FORTINET

1405/03/20

راهنمای جامع مدیریت و اعمال خودکار آدرس آی‌پی‌های مخرب در فایروال FortiGate

مقدمه

به منظور بهبود فرآیند شناسایی و مسدودسازی منابع ناشناخته و مخرب، کانال IRANCTI یک سرویس متمرکز Threat Feed راه اندازی کرده که فهرست آدرس آی‌پی‌های استخراج شده از تله‌های سایبری را از طریق یک دامنه اختصاصی منتشر می‌کند. هدف از ارائه‌ی این راهنما، اتصال دوره‌ای فایروال به این منبع و دریافت آخرین تغییرات بصورت خودکار می‌باشد. همچنین به منظور تسهیل دسترسی کاربران به آخرین فهرست آدرس آی‌پی‌ها و ارائه‌ی برخی آسیب پذیری‌ها، کانال اطلاع‌رسانی IRANCTI در پیام‌رسان‌های بله و ایتا قابل بهره‌برداری می‌باشد.

به منظور اجرای اتوماتیک کردن این فرآیند، فایروال FortiGate قابلیتی تحت عنوان External Threat Feed یا External Resource ارائه می‌کند که به کمک آن می‌توان یک منبع خارجی حاوی لیست آی‌پی‌ها را به فایروال معرفی کرد. پس از انجام این کار، فایروال به‌صورت خودکار و دوره‌ای این لیست را دریافت کرده و در سیاست‌های امنیتی مورد استفاده قرار می‌دهد. این قابلیت امکان مدیریت متمرکز و به‌روزرسانی خودکار لیست‌های مسدودسازی را فراهم می‌کند و نیاز به اضافه یا حذف دستی آدرس‌ها نمی‌باشد.

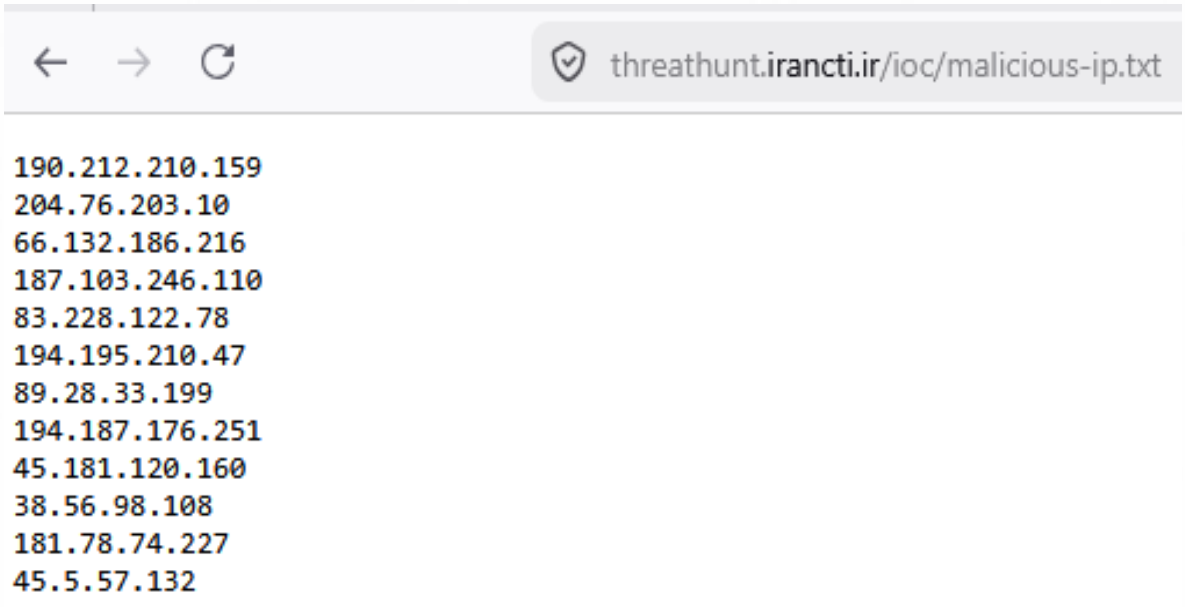
سناریوی عملیاتی

آدرس موردنیاز جهت دسترسی به محتوای آی‌پی‌های مخرب موجود در دامنه IRANCTI به شرح زیر می‌باشد:

https://threathunt.irancti.ir/ioc/malicious-ip.txt

در این آدرس تنها لیست آی‌پی‌های مخرب در ۲۴ ساعت گذشته نمایش داده می‌شود و هیچ اطلاعات دیگری به جز آن وجود ندارد.

محتوای فایل می‌تواند مشابه نمونه زیر باشد:



شکل ۱.دامنه شکارتهدید IRANCTI

هر خط شامل یک آدرس آی‌پی است و FortiGate هنگام دریافت فایل، این مقادیر را استخراج و در اختیار Policy های امنیتی قرار می‌دهد.

نحوه عملکرد FortiGate

پس از معرفی URL مربوط به منبع اطلاعات تهدید درFortiGate ، فرآیند زیر انجام می‌شود:

- فایروال در بازه‌های زمانی مشخص به URL تعریف‌شده متصل می‌شود.
- فایل موجود در URL را دانلود می‌کند.
- محتویات فایل را بررسی می‌کند.
- آی‌پی‌های موجود را استخراج می‌کند.
- لیست داخلی خود را به‌روزرسانی می‌کند.
- تغییرات را درPolicy های مرتبط اعمال می‌کند.

در نتیجه، هر زمان که فایل اصلی تغییر کند، FortiGate نیز پس از همگام‌سازی، تغییرات را دریافت خواهد کرد.

مثال کاربردی

فرض کنید در روز اول محتوای فایل به شکل زیر باشد:

۱۸۵.۱۰.۱۰.۱
۹۱.۲۰۰.۱۰۰.۵
۴۵.۶۶.۷۷.۸۸

فورتی‌گیت این سه آی‌پی را دریافت و آن‌ها را مسدود می‌کند.

در روز دوم فایل به شکل زیر تغییر می‌کند:

۱۸۵.۱۰.۱۰.۱
۹۱.۲۰۰.۱۰۰.۵
۱۰۳.۴۴.۵۵.۶۶

در این حالت:

- آی‌پی جدید ۱۰۳.۴۴.۵۵.۶۶ به لیست اضافه می‌شود و آی‌پی قبلی که ۴۵.۶۶.۷۷.۸۸ می‌باشد از لیست حذف می‌شود. یعنی با هر بار درخواست از Threat Feed فقط آی‌پی‌های موجود در همان درخواست را دریافت و اعمال می‌کند و حتی ممکن است در درخواست بعدی تمام آی‌پی‌ها تغییر و به روزرسانی شوند.

به‌روز رسانی این سرویس می‌تواند از ۱ دقیقه تا ۳۰ روز قابل تنظیم باشد و بهتر است این به روز رسانی توسط فایروال با به روز رسانی منبع اطلاعات تهدید یکسان باشد تا تمام آی‌پی ها در Policyهای امنیتی اعمال شود.(این آی‌پی‌ها در دامنه IRANCTI به صورت هر ۲۴ ساعت یکبار به روز می‌شوند.)

به عنوان مثال اگر آی‌پی های موجود در منبع اطلاعات تهدید به صورت روزانه به‌روز شوند و فایروال به‌گونه‌ای تنظیم شده باشد که آن‌ها را به صورت هفته ای یکبار دریافت کند، فقط آی‌پی های روز هفتم در فایروال اعمال می‌شود و آی‌پی های ۶ روز گذشته را از دست خواهد داد.

استفاده در سیاست‌های امنیتی

پس از اتصال به آدرس موردنظر، تمامی آدرس‌های آی‌پی موجود در فایل به‌صورت خودکار در فایروال بارگذاری می‌شوند و می‌توان آن‌ها را با یک قانون واحد مدیریت و مسدود کرد.

پارامترهای اصلی که باید اعمال شود:

Source Address = ThreatFeed

در این قسمت مبدا ورودی را نام ThreatFeed که در قسمت قبلی تعریف کردیم قرار می‌دهیم.

Action = Deny

در این قسمت هم عملیاتی را که قرار است روی این Policy انجام شود را Deny قرار می‌دهیم.

با این کار ترافیک ورودی از تمام آی‌پی‌های مخربی که روزانه از دامنه IRANCTI استخراج می‌شوند، به صورت خودکار مسدود خواهند شد.

مفهوم Rule تعریف شده

در قانون تعریف شده هر ترافیکی که از آدرس‌های موجود در Threat Feed ارسال شود، توسط فایروال مسدود خواهد شد. همچنین می‌توان از این Threat Feed در بخش Destination Address نیز استفاده کرد تا ارتباط با مقاصد مشخص‌شده نیز مسدود شود.

مزایای استفاده از External Feed

- **مدیریت متمرکز**

تمامی تغییرات در یک نقطه انجام می‌شود و نیازی به اعمال دستی تغییرات روی هر فایروال وجود ندارد.

- **کاهش بار مدیریتی**

مدیر شبکه نیازی به ثبت، ویرایش یا حذف دستی تعداد زیادی آی‌پی نخواهد داشت.

- **به‌روزرسانی خودکار**

هرگونه تغییر در فایل اصلی به‌صورت خودکار در فایروال اعمال می‌شود.

- **مقیاس‌پذیری**

این سرویس می‌تواند همزمان توسط چندین FortiGate در شعب یا مراکز داده مختلف مورد استفاده قرار گیرد.

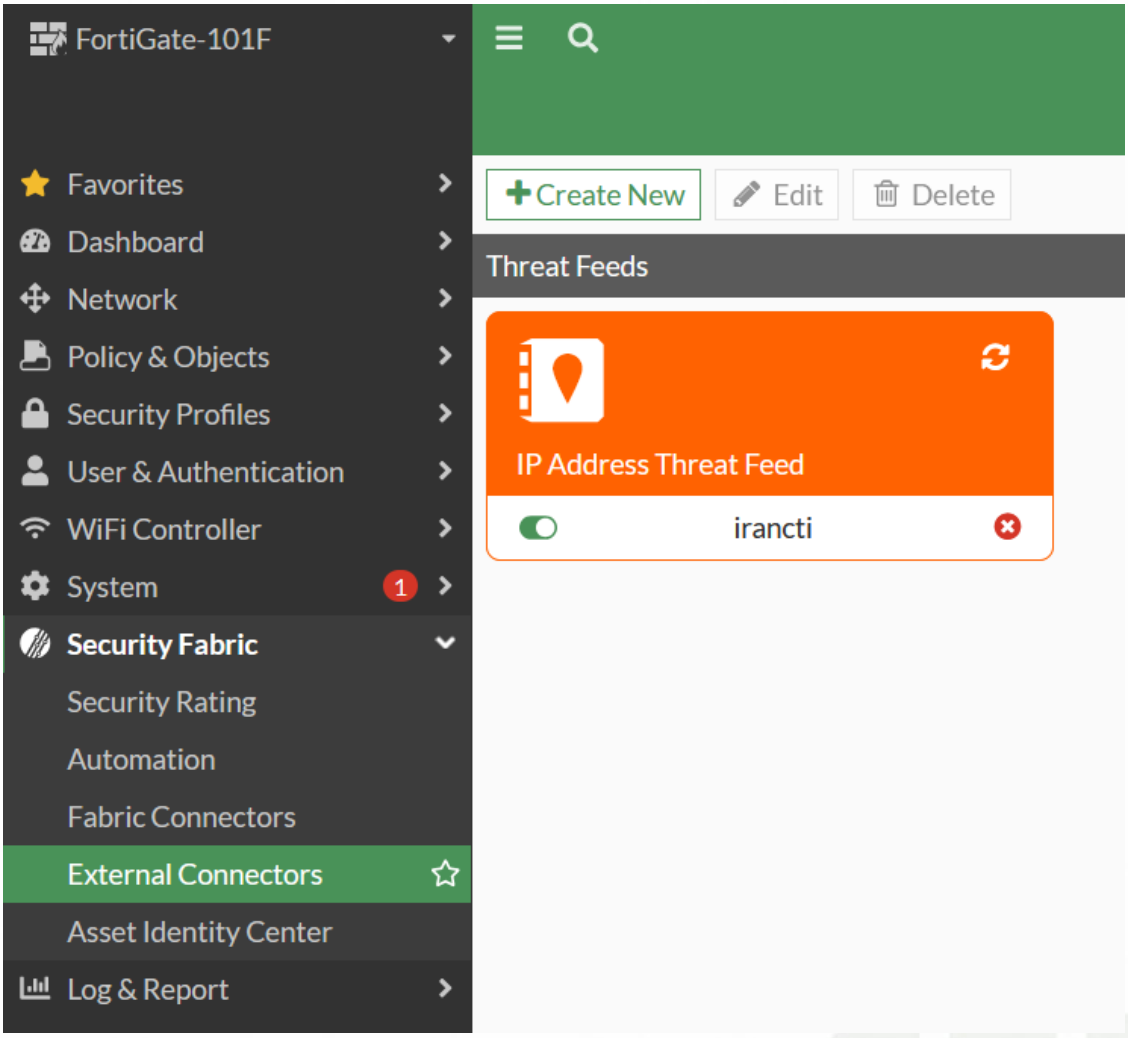
- **کاهش خطاهای انسانی**

حذف فرآیندهای دستی موجب کاهش اشتباهات عملیاتی خواهد شد.

تشریح پیاده سازی

مرحله ۱: ساخت External Threat Feed

ابتدا از قسمت Security Fabric گزینه‌ی External Connectors را انتخاب نموده و سپس با استفاده از گزینه‌ی Create New یک External Threat Feed ایجاد می‌کنیم.



شکل۱.ساخت External Threat Feed

مرحله ۲: انتخاب نوع Feed

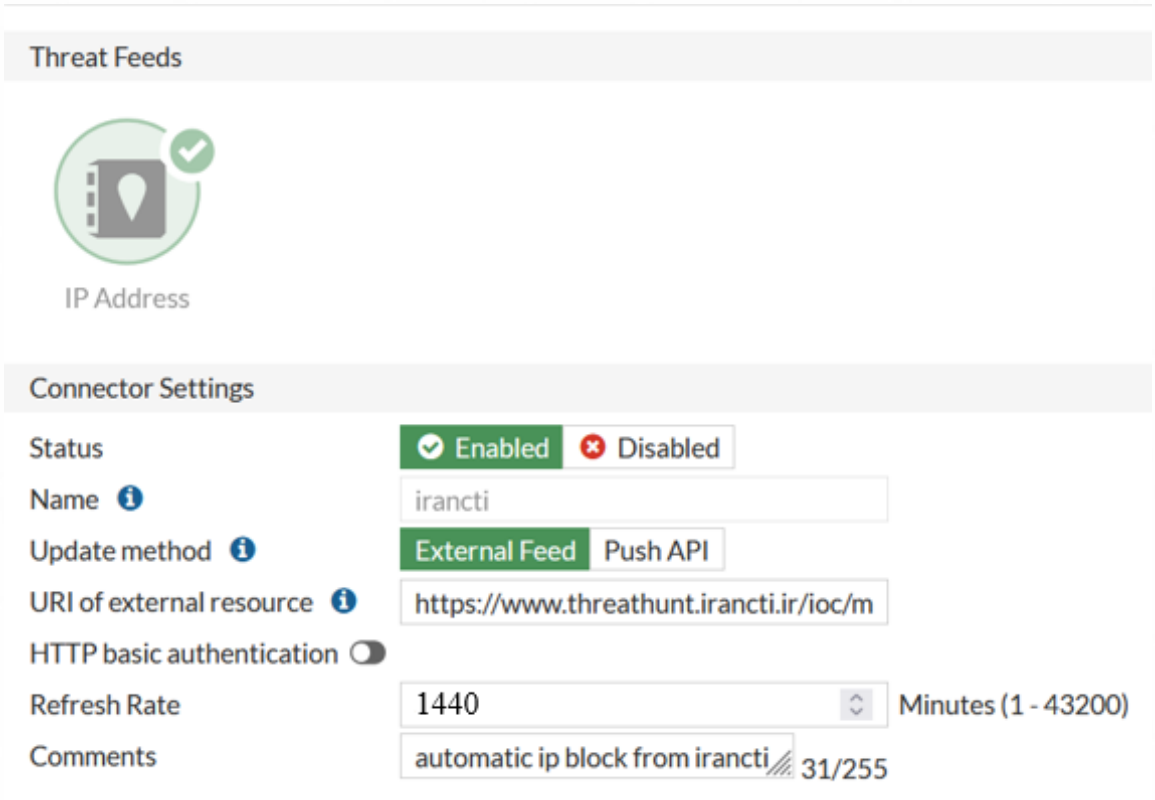
در این مرحله گزینه‌ای مشابه با IP Address Feed یا External IP List را انتخاب می‌نماییم.

مرحله ۳: معرفی URL

در این مرحله URL مدنظر را در فیلد URL of external resource وارد می‌کنیم.

مرحله ۴: تنظیم زمان به‌روزرسانی

در اینجا از گزینه‌ی Refresh Rate برای تنظیم بازه زمانی به‌روزرسانی لیست آی‌پی‌های مخرب از دامنه IRANCTI استفاده می‌کنیم. این به‌روزرسانی می‌تواند بصورت پیشنهادی مثلا هر ۲۴ ساعت (۱۴۴۰ دقیقه) یکبار باشد.



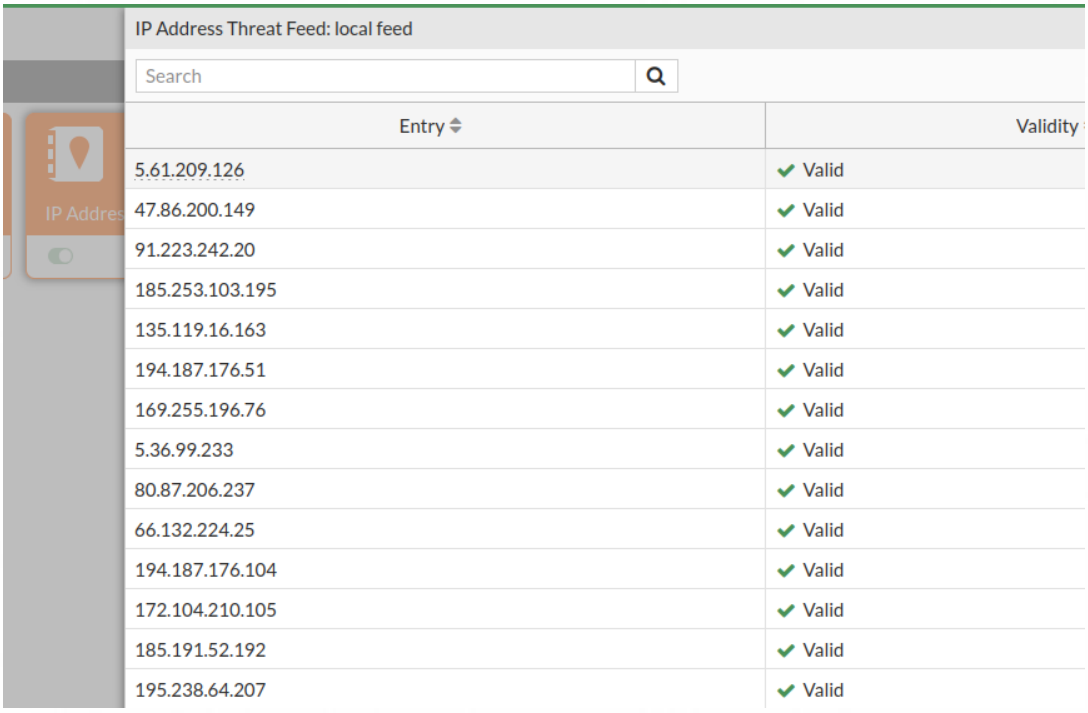
شکل ۲.تعریف Threat Feed

مرحله ۵: ذخیره

پس از ذخیره، فورتی‌گیت تلاش می‌کند فایل را دانلود کند.

اگر فایل قابل دسترس باشد معمولاً تعداد آی‌پی‌های دریافت‌شده را نمایش می‌دهد.

همانطور که در شکل زیر مشاهده می‌کنید فایروال تمام آی‌پی های موجود را در Threat Feed تعریف شده دریافت کرده و در جدول مربوطه لیست کرده است.



شکل ۳. دریافت آی پی ها توسط فایروال

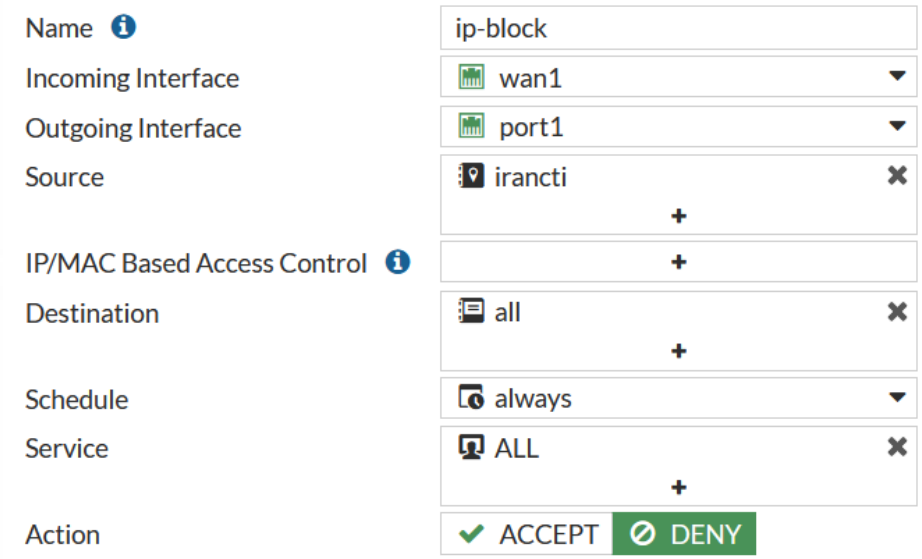
مرحله ۶: استفاده در Policy

بعد از ساخت Feed برای اعمال Policy مدنظر اقدام نموده و یک Rule جدید می‌سازیم:

لازم به ذکر است که در قسمت Source Address نام Feed ساخته شده را جاگذاری می‌نمائیم.

Incoming Interface	WAN
Source Address	**irancti**
Destination	**Internal Network**
Action	**Deny**

به عنوان مثال در شکل زیر تمام ترافیک از آی‌پی‌های دریافت شده از دامنه IRANCTI به تمام مقاصد شبکه و با هر پورت و سرویسی مسدود خواهد شد.



شکل ۴. استفاده در **Policy**

الزامات پیاده‌سازی

برای استفاده صحیح از این قابلیت، موارد زیر باید فراهم باشد:

- FortiGate باید به URL معرفی‌شده دسترسی شبکه داشته باشد.
- در صورت استفاده از HTTPS ، گواهی SSL باید معتبر باشد.
- URL معرفی‌شده باید به‌صورت پایدار در دسترس باشد.
- ساختار فایل باید مطابق فرمت مورد انتظار FortiGate باشد.

ملاحظات امنیتی

توصیه می‌شود:

- Feed از طریق HTTPS منتشر شود.
- محتوای فایل به‌صورت دوره‌ای بازبینی شود.
- دسترس‌پذیری سرور منتشرکننده به‌صورت مستمر پایش شود.

نحوه ارتباط فایروال با منبع خارجی Threat Feed

توضیحات ارائه‌شده در خصوص استفاده از قابلیت Threat Feed زمانی به‌صورت کامل قابل اجرا است که فایروال سازمان به‌صورت مستمر و مطابق با الزامات امنیتی تعریف‌شده، امکان برقراری ارتباط با اینترنت و دریافت به‌روزرسانی‌های موردنیاز را داشته باشد. در این شرایط، فایروال می‌تواند در بازه‌های زمانی مشخص به منبع Threat Feed متصل شده و آخرین فهرست شاخص‌های تهدید شامل آدرس‌های آی‌پی را دریافت و اعمال نماید.

با این حال، در بسیاری از سازمان‌ها به دلیل الزامات امنیتی، سیاست‌های شبکه و یا ملاحظات حاکمیتی، امکان اتصال مستقیم فایروال به اینترنت وجود ندارد. در چنین شرایطی می‌توان از سناریوهای جایگزین زیر برای بهره‌برداری از Threat Feed استفاده نمود:

سناریوی اول: اتصال موقت و دوره‌ای فایروال به اینترنت

در این روش، فایروال در بازه‌های زمانی مشخص و تحت کنترل تیم امنیت، به‌صورت موقت به اینترنت متصل می‌شود تا آخرین اطلاعات Threat Feed را از منبع موردنظر دریافت نماید. پس از تکمیل فرآیند به‌روزرسانی، دسترسی اینترنت مجدداً قطع خواهد شد.

مزایا:

- پیاده‌سازی ساده و بدون نیاز به زیرساخت اضافی.
- مناسب برای سازمان‌هایی که به‌روزرسانی لحظه‌ای Threat Feed برای آن‌ها ضروری نیست.

محدودیت‌ها:

- فرآیند به‌روزرسانی وابسته به مداخله انسانی است.
- اطلاعات تهدیدات با تأخیر نسبت به حالت برخط دریافت می‌شوند.

سناریوی دوم: استفاده از یک سرور واسط در شبکه داخلی

در این سناریو یک سرور داخلی با دسترسی کنترل‌شده به اینترنت در شبکه سازمان مستقر می‌شود. این سرور به‌صورت دوره‌ای اطلاعات Threat Feed را از دامنه IRANCTI یا منبع تولیدکننده Feed دریافت و در اختیار فایروال قرار می‌دهد.

در این حالت فایروال به جای اتصال مستقیم به اینترنت، صرفاً به سرور داخلی متصل شده و فایل‌های Threat Feed را از آن دریافت می‌کند.

مزایا:

- حذف نیاز به اتصال مستقیم فایروال به اینترنت.
- امکان اعمال کنترل‌های امنیتی، ثبت رویدادها و پایش فرآیند دریافت داده‌ها.
- کاهش سطح ریسک دسترسی اینترنتی برای تجهیزات امنیتی.

ملاحظات:

- دسترسی‌های سرور واسط باید حداقل‌سازی شده و مطابق سیاست‌های امنیتی سازمان مدیریت گردد.
- ارتباط میان سرور و فایروال باید صرفاً به سرویس‌های موردنیاز محدود شود.

سناریوی سوم: معماری دو مرحله‌ای (DMZ / Staging Server)

در سازمان‌هایی با الزامات امنیتی سخت‌گیرانه‌تر می‌توان از معماری دو سروری استفاده کرد.

در این روش:

۱. سرور اول دارای دسترسی محدود و کنترل‌شده به اینترنت بوده و اطلاعات Threat Feed را از دامنه IRANCTI دریافت می‌کند.

۲. سرور دوم هیچ‌گونه دسترسی مستقیمی به اینترنت ندارد و اطلاعات را صرفاً از سرور اول دریافت و ذخیره می‌کند.

۳. فایروال تنها به سرور دوم متصل شده و اطلاعات Threat Feed را از این سرور دریافت می‌نماید.

در این معماری، فایروال هیچ ارتباط مستقیمی با اینترنت یا حتی با سرور متصل به اینترنت نخواهد داشت و کلیه تبادل داده‌ها از طریق یک لایه واسط انجام می‌شود.

مزایا:

- بالاترین سطح جداسازی و کنترل امنیتی.
- کاهش ریسک انتقال تهدیدات از محیط اینترنت به تجهیزات امنیتی.
- مناسب برای سازمان‌های حساس، زیرساخت‌های حیاتی و محیط‌های دارای الزامات انطباقی سخت‌گیرانه.

ملاحظات:

- نیازمند زیرساخت و مدیریت بیشتر نسبت به سایر سناریوها.
- تعریف دقیق سیاست‌های انتقال داده میان دو سرور ضروری است.

سناریوی چهارم: انتقال آفلاین Threat Feed

در سازمان‌هایی که هیچ‌گونه ارتباط مستقیم یا غیرمستقیم با اینترنت مجاز نیست، اطلاعات Threat Feed می‌تواند توسط یک سامانه مجاز در خارج از محیط عملیاتی دریافت و پس از انجام کنترل‌های امنیتی لازم، به‌صورت آفلاین به شبکه داخلی منتقل شود. در این روش فایل‌های Threat Feed بر روی یک مخزن یا سرور داخلی بارگذاری شده و فایروال اطلاعات موردنیاز را از همان منبع داخلی دریافت می‌کند.

این سناریو بیشترین سطح جداسازی از اینترنت را فراهم می‌کند، اما فرآیند به‌روزرسانی وابسته به اقدامات دستی بوده و معمولاً برای محیط‌های بسیار حساس و زیرساخت‌های با الزامات امنیتی سخت‌گیرانه مورد استفاده قرار می‌گیرد.

سناریوی پنجم: بارگذاری دستی شاخص‌های تهدید در فایروال

در سازمان‌هایی که امکان استفاده از External Threat Feed و یا استقرار زیرساخت واسط برای توزیع اطلاعات تهدید وجود ندارد، می‌توان شاخص‌های تهدید (IOC) را به‌صورت دستی یا از طریق اسکریپت‌های کنترلی در فایروال بارگذاری نمود.

در این روش، اطلاعات Threat Feed توسط دامنه IRANCTI دریافت شده و پس از انجام بررسی‌های امنیتی و تأیید صحت داده‌ها، فهرست آدرس‌های آی‌پی به‌صورت دستی و یا از طریق API در قالب Address Objectو Address Group در فایروال ثبت می‌شوند.

مزایا :

- عدم نیاز به اتصال فایروال به اینترنت.
- عدم نیاز به سرور واسط یا زیرساخت توزیع Feed
- امکان اعمال کنترل و تأیید کامل بر روی داده‌های واردشده.

محدودیت‌ها:

- فرآیند به‌روزرسانی وابسته به اقدامات دستی یا اجرای اسکریپت‌های مدیریتی است.
- با افزایش تعداد شاخص‌های تهدید، مدیریت و نگهداری اطلاعات دشوارتر خواهد شد.

- امکان تأخیر در اعمال آخرین تغییرات و به‌روزرسانی‌های Threat Intelligence وجود دارد.

این روش معمولاً در سازمان‌هایی مورد استفاده قرار می‌گیرد که به دلیل محدودیت‌های عملیاتی یا الزامات امنیتی، امکان استفاده از مکانیزم‌های خودکار دریافت و به‌روزرسانی Threat Feed را ندارند و ترجیح می‌دهند تمامی داده‌های ورودی پیش از اعمال در تجهیزات امنیتی مورد بررسی و تأیید قرار گیرند.

جمع‌بندی

قابلیت External Threat Feed در FortiGate روشی استاندارد، کارآمد و منعطف برای دریافت و اعمال خودکار شاخص‌های تهدید از منابع خارجی محسوب می‌شود. در این روش تنها با تعریف آدرس منبع Feed، فایروال می‌تواند به‌صورت دوره‌ای اطلاعات موردنیاز را دریافت کرده و از آن‌ها در سیاست‌های امنیتی، مکانیزم‌های مسدودسازی و فرآیندهای دفاعی سازمان استفاده نماید. این قابلیت ضمن کاهش فعالیت‌های دستی، سرعت واکنش به تهدیدات را افزایش داده و مدیریت متمرکز و به‌روزرسانی مستمر داده‌های امنیتی را تسهیل می‌کند.

با این حال، نحوه پیاده‌سازی و به‌روزرسانی Threat Feed باید متناسب با الزامات امنیتی، سطح حساسیت دارایی‌ها و سیاست‌های حاکم بر شبکه سازمان انتخاب شود. اگرچه اتصال مستقیم فایروال به اینترنت ساده‌ترین روش بهره‌برداری از این قابلیت است، اما سازمان‌ها می‌توانند با استفاده از سرورهای واسط، معماری‌های چندلایه، انتقال آفلاین داده‌ها یا حتی بارگذاری دستی شاخص‌های تهدید، ضمن حفظ الزامات امنیتی خود از مزایای Threat Intelligence بهره‌مند شوند. در تمامی این سناریوها، رعایت اصل حداقل دسترسی (Least Privilege)، کنترل و اعتبارسنجی داده‌های دریافتی، ثبت رویدادها و پایش مستمر ارتباطات از الزامات اساسی برای حفظ امنیت و اطمینان از صحت عملکرد سامانه خواهد بود.