GlobalProtect

جلوگیری از نفوذها و ایمن سازی Mobile workforce

GlobalProtect، محافظت از نسل آیندهٔ زیرساخت های امنیتی شبکه های کامپیوتری Paloalto را به اعضای Mobile workforce شما، فارغ از آنکه در کدام موقعیت و مکان قرار داشته باشند، تعمیم می دهد.

جهانی که باید از آن محافظت نمایید، به دلیل نقل مکان کاربران و برنامه‌ها و کاربردها، به مکان‌هایی خارج از شعاع متداول شبکه‌ها، همواره در حال گسترش است. تیم‌های امنیتی، با چالش‌هایی در ارتباط با حفظ میزان آشکار بودن در ترافیک شبکه‌ها و اعمال سیاستگذاری‌های امنیتی به منظور جلوگیری از تهدیدها، روبه‌رو هستند. تکنولوژی‌های متداول به کار رفته به منظور محافظت از تلفن‌های همراه، مانند آنتی ویروس‌های میزبان نهایی، و VPNهایی با دسترسی از راه دور، قادر به جلوگیری از تکنیک‌های پیشرفته مورد استفاده مهاجمین پیچیده‌تر امروزی نخواهند بود.

سرویس امنیت شبکه GlobalProtect شبکه‌های پالو آلتو[1] برای کاربران نهایی، به سازمان‌ها این امکان را می‌دهد تا Mobile workforce را با تعمیم و ایجاد نسل آیندهٔ زیرساخت‌های امنیتی، به کلیه کاربران، فارغ از موقعیت جغرافیایی آنها، محافظت نماید. این سیستم، با استفاده از قابلیت‌های زیرساخت‌ها به منظور درک کاربردهای برنامه، تخصیص ترافیک به کاربران و ابزارها، و اعمال سیاست‌های امنیتی به فن‌آوری‌های نسل آینده، ترافیک و داده‌های منتقل شده را حفاظت می کند.

تمدید محافظت زیرساخت‌ها به صورت خارجی

GlobalProtect، با بررسی تمامی اطلاعات منتقل شده، با استفاده از فایروال های جدید که در درگاه‌های اینترنت مورد استفاده قرار گرفته‌اند، Mobile workforce را چه در محیط پیرامونی، چه در DMZ و چه در فضای ابری، مورد محافظت قرار می‌دهد. لپ تاپ‌ها، تلفن‌های هوشمند و تبلت‌هایی که به برنامه GlobalProtect مجهز هستند، به طور خودکار یک ارتباط SSL/IPsec VPN ایمن را با دیوار آتش نسل آینده ایجاد نموده و بهترین عملکرد ممکن را برای یک مکان بخصوص فراهم می-

[1] Palo Alto Networks GlobalProtect network security client

آورند که در نتیجه تمام ترافیک و مسیرهای انتقال داده، برنامه‌ها، پورت‌ها و پروتکل‌ها را به طور کامل برای سازمان روشن و مشخص خواهد نمود. سازمان، با حذف نقاط کور در مسیر ترافیک Mobile workforce ، چشم‌اندازی مشخص و با ثبات به تمامی برنامه‌ها و کاربردها خواهد داشت.

ایمن‌سازی داخلی شبکه

در شبکه های کامپیوترینیازی نیست تمامی کاربران به تمامی نقاط آن دسترسی داشته باشند. تیم‌های امنیتی در حال کار بر روی دسته‌بندی شبکه هستند تا شبکه‌های خود را به قسمت‌های مختلفی تقسیم نموده و کنترل‌های دقیق را برای دسترسی به منابع داخلی اعمال نمایند. GlobalProtect، سریعترین و دقیقترین شیوه شناسایی کاربران را فراهم آورده است تا این امکان را به سازمان‌ها بدهد که سیاست‌گذاری‌های دقیقی را به اجرا درآورند که بر اساس نیازهای تجاری، امکان دسترسی را فراهم آورده و یا دسترسی‌ها را محدود نماید. بعلاوه، GlobalProtect اطلاعاتی از میزبان فراهم خواهد آورد که معیارهای ابزار مرتبط با سیاست‌گذاری‌های امنیتی را مشخص خواهند نمود. این معیارها، به سازمان‌ها امکان می‌دهند تا گام‌هایی پیشگیرانه را به منظور ایمن سازی شبکه‌های داخلی خود اتخاذ نموده، کنترل‌های شبکه بدون اطمینان را به کار گیرند و سطح حوزه‌های مورد حمله را کاهش دهند.

سناریوها و مزایای استفاده کلیدی

دسترسی از راه دور به VPN

- دسترسی ایمن به کارکردهای تجاری داخلی و مبتنی بر فضای ابری را فراهم می‌آورد.

سیستم‌های پیشرفته جلوگیری از تهدیدها

- ترافیک اینترنت را ایمن سازی می‌کند.
- از رسیدن تهدیدها به هدف خود جلوگیری می‌کند.
- از سیستم‌های کامپیوتری و کاربران در مقابل فیشینگ و سرقت اعتبارات و گواهی‌ها محافظت می‌نماید.

فیلتر URLها

- سیاست‌هایی را برای کاربردهای قابل قبول اعمال می‌نماید.
- دسترسی به Domain مخرب و محتوای مربوط به بزرگسالان را فیلتر می‌نماید.
- جلوی استفاده از ابزارهای اجتناب و فرار را می‌گیرد.

دسترسی ایمن به برنامه‌های SaaS

- دسترسی به کاربردهای SaaS را کنترل کرده و سیاست‌هایی را در ارتباط با آنها اعمال می‌نماید و در عین حال، کاربردهای با منشا نامشخص و بدون ضمانت اجرایی را متوقف می‌نماید.

BYOD

- از استفاده از VPNهای در سطح برنامه، به منظور حفاظت از حریم خصوصی کاربران، پشتیبانی می‌نماید.
- دسترسی بی واسطه همکاران، شرکای تجاری و پیمانکاران را امکان پذیر می‌نماید.

تقویت دسته‌بندی شبکه داخلی

- امکان شناسایی قابل اطمینان کاربران را فراهم می‌آورد.
- اطلاعات میزبان را به منظور شفافیت و اعمال سیاست‌گذاری‌ها، به سرعت و با دقت در اختیار می‌گذارد.
- احراز هویت چند عامله پیشرفته را به منظور دسترسی به منابع حساس، به اجرا در می‌آورد.

آدرس: یوسف آباد- میدان جهاد- خیابان بیستون- خیابان فتحی شقاقی- پلاک ۹۳- طبقه دوم - واحد ۵
تلفن:۱-۸۸۳۵۳۴۰۰-۰۲۱
فکس: ۸۹۷۸۴۲۷۱

هنگامی که GlobalProtect به این شیوه مورد استفاده قرار گیرد، ورودی‌های شبکه داخلی، را می‌توان با حضور و یا بدون حضور یک مسیر VPN، پیکربندی نمود.

بازرسی ترافیک و اعمال سیاست‌گذاری‌های امنیتی

GlobalProtect این امکان را به تیم‌های امنیتی می‌دهد تا سیاست‌گذاری‌هایی را ایجاد نمایند که چه کاربر داخلی باشد و چه از خارج از شبکه مشغول به فعالیت باشد، به شکل هماهنگ اعمال می‌شوند. تیم‌های امنیتی می‌توانند تمامی قابلیت‌های پلتفورم برای مقابله با حملات سایبری را مورد استفاده قرار دهند، از آن جمله:

- **فناوری App-ID** – ترافیک برنامه را، فارغ از تعداد درگاه‌ها، مورد شناسایی قرار داده و به سازمان‌ها این امکان را می‌دهد تا سیاست‌هایی را به منظور مدیریت کاربرد برنامه بر اساس کاربران و ابزارها، بوجود آورند.
- **فناوری User-ID** – کاربران و عضویت‌های گروه را به منظور دستیابی به شفافیت بیشتر، و همچنین اعمال سیاست‌گذاری‌های امنیت شبکه مبتنی بر نقش، شناسایی می‌نماید.
- **رمزگشایی** – برنامه‌ها و کاربردهایی را که با ترافیک SSL/TLS/SSH رمزگذاری شده‌اند، مورد نظارت قرار داده و کنترل می‌نماید. جلوی تهدیدها از سوی ترافیک رمزگذاری شده را می‌گیرد.
- **سرویس تحلیل تهدیدهای مبتنی بر فضای ابری WildFire** – تجزیه و تحلیل محتوا را به صورت خودکار در می‌آورد تا بدافزار[2]های جدید، ناشناخته و به شدت مورد هدف را با توجه به رفتار آنها شناسایی نموده، و هوشمندی لازم در قبال تهدیدها ایجاد نماید تا آنها را در شرایطی تقریبا بلادرنگ متوقف نماید.
- **پیشگیری از تهدیدها برای IPS و آنتی‌ویروس‌ها** – سیستم پیشگیری از نفوذ، جلوی بهره‌برداری‌های مبتنی بر شبکه که برنامه‌ها و سیستم‌های عامل آسیب‌پذیر را هدف گرفته‌اند، حملات DoS و اسکن مدخل‌های ورودی و خروجی

[2] Malware

را خواهد گرفت. آنتی‌ویروس‌ها، با استفاده از یک موتور مبتنی بر جریان داده، جلوی دستیابی بدافزارها و جاسوس افزار[3]ها به کاربران نهایی را خواهند گرفت.

- **فیلتر URLها با استفاده از PAN-DB** – PAN-DB، URLها را بر اساس محتوای آنها در دامنه و سطح فایل و صفحه مورد نظر، دسته‌بندی نموده و به‌روزرسانی‌هایی را از WildFire دریافت می‌کند تا در هنگام تغییر محتوای وب، دسته-بندی‌های مربوطه نیز دستخوش تغییر شوند.
- **مسدودکردن فایل‌ها** – با استفاده از سیستم WildFire، جلوی انتقال فایل‌های ناخواسته و خطرناک را گرفته و در عین حال، فایل‌های مجاز را مورد موشکافی و دقت بیشتر قرار خواهد داد.
- **فیلتر داده‌ها** – این امکان را به مدیران می‌دهد تا سیاستگذاری‌هایی را به اجرا در آورند که می‌توانند برای جلوگیری از جابه‌جایی غیرمجاز داده‌ها، از جمله انتقال اطلاعات مشتریان و یا سایر اطلاعات محرمانه، مورد استفاده قرار گیرند.

شرایط سفارشی‌سازی شده میزبان (برای مثال، شناسایی کاربران و ابزارها)

تایید هویت کاربر

GlobalProtect، تمامی روش‌های تایید هویت موجود در PAN-OS، از جمله Kerberos، RADIUS، LDAP، SAML2.0، گواهینامه‌های مشتریان و یک پایگاه داده کاربران محلی را مورد پشتیبانی قرار می‌دهد. پس از آنکه GlobalProtect، هویت کاربر را احراز نمود، بلافاصله دیوار آتش نسل آینده را با استفاده از نگاشت شناسه آدرس کاربر به IP [4]به شماره شناسه کاربر[5]، برای آن کاربر فراهم خواهد آورد.

[3] Spyware
[4] User-to-IP-address
[5] User-ID

گزینه‌های احراز هویت قوی

GlobalProtect، طیفی از روش‌های احراز هویت چند عامله طرف سوم، شامل کلیدهای رمز یکبار مصرف[6]، گواهینامه‌ها و کارت‌های هوشمند، را از طریق تلفیق RADIUS، مورد پشتیبانی قرار می‌دهد.

این روش‌ها و گزینه‌های مختلف، به سازمان کمک می‌کنند تا تایید هویت به منظور دسترسی به مرکز داده داخلی و یا برنامه‌های SaaS را بیش از پیش تقویت نماید.

GlobalProtect، از گزینه‌هایی بهره می‌گیرد که می‌توانند کاربرد و اجرای سیستم‌های احراز هویت قوی را، حتی ساده‌تر از گذشته نمایند:

- **احراز هویت مبتنی بر Cookie**: ممکن است یک سازمان بخواهد پس از احراز هویت، از یک کوکی رمزنگاری شده[7] برای دسترسی‌های آتی به یک پورتال یا یک مدخل ورودی استفاده نماید.
- **پشتیبانی از پروتکل ثبت گواهی‌های ساده‌سازی شده[8]**: GlobalProtect می‌توانند تعامل با یک PKI تجاری، به منظور مدیریت، صدور و توزیع گواهی برای مشتریان GlobalProtect را به فرایندی خودکار تبدیل نماید.

پروفایل اطلاعات میزبان

GlobalProtect، نقاط نهایی مسیر را مورد بررسی قرار می‌دهد تا فهرست کاملی از نحوه پیکربندی و ایجاد یک پروفایل اطلاعات میزبان تهیه کند که با دیوار آتش نسل جدید به اشتراک گذاشته خواهد شد. دیوار آتش نسل جدید، از پروفایل اطلاعات میزبان استفاده می‌کند تا سیاست‌گذاری‌هایی را برای برنامه‌ها اعمال نماید که امکان دسترسی را تنها هنگامی فراهم می‌آورند که نقطه نهایی به خوبی پیکربندی و ایمن‌سازی شده باشد. این اصول، به ایجاد هماهنگی با سیاست‌گذاری‌هایی کمک خواهند نمود که میزان دسترسی یک کاربر بخصوص به یک ابزار بخصوص را مشخص خواهند کرد.

[6] One-time password tokens
[7] Encrypted cookie
[8] Simplified Certificate Enrollment Protocol Support

سیاست‌گذاری‌های پروفایل اطلاعات میزبان را می‌توان بر اساس چندین ویژگی مشخص بنا نهاد، از جمله:

- سیستم عامل و سطح بسته کاربردی
- نسخه و وضعیت برنامه ضد بدافزار میزبان
- نسخه و وضعیت دیوار آتش میزبان
- ترکیبات و پیکربندی‌های رمزگذاری‌های دیسک
- ساختار و پیکربندی پشتیبان‌گیری از داده‌ها
- شرایط سفارشی میزبان (برای مثال، مدخل‌های رجیستری، نرم‌افزار در حال اجرا)

دسترسی کنترل به برنامه‌ها و داده‌ها

تیم‌های امنیتی می‌توانند سیاست‌گذاری‌ها را بر اساس کاربرد، کاربر، محتوا و اطلاعات میزبان ایجاد نمایند تا کنترلی جزء به جزء بر دسترسی افراد به یک برنامه بخصوص داشته باشند. این سیاست‌گذاری‌ها می‌توانند به کاربران یا گروه‌های بخصوصی مرتبط باشند که در یک فهرست مشخص تعریف شده‌اند تا تضمین نمایند که سازمان‌ها، سطوح مناسبی از دسترسی را بر اساس نیازهای تجاری فراهم می‌آورند. تیم امنیتی همچنین می‌تواند سیاست‌های بیشتری را به منظور احراز هویت چند عاملهٔ پیشرفته‌تر به اجرا در آورد تا مدارک بیشتری برای احراز هویت کاربران در اختیار داشته باشد و سپس منابع و برنامه‌های ویژه و حساس را در اختیار آنها قرار دهد.

BYOD ایمن و توانمندسازی شده

تاثیرات BYOD در حال تغییر تعداد موارد جایگزین مورد استفاده‌ای هستند که تیم‌های امنیتی باید مورد پشتیبانی قرار دهند. ضروری است که دسترسی به برنامه‌ها را، با استفاده از بازه وسیعی از ابزارهای الکترونیک قابل حمل، برای طیف وسیعتری از کارمندان و کارگزارن، فراهم آوریم.

هماهنگی و تلفیق با راه‌حل‌های مدیریت ابزارهای قابل حمل، همچون AirWatch، و MobileIron، به سازمان‌ها در پیاده-سازی GlobalProtect و همچنین فراهم آوردن معیارهای امنیتی بیشتر از طریق تبادل اطلاعات و ترکیب‌بندی‌های میزبان، کمک می‌نماید. استفاده در کنار GlobalProtect، موجب می‌شود که سازمان بتواند شفافیت را حفظ کرده و همچنین سیاستگذاری‌های امنیتی را بر مبنایی برنامه محور اعمال کرده و در عین حال تفکیک داده‌ها از فعالیت‌های شخصی را حفظ نماید تا به انتظارات کاربر از حریم خصوصی خود در سناریوهای BYOD، احترام بگذارد.

GlobalProtect از SSL VPN بدون سرویس گیرنده حمایت می‌نماید تا دسترسی به برنامه‌ها در مرکز داده و فضای ابری، از سوی ابزارهای مدیریت نشده را به شیوه‌ای امن امکان پذیر نماید. این رویکرد، با ایجاد دسترسی به برنامه‌های بخصوصی از طریق یک وب سایت واسط، بدون نیاز به نصب یک سرویس گیرنده یا ایجاد یک مسیر تونل کامل از سوی کاربر، راحتی و امنیت را فراهم می‌آورد.

مسائل معماری

معماری انعطاف‌پذیر GlobalProtect، قابلیت‌های بسیار زیادی را ایجاد می‌نماید که به سازمان‌ها در حل یک آرایه از چالش-های امنیتی کمک خواهند نمود. در پایه‌ای ترین سطح، سازمان‌ها می‌توانند از GlobalProtect، به عنوان جایگزینی برای درگاه متعارف VPN استفاده نمایند و پیچیدگی‌ها و دردسرهای مدیریت یک درگاه VPN مجزای طرف سوم را از میان بردارند.

گزینه‌های موجود برای ارتباطات دستی و انتخاب درگاه‌ها، این امکان را به سازمان‌ها خواهند داد تا ترکیب بندی خود را به نفعی شکل دهند که الزامات تجاری را مطابق با نیازهایشان، مورد پشتیبانی و حمایت قرار دهد.

GlobalProtect، در یک اجرای جامع‌تر از ایمن‌سازی ترافیک اطلاعات، می‌تواند همراه با یک ارتباط VPN همواره روشن به یک تونل کامل پیاده‌سازی شود تا تضمین نماییم که محافظت همواره در جریان بوده و تجربیات کاربر را به طور کامل آشکار نماید.

گذرگاه‌های مبتنی بر فضای ابری

نیروهای کاری از یک موقعیت به موقعیتی دیگر تغییر مکان داده و تغییراتی را در بار ترافیک اطلاعات ایجاد می‌نمایند. این مسئله، بویژه هنگامی صحت خواهد داشت که نحوه تحولات شرکت‌ها را مورد توجه قرار دهیم، چه این تحولات موقت باشند (همچون یک بلای طبیعی در یک ناحیه جغرافیایی) و چه یک تحول دائم و ابدی باشند (همچون ورود به بازارهای جدید).

خدمات فضای ابری GlobalProtect، با استفاده از سیاست‌گذاری‌های امنیتی شما، گزینه‌ای همراه با مدیریت مشترک را برای اجرای پوشش در مکان‌های مورد نیاز سازمان‌ها، ایجاد می‌نماید. این گزینه را می‌توان در کنار دیوارهای آتش موجود مورد استفاده قرار داد تا معماری شبکه شما را با شرایط در حال تغییر وفق دهد.

خدمات ابری GlobalProtect، از مقایس سازی خودکار پشتیبانی می‌نماید که به طور دینامیک، دیوارهای آتش جدیدی را بر اساس میزان بار و تقاضا در یک ناحیه بخصوص، به آن ناحیه تخصیص می‌دهد.

نتیجه‌گیری

محافظت‌های فراهم شده توسط پلتفرم امنیتی نسل جدید شبکه‌های پالو آلتو، نقشی کلیدی در جلوگیری از نفوذهای امنیتی ایفا می‌کنند. با استفاده از GlobalProtect می‌توانید محافظت پلتفرم را در تمام مکان‌ها به کاربران مختلف، تعمیم دهید. با استفاده از GlobalProtect، سازمان‌ها می‌توانند سیاست‌گذاری‌های امنیتی را به طور مناسب و هماهنگ به اجرا در آورند تا حتی هنگامی که کاربران ساختمان را ترک می‌کنند، محافظت از آنها در مقابل حملات سایبری، به قوت خود، پابرجا باقی بماند.

آدرس: یوسف آباد- میدان جهاد- خیابان بیستون- خیابان فتحی شقاقی- پلاک ۹۳- طبقه دوم - واحد ۵
تلفن:۱-۸۸۳۵۳۴۰۰-۰۲۱
فکس: ۸۹۷۸۴۲۷۱