باسمه تعالی

شبکه توزیع محتوا (CDN) و سامانه امنیت ابری برای سایت های دولتی

تحت نظارت سازمان فناوری اطلاعات و ارتباطات ایران

بر پایه فناوری نوین شرکت دانش بنیان «نویان ابر آروان»

مرداد ۱۳۹۶

چکیده طرح

حملات روز افزون سایبری همواره وب سایت‌ها و سامانه های حاضر در شبکه اینترنت را تهدید می‌کنند. مقابله با این تهدیدات نیازمند دانش، تجربه و تجهیزات متنوعی است. از جمله حملات رایج حملات DDOS است که در برخی انواع آن تنها راهکار عملی مقابله با آن افزایش ظرفیت پاسخگویی سرویس دهنده به حجم بالای درخواست‌ها است. مرکز ماهر بمنظور کمک به وبسایت‌های دولتی در پاسخگویی به حجم درخواست‌ها و مراجعات بالا و همچنین حفاظت از آن‌ها در برابر حملات رایج با همکاری ابر آروان، اقدام به ارایه خدمات حفاظت سامانه‌های تحت وب نموده است.

ابر آروان به عنوان اولین شبکه توزیع محتوای عمومی (CDN)، شتاب دهنده وب و سامانه امنیت ابری ایرانی تلاش دارد تا با ارائه خدمات مبتنی بر شبکه توزیع محتوا (CDN) کیفیت خدمات آنلاین را ارتقاء دهد.

استفاده از شبکه توزیع محتوا و سامانه امنیت ابری آروان به اختصار مزایای زیر را خواهد داشت:

۱ – توزیع محتوای آنلاین مورد نظر در تمام نقاط مهم دنیا و سراسر ایران و ارائه محتوا به کاربران از نزدیک‌ترین نقطه جغرافیایی
۲ – افزایش سرعت بارگذاری محتوای آنلاین
۳ – ارائه راهکار DNS ابری و حل مشکل تفسیر نام در داخل و خارج از کشور
۴ – محافظت از محتوای اینترنتی در برابر حملات سایبری از جمله حملات منع سرویس توزیع شده DDoS
۵ – فشرده‌سازی و بهینه‌سازی محتوای آنلاین
۶ – ارائه پشتیبانی شبانه‌روزی
۷ – دسترسی همیشگی سایت خدمات گیرنده حتی در صورتی که هاست اصلی از سرویس دهی خارج شده باشد

نیازمندی‌های اجرا

برای قرارگرفتن وب‌سایت تحت حفاظت ابری نیاز به هیچ تغییری در ساختار وب‌سرور و نرم‌افزار وب نیست. تنها لازم است کارگزار نام دامنه (DNS Server) وب‌سایت به سرور DNS توزیع شده آروان انتقال یابد. پس از آن از طریق کنسول وب سامانه آروان تنظیمات جهت فعال سازی حفاظت ابری انجام می‌پذیرد.

مراحل اجرا

مراحل قرارگیری وبسایت تحت حفاظت ابری مرکز ماهر عبارتند از:

۱. ارسال درخواست استفاده از خدمت و فهرست وبسایت‌ها به همراه معرفی نماینده سازمان درخواست کننده
۲. ایجاد حساب کاربری در فضای ابری برای نماینده سازمان
۳. ایجاد رکوردهای DNS دامنه بر روی سرویس ابری (در صورت تعدد رکوردهای دامنه امکان انتقال یکباره آنها از طریق zone-transfer و یا ارئه zone file وجود دارد)
۴. سنجش صحت تنظیمات و عملکرد DNS و شبکه توزیع محتوا
۵. تنظیم کارگزار نام دامنه (برای دامنه‌های ir. در nic.ir) و هدایت آن بسوی کارگزارهای ابری نام دامنه آروان
۶. فعال سازی ابر

۷. فعال سازی قابلیت‌های امنیتی و تنظیم WAF ابری

از میان مراحل فوق، درخواست کننده خدمت حفاظت ابری تنها لازم است موارد ۱ و ۵ را انجام دهد. سایر موارد توسط کارشناسان آروان انجام می پذیرد.

شبکه توزیع محتوا

ابر آروان به عنوان یک تکنولوژی ایرانی همگام با پیشروترین CDN های روز جهان، امکانات مختلف توزیع محتوا، خدمات آنلاین امنیتی و شتاب‌دهی وب را برای شما به ارمغان می‌آورد. در این جا به اختصار به ویژگی‌های اصلی ابر آروان اشاره می‌کنیم:

توزیع جهانی سرورها

مهم‌ترین وظیفه یک شبکه توزیع محتوا یا همان CDN، تحویل محتوای آنلاین از نزدیک ترین نقطه جغرافیایی به دست کاربران است. این امر کمک می‌کند که وب سایت و یا هر گونه محتوای آنلاین با سرعت و کیفیت بسیار بالاتری بارگذاری شده و موجب ارتقای تجربه کاربری شود.

ابر آروان در تمام نقاط مهم ایران و جهان پاپ‌سایت‌های خود را مستقر کرده است تا بتواند با بالاترین کیفیت ممکن هرگونه درخواست احتمالی را پاسخ دهد. چندین نقطه در آمریکا، اروپا، آسیای شرقی و همچنین حضور در استانهای مختلف کشور و قرارگیری در دیتاسنتر بزرگترین سرویس دهندگان اینترنتی ایران باعث شده است ابر آروان تجربه مرور وب را به شکل چشم‌گیری بهبود دهد.

افزایش بازدهی وب

یکی از وظایف مهم شبکه‌های توزیع محتوا افزایش سرعت بارگذاری محتوا است. مهم‌ترین عامل این افزایش سرعت بارگذاری محتوا از نزدیک ترین نقطه جغرافیایی است. در واقع کاربران در هر منطقه جغرافیایی که باشند با توجه به تنظیمات caching آن دسته از محتوا را که قابل نگهداشتن باشد از سرورهای لبه‌ی همان منطقه جغرافیایی دریافت خواهند کرد.

همچنین به کمک پروتکل HTTP نسخه ۲، محتوا از طریق ابر آروان با تعداد درخواست کمتر و با سرعت بسیار بیشتری بارگذاری خواهد شد، به این طریق می‌توان انتظار افزایش سرعت ۲۰۰ درصدی نسبت به پروتکل نسخه ۱,۱ داشت.

از دیگر نکات مهمی که باعث افزایش سرعت و کاهش حجم صفحات خواهد شد فشرده‌سازی محتوا، بازنویسی صفحات HTML, CSS و جاوا اسکریپت و همچنین تبدیل و بهبود فرمت تصاویر است که می‌تواند تا چندین برابر سرعت بارگزاری محتوا را افزایش دهد.

محافظت در برابر حملات

ابر آروان می‌تواند از وب‌سایت‌ها و محتوای آنلاین در برابر انواع حملات سایبری از جمله حملات منع سرویس توزیع شده (DDoS) حتی در انواع پیشرفته آن محافظت کند. سامانه امنیت ابری آروان به شما اجازه می‌دهد تا به راحتی و در یک فضای ابری قوانین امنیتی را بدون نیاز به تجهیزات فیزیکی تدوین نمایید.

مهم‌ترین امکانات قابل ارایه در سیستم امنیت ابری ابر آروان به شرح زیر است:

- سامانه جلوگیری از حملات DDoS
- دیواره آتش ابری (Firewall)
- دیواره آتش وب (WAF)
- محدودیت درخواست‌ها
- پشتیبانی از SSL و HSTS

جلوگیری از حملات DDoS پیشرفته

حملات denial-of-service یا منع سرویس (DOS) و منع سرویس توزیع شده (DDOS) به مجموعه حملاتی گفته می‌شود که به کمک آن هکرها تلاش می‌کنند یک سرویس خاص و یا یک سیستم خاص را از دسترس خارج کرده و اتصال کاربران به آن را کاملا مختل و یا با مشکل مواجه سازند.

مقابله با حملات منع سرویس توزیع شده یکی از پیچیده‌ترین مشکلات همیشگی سرویس‌دهندگان بزرگ اینترنتی است، اما روش‌های پیچیده‌ی نوینی وجود دارد که از بیشتر حملات DDOS جلوگیری می‌کند و ابر آروان به کمک این روش‌ها، از شما در برابر این حملات محافظت خواهد کرد.

حملات لایه ۳ و ٤

جریان سیل‌آسای سین (SYN Flood)

ایجاد یک اتصال پایدار در پروتکل TCP به کمک یک گفتگوی ۳ قسمتی آغاز می‌شود. در این نوع حمله نفوذگر تعداد بیشماری بسته شروع ارتباط با آدرس فرستنده جعلی تولید کرده و به قربانی ارسال می‌کند. قربانی با فرستادن پاسخ تلاش می‌کند که این ارتباط را ایجاد کند، اما از آنجا که آدرس فرستنده بسته‌ها جعلی بوده است ارتباط نیمه باز باقی می‌ماند. در این صورت ۲ اتفاق مهم می‌افتد، یکی اینکه ممکن است تعداد connection های مجاز سرور به پایان برسد و دیگر اینکه تمام یا اکثر منابع سرور صرف این اتصالات جعلی شده و امکان سرویس‌دهی عادی سلب شود.

جریان سیل‌آسای UDP

در این روش نفوذگر اقدام به ارسال بیش از حد بسته های UDP به پورت های مختلف و تصادفی می‌کند. سیستم عامل ابتدا تلاش می‌کند که از باز بودن پورت مورد نظر اطمینان حاصل کند، پس از این کار و اطمینان از اینکه هیچ سرویسی بر روی این پورت به حالت شنود قرار نگرفته، بسته‌های ICMP از نوع Destination Unreachable ارسال می‌کند که مقدار زیادی از منابع سرور را به خود اشغال می‌کند.

حملات انعکاسی و انعکاسی افزاینده (Reflected Attack and Amplification)

در این نوع حملات که یکی از خطرناک‌ترین حملات منع سرویس است، نفوذگر تعداد زیادی بسته جعلی با IP قربانی را به سرورها و کامپیوترهای مختلف ارسال می‌کند، سپس تمام این کامپیوترها پاسخ خود را به آدرس قربانی ارسال می‌کنند. به این ترتیب به تعداد بیشماری سیستم شروع به ارسال بسته های اطلاعاتی کرده و در نتیجه پهنای باند و سایر منابع قربانی مصرف شده و سرویس‌دهی مختل می‌شود.

در نوع پیشرفته‌تر که به amplification مرسوم است، هکر از درخواست هایی استفاده می‌کنند که پاسخ بزرگ‌تری در پی داشته باشد. این پاسخ ها در نوع NTP amplification تا ۵۵۶ برابر و در نوع DNS amplification تا ۱۷۹ برابر بسته ارسالی خواهند بود. به طور مثال یک هکر می‌تواند با صرف ۱ گیگ پهنای باند ۵۵۶ گیگابایت اطلاعات را به سمت قربانی شناور کند.

مقابله با این حملات

در حالت عادی سرور شما بدون هیچ محافظی (و یا تنها با firewall های عادی) در حال سرویس‌دهی به کاربران است. هر نوع حمله منع سرویس می‌تواند به طور کلی سیستم شما را با اختلال کامل مواجه کند.

اما با سرویس امنیت ابری آروان تمام اتصالات ابتدا با توجه به موقعیت جغرافیایی از فیلتر ابر آروان می‌گذرد. در این مرحله کلیه حملات توسط ابر آروان جذب شده، رقیق شده و از ترافیک عادی تفکیک می‌شود، سپس تنها ترافیک عادی به سمت سرور شما ارسال می‌گردد. و البته در هر صورت و در هر شدتی حملات مناطق مختلف برروی سایر مناطق بی اثر خواهند بود. به طور مثال بات‌های مهاجم از چین هیچ تاثیری در سرویس دریافتی کاربران داخل ایران نخواهد داشت.

حملات لایه ۷

شاید پیچیده‌ترین نوع حملات DDOS از نوع حملات لایه ۷ باشد. زمانی که بیش از چند صد هزار سیستم آلوده متشکل از کامپیوتر خانگی، سرورهای مختلف و یا حتی مودم های اینترنت خانگی ای که درست تنظیم نشده باشند، به سمت یک سایت یک درخواست قانونی ارسال کنند. در این حالت اکثر روش های ذکر شده در بالا ناکارآمد بوده و سرور یا وبسایت مورد هدف قرارگرفته، به راحتی از دسترس خارج خواهد شد. در تنظیمات مربوط به مقابله به حملات منع سرویس پنل کاربری ابر آروان سه سطح در جهت مقابله با این امر در نظر گرفته شده است:

عمومی:

در این حالت کاربران متوجه هیچ تغییری در سایت شما نخواهند شد، اما از ورود بسیاری از بات ها که توانایی تنظیم cookie و استفاده از آن در سایر اتصالات را نداشته باشند جلوگیری خواهد شد.

حرفه‌ای:

اگر بات‌های حمله‌کننده به سایت شما از نوع هوشمندتری باشند جهت مقابله با آن‌ها می‌توانید از این سطح از مقابله استفاده کنید. به کمک این روش حتی از بات‌هایی که تلاش می‌کنند رفتار انسان را شبیه‌سازی کنند به کمک یک نوع عملیات رمزنگاری جلوگیری می‌شود. کاربران شما اولین اتصال خود به سایت شما برای چند لحظه صفحه‌ای را مشاهده می‌کنند که تلاش می‌کند غیر ربات بودن آن‌ها را تشخیص دهد.

پیشرفته:

فرض کنیم که بات‌های طراحی شده جهت حمله به سایت شما قدرتمندتر از معمول بودند. در این حالت با تنظیم حالت مقابله برروی حالت پیشرفته به کاربر یک کد امنیتی یا captcha نمایش داده می‌شود و از او خواسته می‌شود چند تصویر را به درستی تشخیص دهد. از آنجایی که ترافیک نمایش این صفحات و پردازش آن‌ها خارج از سرور شما صورت می‌گیرد، می‌توان این روش را از پیشرفته‌ترین و کارآمدترین روش‌های مقابه با حملات منع سرویس لایه ۷ محسوب کرد.

حملات منسوخ شده

گاهی از حملاتی چون Nuke، Ping of Death، Teardrop، SMURF و... به عنوان سایر روش‌های منع سرویس یاد می‌شود. این حملات که غالبا منسوخ شده و یا تاثیرگذاری خود را از دست داده، برروی تجهیزات و زیرساخت‌های قدیمی کاربرد دارد و به راحتی قابل جلوگیری است. ابر آروان کلیه این حملات را نیز بررسی کرده و تدابیر لازم را در جهت مقابله با آن‌ها در نظر گرفته است.

حملات برپایه Exploit

گاهی حملات منع سرویس به کمک اجرای یک کد مخرب (Exploit) که بر پایه یک آسیب‌پذیری بالقوه به وجود آمده است صورت می‌گیرد. به طور مثال نفوذگر به کمک یک آسیب پذیری قدیمی کشف شده و یا یک آسیب پذیری 0-day برروی یک وب سرور (مثلا IIS و یا Apache) کدی را برروی وب سرور اجرا می‌کند و باعث از کار افتادن آن سرویس و یا سرور می‌شود.

ولی ابر آروان در لایه بررسی امنیتی کلیه آسیب‌پذیری‌های کشف شده را شناسایی می‌کند و در مورد آسیب‌پذیری‌های نامکشوف نیز تلاش می‌کند برپایه رفتار شناسی از انجام حمله موفق جلوگیری کند.

سایر امکانات

معماری Anycast

یکی از چالش‌های مهم در یک شبکه توزیع محتوا تشخیص دقیق موقعیت جغرافیایی کاربر است. اگرچه روش‌های سنتی تشخیص موقعیت جغرافیایی به کمک DNS سرورها در سال‌های اخیر رشد چشم‌گیری داشته‌اند، اما همچنان از دقت کافی برخوردار نبوده و پیاده‌سازی یک ساختار پایدار یکپارچه را با مشکلاتی همراه می‌سازند.
ابر آروان جزو معدود شبکه‌های توزیع محتوا در جهان است که نه تنها در لایه تفسیر نام (DNS) بله حتی در لایه ارائه سرویس نیز به صورت یکپارچه بر پایه مسیریابی anycast عمل می‌کند. به کمک این روش آدرس‌های IP ابر آروان به صورت واحد در نقاط مختلف و سراسر جهان تبلیغ شده و هر کاربر حتی در اولین اتصال به نزدیک‌ترین سرور لبه متصل شده و از آن سرویس خود را دریافت می‌کند.

سرویس DNS ابری

ساختار BGP anycast ابر آروان باعث می‌شود آدرس‌های شما پس از انتقال به ابر آروان از نقاط مختلف دنیا به صورت یکپارچه و با کمترین تاخیر و با تحمل حملات DDoS با ظرفیت 800 Gbps سرویس‌دهی نماید.

همچنین یک پنل ساده و کارآمد در اختیار شما قرار می‌گیرد تا به کمک آن به تعداد نا محدودی رکورد DNS تعریف کرده و مشخص کنید کدام یک می‌بایست از داخل ابر آروان عبور کرده و کدام یک مستقیما به آدرسی که شما معرفی می‌کنید منتقل شوند.

پشتیبانی از SSL

در ابر آروان این امکان وجود دارد تا Certificate خود را بارگذاری کنید، و یا این درخواست را داشته باشید تا آروان برای شما Certificate معتبری تهیه کرده و امکان فعال‌سازی پروتکل HTTPS را مهیا کند. به این طریق به راحتی و تنها با چند کلیک امکان استفاده از این پروتکل امن برای شما فراهم می‌شود.

پشتیبانی از پروتکل HSTS

استفاده از روش‌های عادی انتقال درخواست‌های HTTP به HTTPS می‌تواند مخاطرات امنیتی بسیاری را به همراه داشته باشد. Strict Transport Security و یا به اختصار HSTS مجموعه سیاست‌های امنیتی است که به صورت امن به وب‌سایت‌ها اجازه می‌دهد تنها از طریق پروتکل HTTPS قابل دسترس باشند و یا به کاربران اجازه می‌دهد تنها با سایت‌هایی با پروتکل امن ارتباط برقرار بکنند.

پشتیبانی از پروتکل HTTP2

HTTP2 آخرین نسخه از پروتکل HTTP است. این پروتکل پس از پروتکل SPDY و برای سرعت بخشیدن و رفع نواقص نسخه ۱,۱ این پروتکل ایجاد گردید. HTTP2 تلاش می‌کند تا به کمک فشرده‌سازی، یکپارچه‌سازی و اولویت‌دهی کمترین تاخیر (latency) در بارگذاری صفحات را به وجود آورد.

قابلیت «دسترسی همیشگی»

در حالت عادی کوچک ترین اختلال در یک وب سایت یا وب سرور باعث خواهد شد به طور کلی وب سایت از دسترس خارج شود. قابلیت «دسترسی همیشگی» هنگامی که سرور به هر دلیلی از دسترس خارج شود، آخرین نسخه از محتوای وب سایت را به کاربران نمایش می‌دهد.

ساختار GSLB ابر آروان

یکی از شاخصه‌های بررسی شبکه‌های توزیع محتوا میزان پایداری این سرویس‌ها از نقاط مختلف است. معماری ابر آروان بر پایه تکنولوژی Global Server Load Balancing یا GSLB است. به کمک این تکنولوژی، ترافیک در مکان‌های جغرافیایی مختلف و بر روی سرورهای مختلفی پخش و توزیع خواهد شد، اما در هر لحظه وضعیت کیفی هر نقطه رصد شده و نسبت به اختلالات احتمالی آن واکنش نشان داده می‌شود.

از مزایای بسیار مهم این تکنولوژی قابلیت انعطاف‌پذیری و هوشمندی بسیار بالا در هنگام مواجه شدن با مشکلات گوناگون است. مثلا هنگامی که یک سرور خاص با اختلال مواجه شود، این تکنولوژی به‌طور کاملا خودکار ترافیک را به نزدیک‌ترین سرور بعدی هدایت می‌کند. در تمامی این فرآیند، کاربر هیچ تغییری در نحوه دریافت سرویس احساس نمی‌کند و در چند ثانیه کلیه این فرآیند به‌طور کاملا اتوماتیک اتفاق می‌افتد. در این تکنولوژی همواره وضعیت سرورها و node ها در حال بررسی است و در صورت از دسترس خارج شدن یک سرور خاص، جریان ترافیک به سمت سرورهای دیگر هدایت شده و آن سرور از مدار خارج می‌شود.

توزیع بار

بسیاری از وب‌سایت‌های بزرگ از بیش از یک سرور برای میزبانی محتوای خود استفاده می‌کنند. یکی از چالش‌های مطرح در این موارد توزیع بار به صورت هوشمند بین این سرورهاست. به خصوص در مواردی که این سرورها برای دسترسی بهتر در بیش از یک نقطه (دیتاسنتر) قرار گرفته باشد نیاز به توزیع بار جند نقطه‌ای وجود دارد (Multi-Site Load Balancing). ابر آروان نه تنها بار ترافیکی را در لایه اول (ارتباط کاربران با سرورهای لبه‌ی ابر آروان) به صورت هوشمند توزیع می‌کند، بلکه می‌تواند درخواست‌های سرورهای لبه‌ی ابر آروان به سرورهای اصلی (میزبان‌های محتوا) را نیز به صورت متوازن توزیع می‌کند. چنانچه وبسایتی از بیش یک سرور یا یک دیتاسنتر جهت میزبانی وب خود استفاده می‌کند، با مهاجرت به ابر آروان نیز همچنان می‌تواند آن ساختار را جهت کاهش ضریب خطا، برای خود حفظ کند.

در ابر آروان این امکان وجود دارد که بیش از یک گروه سرور تعریف و در هر گروه به هر تعداد سرور متفاوت با وزن متفاوت تعریف و مدیریت گردد. همچنین می‌توان تعداد خطاهای مورد نظر جهت از رده خارج شدن یک سرور را مشخص کرد، تا بلافاصله جهت ارائه سرویس از سایر سرورهای در دسترس استفاده شود.

روش توزیع بار نیز قابل تنظیم خواهد بود، توزیع بار نوبتی، توزیع بار برپایه درخواست‌دهنده، توزیع بار بر پایه کمترین اتصال به یک سرور و همچنین توزیع بار بر پایه موقعیت جغرافیایی. در مورد آخر به طور مثال قابل تنظیم خواهد بود که کلیه سرورهای لبه داخل ایران ابر آروان برای دریافت محتوا به یک سرور مشخص متصل و تمامی سرورهای لبه خارج از کشور به سرور دیگری متصل شوند، و در صورت از دسترس خارج بودن هر کدام از این سرورها، سرور دیگر جایگزین شود.

گزارشات

در پنل اصلی ابر آروان گزارشات متنوعی در اختیار مدیران وب قرار خواهد گرفت. به این طریق میزان ترافیک در بازه‌های زمانی مختلف، تعداد درخواست‌ها، صفحات و محتوای پر بازدید، سرعت دریافت محتوا و... مورد ارزیابی قرار خواهند گرفت. گزارشات در ابر آروان به سه دسته مختلف تقسیم می‌شود:

- گزارشات تحلیلی از حملات امنیتی
- گزارشات تحلیلی از افزایش بازدهی
- گزارشات تحلیلی از کاربران سایت و آمار بازدید

پشتیبانی ۲۴ ساعته

یکی از مهمترین وظایف تیم ابر آروان ارائه پشتیبانی شبانه‌روزی به مشتریان سازمانی است. پشتیبان های مشتریان سازمانی در طول ساعات کاری از طریق تلفن شرکت، تیکت و شبکه‌ی اجتماعی مورد نظر این شرکت در دسترس بوده و در ساعات غیر کاری از طریق تلفن همراه قابل دسترس هستند.

علاوه بر پشتیبان‌های تمام وقت، ارتباط با هسته اصلی ابر آروان برقرار بوده و در صورتی که مشکل پیش‌بینی نشده‌ای رخ دهد به این واحد ارجاع داده شده تا به سرعت مرتفع گردد.