Soal 3: User Identification Sub-CLO0723, Bobot / Weight (20%)











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.