Antivirus Security Profile

وفقا ل AV-Test Institute يتم اكتشاف حوالي 450,000 برنامج ضار يومياً.

وبسبب كدا اصبح واحد من اهم الخصائص اللي أصبحت مدمجة فال UTM , NGFW هي القدرة على فحص دقيق للبيانات بشكل يضمن آمان عالي فالترافيك اللي بيمر ومنها حماية المؤسسة.

فالملف دا هنتكلم عن ال Anti Virusوازاي بيشتغل وازاي تطبقه بشكل يضمن ان ما يكون في ڤايروسات عندي وتضر الشبكة.

Virus concept and its Types

هو سوفت وير اتعمل عشان يضر الجهاز بشكل أو بآخر

Worm: دا نوع من الڤايروسات بيقدر يكرر نفسه فالشبكة وممكن يكون له تأثيراتNetwork Congestion وممكن تتسبب ان ممكن تستهدف زي ال Service معينة

Trojan: دا ڤايروس بيكون في ملف او سوفتوير انت بتنزله بيبدأ اول ما تفتح الملف دا مش بيكون واضح من البداية انه ڤايروس بياخدaction.ال

Ransomware: دا ڤايروس الفدية لو اتعمل بيعمل encryption للترافيك وعشان تفكه محتاج تدفع ودا اصاب اجهزة كتير

Virus Detection Methods

Signature -Based

دا النوع الأكثر انتشاراً بيشتغل عن طريق وجود Database موجود فيها ال Signaturesللڤايروسات اللي تم اكتشافها وتسجليه بطريقة اني اقدر استخدمها بعدين اني اقارن ال signaturesالخاصة بال fileبال signaturesاللي موجودة عندي للڤايروسات دي ولو في اي تشابة يصنف الملف انه ڤايروس وبيتم تسجيل ال signatureبالشكل دا

Virus names: <vector>/<pattern>

وكل شركة بيكون لها ال engines الخاصة بيها وال databaseالخاص بيها فالعملية دي

Heuristic-Based

فالنوع دا لا يقارن مع Signatures مسبقة عندي ولكن يعتمد على فحص ال Source codeنفسه ويحلل ال codeبيكون له دور كبير فال Zero Day attacksيعني ڤايروس لم يتم اكتشافه من قبل.

ولكن ممكن يكون سبب في وجود ال false positive بشكل اكبر يعني يعمل false alarm

Sandbox Detection

فالحالة دي انت بتعمل Run لل malicious code على virtual invironment

ونبدأ نحلل تأثيره وضرره والهدف من ال Icode وطبعا امكانية ربطه مع NGFW

Antivirus Security profile FortiGate

FortiGate Antivirus Databases

شركة Fortinet عندها ال Databases , engines الخاصين بيها وتم تصنيف ال Databasesدي لنوعين

Extended Database

Default بيكون شغال على أغلب أجهزة فورتي

يحتوي على أغلب الفايروسات التي تم اكتشافها مؤخرا سواء مازالت تعمل ام توقفت عن العمل التي تم اكتشافها من فريق FortiGuard Global Security Research Team

Extreme Database

بتكون Database اكثر شمولاً للفايروسات حيث يتم اضافة الفايروسات التي لم تعد تعمل منذ وقت طويل على اعتبار انها ممكن تكون خطر فالمستقبل لو تم إعادة تفعيلها بتسمى ال.Zoo Viruses

لا تكون By Default ولكن يتم تطبيقها فال Top Security Environments

وعشان تفعلها باستخدام فورتي باستخدام CLI فقط

```
#config antivirus settings

#set use-extreme-db {enable | disable}

#End
```

Antivirus Scan Techniques Detection

عشان نوقف ڤايروس معين بنمر بعدة مراحل ما

Searching

دي مرحلة بنطبق فيها الاعدادات اللي هنشتغل عليها و ال Databaseاللي هنستخدمها

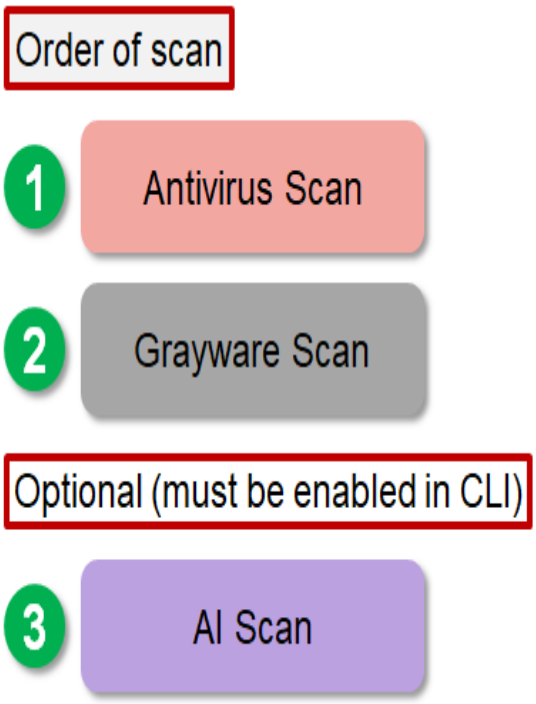
Detection

الطريقة اللي بيتسخدمها الجهاز انه يحدد ان هذا ڤايروس.

Action

بعد ما تأكدنا ان هذا ڤايروس نبدأ نعمل ال Actionمثل , Remove Quarantine.

FortiGate Detection Methods



1. Antivirus Scan

ابسط واسرع طريقة اني اكتشف فايروس ويقدر يعمل scan ويحدد الڤايروس فال , Real timeيقدر يمنع انتشاره

بيستخدم ال Signature method

2.Greyware Scan

دي بعض البرامج اللي بتنزل على جهازك غالبا بدون علمك وهي لا تعتبر antivirusولكن ممكن يكون لها تاثير على جهازك زي انه يكون أبطأ او تعرض اعلانات مثلا فالأفضل انها تحذف ولا يسمح بها.

FortiGateبيقوم ب scanمعين يقدر يوقف النوع دا عن طريق ال Greyware scan

3.AI Scan (optional)

ممكن يكون في طرق لبعض الفايروسات انها انها لن يتم اكتشافها ؛ عشان كدا.محتاجين نزود Scan جديد تعتمد بشكل أساسي على الذكاء الصناعي ودا بيستخدم بشكل أساسي mitigation for Zero Day Attacks.

ولكن ضع فالحسبان انه بيحتاج Resources عالية عشان يشتغل يعني تشغله في حالة انت محتاجه فقط فال.Top Security environment s

بم ان النوع دا من ال Scanممكن يعطي false positive ممكن نحدد ال Actionاللي هياخده لو اكتشف فايروس

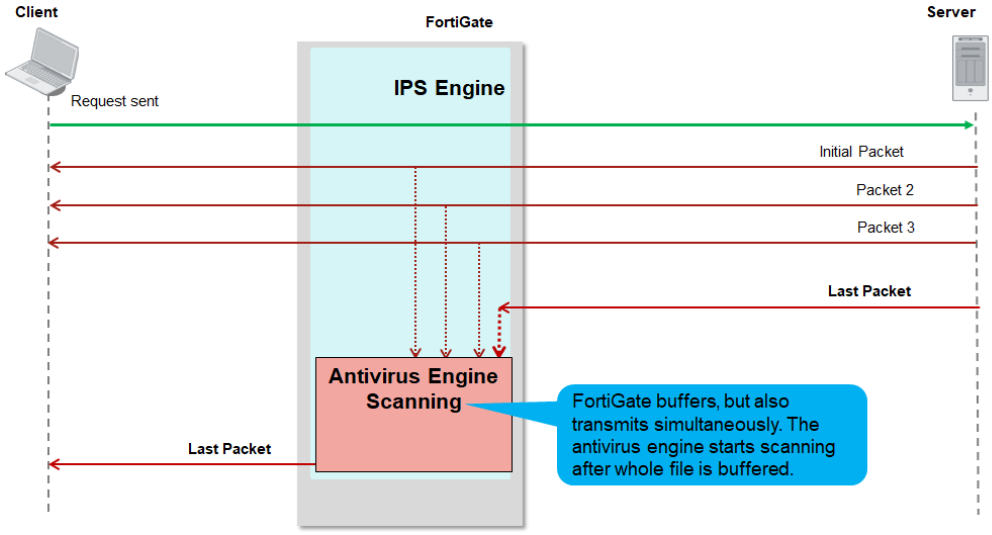
ولكي يتم تفعيلة باستخدام cli فقط.

```
#config antivirus settings

#set av-ai-mode enable

#set av-ai-action block

#end
```

Antivirus Security FortiGate

عندنا على FortiGate نوعين من Inspection شرحتهم في ملف Web Filteringوالفرق بينهم

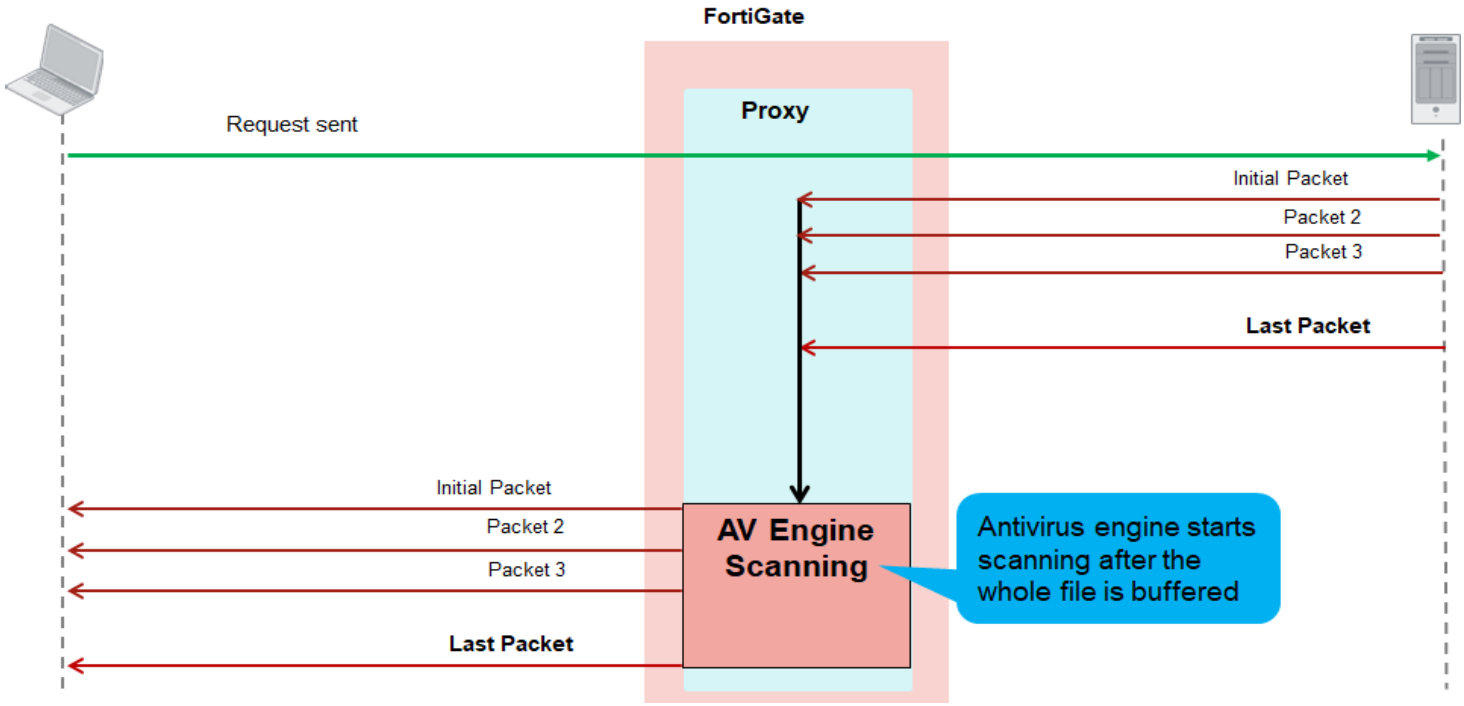
1.Flow-Based mode (Default mode)



فال mode دا فورتي بيبدأ يعمل Inspection باستخدام IPS engine ويقرأ كل ال packetوياخد منها. نسخة ويعمل فخص اثناء عملية الارسال ويوقف آخر packet فقط لحد ما يشوف.الملف virus ام لا

FortiGate : Virus Detectedبيعمل reset لل connection عن طريق انه بيبعت TCP resetوبكدا الفايل مش هيتبعت بشكل سليم. ثم يبدأ IPS يعمل caching لل URL للفايل دا ولو حصل ان الملف اتبعت تاني خلاص مش بيعيد ال inspection تاني و يتم ارسال replacement message مباشرةً.

2. Proxy-Based mode



لو هتشتغل على ال mode دا مهم ال Policyاللي متطبق فيها ال Security profileدا تكون هي كمانProxy mode

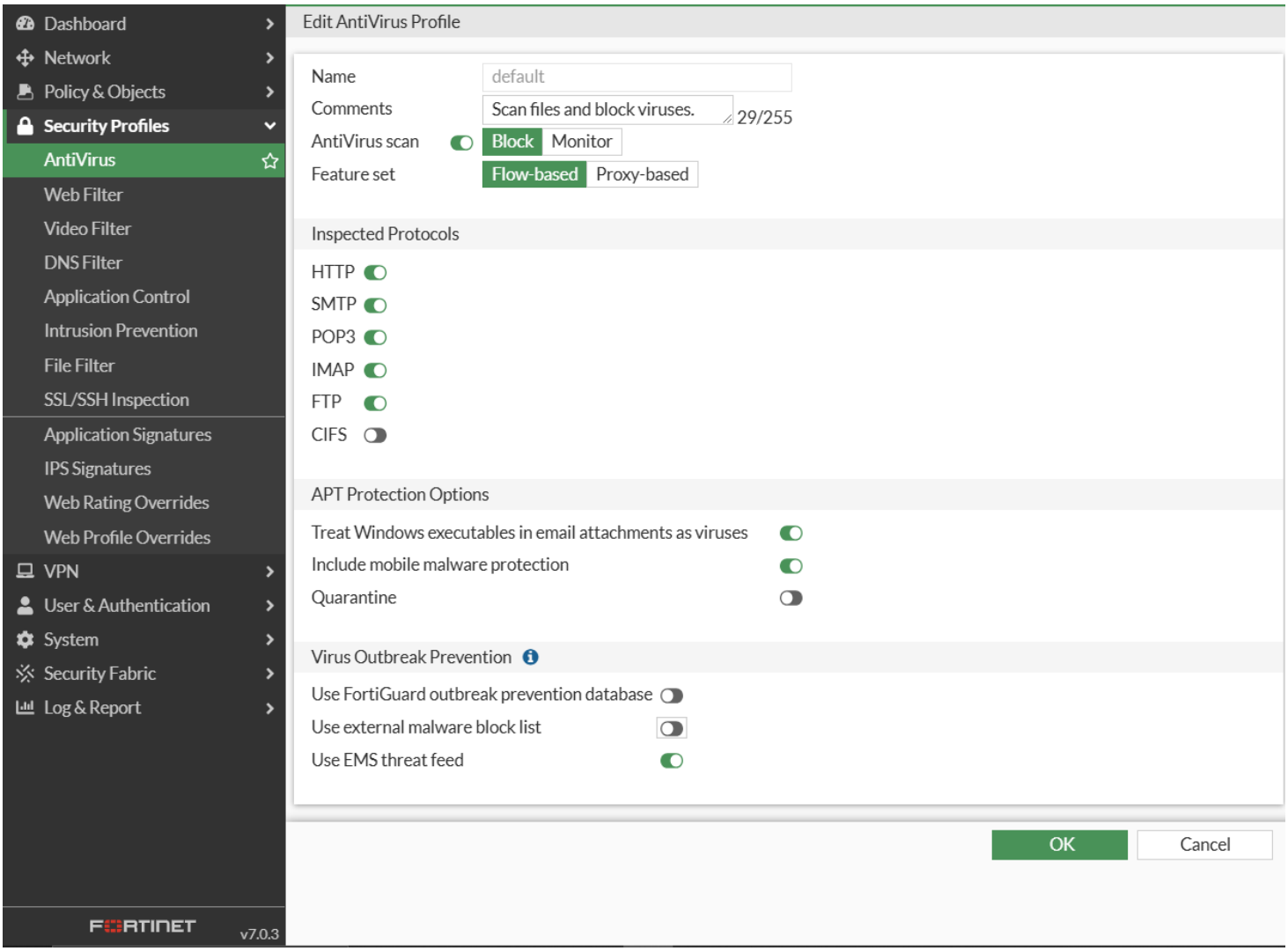
فال mode دا بيتعمل Buffering للداتا بشكل كامل قبل ارسالها حتى يتم عمل inspectionلها في حال تم اكتشاف Virus

بيتم ارسال Block message فالحال.

المشكلة فالمود دا انه بطيء اكتر وبيحتاج resources ، time وممكن الاتصال ينقطع قبل ما يتم الفحص.

Antivirus Security Profile Configuration

Flow-Based Antivirus Security Profile



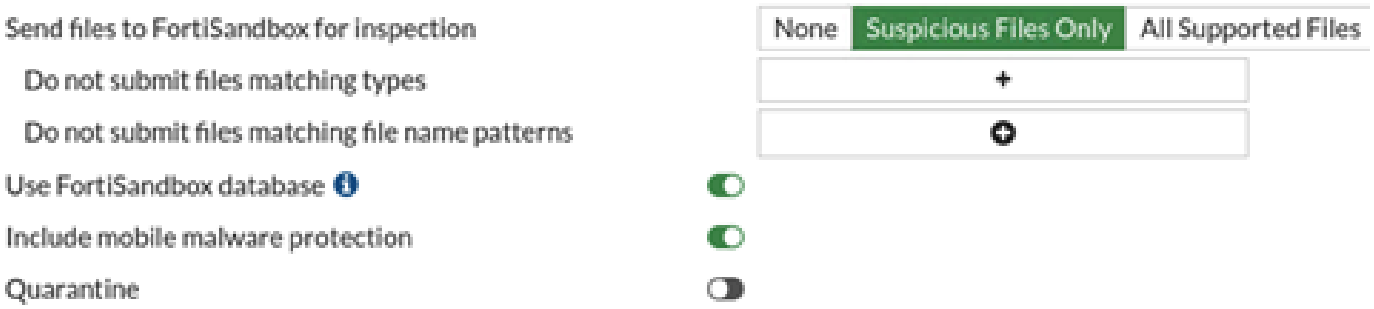
في خانة **Inspected Protocols**

بنحدد البروتوكولات اللي هيتعمل لها فحص

APT Protection Options

Treat Windows executables in email attachments as virus.

اي ملف هيكون exe. هيتيعت فال emails هيعتبره virus بشكل مباشر ودا اجراء سليم من ناحية الآمان



Send files to FortiSandbox for inspection

لا يظهر هذا الخيار الا اما يكون عندك FortiSandbox سواء كان appliance فالشبكة ومربوط مع FortiGate او كان Cloud.

بيوفر لك آمان اكتر ف عملية ال inspection زي ما شرحنا فوق

وتقدر تحدد انه يتم ارسال الملفات المشكوك فيها فقط او كل الملفات ل FortiSandboxعلى حسب احتياجك مع مراعاة ال Resources consuming and delay

Use FortiSandbox database

تقدر تستخدم ال Database الخاصة ب FortiSandbox ويتطلب يكون موجود رخصة له مسبقة بيوفر آمان أعلى بسبب وجود Database اكبر

Include mobile malware protection

دي بعض ال Database الخاصة بال Mobile virus منFortiGuard.

Virus Outbreak Prevention

لابد يكون معاك License اضافية لكي تفعله وهي (Virus Outbreak Prevention Service)VOS

Use FortiGuard outbreak Prevention database

بيكون ربط FortiGate مع third part malware analysis وهو FortiGurad Global Treat Prevention

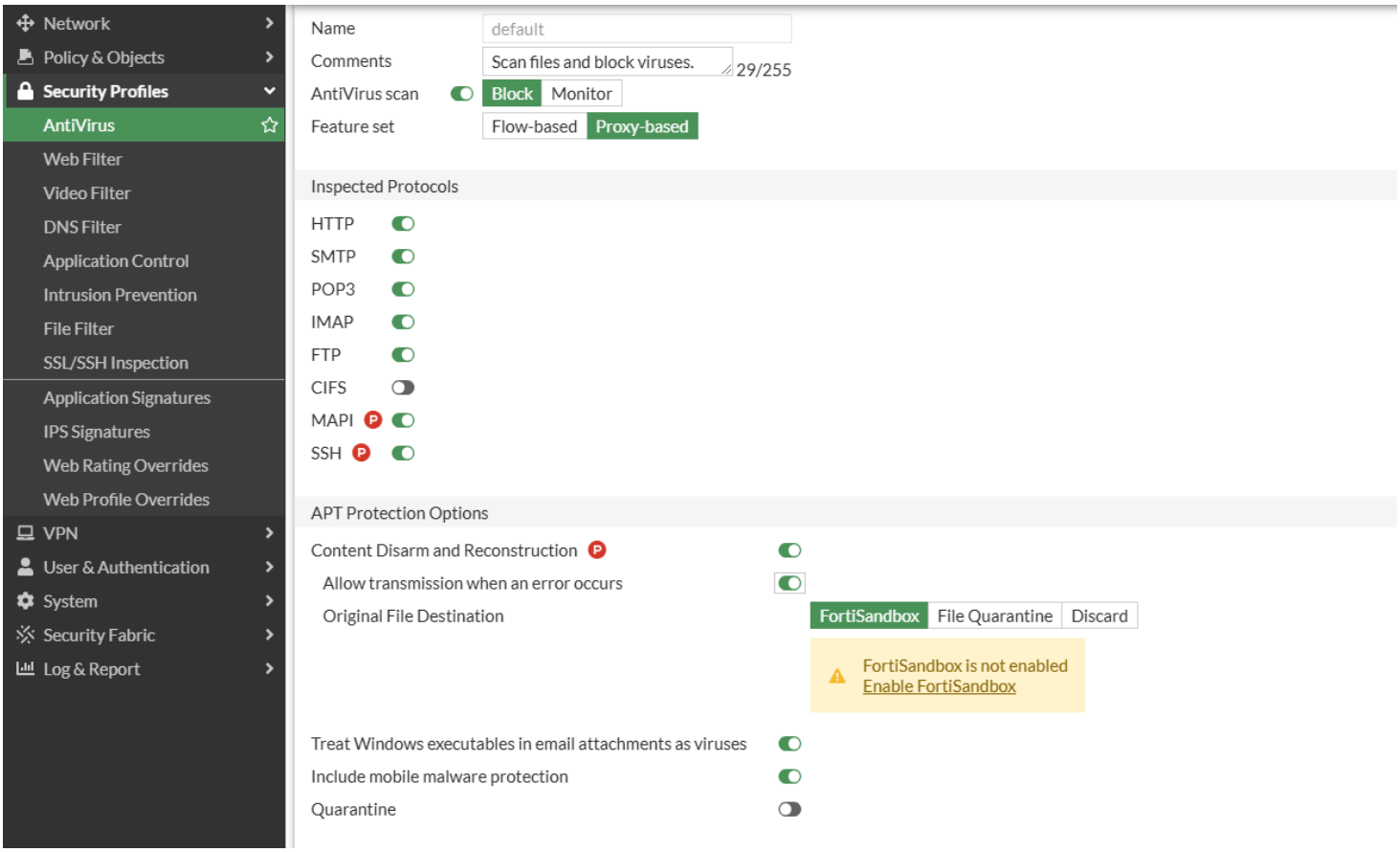
Use External malware block list

ممكن تستعين بـweb server خارجي عليه hashing للAntiviruses انت اكتشفتها قبل كدا او لو عندك Malware analysis team

Use EMS threat feed

بيعمل inspection للڤايروسات من خلال ال EMS Threat feed بيبدأ يتصل مع FortiClient EMS اللي بيكون عليه بعض بعض الdatabases الاضافية

Proxy-Based Antivirus Security Profile



بعض الخواص الخاصة فقط بال Proxy mode

Content disarm and Reconstruction

بيعمل فحص كامل للملف ولو فيه مثلا Link ضار بداخله بيحذفه ويبعت باقي الملف

Allow Transmission when error occurs

لو فعلته بيجعله يسمح بال inspection لو حصل خطأ فالفحص

Original File Destination

في حالة تم اكتشاف ايه ال Actionاللي ياخده

FortiSandbox

يرسله ل Sandbox عشان يحلله ويعمل التقرير عنه ويتطلب وجود جهاز او Cloud

File Quarantine

بيعمل quarantine للملف دا انه يتنقل مرة تانية.

Discard

بيعمل discard للملف يعني لا يسمح بإرساله.

- Antivirus Scanning Modes Comparison

	Flow-based (hybrid)	Proxy-based
Catching Rate	Highest	Highest
Sandbox Support	Yes	Yes
Advanced Heuristic	Yes	Yes
Memory	High	High
Perceived Latency	High	Highest
MAPI, NNTP Scanning	No	Yes
SMB Scanning	Yes	No
HTTP, FTP, IMAP, POP3, SMTP Scanning	Yes	Yes
Use FortiSandbox Database	Yes	Yes
Use Mobile Malware Protection Service	Yes	Yes

https://www.linkedin.com/in/ahmed-tarek-shehata

