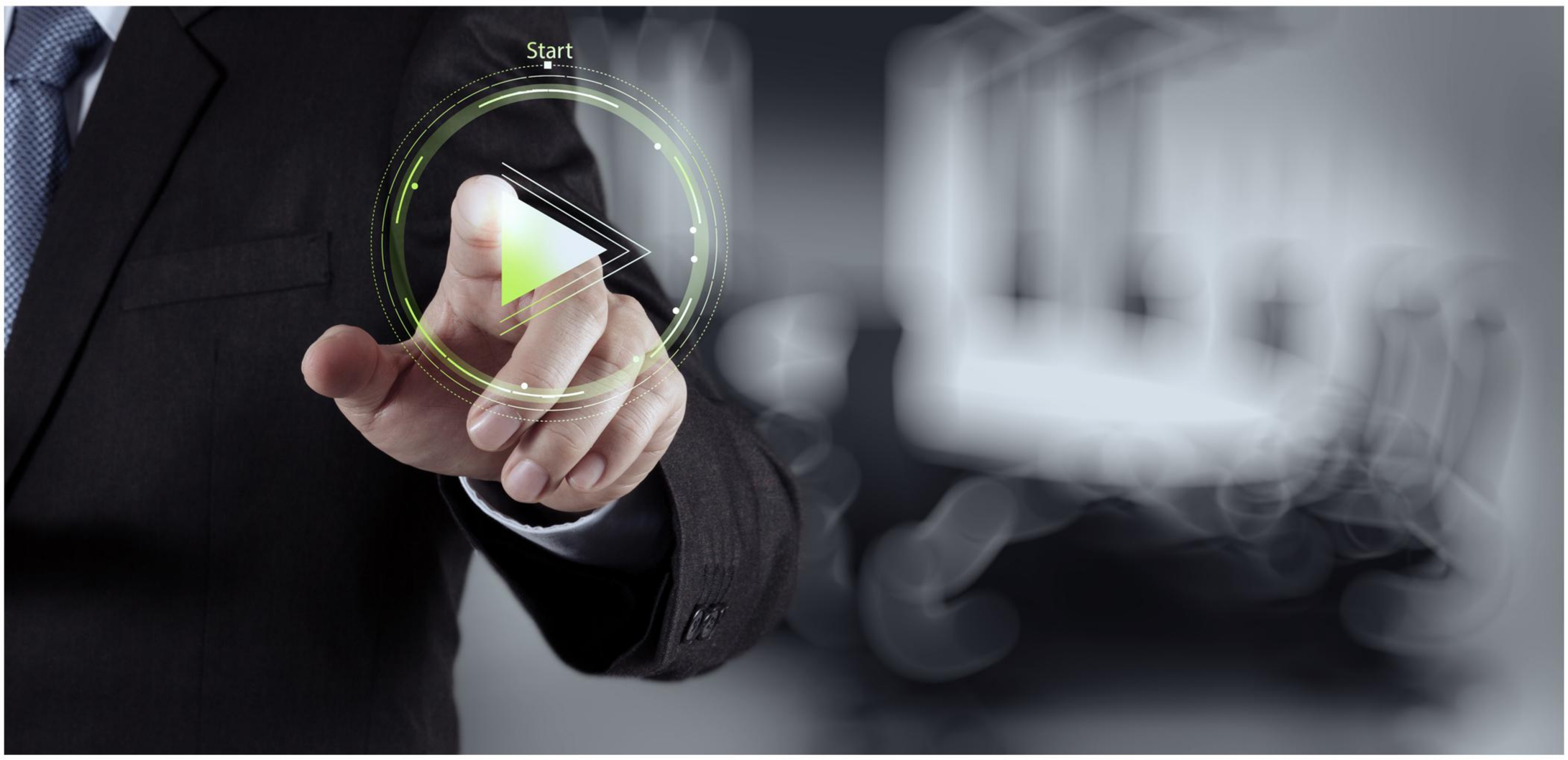
SIBTA

سامانه یکپارچه بروزرسانی تجهیزات امنیتی

فورتی گیت / فورتی وب

https://partian.co



مقدمه:

در دنیای پرشتاب امروزی، استفاده از شبکه های کامپیوتری و موبایل با سرعت زیادی در حال گسترش می باشد. شرکت های خصوصی و دولتی زیادی وجود دارند که تنها با وجود شبکه ای منظم و منسجم قادر به ادامه ی حیات خود هستند. زیرا این زیرساخت های نرم افزار و سخت افزاری است که بستر مناسب را جهت ارائه ی خدمات در اختیار آنان قرار می هد.

دراین بین، برقراری امنیت در این شبکه ها به موضوعی بسیار مهم بدل خواهد شد. چرا که در سایه ی امنیت، یک شبکه قادر به پاسخگویی مناسب به درخواست های کاربران خواهد بود.

همواره امنیت شبکه یکی از پر چالش ترین مباحثی بوده است که شرکت ها و سازمان های بزرگ نیز با آن دست و پنجه نرم می کنند.

افزایش امنیت شبکه در یک سازمان علاوه بر ارتقاء کیفیت سرویس دهی، میتواند از حریم خصوصی کاربران و همچنین نشت اطلاعات جلوگیری نماید.

حملات سایبری نیز یکی دیگر از مشکلاتی است که عمدتاً شبکه های سازمان های بزرگ و حیاتی همواره با آن مواجه هستند. در صورت وجود سیستم های مناسب در لبه و هسته ی شبکه، احتمال وقوع حملات و آسیب پذیری سیستم ها به شدت کاهش می یابد.

در بین تمامی شرکت های تولید کننده تجهیزات امنیتی در دنیا، شرکت Fortinet یکی از بزرگترین و مطرح ترین شرکت ها، در این حوزه می باشد. به طوری که در بسیاری از شبکه های سازمان های دولتی و شرکت های خصوصی در ایران، از تجهیزات این شرکت بزرگ و موفق استفاده می شود.

شرکت Fortinet به صورت تخصصی بر روی تجهیزات امنیت شبکه تمرکز کرده و با ارائه ی محصولات بروز و کاملاً پایدار، توانسته در بسیاری از حوزه های امنیت در مقام Leader جایگاه خود را تثبیت کند.

مهمترین محصول این شرکت FortiGate نام دارد. FortiGate به عنوان اصلی ترین محصول Fortinet توانسته است طی سال های اخیر در سطح دنیا جایگاه بسیار بالایی را کسب نماید. از دلیل این موفقیت میتوان به موارد ذیل اشاره کرد:

سهولت در استفاده از GUI و CLI / پایداری فوق العاده سخت افزار / خدمات پشتیبانی قابل قبول / ارائه ی آپدیت های متنوع / امکان آپدیت دستگاه به صورت آفلاین / عدم نیاز به لایسنس برای راه اندازی و ....

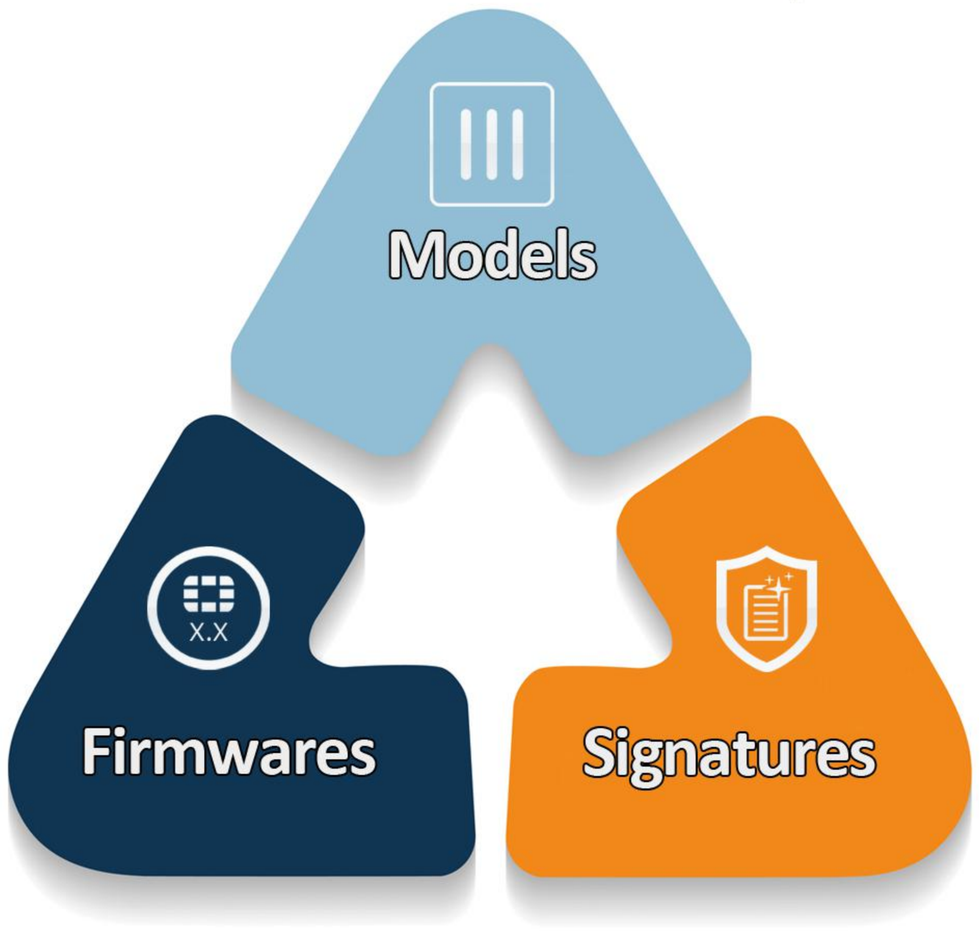
معرفی سیبتا:

شاید شما هم جزء آن دسته از مدیران شبکه ای هستید که برای آپدیت کردن Signature های فایروال خود با مشکل مواجه شده اید.
بازه ی این مشکلات میتواند شامل قیمت بالای لایسنس های آنلاین تا بلک لیست بودن تجهیزات شما باشد.
در نتیجه تنها راه پیش روی شما، دریافت فایل های آپدیت و نصب آنها بر روی تجهیزات خود به صورت دستی و Offline خواهد بود. در این روش شما نیازمند به داشتن دسترسی به سایت مرجع و اکانت آن خواهید بود که با توجه به مطالب فوق، این امر برای همه ی شرکت ها و مجموعه ها میسر نیست.

شرکت مهندسی پارتیان ابتکار پایدار با گرد هم آوری یک تیم نرم افزاری و یک تیم فنی، اقدام به طراحی و ساخت نرم افزار سیبتا نموده است.
سیبتا (سامانه یکپارچه بروزرسانی تجهیزات امنیتی) یک نرم افزار متمرکز و کارآمد جهت بروزرسانی تجهیزات امنیت شبکه خانواده Fortinet می باشد.

این شرکت بر پایه ی دانش فنی و استفاده از نیروی متخصص در حوزه ی نرم افزار و امنیت شبکه، موفق به دریافت مدرک دانش بنیانی از معاونت علمی و فناوری ریاست جمهوری نیز شده است.

سیبتا قادر خواهد بود، تجهیزات امنیت شبکه FortiGate و FortiWeb را در تمامی مدل های ساخته شده ی بعد از سال 2015 و در تمامی سیستم عامل های بالاتر از ورژن 5.4.0 برای FortiGate و 6.3.6 برای FortiWeb پشتیبانی نماید.
از این رو طیف وسیعی از تجهیزات موجود در شرکت های ایران که در حال کار هستند، قادر خواهند بود با استفاده از این سامانه نسبت به بروزرسانی Signature های خود اقدام نمایند.



قابلیت های سیبتا:

از آنجا که شرکت Fortinet طیف وسیعی از تجهیزات FortiGate و FortiWeb در مدل های مختلف تولید و عرضه میکند، طبیعتاً سیستم عامل های متنوع و متفاوتی نیز برای آنها ها وجود خواهد داشت. نرم افزار سیبتا امکان بروزرسانی تمامی مدل های ساخته شده توسط Fortinet را دارا خواهد بود.

- FortiGate Series 60,70,80,90 / D,E,F
- FortiGate Series 100,200 / D,E,F
- FortiGate Series 300,400 / C,D,E,F
- FortiGate Series 500,600 / C,D,E,F
- FortiGate Series 800,900 / C,D
- FortiGate Series 1000 / C,D,E,F
- FortiGate Series 1800 / F
- FortiGate Series 2000 / E,F
- FortiGate Series 3000 / C,D,E
- FortiGate Series 4000 / F
- FortiGate Series 5000 / C,D,E
- FortiGate Series 6000 / F
- FortiGate Series 7000 / E
- FortiGate All VM Series

- FortiWeb Series 100 / D,E
- FortiWeb Series 400 / C,D,E,F
- FortiWeb Series 600 / D,E,F
- FortiWeb Series 1000 / C,D,E
- FortiWeb Series 2000 / E,F
- FortiWeb Series 3000 / C,D,E,F
- FortiWeb Series 4000 / C,D,E,F
- FortiWeb VM All Series

ویژگی های سیبتا:

- دانلود و نصب اتوماتیک فایل های آپدیت
- کنسول مدیریتی بسیار ساده و در عین حال کارآمد
- قابلیت زمانبندی انجام عملیات آپدیت
- قابلیت اجراء به صورت Service Base
- قابلیت آپدیت تمام Signature های متعارف
- امکان آپدیت Signature صنعتی Industrial Definition
- امکان آپدیت Signature موبایل Mobile Malware
- ذخیره Log از تمام فرایندهای آپدیت
- قابلیت آپدیت چندین دستگاه به صورت همزمان
- اطمینان از آپدیت بودن همیشگی تجهیزات
- کاهش هزینه های سازمان در مقایسه با لایسنس آنلاین
- آپدیت بدون نیاز به اینترنت برروی FortiGate و FortiWeb
- کاهش خطر Black List شدن دستگاه
- حذف نیروی انسانی جهت انجام پروسه ی آپدیت
- ارسال کد OTP برای کاربران به وسیله پیامک
- تهیه Backup اتوماتیک از تنظیمات FortiGate و FortiWeb

قابلیت های کلیدی سیبتا

All Signatures

در لایسنس های آنلاین استاندارد، شما امکان دریافت تنها چهار Signature جهت بروزرسانی FortiGate را خواهید داشت. اما در سیبتا امکان آپدیت هفت Signature برای تجهیزات شما فراهم خواهد بود.

All Models

نرم فزار سیبتا، قابلیت بروزرسانی تمامی مدل های FortiGate و FortiWeb را برای شما فراهم می سازد. حتی اگر تجهیزات شما وارد لیست سیاه شرکت Fortinet شده باشند، سیبتا قادر خواهد بود همانند لایسنس های آنلاین، تجهیزات شما را بروزرسانی نماید.

All Firmwares

با توجه به نوع طراحی و برنامه نویسی نرم افزار سیبتا، فارغ از ورژن سیستم عامل FortiGate یا FortiWeb خود و همچنین تنظیمات احتمالی VDOM بر روی آن، به سادگی امکان آپدیت تجهیز خود را خواهید داشت.

محدودیت ها در کشورهای تحریمی:

با توجه به تحریم هایی که حدوداً در اوایل سال 2012 میلادی بر علیه ایران اعمال شد، دسترسی IP های ایران جهت دریافت آپدیت های آنلاین به چندین شرکت بزرگ تولید کننده تجهیزات امنیت شبکه در دنیا محدود شد. ازاین رو شرکت پارتیان و دیگر شرکت های فعال در این حوزه، شروع به کشف راهکارهایی جهت دورزدن این مانع بزرگ برای دریافت لایسنس آنلاین شدند. در این بین، دستگاه های زیادی به دلیل ارتباط مستقیم با سایت Fortinet وارد Black List شدند و دیگر امکان دریافت آنلاین آپدیت ها را از دست دادند.

هرچند که در حال حاضر امکان دریافت لایسنس آنلاین برای تجهیزاتی که جدیداً خریداری می شوند فراهم است، اما به دلیل قیمت بالای لایسنس های آنلاین، بسیاری از سازمان ها و شرکت ها تمایلی به خرید و تمدید لایسنس های آنلاین ندارند.

سیبتا با ارائه ی روزانه ی فایل های آپدیت به صورت آفلاین و نصب اتوماتیک آن بر روی تجهیزات FortiGate و FortiWeb، و با کاهش هزینه های سازمان، کمک شایانی در برقراری امنیت شبکه در شرکت ها و سازمان ها خواهد کرد.

IP Geography Database

ارائه سرویس IP Geo Location

همواره تشخیص اینکه کاربران از کدام موقعیت جغرافیایی به شبکه شما دسترسی دارند دشوار بوده است. با ارائه ی سرویس IP Geo Location این مشکل تا حد زیادی مرتفع شد. اما تنها در صورتی که شما لایسنس آنلاین در اختیار داشته باشید.

در غیر این صورت، امکان آپدیت لیست IP های کشورها، برای شما فراهم نخواهد بود. و از آنجا که IP ها در سطح جهان مرتباً در حال جابجایی بین کشورهای مختلف می باشد، اجازه ی دسترسی به کاربران یک کشور خاص با چالش جدی مواجه میگردد.

سیبتا با جمع آوری اطلاعات مربوط به IP کشورها از چندین منبع مختلف، و تجمیع آنان با یکدیگر، Database بسیار کاملی از IP های کشور ایران را در اختیار شما قرار خواهد داد.

این اطلاعات برای شرکت هایی که در حوزه ی پرداخت (Fintech و Loantech) فعالیت دارند، بسیار حائز اهمیت خواهد بود. چرا که از الزامات شاپرک و بانک مرکزی ایران، ارائه ی دسترسی به شبکه پرداخت تنها از طریق IP های ایران است.

FORTINET

[این سرویس بر روی تجهیزات **FortiGate** و **FortiWeb** قابل ارائه خواهد بود.]

FORTINET®

مجوعه کامل Signature 7
جهت بروزرسانی تجهیزات امنیتی FortiGate

Application Definition
شناسایی نرم افزارهای استفاده شده در سطح شبکه به همراه امکان Monitor کردن و یا Block کردن آنها.

Attack Definition (IPS)
شناسایی و جلوگیری از حملات در سطح شبکه و محافظت از Server ها و سرویس های بر روی اینترنت.

Antivirus Definition
آنتی ویروس با پالایش فایل ها بر روی پروتکل های منتخب، از ورود ویروس به داخل شبکه جلوگیری می نماید.

Industrial Definition
جلوگیری از حملات سایبری بر روی تجهیزات و سخت افزارهای صنعتی به صورت تخصصی.

Mobile Malware
محافظت از سیستم عامل های تلفن همراه و جلوگیری از تهدیدات احتمالی بر روی آنها.

Internet Service
ارائه لیست بسیار کاملی از ارائه دهنگان سرویس های ابری در سطح دینا جهت اعمال دسترسی خاص به آنها.

Botnet IP Database
ارائه لیست IP هایی که به عنوان Botnet شناسایی شده اند و مسدود سازی دسترسی به آنها.

GEO IP Database
ارائه لیست IP های کشور ایران جهت محدود سازی دسترسی از خارج از ایران و افزایش سطح امنیت.

SIBTA
Unified Security System Updater

Application Control

ماژول Application Control در FortiGate یک قابلیت مهم امنیتی است که به کمک آن میتوانید دسترسی و استفاده از برنامه ها و نرم افزارهای مختلف را در شبکه کنترل کنید. این قابلیت به شما اجازه میدهد تا براساس سیاستهای امنیتی خود، اجازه یا ممنوعیت استفاده از برنامه های خاص را برای کاربران یا دستگاه های مختلف تعیین کنید.

از طریق Application Control، میتوانید محدودیت هایی را برای نصب و اجرای برنامه ها در شبکه ی سازمانی تان اعمال کنید. به عنوان مثال، میتوانید برنامه های خاص را ممنوع کرده و یا محدودیت هایی مانند تنظیمات دسترسی، نسخه های مجاز برنامه ها و حتی زمانبندی استفاده از آنها را اعمال کنید.

Intrusion Prevention - IPS

ماژول Application Control در FortiGate یک قابلیت مهم امنیتی است که به کمک آن میتوانید دسترسی و استفاده از برنامه ها و نرم افزارهای مختلف را در شبکه کنترل کنید. این قابلیت به شما اجازه میدهد تا براساس سیاستهای امنیتی خود، اجازه یا ممنوعیت استفاده از برنامه های خاص را برای کاربران یا دستگاه های مختلف تعیین کنید.

از طریق Application Control، میتوانید محدودیت هایی را برای نصب و اجرای برنامه ها در شبکه ی سازمانی تان اعمال کنید. به عنوان مثال، میتوانید برنامه های خاص را ممنوع کرده و یا محدودیت هایی مانند تنظیمات دسترسی، نسخه های مجاز برنامه ها و حتی زمانبندی استفاده از آنها را اعمال کنید.

Antivirus Definition

ماژول Antivirus در FortiGate جهت افزایش سطح امنیت شبکه ها و سیستم های سازمانی در برابر تهدیدات امنیتی مختلف، به ویژه Virus ها وTrojan ها و نرم افزارهای مخرب طراحی شده است.

Antivirus به عنوان بخشی از ماژول های امنیتی FortiGate ارائه میشود و از تکنولوژی های مختلف مانند موتورهای تشخیص و جلوگیری از تهدید، امضای الکترونیکی، تحلیل رفتاری، فیلترینگ و بلاک کردن تهدیدات مخرب بهره میبرد.به کمک الگوریتم های پیشرفته، Antivirus در FortiGate تلاش میکند تا تشخیص و مسدود سازی هرگونه فعالیت مشکوک یا خطرناک در شبکه را بر عهده داشته باشد.

Industrial Definition

اصطلاح Industrial Definition در FortiGate به معنای تعریف یک سطح صنعتی یا استفاده از تنظیمات استاندارد برای محیط های صنعتی است. در امنیت شبکه، محیط های صنعتی نیازهای منحصر به فرد خود را دارند. به عنوان مثال، یک محیط صنعتی ممکن است دارای ابزارها و دستگاه های خاصی باشد که نیازمند تنظیمات امنیتی خاصی نیز هستند.

FortiGate این قابلیت را دارد که تنظیمات و قابلیت های خود را برای محیط های صنعتی بهینه کند. این به معنای ارائه تنظیمات پیش فرض و قابل تنظیم برای این نوع محیط ها است تا امنیت آنها را تضمین کند. به عنوان مثال، FortiGate ممکن است قابلیت های خاصی برای محافظت از دستگاه ها یا شبکه های محیط های صنعتی ارائه دهد که با استفاده از قابلیت های استاندارد ممکن نباشد.

Mobile Malware

FortiGate یکی از ویژگی‌های مهم خود را برای مقابله با بد افزارهای موبایل (Mobile Malware) ارائه می دهد. این دستگاه امنیتی قابلیت های مختلفی برای شناسایی و محافظت از تمامی دستگاه های موبایل هوشمند در شبکه‌های مختلف را فراهم می کند. این قابلیت ها می توانند شامل موارد زیر باشند:

شناسایی و حفاظت از بد افزارها: FortiGate قادر است بد افزارهای موبایل را شناسایی کرده و در صورت شناسایی، اقدامات لازم برای محدود کردن یا جلوگیری از ورود آنها به شبکه را انجام دهد. کنترل دسترسی: قابلیت های FortiGate به مدیران اجازه می دهد تا دسترسی به دستگاه های موبایل را محدود کنند و سیاست های دسترسی به شبکه را تنظیم کنند. پشتیبانی از دستگاه های مختلف: FortiGate از سیستم عامل ها و دستگاه های موبایل متنوعی از جمله iOS و Android پشتیبانی می کند.

Internet Service Database

ماژول Internet Service Database یا به اختصار (ISDB) یک پایگاه داده است که اطلاعات مربوط به سرویس های اینترنتی مختلف را شامل میشود. این پایگاه داده حاوی اطلاعاتی مانند پورت های استاندارد برای سرویس های مختلف، پروتکل های استفاده شده، ساختار بستر شبکه و مواردی از این قبیل است.

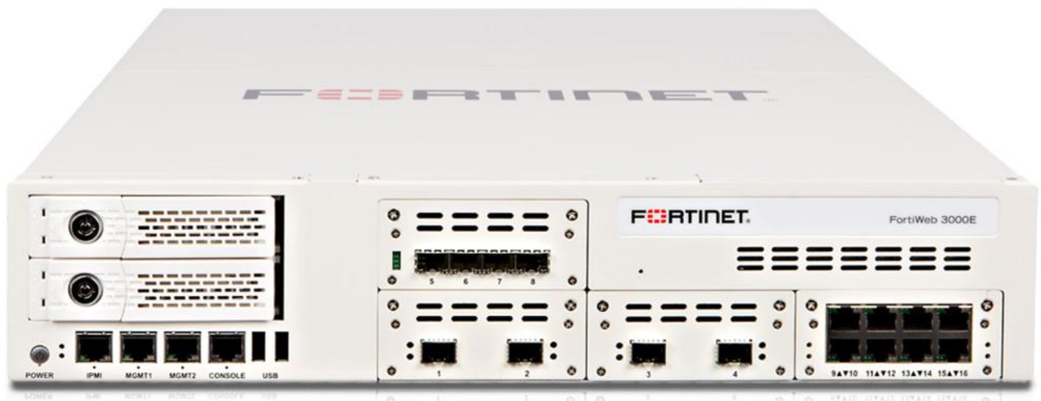
با استفاده از ISDB در FortiGate میتوان بهترین عملکرد را برای مسائل مختلفی مانند مدیریت ترافیک، تشخیص تهدیدات، مسدود سازی یا محدود کردن دسترسی به سرویس های خاص را انجام دهد.

Botnet IP Database

Botnet IP در FortiGate به IP هایی اشاره دارد که به عنوان بخشی از Botnet ها شناخته میشوند. Botnet ها معمولاً شبکه هایی از دستگاه های مختلف و کنترل شده توسط مهاجمان هستند که برای انجام حملات مختلف از جمله حملات DDoS، ارسال اسپم، سرقت اطلاعات و ... به کار میروند.

در FortiGate، لیستی از IPهای شناخته شده به عنوان بخشی از Botnet ها در دسترس است و میتوانید از این لیست برای محدود کردن دسترسی یا جلوگیری از ارتباط با این IP ها در شبکه خود استفاده کنید. این کار میتواند به عنوان یک ابزار دفاعی در برابر حملات Botnet ها و تهدیداتی که از آنها ناشی میشوند، مورد استفاده قرار گیرد.

FORTINET®



مجوعه کامل Signature 5 جهت بروزرسانی تجهیزات امنیتی FortiWeb

Security Service
جلوگیری از حملات بر روی وب سرورها و به طور خاص تمرکز بر روی پروتکل های HTTP و HTTPS.

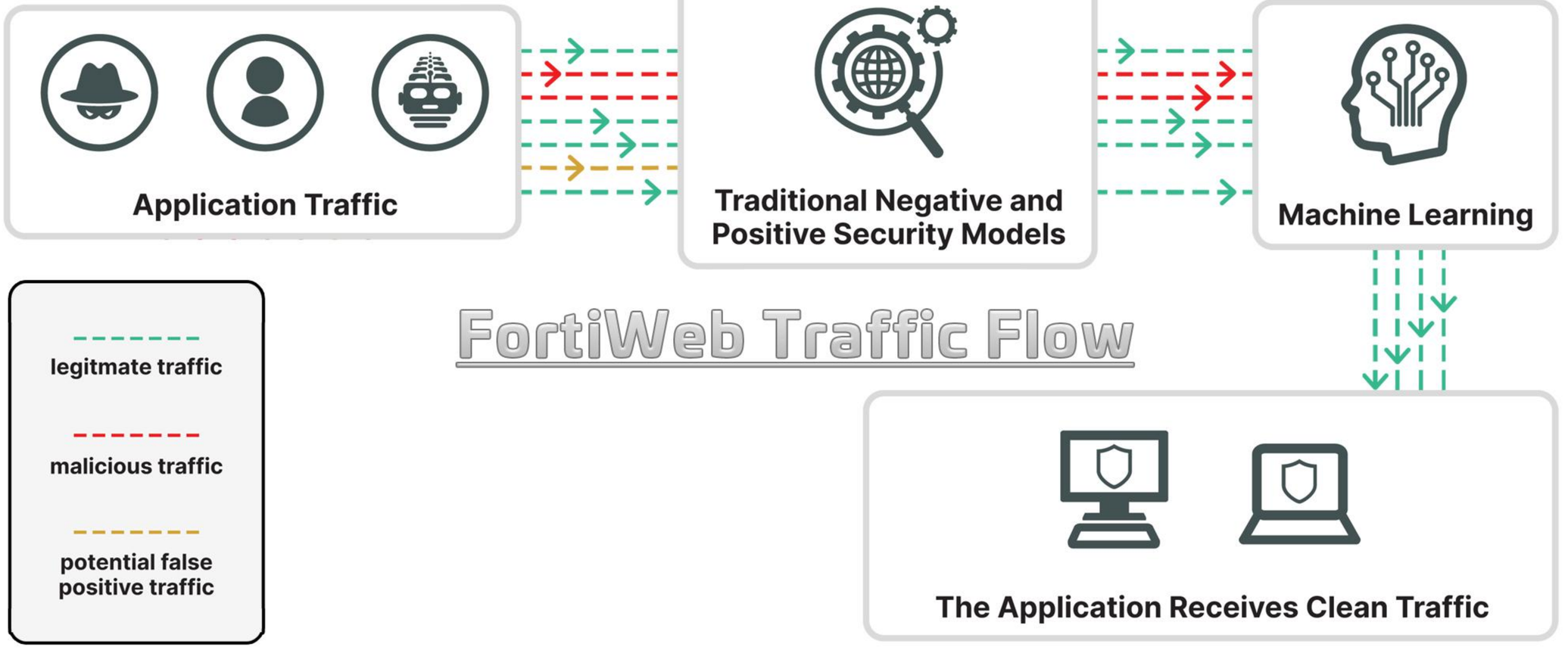
Antivirus
آنتی ویروس فورتی وب با پالایش فایل ها، از ورود ویروس به داخل وب سرور جلوگیری می نماید.

Antivirus Extended
نسخه پیشرفته آنتی ویروس در فورتی وب امکان شناسایی تعداد بیشتری از ویروس ها را در اختیار شما قرار میدهد.

IP Reputation Service
بررسی و اعتبار سنجی IP ها در چندین سطح جهت جلوگیری از دسترسی های مشکوک و ربات ها به سرویس ها.

GEO IP Location
ارائه لیست IP های تمامی کشور های جهان جهت محدود سازی دسترسی از یک مبداء خاص.

SIBTA
Unified Security System Updater



FortiWeb Traffic Flow

Security Service

این Signature جهت محافظت از برنامه‌ها و وب سایت‌ها در برابر حملات و تهدیدات امنیتی طراحی شده است. این سرویس امکانات مختلفی را ارائه می‌دهد که به محافظت از برنامه‌های وب از جمله حملات DDoS، حملات Cross-Site Scripting یا XSS حملات SQL Injection و بسیاری از حملات دیگر کمک می‌کند.

یکی دیگر از مهمترین حملاتی که به وسیله ی این Signature امکان دفع آن را خواهید داشت Command Injection می باشد. حمله Command Injection یک نوع حمله امنیتی است که در آن، مهاجمان سعی می‌کنند دستورات یا فرمان‌های خط فرمانی را به سیستم یا برنامه‌هایی که به شبکه متصل هستند، تزریق کنند. این نوع حمله اغلب در برنامه‌های وب و سیستم‌هایی که ورودی‌های کاربر را پردازش می‌کنند اتفاق می‌افتد، به ویژه در صورتی که این برنامه‌ها ورودی های خود را به‌صورت نادرست یا ناامن پردازش کنند.

به طور کلی با بروزرسانی این Signature شما قابلیت مقابله با انواع حملات زیر را خواهید داشت:

OWASP Top 10 / Cross Site Scripting / SQL Injection / Cross Site Request Forgery / Session Hijacking

این Signatue همچنین جهت محافظت از API ها نیز مورد استفاده قرار میگیرد:

Machine Learning API / Discovery and Protection / XML and JSON protocol / Schema verification / API Gateway

Antivirus

ماژول Antivirus در FortiWeb جهت افزایش سطح امنیت وب سرورها طراحی و ساخته شده است. نحوه کار این ماژول به این شکل می باشد که، در صورت آپلود فایل از جانب کاربر بر روی وب سرور، Antivirus موجود بر روی FortiWeb ضمن اسکن فایل مذکور، در صورت ایمن بودن آن، اجازه ی نوشتن آن فایل را در سرور مربوطه صادر می نماید.

همواره استفاده از Antivirus های چند لایه در سطح شبکه برای سیستم های سرور بسیار حائز اهیمت بوده است. چرا که در صورت وجود تنها یک Antivirus بر روی سیستم عامل وب سرور، شما تنها با یک Engine قادر به اسکن فایل ها و تهدیدات احتمالی خواهید بود. ولی در این حالت شما به طور همزمان هم از Antivirus تجهیزات FortiWeb استفاده نموده اید و هم از Antivirus نصب شده بر روی وب سرور و این امر باعث افزایش حداکثری سطح امنیت بر روی سرورهای شما خواهد شد.

Antivirus Extended

به طور کلی در FortiWeb دو Database برای Antivirus وجود دارد. یکی Regular Virus Database که توضیح آن در بالا ارائه شد و دیگری Extended Virus Database.

در بخش Extended Database شما امکان چک و آنالیز تعداد بسیار بیشتری از Virus ها را خواهید داشت.

معمولاً در این Database نوع های متفاوتی از Virus های متداول وجود خواهد داشت. استفاده از این قابلیت برای محافظت پیشرفته تر و وب سایت های حساس تر پیشنهاد می گردد. البته در صورت استفاده از Database مربوط به Extended Virus مقدار حجم بیشتری از RAM و CPU طبیعتاً مورد استفاده قرار خواهد گرفت.

IP Reputation Service

IP Reputation به معنای اعتبار شناسه آدرس IP است. این مفهوم بر اساس تاریخچه و عملکرد یک آدرس IP خاص در شبکه ها و اینترنت است. اعتبار یک آدرس IP ممکن است توسط سرویس‌ها و سیستم‌های امنیتی مورد استفاده قرار گیرد تا تشخیص دهند که آیا یک آدرس IP خاص دسترسی به سرویس‌ها یا منابع را داشته باشد یا خیر.

این مفهوم اعتبار IP براساس فعالیت‌های آدرس IP، از جمله ارسال ایمیل‌های ناموجه (Spam)، حملات DDoS، فعالیت‌های مرتبط با بدافزار، سرورهای غیرقانونی، وب سایت های Phishing و سایر فعالیت‌های مخرب یا نامناسب محاسبه می‌شود.

به عبارت دیگر، اگر یک آدرس IP خاص به عنوان یک منبع مشکوک شناخته شود، ممکن است به صورت اتوماتیک مسدود شود یا تحت مراقبت قرار گیرد تا از آسیب دیدن یا نفوذ به شبکه‌ها جلوگیری شود.

اطلاعات مرتبط با اعتبار آدرس IP معمولاً توسط شرکت‌های امنیتی و سرویس‌های مربوط به امنیت شبکه جمع‌آوری می‌شود و از این اطلاعات برای ارزیابی وضعیت امنیتی آدرس‌های IP مختلف استفاده می‌شود.

GEO IP Location

بروزرسانی لیست IP های کشورهای دنیا برای بعضی از وب سایت های بسیار مهم و حائز اهمیت می باشد. از آنجا که بعضی از این سرویس ها و خدمات نیازی به دسترسی از خارج از ایران به آنها نمی باشد.

با بروزرسانی GEO IP در تجهیزات FortiWeb شما قادر خواهید بود تا بتوانید تنها ترافیک ورودی از یک کشور خاص را اجازه عبور دهید. این کار باعث افزایش سطح امنیت در شبکه شما خواهد شد. سرویس GEO IP Location در تجهیزات فورتی وب میتواند لیست IP های تمامی کشورهای دنیا را بروزرسانی کرده و از ورود کاربران از دیگر کشورها به داخل شبکه و سرور جلوگیری کند.

Two-Factor Authentication

- FAST
- SIMPLE
- SECURE
- ACCESSIBLE

احراز هویت دوعاملی / Two-Factor Authentication

استفاده از Two-Factor Authentication - 2FA یا احراز هویت دو عاملی، یک روش امنیتی است که از دو عامل جهت احراز هویت کاربر استفاده می‌کند.

۱- عامل دانشی مانند: نام کاربری و رمز عبور

۲- عامل مالکیتی مانند: یک دستگاه تأیید هویت (مثل تلفن همراه، ایمیل و یا کلید امنیتی)

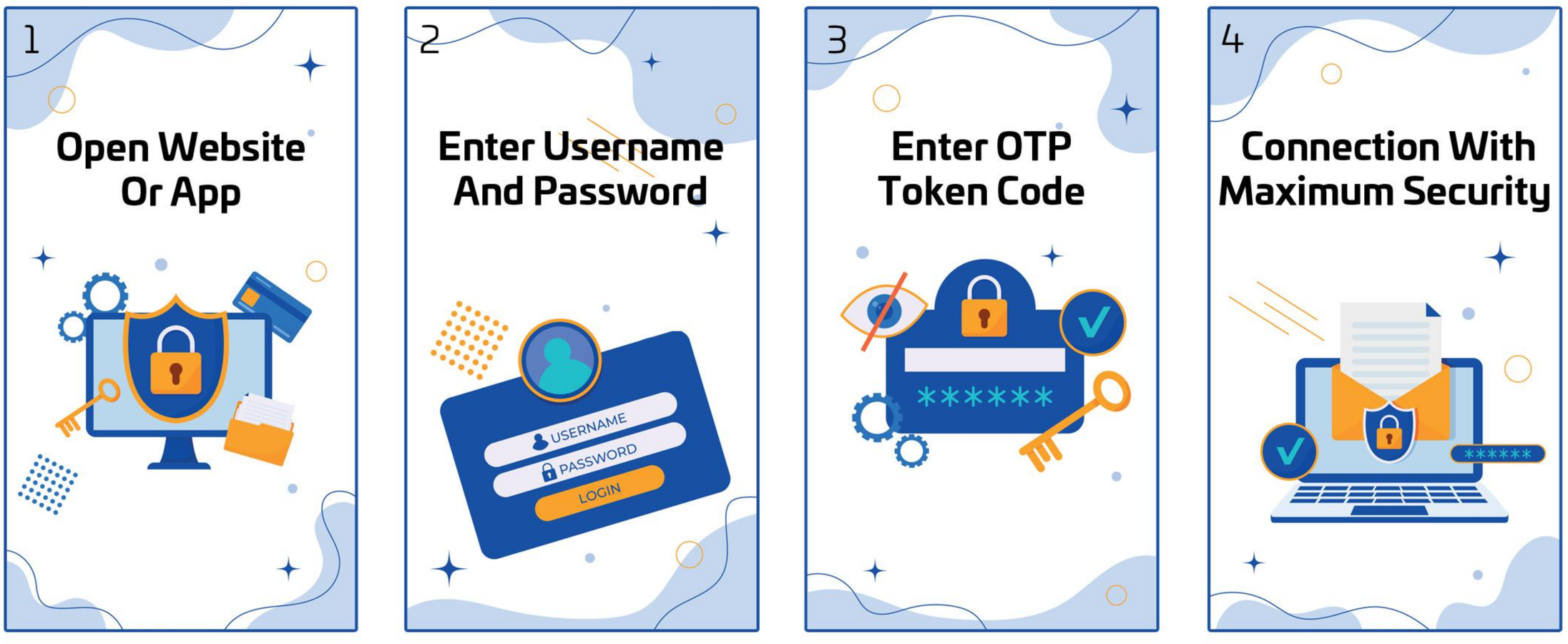
استفاده از 2FA در شبکه‌های کامپیوتری به دلایل زیادی صورت می‌گیرد:

۱- افزایش امنیت: استفاده از دو مرحله برای احراز هویت باعث افزایش سطح امنیت می‌شود. حتی اگر یکی از عوامل مورد نظر (رمز عبور یا دستگاه تأیید هویت) توسط مهاجم دزدیده شود، دسترسی به حساب کاربری بدون داشتن عامل دیگر تقریباً غیرممکن است.

۲- مقابله با نفوذهای آنلاین: امروزه حملات نفوذ به حساب های کاربری بسیار رایج شده است. با اجرای 2FA حتی اگر رمز عبور کاربر توسط حمله کننده دزدیده شود، برای ورود به حساب نیاز به یک دستگاه یا اطلاعات دیگر خواهد بود.

۳- حفاظت در برابر فراموشی یا آسیب پذیری رمز عبور: شما با استفاده از قابلیت 2FA به کاربران اجازه می‌دهید که برخی از نگرانی‌های مرتبط با فراموشی رمز عبور یا وجود رمزهای ضعیف را کاهش دهند. حتی اگر یک رمز عبور ضعیف داشته باشند، هنوز با داشتن عامل دوم، امنیت حساب کاربری آنها حفظ می‌شود.

۴- پیشگیری از نفوذ به چندین حساب: بسیاری از افراد برای تسهیل در یادآوری، از رمزهای عبور یکسانی برای سامانه هایی که با آنها در ارتباط هستند استفاده می کنند. با استفاده از 2FA، حتی اگر یک حساب کاربری دچار نقض شود، حساب‌های دیگر در امان خواهند بود.



سرویس OTP در نرم افزار سیبتا:

نرم افزار سیبتا امکان ارسال کد های OTP تولید شده توسط FortiGate را برای کاربران شما فراهم می آورد. ارسال کد های OTP به دو صورت SMS و Email امکان پذیر خواهد بود.

از OTP به عنوان یک فرم از Two-Factor Authentication استفاده می‌شود. OTP یک رمز عبور یکبار مصرف است که برای ورود به یک حساب کاربری یا سیستم مورد استفاده قرار میگیرد و بعد از یک بار استفاده دیگر قابل استفاده نخواهد بود.

از سرویس بسیار کاربردی OTP در FortiGate می توانید بر روی بسترهای زیر استفاده نمایید:

- FortiClient SSL VPN *(Windows, Linux, MAC, IOS, Android)*
- FortiClient IPsec VPN *(Windows, Linux, MAC, IOS, Android)*
- HTTP & HTTPS *(Chrome, FireFox, Opera, Edge, Safari)*
- SSL VPN Web *(Chrome, FireFox, Opera, Edge, Safari)*

ارسال کد OTP به وسیله ی SMS برای کاربران و مدیران شبکه بسیار ساده و به دور از هرگونه پیچیدگی می باشد، اما در عین حال مشکلی که بعضاً ممکن است رخ دهد، Deliver شدن همراه با تاخیر، به گوشی کاربران خواهد بود.
سیبتا برای حل این مشکل، به طور همزمان قادر خواهد بود تا کد OTP را هم برای کاربر SMS و هم Email نماید. در عین حال با توجه به مشکلات احتمالی در شبکه ی داخلی اپراتورهای ارائه دهنده خدمات پیامکی، شما این امکان را خواهید داشت تا در صورت نیاز بتوانید اپراتور ارسال کننده SMS را تغییر دهید.
با این کار در صورت بروز مشکل و یا اختلالی در شبکه داخلی هر یک از اپراتورهای ارائه کننده خدمات پیامکی، مدیر سیستم می تواند در کمترین زمان ممکن نسبت به تغییر اپراتور اقدام نماید.

پارتیان ابتکار پایدار

Keep in touch

Address: Unit 5, No. 394, Pasdaran Ave, Tehran, IRAN
sales@partian.co - info@Partian.co

https://partian.co
https://sibta.partian.co

+9821-72 98 3000

Fortinet_Partian