What is DMZ?

پروژه اول درس شبکه‌های کامپیوتری

استاد درس:
دکتر علی زارع

سارا حیدری
۸۱۰۳۰۳۰۶۷

مهرماه ۱۴۰۳

DMZ چیست؟

DMZ → Demilitarized Zone — منطقه غیر نظامی

- عبارت DMZ یا همان منطقه غیر نظامی برای تعریف خطوط مرزی بین دو کشور در علوم جغرافیایی و سیاسی به کار می‌رود که وارد فناوری شده است.

- شبکهٔ DMZ نوعی زیر شبکهٔ محافظ است که به‌عنوان پل ارتباطی بین یک شبکهٔ ایمن داخلی با شبکهٔ غیرایمنی مثل اینترنت عمل می‌کند.

- هدف DMZ، فراهم‌کردن یک لایه امنیتی بیشتر برای محافظت از شبکه‌های داخلی در برابر تهدیدات خارجی است.

DMZ و سفینه فضایی!

یک مثال ملموس برای درک بهتر!

شبکهٔDMZدر واقع، مانند اتاقک ورودوخروج سفینه عمل می‌کند و با ایجاد یک منطقهٔ امن، ارتباط شبکهٔ داخلی سازمان‌ها را با شبکهٔ اینترنت فراهم می‌کند.

شبکهٔDMZچگونه کار می‌کند؟

DMZ یک ناحیه مستقل بین شبکه داخلی و خارجی است که از دو فایروال استفاده می‌کند:

فایروال اول: ترافیک ورودی از اینترنت بهDMZ را کنترل می‌کند.

فایروال دوم: ترافیک بین DMZ و شبکه داخلی را کنترل می‌کند.

هر فایروال قوانین خاصی را برای جلوگیری از دسترسی‌های غیرمجاز تنظیم می‌کند:

کاربران اینترنت می‌توانند به سرویس‌های موجود درDMZ دسترسی داشته باشند اما به شبکه داخلی دسترسی ندارند.

شبکه داخلی می‌تواند به DMZ دسترسی داشته باشد، اما DMZ نمی‌تواند به شبکه داخلی نفوذ کند.

کاربردهای شبکه DMZ

DNS

سرورهای DNSدر DMZ قرار می‌گیرند تا درخواست‌های تبدیل نام دامنه به آدرس IPرا از کاربران خارجی و داخلی مدیریت کنند.

این سرورها باید از اینترنت قابل‌دسترس باشند، اما در عین حال نمی‌توانند به شبکه داخلی دسترسی مستقیم داشته باشند.

مثال: یک سرورDNSکه برای دسترسی به وب‌سایت‌های شرکت توسط کاربران خارجی استفاده می‌شود.

Web servers

وب سرورهایی که برای ارائه خدمات عمومی به کاربران اینترنتی طراحی شده‌اند، باید در محیطی امن قرار گیرند تا در صورت حمله، شبکه داخلی دچار آسیب نشود. DMZ این امکان را فراهم می‌کند که وب سرورها در این محیط قرار گیرند و دسترسی به آن‌ها محدود شود.

مثال: وب‌سایت‌های شرکت‌ها که برای عموم قابل‌دسترسی است.

Mail servers

سرورهای ایمیل نیاز به ارتباط با دنیای خارج دارند تا ایمیل‌ها ارسال و دریافت شوند. اگر این سرورها در شبکه داخلی قرار بگیرند، در معرض حملات سایبری هستند. در DMZ، سرور ایمیل قرار داده می‌شود تا در صورت حمله به سرور ایمیل، شبکه داخلی مصون بماند.

مثال: سرویس‌های ایمیلی که کاربران داخلی و خارجی از آن استفاده می‌کنند.

FTP

سرورهای FTPبرای اشتراک‌گذاری فایل‌ها بین کاربران داخلی و خارجی استفاده می‌شوند. این سرورها اگر در DMZقرار گیرند، کاربران خارجی بدون دسترسی به شبکه داخلی، می‌توانند فایل‌ها را آپلود یا دانلود کنند. این روش از دسترسی غیرمجاز به شبکه داخلی جلوگیری می‌کند.

مثال: بارگذاری و دانلود فایل‌های عمومی یا خصوصی توسط کاربران از طریق پروتکل FTP.

مزایا و معایب راه‌اندازی شبکه‌ی DMZ

مزایا

دسترسی عمومی امن‌تر: سرویس‌هایی که باید در دسترس عموم باشند، بدون قرار دادن شبکه داخلی در خطر، ارائه می‌شوند.

افزایش امنیت: با جداسازی سرویس‌های عمومی از شبکه داخلی، ریسک نفوذ به سیستم‌های داخلی کاهش می‌یابد.

کنترل ترافیک: امکان کنترل دقیق ترافیک ورودی و خروجی بین اینترنت و شبکه داخلی.

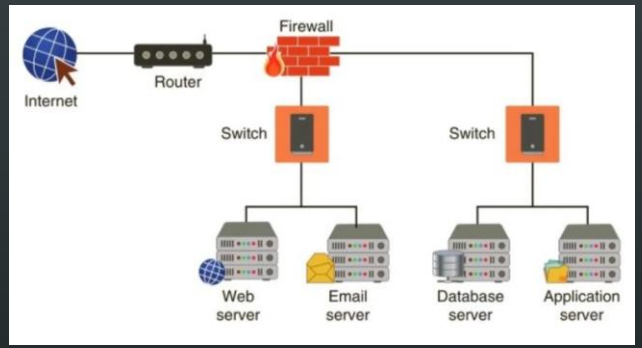
معایب

پیچیدگی بیشتر: ایجاد و مدیریت DMZ نیازمند پیکربندی دقیق و پیچیده است.

هزینه: نیاز به سخت‌افزارهای بیشتر (مثل فایروال‌های جداگانه) و زمان بیشتر برای مدیریت شبکه.

نقص امنیتی: اگر یک سرور در DMZهک شود، مهاجم می‌تواند تلاش کند به شبکه داخلی نفوذ کند.

طراحی و ساختار شبکه‌ی DMZ

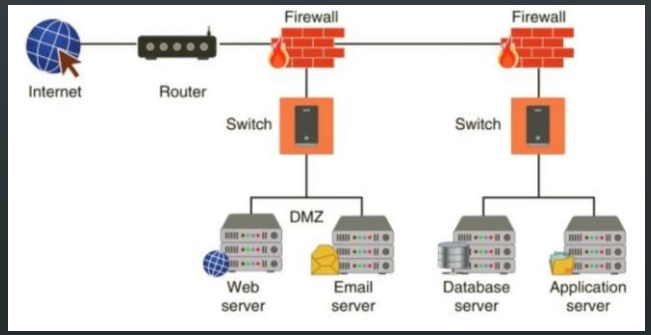


شبکه با فایروال منفرد

شبکهٔ DMZبا یک فایروال سه بخش اصلی دارد که شامل فایروال، سوئیچ‌ها و سرورها می‌شوند. علاوه بر این، شبکهٔ DMZ تک فایروال حداقل، نیاز به ۳ رابط شبکه دارد و ممکن است در بعضی ساختارها تعداد رابط‌های شبکه بیشتر باشد. رابط شبکه به‌طور خلاصه، به آنچه بین تجهیزات دیجیتالی ارتباط ایجاد می‌کند، گفته می‌شود. این رابط‌ها ممکن است نرم‌افزاری یا سخت‌افزاری باشند.

در شبکهٔDMZ با یک فایروال اولین رابط «شبکهٔ خارجی» است که اتصال اینترنت عمومی را به فایروال وصل می‌کند. دومین رابط «شبکه داخلی» را تشکیل می‌دهد و سومین رابط به شبکهٔ DMZ متصل می‌شود. قوانین مختلفی ترافیک داده‌های شبکه را برای دسترسی به DMZ بررسی و کنترل می‌کنند و اتصال به شبکه‌ی داخلی را محدود خواهند کرد.

طراحی و ساختار شبکه‌ی DMZ



شبکه با فایروال دوگانه

استقرار شبکهDMZبین دو فایروال اغلب روش ایمن‌تری است. اولین فایروال فقط اجازه‌ی عبور ترافیک خارجی به شبکهٔ DMZرا می‌دهد و فایروال دوم فقط اجازهٔ عبور ترافیک از DMZ به شبکه داخلی را می‌دهد. بنابراین، هکر برای نفوذ به شبکهٔ محلی سازمان باید از دو فایروال عبور کند.
طبق این ساختار، شبکهٔ DMZبا دو فایروال نیز از سه بخش تشکیل می‌شود: فایروال‌ها، شبکه DMZ و شبکهٔ محلی.
همچنین، سازمان‌ها می‌توانند برای افزایش ضریب ایمنی در بخش‌های مختلف شبکه ایستگاه‌های کنترل امنیتی مختلفی ایجاد کنند. به بیانی دیگر، به‌کارگیری سامانه‌های تشخیص نفوذ (IDS) و سامانه‌های جلوگیری از نفوذ (IPS) درون شبکه DMZ امکان مسدودسازی ترافیک هر داده‌ای را فراهم می‌کند و فقط به درخواست‌های پروتکل امن انتقال ابرمتن (HTTPS) روی لایه‌ی TCPو پورت ۴۴۳ اجازه‌ی عبور خواهد داد.

جمع‌بندی

شبکهٔ DMZنوعی حائل است که به‌عنوان لایه‌ی حفاظتی عمل می‌کند و می‌تواند ترافیک ورودی به شبکهٔ داخلی را فیلتر کند و با بررسی داده‌های ورودی و خروجی از نفوذ هکرها و نشت اطلاعات جلوگیری کند. در واقع، این فضا فرصتی ایجاد می‌کند که سامانه‌های تشخیص نفوذ و سامانه‌های جلوگیری از نفوذ بتوانند ابتکار عمل را در مواجه با مهاجمان به دست بگیرند.