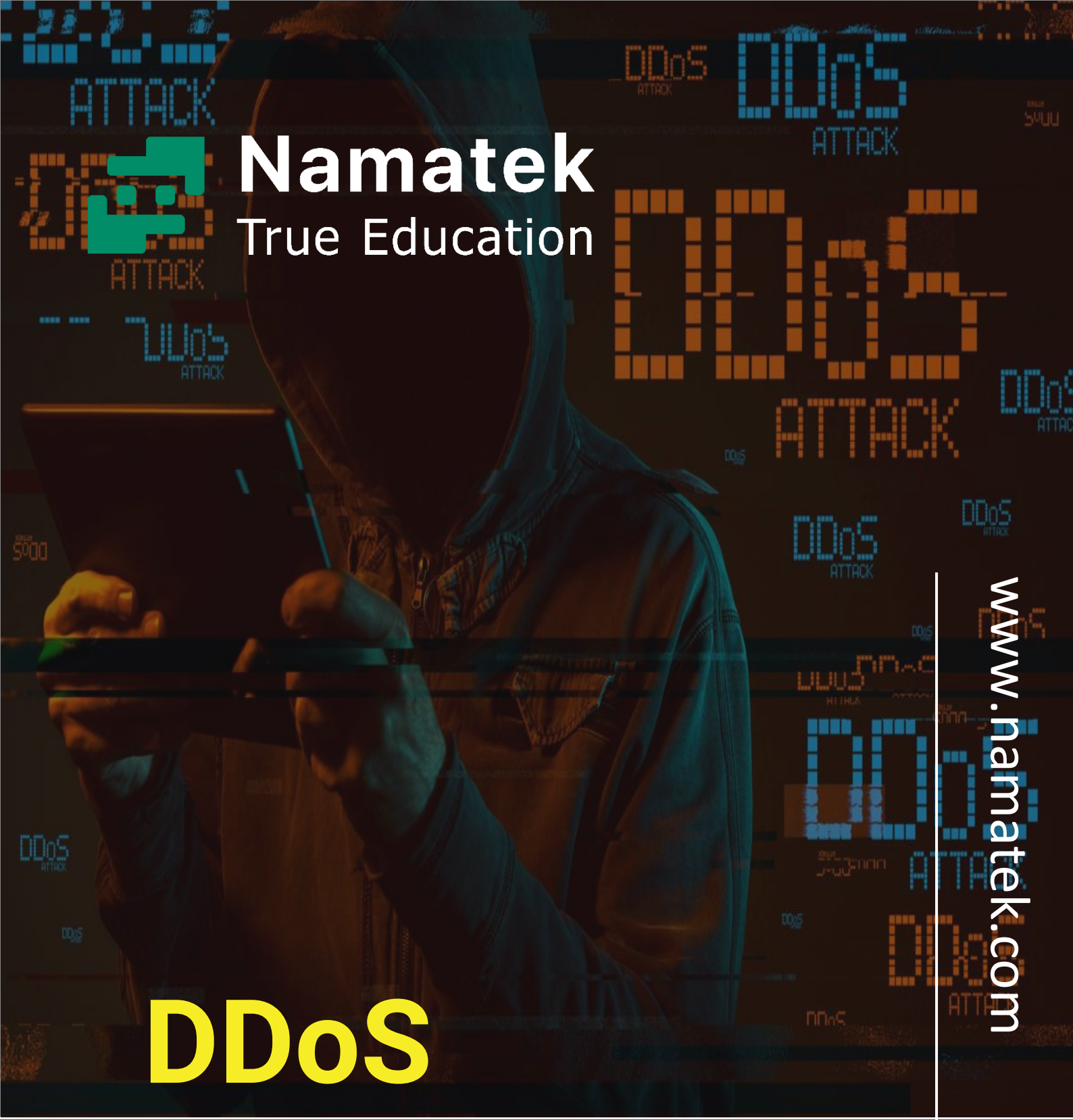



# حمله دیداس چیست؟

# فهرست مطالب


۱. دیداس چیست؟ (DDoS)

۲. انواع حمله دیداس (DDoS attacks)

۳. علائم حمله دیداس چیست؟ (DDoS attack symptoms)

۴. حمله DDoS چگونه انجام می شود؟

۵. راه های محافظت در مقابل حملات دیداس چیست؟

حمله دیداس چیست و چگونه عملکرد سرویس دهنده ها را مختل و یا از دسترس خارج می کند؟ با توجه به شباهت این حمله به ترافیک عادی، چطور می توان این حملات را تشخیص داد و با آن ها مقابله کرد؟ این ها پرسشی های است که همیشه ذهن صاحبان سرویس های آنلاین را به خود مشغول می کند. برای پاسخ به این پرسش ها و کسب اطلاعات بیشتر در مورد حملات DDoS در ادامه با ما همراه باشید.

## #۱ دیداس چیست؟ (DDoS)

حمله دیداس یا DDoS مخفف Distributed Denial of Service به معنی محروم سازی از سرویس توزیع شده، تلاشی مخرب برای ایجاد اختلال هدفمند و عدم دسترسی به سرویس دهنده های مختلف اینترنتی است. این حملات می تواند انواع سرویس دهنده های موجود در شبکه را تهدید کند. به عنوان مثال:

- سرورها
- دستگاه ها
- خدمات
- شبکه ها
- برنامه ها
- سرویس های معاملات خاص در داخل برنامه ها

این حمله با ارسال بیش از حد درخواست های سرویس، هدف یا زیرساخت های سرویس دهنده را با ایجاد ترافیک اسپم اینترنتی دچار اختلال می کند. حملات می تواند ارسال تعداد زیادی درخواست به یک وب سرور برای ارائه یک صفحه باشد یا می تواند یک پایگاه داده را با سیلی از پرس و جو مورد هدف قرار دهد.

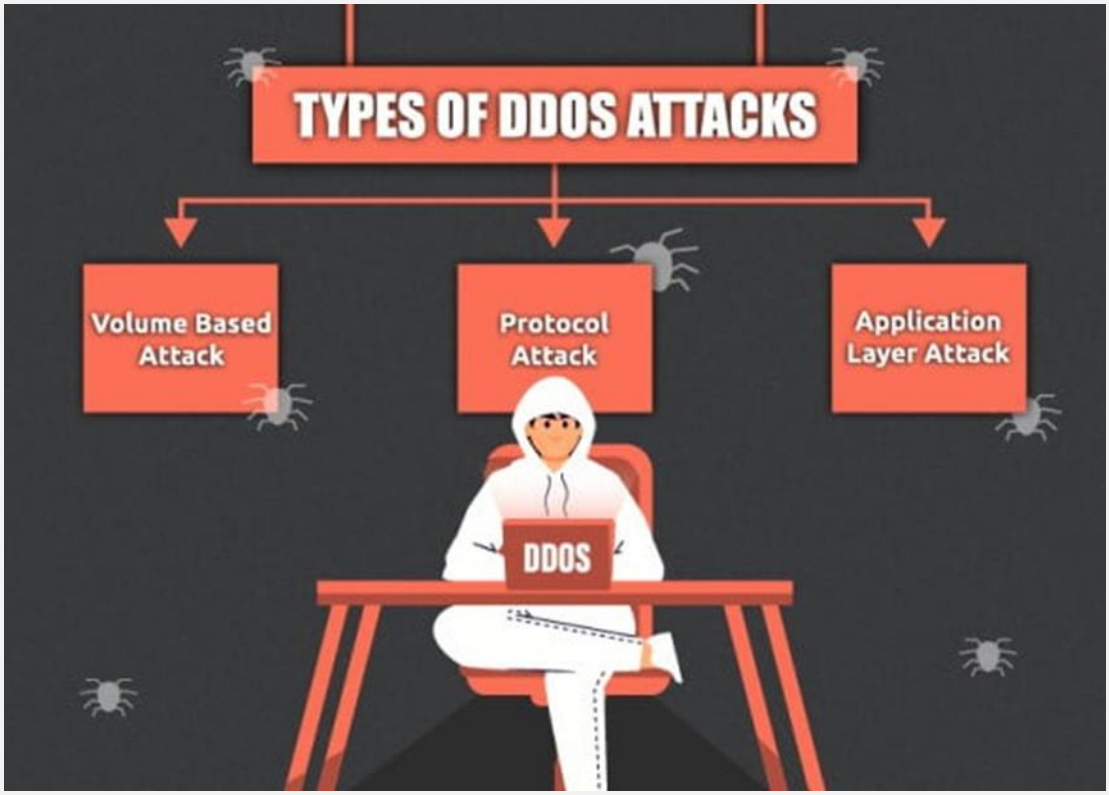

شاید برایتان جالب باشد که بدانید هدف نهایی حمله دیداس چیست. حمله دیداس پهنای باند اینترنت، CPU و RAM را بیش از حد قابل استفاده به کار می گیرد که در نهایت سیستم را از دسترس خارج می کند. به بیان ساده تر، حمله DDoS مانند یک ترافیک غیر منتظره در یک بزرگراه عمل می کند که می تواند به راحتی آن را مسدود و از رسیدن خودروها به مقصد جلوگیری کند.

این حمله مشابه حمله DoS است؛ اما با این تفاوت که حملات DDoS با استفاده از چندین سیستم رایانه ای برای ایجاد این ترافیک استفاده می

کنند. سیستم های مورد استفاده در این حملات می توانند شامل رایانه و سایر منابع شبکه ای مانند دستگاه های اینترنت اشیا باشند.

## #۲ انواع حمله دیداس (DDoS attacks)

با این که در هر نوع از حمله دیداس به منابع شبکه، هدف همیشه از کار انداختن یا کند کردن سرورها است؛ اما این حملات با روش ها و اهداف مختلفی انجام می شود که سه طبقه بندی اصلی برای آن ها وجود دارد:




۱. حملات مبتنی بر حجم (Volume-based attacks)

حملات مبتنی بر حجم، از حجم گسترده ای از ترافیک ساختگی برای غلبه بر منبعی مانند وب سایت یا سرور استفاده می کنند. این حملات شامل موارد زیر هستند.

- ICMP
- UDP
- ایجاد بسته های جعلی

اندازه یک حمله مبتنی بر حجم بر حسب بیت بر ثانیه (bps) اندازه گیری می شود.

۲. حملات پروتکل یا لایه شبکه (Protocol or network-layer attacks)

اما روش حملات پروتکل یا لایه شبکه در حمله دیداس چیست؟ در این روش تعداد زیادی بسته را به زیرساخت های شبکه هدف و ابزارهای مدیریت زیرساخت می فرستد. حملات پروتکل شامل موارد زیر است.

- SYN floods
- Smurf DDoS

و سایر موارد

اندازه این حملات بر اساس بسته در ثانیه (PPS) اندازه گیری می شود.

۳. حملات لایه کاربرد (Application-layer attacks)

حملات لایه کاربردی با غرق کردن برنامه ها در درخواست های نادرست انجام می شود. حملات لایه کاربرد بر اساس درخواست در ثانیه (RPS) اندازه گیری می شود.

## #۳ علائم حمله دیداس چیست؟ (DDoS attack symptoms)

بارزترین نشانه حمله دیداس چیست؟


بارزترین علامت حمله DDoS، کند شدن یا در دسترس نبودن سایت یا سرویس است؛ اما از آن جا که درخواست های غیر مخرب نیز می توانند موجب ایجاد مشکل در دسترسی شوند، معمولا بررسی بیشتر لازم است.

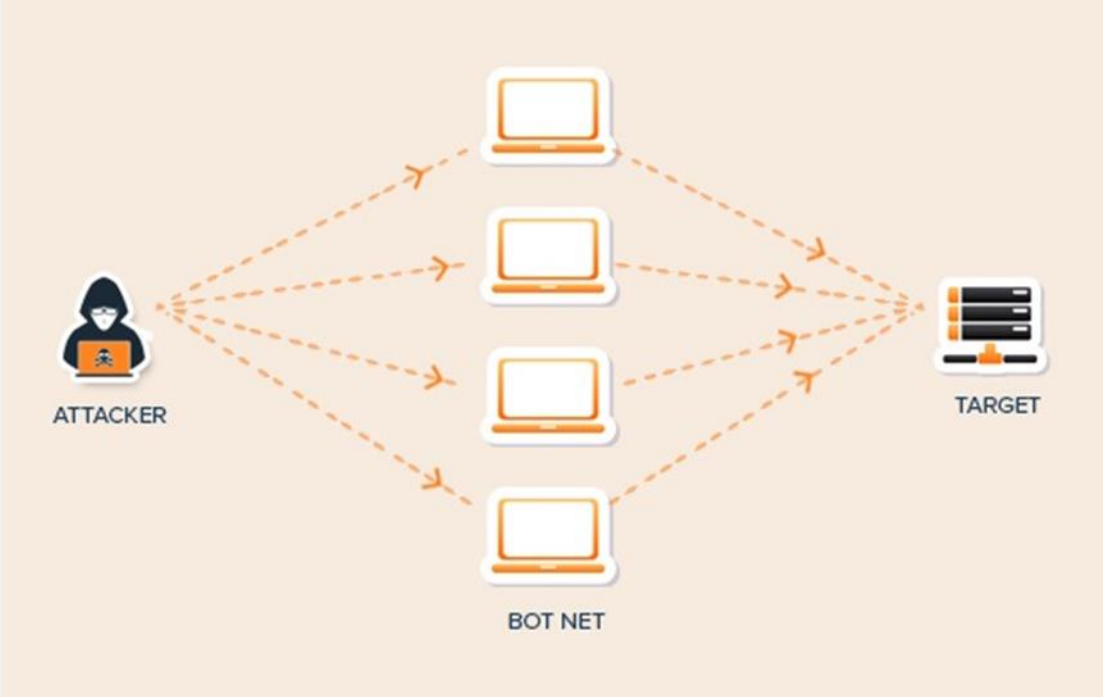
به عنوان مثال ابزارهای تجزیه و تحلیل ترافیک می توانند به شما کمک کنند برخی علائم یک حمله DDoS را تشخیص دهید:

- میزان مشکوکی از ترافیک مربوط به یک آدرس IP یا محدوده ای از IPباشد.
- سیل ترافیکی از کاربرانی که یک ویژگی رفتاری یکسان دارند، مانند نوع دستگاه، موقعیت جغرافیایی یا نسخه مرورگر وب
- افزایش غیر قابل توضیح درخواست ها به یک صفحه یا محلی خاص
- الگوهای ترافیکی عجیب و غریب مانند افزایش در ساعات فرد، روز فرد، یا الگوهایی که غیر طبیعی به نظر می رسند (به عنوان مثال افزایش در هر ۱۰ دقیقه)

علاوه بر این علامت ها، علائم ثابت و مشخص دیگری از حمله DDoS وجود دارد که بسته به نوع حمله می تواند متفاوت باشد؛ اما به طور کلی، از آن جا که این ربات ها در واقع دستگاه های اینترنتی مجاز هستند، جدا کردن ترافیک مخرب حمله DDoS، از ترافیک عادی ممکن است دشوار باشد.

## #۴ حمله DDoS چگونه انجام می شود؟

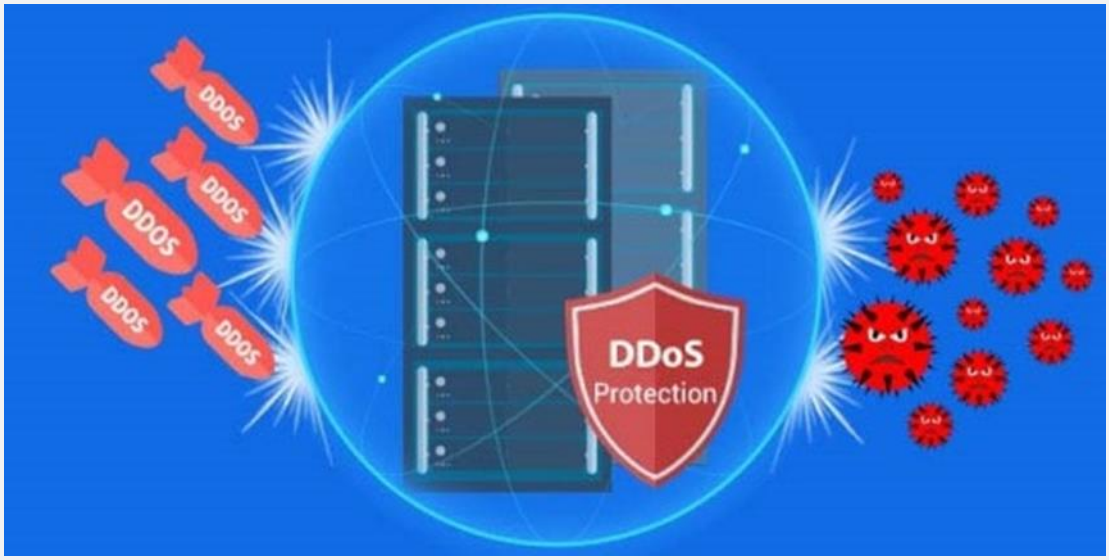
حملات DDoS با استفاده از شبکه ای متصل به اینترنت انجام می شود. این شبکه ها شامل رایانه ها و سایر دستگاه هایی که به بدافزار آلوده شده اند هستند که امکان کنترل از راه دور توسط یک مهاجم را دارند. نام دستگاه های منفرد در حملات دیداس چیست؟




دستگاه های منفردی که در این حملات استفاده می شوند به نام ربات شناخته می شوند. همچنین به گروهی از این ربات ها، بات نت (botnet) گفته می شود. هنگامی که بات نت ایجاد شد، مهاجم می تواند با ارسال دستورالعمل هایی از راه دور به هر ربات، حمله را هدایت کند. زمانی که سرور یا شبکه قربانی به وسیله یک گروه از کامپیوترهای مخرب (botnet) مورد هدف قرار می گیرد، هر ربات موجود در گروه botnet، درخواست هایی را به آدرس سرور یا شبکه هدف ارسال می کند.

تعداد درخواست ربات ها آنقدر افزایش می یابد تا بیش از حد توان پاسخگویی سرور یا شبکه باشد. در نتیجه باعث عدم پذیرش سرویس برای ترافیک عادی می شود.

## #۵ راه های محافظت در مقابل حملات دیداس چیست؟




### #۵-۱ کاهش رابط های قابل حمله

یکی از اولین تکنیک های کاهش حملات DDoS، به حداقل رساندن سطح قابل حمله است. بدین ترتیب گزینه های حمله کننده ها محدود می شود و به شما امکان می دهد از یک مکان مشخص و واحد محافظت کنید.

در ابتدا می بایست اطمینان حاصل کنید که برنامه یا منابعی که نیاز به ارتباط با دنیای بیرون از شبکه را ندارند، در معرض پورت ها، پروتکل ها یا درخواست های خارجی قرار نمی دهید. از این طریق می توانید نقاط احتمالی حمله را به حداقل برسانید؛ اما روش مناسب برای کاهش رابط ها در مقابل حمله دیداس چیست؟

در برخی از موارد می توانید این کار را با استفاده از روش های زیر انجام دهید:

۱) از CDN یا شبکه های توزیع محتوا استفاده کنید.

CDN ها سرورهای جهانی هستند که نسخه ای از وب سایت شما را روی شبکه خود نگهداری کرده و با توجه به موقعیت جغرافیایی کاربران، نزدیک ترین آن ها به کاربر سرویس دهی می کند؛ بنابراین در صورت حمله تنها سرور پاسخگو به بات نت دچار مشکل خواهد شد و وب سایت شما در سایر سرورهای شبکه، آنلاین خواهد بود. اگر چه احتمال مختل شدن سرورهای CDN به دلیل منابع و امنیت بالا، بسیار کم است.

۲) از Load Balancer ها استفاده کنید.

Load Balancer ها بین کاربر و سرور قرار می گیرند و زمانی که یک هاست از دسترس خارج شود، درخواست های کاربران را به سمت سرورهای سالم انتقال می دهد.

۳) ترافیک مستقیم اینترنت را به زیرساخت ها محدود کنید.

می توانید ترافیک مستقیم اینترنت را به قسمت های خاصی از زیرساخت خود مانند سرورهای پایگاه داده خود محدود کنید تا از حملات اینترنتی مانند حمله DoS و DDoS به آن ها جلوگیری کنید.

٤) از ابزارها و سرویس های امنیتی استفاده کنید.

می توانید از فایروال ها یا ACL ها (Access Control Lists) برای کنترل میزان دسترسی به برنامه های خود استفاده کنید.

## #۲-۵ برنامه ریزی برای پیشگیری از حملات DDoS


بیشتر حملات دیداس حملات حجمی هستند که منابع زیادی را مصرف می کنند؛ بنابراین مهم است که شما بتوانید به سرعت منابع محاسباتی خود را افزایش یا کاهش دهید. می توانید این کار را با استفاده از

سرورهای منابع محاسباتی بزرگتر یا شرکت های سرویس دهنده پیشرفته ای که حجم بیشتری را پشتیبانی می کنند، انجام دهید.

## #۳-۵ تشخیص ترافیک طبیعی و غیرطبیعی

هرگاه سطح بالایی از ترافیک ارسالی به سرور تشخیص داده شد، روش مقابله برای حمله احتمالی دیداس چیست؟ راه اصلی مقابله این است که فقط تنها به اندازه قدرت و منابع سرورها ترافیک را بپذیریم، بدون این که بر میزان دسترسی آن تأثیر بگذارد. به این مفهوم نرخ محدود کننده یا Rate limiting گفته می شود. تکنیک های حفاظت پیشرفته تر می توانند یک گام جلوتر بروند و با تجزیه و تحلیل بسته های جداگانه، ترافیکی را که مجاز است بپذیرند.

برای انجام این کار، شما باید ویژگی های ترافیک خوب را درک کنید و بتوانید هر بسته را بر اساس آن مقایسه کنید. به عنوان مثال ترافیک های ارسال شده از یک کشور یا IP خاص را بلاک کنید.