تسهیل دورکاری و راهکار حفظ امنیت شبکه و دسترسی امن از بیرون سازمان

اهمیت راهکار حفظ امنیت شبکه و دسترسی امن از بیرون سازمان در شرایط شیوع بیماری کرونا و نیاز به دورکاری برکسی پوشیده نیست. راهکارهای امن اتصال به شبکه و بستر نرم‌افزارهای دیدگاه ارزش مهمی است که چارگون برای صدها سازمان مشتری فراهم کرده تا در شرایط جدید با کمترین دغدغه دورکاری را برای کارکنان خود ایجاد کنند.

مدیران سازمان‌ها در شرایط **شیوع بیماری کرونا** دغدغه زیادی برای تسهیل **دورکاری** دارند و انتخاب **راهکار حفظ امنیت شبکه** و ایجاد بستر مناسب **ن**داخلی سازمان دارند،چرا که وقتی اطمینان از **امنیت شبکه و نرم افزار** نقش مهمی در **تسهیل دورکاری** دارد.

مجموعه نرم‌فزاری دیدگاه از قدیم به عنوان نرم‌افزار سازمانی یکپارچه با استفاده از تکنولوژی‌های تحت وب با این هدف گسترش و تولید شده بود که حداکثر ضریب نفود و سهولت پرسنل برای دسترسی به نرم‌افزار را پوشش دهد. ضریب اهمیت دیدگاه در سازمان و تحت وب بودن این سامانه باعث شده است که متولیان امر و صاحبان کسب و کار «دیدگاه» را به عنوان یکی از سهل الوصول و اصلی‌ترین ابزار دور کاری در نظر بگیرند.

مجموعه زیادی از **مشتریان چارگون** از قبل با رعایت تدابیر امنیتی دسترسی لازم برای اتصال به «**دیدگاه**» از خارج از سازمان را فراهم کرده‌اند، البته بعضی از مشتریان هم با صلاحدید و رعایت تدابیر لازم خود اقدام به این امر نموده‌اند. به همین دلیل به جرات می‌شود گفت که «**دیدگاه**» انعطاف زیادی برای ایجاد دسترسی به روش‌های مختلف را داراست و عملا راهبرهای شبکه برای تصمیم‌گیری برای نحوه و معماری پیاده‌سازی انتخاب‌های گوناگونی دارند.

این روزها با توجه به شرایط موجود در دنیا درخواست‌های زیاد در جهت مشاوره و کمک برای ایجاد این دسترسی برای خارج از سازمان به تیم فنی چارگون داده شده است به همین جهت تصمیم گرفتیم روش‌ها و ایده‌هایی که می‌شود برای این امر استفاده کرد تا جایی که امکان پذیر است با هم بررسی کنیم تا مشتریان ما برای تصمیم‌گیری در این خصوص به صورت شفاف به لیستی از ابزارها و روش‌ها دسترسی داشته باشند.

پیش‌نیازهای اصلی برای امنیت شبکه و دسترسی امن به دیدگاه خارج از سازمان

برای Publish یا ایجاد **دسترسی نرم‌افزار سازمانی** با اهمیت دیدگاه برای خارج از شبکه سازمانی، نیاز به ایجاد یک سری ملاحظات و تمهیدات است. شبکه سازمان شما بر اساس سیاست‌های متولیان امر فناوری اطلاعات پیاده‌سازی شده و امینت آن به صورت فیزیکی حفظ می‌شود.

مثلاً ممکن است در شبکه محلی شما همه‌ی سیستم‌ها دارای **آنتی‌ویروس** به‌روز باشند، **سیستم‌عامل‌های کاربران** را بروز کرده و یا نسخه‌ی جدیدی داشته باشید. یا کاربران

دسترسی نصب نرم‌افزار روی سیستم خود نداشته باشند، به همین دلیل از این بابت که ممکن است کسی در شبکه‌ی شما ترافیک شبکه‌ای را شنود یا به اصطلاح Sniff کند کم است، یا اینکه دسترسی لاگ این کاربران را توسط **مرکز مدیریت دیدگاه** به PC-Name یا IP محلی کاربران محدود کرده باشید، یا اینکه اصولاً نسبت به کاربران خود اطمینان کامل دارید، اما وقتی مقرر گردید که دسترسی به شبکه‌ای بیرون از سازمان ایجاد شود می‌بایست ملاحظاتی مورد توجه قرار بگیرد.

افزایش و ارتقاء امنیت شبکه و راهکار اتصال بیرون از سازمان

قبل از هر اقدامی **نرم‌افزار** مورد استفاده شما باید **امن** باشد، در واقع اگر این سامانه استانداردهای رایج مثل OWASP را رعایت نکرده باشد عملاً کار شما برای ایمن کردن نرم‌افزار با استفاده از تجهزات امنیتی و یا سیاست‌های سختگیرانه برای کاربران بسیار دشوار و یا غیرممکن می باشد.

مجموعه نرم‌افزاری دیدگاه به عنوان یک نرم‌افزار یکپارچه سازمانی استانداردهای امنیتی رایج را در زیرساخت همه **نسخه‌های دیدگاه۴**، دیدگاه۵ **(زاگرس)** و دیدگاه همراه اعمال نموده و گواهی‌های رایج توسط مراکز ذی‌صلاح رسمی و متخصص در این امر را در کشور کسب کرده است. لحاظ این استانداردها در همه‌ی لایه‌های نرم‌افزار اعم از لایه زیرساخت و لایه وب جز اصول و اولویت‌ها در چارگون جهت برنامه‌نویسی و توسعه در نظر قرار می‌گیرند، اما بخش عمده‌ای از استانداردهای امنیتی مستلزم اعمال تنظیماتی روی سیستم عامل سرور، SQL Server، IIS و حتی **مرکز مدیریت دیدگاه** است. با توجه به اینکه اعمال اکثر این تنظیمات نیاز به رعایت مجموعه‌ای از پیشنیازها

در شبکه و کلاینت کلیه کاربران می‌باشد به صورت پیش‌فرض توسط چارگون بر روی همه‌ی سرورها انجام نمی‌شود. طبق درخواست و تایید کارفرما پس از کنترل پیشنیازها و اعلام آن به شرکت چارگون با هماهنگی راهبر مجموعه در دستور کار قرار می‌گیرند. لیستی از این تغییرات و پیش‌نیازهای مهم توسط واحد پشتیبانی و یا در پرتال مشتریان قابل دریافت و ارایه است.

HTTPS و تهیه گواهی‌هایSSL استاندارد و معتبر برای وب‌سرورها

بعد از کنترل موارد فوق اصلی‌ترین پیشنهادی که می‌بایست برای Publish نرم‌افزار تحت وب به شبکه‌ی خارج از سازمان انجام شود تهیه **گواهی‌هایSSL** استاندارد و معتبر برای وب‌سرورهاست، این گواهی می‌تواند از هر ارایه دهنده‌ی مجاز و معتبری تهیه شوند. همچنین برای انجام این مهم، ابتدا نیازمند دریافت پیش‌نیازها از همکاران پشتیبانی چارگون هستید و پس از بررسی و فراهم‌سازی آنها و بعد از نصب گواهی تهیه شده روی **سرور(های) وب دیدگاه** توسط کارفرما، تنظیمات با هماهنگی توسط **پشتیبانی فنی چارگون** باید برای دیدگاه لحاظ می‌شود.

Hardening و افزایش افزایش و ارتقاء امنیت سیستم عامل

همانطور که می‌دانید دیدگاه بر روی **سیستم عامل Windows Server** نصب و از وب سرور IIS و **SQL Server** به عنوان نرم‌افزار بانک اطلاعاتی بهره می‌گیرد. با توجه به گستردگی استفاده از این مجموعه زیرساخت‌ها، شرکت **مایکروسافت** مجموعه زیادی از تنظیمات را به صورت پیش‌فرض در هنگام نصب به صورت خودکار انجام می‌دهد

که حداکثر سازگاری با انواع مختلف سناریوهای کاربردی و حداقل پیچیدگی در راه‌اندازی سرویس‌ها را داشته باشد.

اما این سازگاری زیاد باعث می‌شود که تا حد زیادی تنظیمات بدون استفاده وجود داشته باشد که باید حذف شوند. به این فرایند، افزایش و ارتقاء امنیت سیستم عامل، IIS و اصطلاحاً **Hardening** گفته می‌شود.

همانطور که گفته شد بخش عمده‌ی از این تنظیمات به دلیل سازگاری هر چی بیشتر زیر ساخت به صورت پیش‌فرض تعبیه شده‌اند به همین دلیل حذف آنها ممکن است باعث اختلالاتی در نحوه کار کاربران از نرم‌افزار شود. به عنوان مثال در **استانداردهای امنیتی** آمده است که نسخه‌ی TLS v1به دلیل ضعف‌های امنیتی که دارد باید از روی سیستم عامل سرور غیرفعال شده و سیستم عامل به نحوی تنظیم شود که فقط از TLS v1.1 و TLS v1.2 برای ارتباطات شبکه‌ای در لایه‌های ۴ به بالا استفاده کند،

به این معنی هست که به عنوان مثال اگر کاربری در کلاینت خود از ویندوز Windows XP استفاده کند امکان برقراری ارتباط با این سرور و مجموعه نرم‌افزاری را نخواهد داشت. در Windows 7 هم برای سازگاری با این نسخه‌ها ازTLS باید Service Pack 1 و Hotfix خاصی نصب شود. راهبران، متولیان امر در فناوری اطلاعات و ادمین سازمان‌ها با آگاهی کامل از تبعات و شرایطی که با اعمال **Hardening** ایجاد می‌کنند باید این اقدامات را در نظر و اعمال نمایند، مجموعه‌ای از پیش‌نیازهای شناخته شده‌ای که باید کنترل شده و کاملاً مرتبط با **مجموعه نرم‌افزاری دیدگاه** هستند قبلاً توسط **شرکت چارگون** و در اختیار تیم پشتیبانی قرار گرفته که در صورت نیاز کارفرما قابل

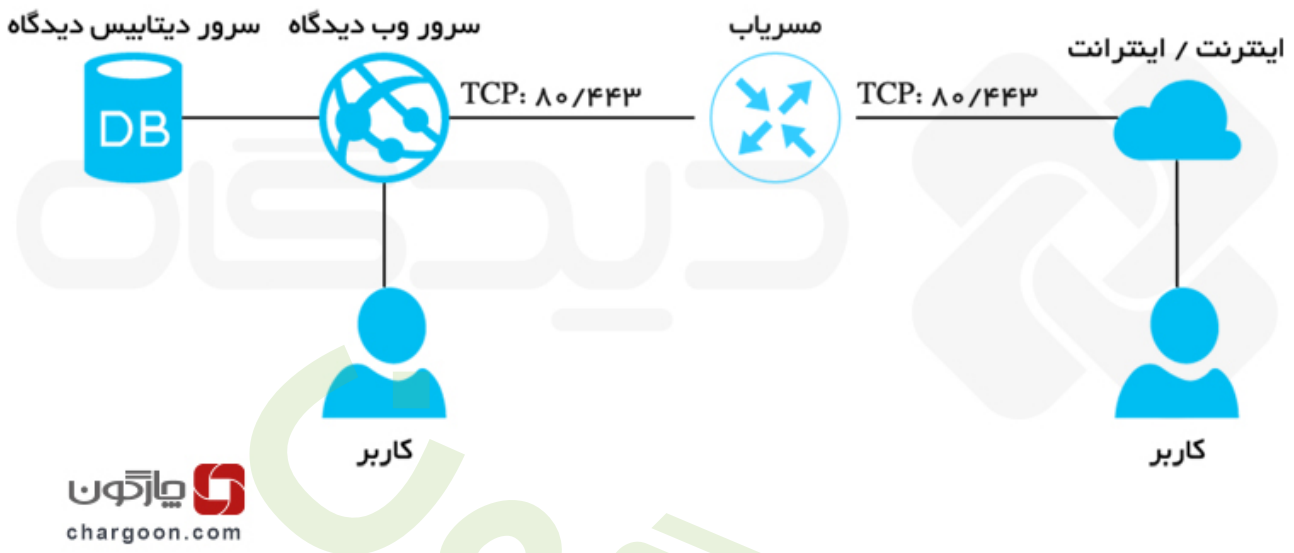
ارائه بوده که پس از تایید این پیشنیازها، موارد امنیتی مورد نظر با هماهنگی راهبر مجموعه توسط پشتیبانی فنی انجام می‌شود.

روش‌ها:

راهکار حفظ امنیت شبکه و بازکردن دسترسی امن از بیرون با استفاده از NAT-Router

در این روش که سهل الوصول‌ترین روش برای بازکردن دسترسی سرویس از داخل به بیرون شبکه است، فقط کافی است دستگاه مسیریاب لایه بیرون شبکه را (Edge Router) به نحوی تنظیم کنید که یک پورت از روی IP Public مسیریاب به پورت ۸۰ یا ۴۴۳ **سرور وب دیدگاه** اصطلاحاً NAT شود، به عبارت دیگر به روتر یاد می‌دهیم هر درخواستی که روی پورت xxx را دریافت کرد به سمت پورت ۸۰ یا ۴۴۳ (https/http) سرور **دیدگاه** منتقل کند.

از مزایا این روش سادگی معماری و راحتی انجام آن را می‌توان نام برد، این مدل معماری باعث می‌شد که همه پورت‌های اضافه‌ای که دیدگاه به آن ها نیازی ندارد به سمت کاربران (و حمله کنندگان) بسته باشد تا حدی امنیت ترافیک شبکه‌ای را پوشش می‌دهد اما مشکلی که دارد این است که نمی‌تواند از حمله‌های لایه‌ی ۷ شبکه جلوگیری کند.



بازکردن دسترسی به شبکه از بیرون با استفاده از NAT- Router

راهکار حفظ امنیت شبکه و بازکردن دسترسی امن از بیرون با استفاده از Firewall

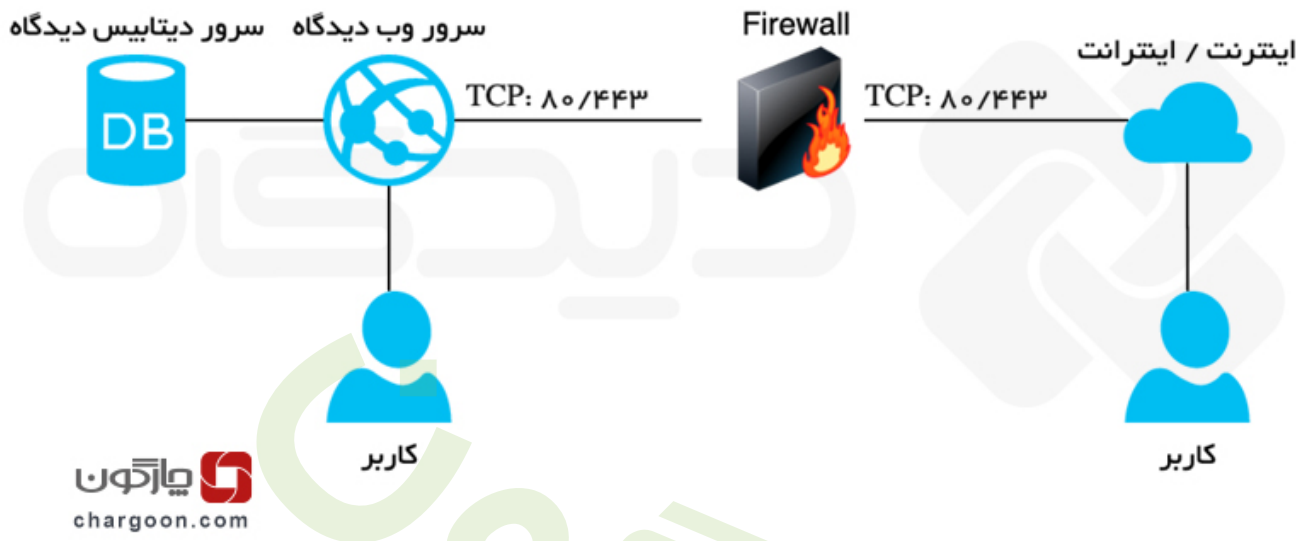
در این روش کمی معماری پیچیده‌تر می‌شود و علی‌رغم وجود Edge Router و فرآیند NAT یک **فایروال** نیز وجود دارد که **ترافیک شبکه‌ای** گذرا را بررسی می‌کند و در صورت مشاهده ترافیک مشکوک سعی می‌کند تا منبع ترافیک را قطع کند، **فایروال** ها انواع مختلفی دارند و هر یک در حوزه‌ی خاصی تخصص دارند. به عنوان مثال بعضی‌ها هوشمندی بیشتری دارند و نسبت به نشست آگاه هستند (Stateful) و می‌توانند در لایه۵ بعضی از بسته‌های مشکوک را تشخیص دهد یا اینکه بعضی‌ها بر اساس تاریخچه‌ای از Stream بسته‌های شبکه‌ای گذرا با در اختیار داشتن بانک قوی و کامل می‌تواند از روی

این بسته‌ها حمله قبل از رخداد را حدس زده و دستور به قطع ارتباط با منبع حمله کننده را صادر کند (IDS/IPS) دستگاه هایی مثل **Cisco NGIPS، Juniper SRX** از این دست دستگاه‌ها هستند.

مجموعه دیگر **فایروال** هم نیز وجود دارد که که اصطلاحات **UTM** گفته می‌شوند. این **دستگاه‌های Unified Threat Management** در واقع همانطور که از اسم آنها مشخص است برای **مدیریت خطرات در شبکه** ساخته شده و این دستگاه‌ها مجموعه از ابزارهای امنیتی را به صورت یکپارچه در اختیار مدیر شبکه قرار می‌دهد.

دستگاه‌های **Kerio، FortiGate و Cyberoam** از این جنس هستند که مدیریت راحتری دارند و قابلیت های مختلفی مثل IDS, Antivirus, Web Publish را در خود دارند که تقریباً می‌شود گفت به راحتی چند کلیک می‌توان آنها را تنظیم کرد.

انواع دیگری از فایروال‌های مثل NGFW هم وجود دارد که با توجه به این قصد نداریم در این نوشته مباحث تخصصی این دستگاه رو پوشش دهیم فقط به نام آنها بسنده می‌کنیم.



بازکردن دسترسی به شبکه از بیرون با استفاده از فایر وال

حفظ امنیت شبکه با استفاده از سرور واسط فقط برای Reverse Proxy

روش‌های فوق همگی در **لایه‌های پایین شبکه** فعالیت می‌کنند و عملاً خیلی به ندرت وارد ترافیک **HTTP** می‌شوند اگر هم وارد بشوند به صورت کلی برای چک کردن المان های کلی و typical اقدام می‌کنند.

داستان از آنجا شروع می‌شد که ممکن است شما در سناریوهایی نیاز باشد تنظیمات زیر ساختی خاصی در **سیستم عامل** و یا **وب سرویس (IIS)** انجام دهید.

مثلا قصد دارید Cipher Suiteهای غیر ایمن خانواده RC4 را غیر فعال کنید اما همزمان می‌دانید برخی کاربران شما به دلیل استفاده از نرم‌افزار قدیمی نخ‌نما شده‌ای مجبور هستند که از Windows XP یا مرورگر با نسخ خیلی قدیمی استفاده کنند.

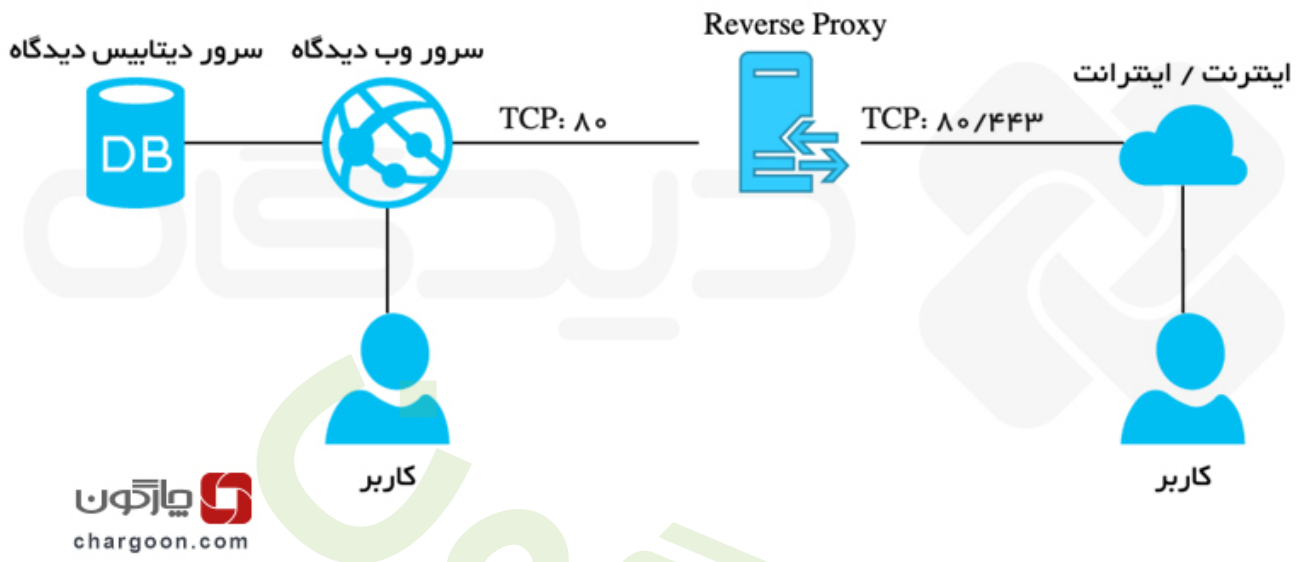
خاموش کردن این Cipher Suite عملاً باعث می‌شود کارکرد روزمره این کاربران متوقف شده و از طرفی نیاز دارید هر چه سریع‌تر «دیدگاه» را در دسترس عموم و خارج از سازمان قرار دهید ولی حاضر نیستید که از اولویت‌های امنیتی خود دست بکشید (من به شخصه به شما حق می‌دم)، در این شرایط تکلیف چیست؟

یا مثلا نیاز دارید یک URL خاصی که مد نظر شماست در داخل شبکه محلی کار کند ولی کاربران بیرون از سازمان امکان دسترسی به آنرا نداشته باشند،

یا نیاز دارید آپلود فایل با پسوند مشخصی از بیرون از شبکه محلی به دیدگاه امکان پذیر نباشد،

یا به دلیل حجم بالا تراکنش‌های کاربران و منابع محدود سرور وب دیدگاه صلاح نمی‌بینید که بار **Encryption/decryption برای HTTPS** به سرور اضافه شود دوست دارید این امر توسط سرور یا ماژول دیگری انجام شود که اصلاحات **SSL-Offloading** نامیده می‌شود، تکلیف چیست؟

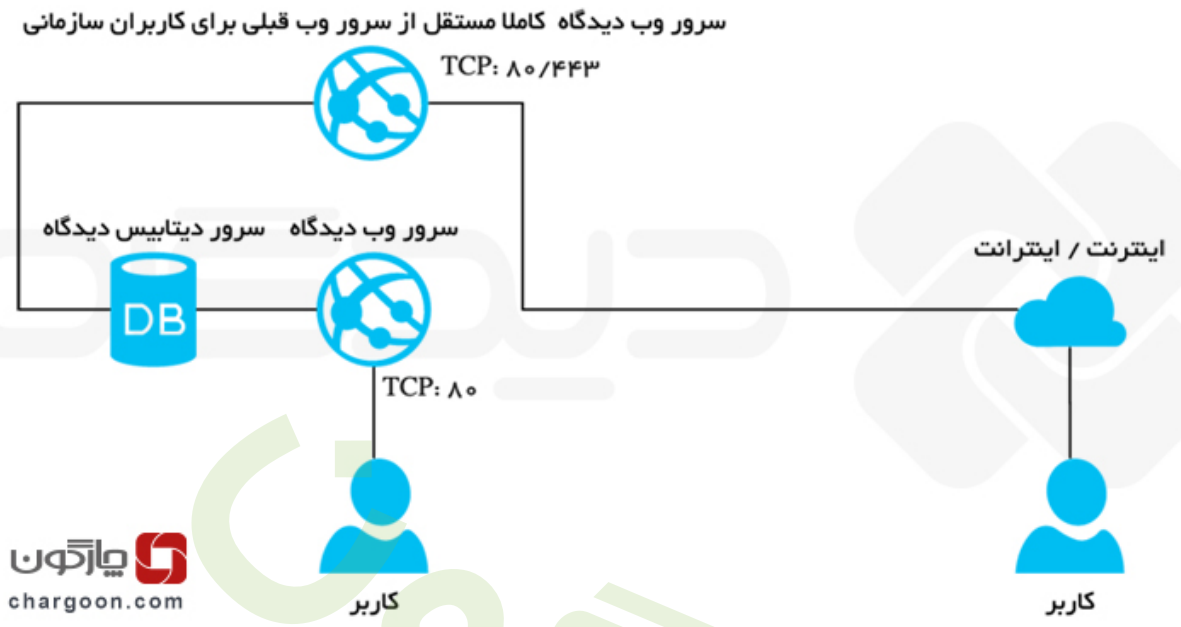
برای پاسخگویی به نیازهایی مثل موارد ذکر شده در فوق می‌توان وب سرور جدید از سرور قبلی راه‌اندازی کرد که تنها وظیفه آن دریافت درخواست‌های کاربران، ترجمه ،ممیزی آنها، ارسال به **سرور اصلی**، دریافت پاسخ از سرور اصلی و نهایتا ارسال پاسخ به کاربر باشد.



بازکردن دسترسی به شبکه از بیرون با استفاده از سرور واسط فقط برای Reverse Proxy

بازکردن دسترسی امن از بیرون با استفاده از سرور وب مستقل دیدگاه

در بعضی از سناریو های ممکن است، شرایط به نحوی پیش برود که حمله کنندگان از نقطه ضعف پیش‌بینی نشده‌ای استفاده کنند و **وب‌سرور** را آلوده نماید، در این سناریو **مدیر شبکه یا ادمین** به هیچ‌وجه نمی‌خواهد که این آلودگی به کارکرد نرم‌افزار اختلالی ایجاد کند یا این آلودگی به سرور وب اصلی دیدگاه سرایت کند. یکی از بنیادی‌ترین روش ها راه‌اندازی یک **وب‌سرور در DMZ**، کاملاً مجزا از سرور(های) اصلی دیدگاه باشد که ارتباطات شبکه‌ای لازم با سرورهای زیر ساختی دیدگاه مثل **سرور دیتابیس** به صورت موردی (تک به تک) باز شود.



بازکردن دسترسی به شبکه از بیرون با استفاده از سرور وب مستقل دیدگاه

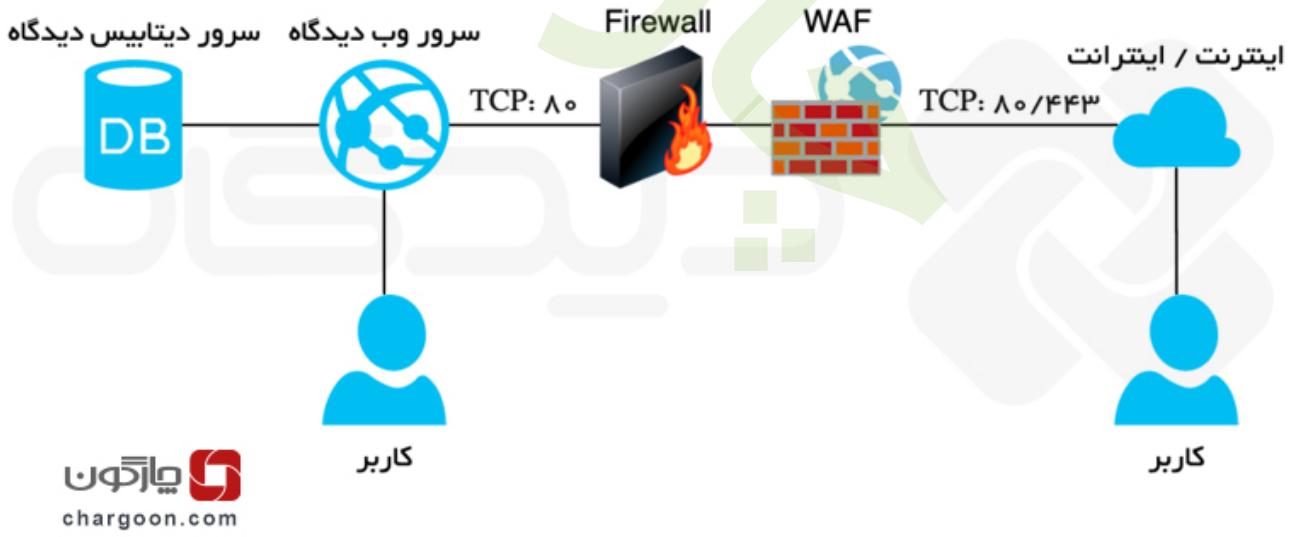
راهکار حفظ امنیت شبکه با استفاده از WAF

Web application firewallها دستگاه‌هایی هستند که به صورت تخصصی به بررسی **ترافیک لایه وب** می‌پردازند. قابلیت‌هایی مثل بررسی ترافیک مشکوک وب، بررسی انواع حملات سطح بالا بر اساس Signature های که در دیتابیس‌های خود دارند اکثر حملات رایج را تشخیص می‌دهند.

به عنوان مثال **حملات file inclusion**، **cross-site-scripting (XSS)**، **cross-site forgery** و **SQL injection** به راحتی توسط این دستگاه قابل جلوگیری است. البته لازم به ذکر است تا حد امکان زیرساخت **مجموعه نرم‌افزاری دیدگاه** به صورت مستقل از جهت اینگونه موارد ایمن شده و این دست حملات شناخته شده را تشخیص و

جلوگیری می‌کند. اما زمانی که بحث امنیت می‌شود هیچ وقت کار از محکم کاری عیب نمی‌کند با حداقل تنظیماتی، دیدگاه می‌تواند بدون تغییر با این نوع فایروال‌ها سازگار شود، از دیگر قابلیت این دستگاه **فرآیند SSL-Offloading** است اکثر دستگاه‌های رایج مثلا Big-IP-F5، Forti Web این قابلیت‌ها را دارند.

اما همانطور که گفته شد این نوع فایروال‌ها فقط در لایه 7 شبکه فعالیت نموده و نمی‌توانند همه‌ی حملات را تشخیص دهند. البته نسخه‌هایی از این دستگاه‌ها وجود دارد که به صورت یکپارچه چندین لایه نرم‌افزار برای پوشش را در **لایه‌های مختلف شبکه** در دورن خود دارند.



بازکردن دسترسی به شبکه از بیرون با استفاده از WAF

دسترسی امن از بیرون با استفاده از WAFهای آنلاین و ابری

فایروال‌های لایه هفت یا WAF عمدتاً پیچیدگی های فنی زیادی دارند. این فایروال‌ها می‌توانند یا سخت‌افزاری باشند یا نرم‌افزاری که معمولا از نظر هزینه‌های مالی نیز در جزو ابزارهای گران دسته‌بندی می‌شوند. به این دو دلیل برای خیلی از مجموعه‌ها و سازمان‌ها به صرفه نیست که WAF تهیه کنند یا صلاح نمی‌دانند که اینچنین پیچیدگی را وارد شبکه خود کنند.

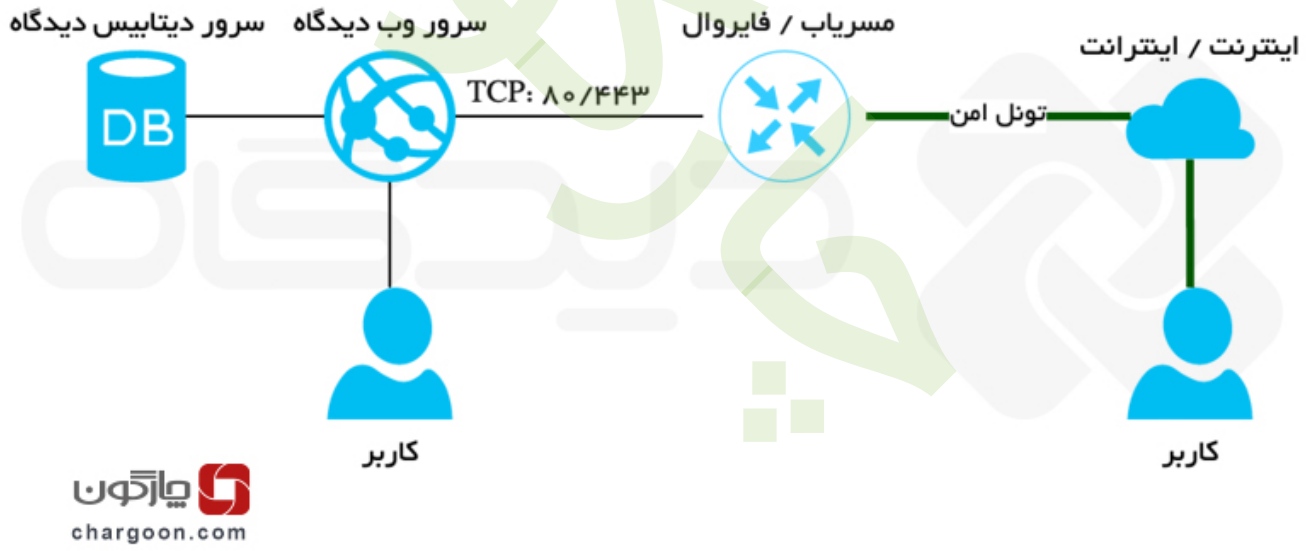
یکی از راه‌کارهایی که این سال‌ها باب شده **راهکارهای ابری** برای استفاده از سرویس هاست، چندین سرویس‌دهنده‌ی داخلی و خارجی وجود دارند در قبال دریافت مبالغی یا حتی به صورت رایگان برای ترافیک‌های کم به شما این امکان را می‌دهند که **نرم‌افزار تحت وب** خود را به پشت **WAF غیر متمرکز** آنها قرار دهید. در این مقاله درباره بایدها و نبایدهایی برای انتخاب راهکارهای ابری صحبت کرده‌ایم.

معمولاً این راه‌کارهای ابری از **تکنولوژی IP Anycast** استفاده می‌کنند. به آنها این امکان را می‌دهد که زیر ساخت‌های خود را به صورت توزیع شده در گستره جغرافیایی داشته باشند و نزدیک‌ترین مسیر (route) بین سرور شما و زیر ساخت خود و از زیرساخت خود تا کاربران شما را پیدا نموده که تا حد ممکن کاهش **latency** شبکه را به ارمغان خواهد آورد.

با توجه **ابری بودن زیر ساخت (Cloud Based Infrastructure)** و در واقع مستقر بودن آنها در چندین **دیتاسنتر** به صورت همزمان عملاً پهنای باند بسیار وسیعی در اختیار دارند که به آنها اجازه می‌دهد که بتوانند تا حد زیادی با **حملات Denial of**

Service توزیع شده با اصطلاحا **DDoS** مقابله کنند.

از دیگر مزایای این راه‌کارها جامع بودن دیتابیس Signatureهای حملاتی هست که می‌توانند تشخیص دهند. برای جلب رضایت مشتریان سعی می‌کنند که از دیتابیس‌ها و روش‌های تشخیصی متنوعی را پوشش دهند. اکثر این راه‌کارهای ابری حتی **قابلیت SSL-Offloading** را دارا بوده و تا حد ممکن Hardening لایه edge را انجام می‌دهند.



بازکردن دسترسی به شبکه از بیرون با استفاده از WAFهای آنلاین و ابری

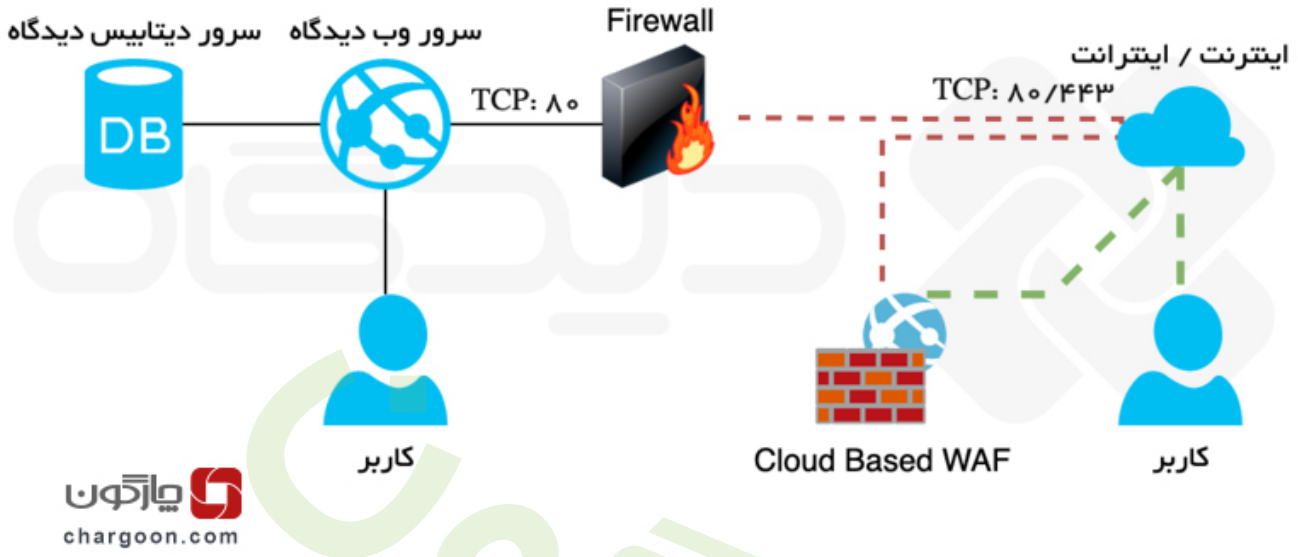
حفظ امنیت در شبکه با استفاده از زیر ساخت‌های VPN

یکی دیگر از روش‌های حفظ امنیت در شبکه ایجاد دسترسی برای کاربران خارج از

سازمان، ایجاد **دسترسی VPN** برای آنهاست، این روش که جزو روش‌هایی که به راحتی قابل پیاده سازی است و از امنیت شبکه‌ای نسبتاً خوبی برخوردار بوده اما ممکن است کاربران برای انجام تنظیمات آن روی کامپیوترهای خود دچار مشکل شوند.

مشکل دیگری که ایجاد می‌کند این است که با توجه ذات این **تکنولوژی** که تونل امنی در **لایه شبکه** بین کامپیوتر کاربر و **شبکه داخلی سازمان** ایجاد می‌کند، همه **ترافیک کامپیوتر کاربر** را به سمت تونل روانه می‌کند این امر به این معنی است که هر درخواست شبکه‌ای کاربر در سیستم خود انجام می‌دهد از **Routerها** و **Firewallهای** سازمان می‌گذرد و سیاست‌های سازمان روی آن اعمال می‌شد تا به اینجا خیلی بد نیست، مشکل از جایی شروع می‌شود که این امر باعث استفاده زیادی از پهنای باند شبکه‌ای سازمان می‌شود برای بسته‌های شبکه‌ای که اصلاً نیاز نیست وارد شبکه سازمان شوند.

برای حل این مشکل تقریبا **VPNهای استاندارد** کمکی نمی‌کنند شما باید از ابزارهای مثل **OpenVPN، Cisco AnyConnect و یا Kerio Connect** استفاده کنید که به شما اجازه می‌دهند **Client Side Routing** داشته باشید به این معنی که برای شما تصمیم بگیرد کدام بخش ترافیک کاربر باید از تونل رد شود و کدام مستقیما وارد شبکه محلی کاربر شود.



بازکردن دسترسی به شبکه از بیرون با استفاده از زیر ساخت‌های VPN

از دیگر مزایایی **راه‌کار VPN** این است که شما می‌توانید بخش زیادی از سرویس‌های حتی غیر Web را نیز به صورت ایمن در اختیار کاربران قرار بدهید. مثلاً VoIP یا سرویس SQL یا Email یا هر چیزی که به مرور زمان نیاز دارید با چند کلیک دسترسی را ایجاد یا حذف کنید.

تسهیل دورکاری با محصولات موبایلی دیدگاه

در شرایط شیوع بیماری کرونا، **دورکاری** پرسنل سازمان‌ها و شرکت‌ها و کاهش رفت و آمدهای عمومی اهمیت زیادی پیدا کرده است. با توجه به توسعه زیر ساخت مجموعه نرم‌افزاری دیدگاه در بستر موبایل، مشتریان چارگون می‌توانند از امکانات **محصولات موبایلی دیدگاه** برای اجرای فرآیندهای اداری استفاده کنند.

مجموعه نرم‌افزاری دیدگاه با ارائه اپ‌های کاربردی روی سیستم عامل اندورید و iOS به کاربران و مشتریان نرم‌افزارهای خود امکان می‌دهد بر بستر موبایل فرآیندهای اداری پرکاربرد حوزه اتوماسیون اداری و منابع‌انسانی و **لجستیک** را دنبال کنند. **تسهیل دورکاری در سازمان‌ها و شرکت‌ها با محصولات موبایلی دیدگاه با استفاده از محصولات موبایلی دیدگاه** که با نام تجاری **دیدگاه همراه** ارائه شده‌اند انجام می‌شود .

این اپ‌ها در حال حاضر شامل موارد زیر هستند:

دیدگاه، مکاتبات، پیشخوان، جلسات، انباردار، جمع‌دار.

درنهایت در این نوشته سعی کردیم انواع روش‌های تا حدی منطقی برای ایجاد دسترسی **مجموعه نرم‌افزاری دیدگاه** به اینترنت/ اینترانت را با هم مرور کنیم اما همیشه در مباحث امنیتی گفته می‌شود که امنیت هیچ وقت صد درصد نیست و مفهومی نسبی است. همیشه سعی می‌کنیم کمی از قبل ایمن‌تر باشیم، روش‌های گفته شده ممکن است هریک به تنهایی کافی نباشند بلکه روش‌های ترکیبی به نظر معقولانه‌ترین راه‌کار هستند.

درخواست دمو نرم‌افزارهای مجموعه دیدگاه