دیوار آتش

فهرست

مقدمه

گسترش روزافزون استفاده از اینترنت در زمینه‌ها ی مختلف باعث شده است که سازمان‌ها، شرکت‌ها و مؤسسات، خواهان راه‌حل‌های مناسب برای رفع نگرانی‌های امنیتی خود باشند. یک راه‌حل برای مواجهه با مشکلات امنیتی شبکه، دیواره‌آتش یا حفاظ است. دیواره‌آتش یک ابزار نرم‌افزاری (یا ترکیبی با سخت‌افزار) است که برای امن‌سازی یک شبکهٔ در مقابل حملاتی که از خارج آن صورت می‌گیرد، استفاده می‌شود. هدف اصلی دیواره آتش، کنترل دسترسی شبک همورد حفاظت‌است. دیواره‌آتش با قرار گرفتن در محل اتصال یک شبکهٔ محلی به شبکهٔ سراسری، داده‌هایی را که از این مسیر در هر دو جهت عبور می‌کنند، بازرسی و ارزیابی می‌کند.

دیواره‌آتش‌ها به عنوان یک کنترل امنیتی پرکاربرد، سیر توسعه و پیشرفت زیادی در سال‌های اخیر داشته‌اند. اگرچه دیواره آتش‌ها در بدو تولد تنها شامل چندین مکانیسم امنیتی مشخص بودند، ولی امروزه مکانیسم‌های امنیتی زیادی توسط تولیدکنندگان دیواره‌آتش در این محصولات تعبیه می‌شود.

فصل ۱

ضرورت استفاده از دیواره آتش

به منظور جلوگیری از انجام حملات از میزبان‌های خارج از شبکهٔ محلی به میزبان‌ها و کارگزارهای داخل آن، استفاده از دیواره آتش ضروریاست. این کارگزارها عمدتاً به علت استفاده از خدمات ناامن قرارداد TCP/IP در معرض حمله قرار دارند. در یک محیط بدون دیواره آتش، امنیت شبکه وابسته به امنیت تک‌تک میزبان‌های داخل شبکه است و تمام میزبان‌ها باید برای دستیابی به سطح بالاتری از امنیت در مقایسه با حالت منفرد، با یکدیگر همکاری کنند. در نتیجه هر چه شبکهٔ محلی بزرگتر و تعداد میزبان‌های آن بیشتر باشد، نگهداری میزبان‌ها در سطح یکسانی از امنیت مشکل‌تر می‌شود. دیواره آتش می‌تواند با قرار گرفتن در سر راه اتصال شبکهٔ داخلی به شبکهٔ سراسری، امنیت یکسانی را در یک سطح بالا و قابل قبول برای کلیهٔ میزبان‌های شبکهٔ داخلی تأمین کند.

فواید استفاده از دیواره‌آتش

استفاده از دیواره‌آتش فواید زیادی در حوزه تأمین امنیت در یک شبکه به همراه دارد. فواید اصلی استفاده از دیواره‌آتش عبارتند از:

- حفاظت در مقابل خدمات ناامن: دیواره آتش می‌تواند به عنوان یک صافی برای خدمات اینترنت عمل کند و قراردادهایی را که امنیت شبکهٔ داخلی را به خطر می‌اندازند، از شبکهٔ محلی دور نگاه دارد.
- دسترسی کنترل‌شده به میزبان‌های داخلی: با استفاده از دیواره آتش می‌توان دسترسی به میزبان‌های داخلی را کنترل و مدیریت کرد. درنتیجه بعضی از میزبان‌ها می‌توانند از خارج از شبکهٔ محلی مورد دسترسی قرار گیرند در حالی‌که سایر میزبان‌ها غیرقابل دسترس هستند.
- امنیت متمرکز: استفاده از دیواره آتش می‌تواند برای یک سازمان بسیار مقرون‌به‌صرفه باشد چون اکثر نرم‌افزارهای امنیتی می‌توانند به‌جای این‌که روی کلیهٔ میزبان‌های داخلی قرار گیرند، تنها روی دیواره آتش قرار داده شوند.
- محرمانگی پیشرفته: منظور از محرمانگی، دور نگه‌داشتن کلیهٔ اطلاعات داخلی – حتی اگر محرمانه به نظر نرسند – از دسترس افراد غیرمجاز می‌باشد. هر اطلاعی که در ظاهر بی‌خطر به نظر می‌رسد، ممکن است حاوی داده‌هایی باشد که برای مهاجمان مفید است ومی تواند در انجام حملات آن‌ها را یاری دهد.
- رویدادنگاری و آمارگیری روی میزان استفاده و سوءاستفاده از شبکه: با توجه به این‌که تمامی دسترسی‌ها از شبکهٔ محلی به اینترنت و بالعکس از

دیواره‌آتش عبور می‌کنند، دیواره آتش می‌تواند آن‌ها را ثبت کند و آمار باارزشی را دربارهٔ آن‌ها در اختیار سرپرست شبکه قرار دهد.

- پیاده‌سازی سیاست‌های امنیتی سازمان: دیواره آتش روشی برای پیاده‌سازی و اجباری کردن رعایت سیاست های دسترسی به شبکه است.

ویژگی‌های دیواره‌آتش

مهمترین ویژگی یک دیواره‌آتش مقاومت آن در برابر حملات مختلفی است که به یک شبکه صورت می‌گیرد. این حملات می‌تواند به علل مختلفی صورت گیرد. بسیاری از حملات شناخته شده، در نتیجهٔ ضعف‌های امنیتی در قراردادها و خدمات اینترنت و قرارداد TCP/IP صورت می‌گیرند . بعضی دیگر از حملات، به‌خاطر عدم آموزش مناسب کاربران محلی پایه‌ریزی می‌شوند که معمول‌ترینِ آن‌ها، حملاتی است که برمبنای حدس گذرواژه قرار دارند. بعضی دیگر از حملات در نتیجه عدم دقت در پیکربندی خدمات مختلف شبکه ایجاد می‌شوند. دیواره‌آتش باید به گونه‌ای عمل کند که شبکهٔ محلی را در برابر کلیهٔ این حملات و سایر حملاتی که به یک شبکه صورت می‌گیرد، امن سازد.

تمامی بسته‌هایی که بین طرفین دیواره آتش ردوبدل می‌شود، باید از دیواره‌آتش رد شده و در آن بررسی شوند. درنتیجه این امکان وجود دارد که دیواره‌آتش باعث کند شدن سرعت انتقال اطلاعات شود و یک گلوگاه در محل دیواره‌آتش ایجاد شود. در نتیجه طراحی دیواره‌آتش باید به گونه‌ای باشد که کارایی بالایی داشته باشد و کمترین تاثیر را در سرعت انتقال اطلاعات بین شبکهٔ محلی و شبکهٔ سراسری داشته باشد.

طرز کار دیواره‌آتش باید به گونه‌ای باشد که در کنار اعمال کنترل‌های لازم روی اطلاعات، از دید کاربران شبکه مخفی باشد. به این معنی که دیواره آتش –تا

زمانی که سیاست امنیتی سازمان ایجاب نکرده است - باید کمترین محدودیت را در دسترسی کاربران به امکانات و خدمات شبکه پدید بیاورد.

مشکل اصلی در هنگام استفاده از دیواره آتش در یک سازمان، مشکل ارائهٔ خدمات اطلاعاتی نظیر خدمت تورجهان‌گستر و خدمت انتقال فایلِ بدون نام [1] به کاربران خارج از شبکهٔ محلی است. در این نوع خدمات هیچ نوع کنترلی بر روی کاربرانی که به این خدمات دسترسی پیدا می‌کنند اعمال نمی‌شود و از دید این خدمات، کلیهٔ کاربران شبکهٔ سراسری ، کاربران مجاز شناخته می‌شوند . در صورتی‌که کارگزارهای این خدمات در ناحیهٔ پشت دیواره آتش قرار گیرند، راه نفوذ به شبکهٔ محلی باز می‌شود. برای این‌که در کنار دیواره آتش بتوان این نوع خدمات را نیز ارائه کرد، می‌توان از یک هم‌بندی دیگر استفاده کرد. در این هم‌بندی شبکه به سه ناحیه تقسیم می‌شود:

- بخش حفاظت شده: در این بخش میزبان‌هایی از شبکهٔ محلی که باید بوسیلهٔ دیواره‌آتش محافظت شوند، قرار می‌گیرند.
- بخش DMZ[2]: این بخش حد فاصل میان دیواره آتش و مسیریاب دسترسی به شبکه است. میزبان‌هایی از شبکهٔ محلی که نیاز به حفاظت توسط دیواره آتش ندارند، در این ناحیه قرار می‌گیرند. کارگزارهای اطلاعاتی نظیر کارگزار تورجهان‌گستر و کارگزار انتقال فایلِ بدون‌نام در این ناحیه قرار داده می‌شوند و به این ترتیب دسترسی نامحدود به آن‌ها، میزبان‌های موجود در بخش حفاظت‌شده را با هیچ خطری مواجه نمی‌کند.
- بخش خارجی: این بخش شامل کلیهٔ میزبان‌های اینترنت می‌شود که در بیرون مسیریاب دسترسی به شبکه قرار دارند.

---

[1] Anonymous FTP
[2] Demilitarized Zone

فصل ۲

مکانیسم‌های امنیتی در دیواره‌آتش

در ادامه به مهمترین مکانیسم ها تعبیه شده در یک فایروال مناسب اشاره شده است.

بسته‌صافی

یکی از مولفه‌های اصلی یک حفاظ، بسته‌صافی است. بسته‌صافی وظیفهٔ بازرسی بسته‌ها در لایه‌های پایین‌تر از لایهٔ کاربرد را به عهده دارد. این بازرسی بر روی سرآیندهای لایه‌های شبکه و انتقال صورت می‌گیرد. به این ترتیب بسته‌هایی که به دیواره‌آتش می‌رسند، ابتدا در بسته‌صافی بازرسی می‌شوند و سپس در صورت لزوم به دروازه‌های کاربرد در لایهٔ کاربرد و یا مکانیسم‌های امنیتی دیگر تحویل داده می‌شوند.

ترجمهٔ آدرس

با توجه به اینکه نمی‌توان جایگزینی IPV6 به جای IPV4 را در مدت کوتاهی انجام داد، باید چندین سال از IPV4 استفاده کرد و به دنبال راه‌حل‌هایی کوتاه‌مدت برای مشکل محدودیت فضای آدرس IP بود.

یک روش مناسب این است که زمانی که بسته‌ها قرار است به اینترنت ارسال شوند، آدرس‌های داخلی آن‌ها به آدرس‌های معتبر تبدیل شود. از آنجا که در هر زمان تعداد میزبان‌هایی از شبکهٔ داخلی که با اینترنت تبادل دارند به مقدار قابل ملاحظه‌ای کمتر از کل تعداد میزبان‌ها است، این روش باعث صرفه‌جویی در تعداد آدرس مصرفی می‌شود. چون این روش در لایهٔ IP صورت می‌گیرد مستقل از کاربرد است و در این لایه هیچ‌گونه دادهٔ مربوط به کاربرد ذخیره نمی‌شود. در واقع عمل ترجمهٔ آدرس کاملاً از دید لایهٔ کاربرد مخفی خواهد بود. به این روش «ترجمهٔ آدرس شبکه[1]» یا به اختصار NAT گفته می‌شود.

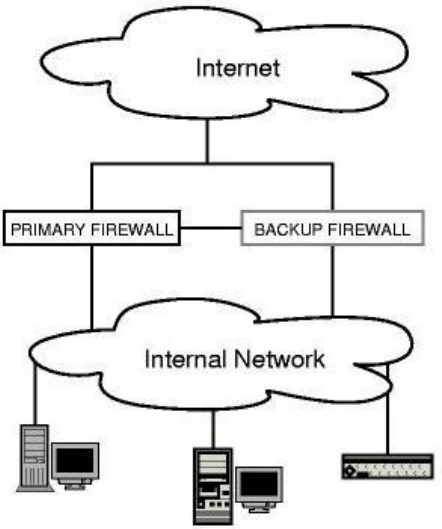
دسترس‌پذیری بالا[2]

در اکثر شبکه‌ها، دیواره آتش یک نقطه شکست است، بدین معنی که اگر دیواره آتش از کار بیافتد کاربران داخلی نمی‌توانند وب را پیمایش کنند، وب‌سایت برای دنیای بیرون از کار می‌افتد و مشکلات متعدد دیگری رخ می‌دهد.

برای رفع این مشکلات لازم است که حداقل دو دیواره آتش به صورت موازی در توپولوژی شبکه در نظر گرفته شود. در این حالت تمام ترافیک از دیواره‌آتش اصلی می‌گذرد وقتی آن دیواره آتش از کار می‌افتد دیواره آتش پشتیبان خود را به عنوان دیواره‌آتش اصلی معرفی می‌کند، تمام اتصالات موجود حفظ می‌شود و ترافیک شبکه ادامه می‌یابد مانند این که هیچ اتفاقی در سیستم رخ

[1]Network Address Translation
[2]High Availability

نداده است. شکل۱ توپولوژی یک شبکه با دو دیواره آتش برای پیاده‌سازی دسترس‌پذیری بالا را نشان می‌دهد.



شکل۱ دو دیواره‌آتش در توپولوژی شبکه

این پیکربندی نه تنها قابلیت اعتماد شبکه را افزایش می‌دهد، بلکه با روش های ظریفی امنیت را نیز افزایش می‌دهد. در این حالت یک دیواره‌آتش را می‌توان از سیستم خارج نمود، آن را بروزرسانی کرد، وصله‌های امنیتی آن را اعمال نمود بدون این‌که مشکلی در سیستم ایجاد شود.

مدیریت پهنای باند

مدیریت پهنای باند تکنیکی است که با استفاده از آن می‌توان ترافیک شبکه را براساس سیاست‌های شبکه‌ای بین سرویس‌های مختلف شبکه و کاربران اولویت‌دهی، توزیع و تنظیم نمود. با استفاده از این تکنیک می‌توان از ترافیک‌های شبکه با پهنای باند بالا که باعث می‌شود تا ترافیک‌های شبکه‌ای دیگر مانند Webغیرقابل استفاده شوند، جلوگیری نمود و به آن‌ها اولویت پایین‌تری داد.

همچنین می توان با محدود نمودن بعضی از انواع ترافیک شبکه از حملات DoS جلوگیری نمود.

شبکه خصوصی مجازی

در حال حاضر، ابزارهای گوناگونی برای پیاده‌سازی شبکه‌های خصوصی مجازی وجود دارند که یکی از آن‌ها استفاده از دیواره آتش است. اهمیت پیاده‌سازی شبکه‌های خصوصی مجازی به گونه‌ای می‌باشد که دارا بودن چنین قابلیتی در حفاظ، جزء وظیفه‌مندی‌های اساسی یک دیواره‌آتش تلقی می‌شود.

سیاست امنیتی در دیواره‌آتش

یکی از پارامترهای اصلی در ارزیابی و انتخاب یک دیواره آتش نحوه تعریف سیاست‌های امنیتی در آن می‌باشد. بدیهی است تعریف اشتباه سیاست‌های امنیتی در یک محصول نه‌تنها سیاست‌های امنیتی سازمان را برآورده نمی‌کند بلکه می‌توان منجر به ایجاد آسیب‌پذیری امنیتی نیز شود. به همین منظور یکی از موارد اصلی که تولید کنندگان به آن توجه می‌کنند، ارائه یک مدل مناسب برای مدیران سیستم،جهت تعریف سیاست‌های امنیتی سازمانی روی دیواره‌آتش است.

با توجه به حضور مکانیسم‌های امنیتی متنوع در دیواره‌آتش‌ها، سیاست‌های امنیتی نیز متنوع و بعضاً پیچیده خواهند شد. برای نمونه در حالتی که یک دیواره‌آتش شامل بازرسی حالت‌مند بسته‌ها و ترجمه آدرس باشد، بدیهی است که سیاست‌های تصفیه بسته‌ها در این دیواره آتش متاثر از سیاست‌های ترجمه آدرس خواهد بود. همچنین در شرایطی که مکانیسم‌هایی نظیر تشخیص هویت، VPN و رویدادنگاری نیز وجود داشته باشند، بر پیچیدگی سیاست‌های امنیتی افزوده می‌شود.

مدیریت دیواره‌آتش

با وجود این‌که دیواره‌آتش معمولاً به عنوان یک عنصر حیاتی در امنیت شبکه مورد استفاده قرار می‌گیرد ولی در صورت پیکربندی نادرست، دیواره آتش می‌تواند خود منشأ آسیب‌پذیری شود. به‌طور معمول نیز اولین نقطه مورد تهاجم در شبکه‌ها، دیواره آتش‌ها می‌باشند چرا که یک مهاجم با از کاراندازی دیواره‌آتش می‌تواند به دیگر نواحی شبکه نیز دسترسی داشته باشد. همچنین باید توجه داشت که دیواره‌آتش در نقطه عبور کل ترافیک شبکه قرار می‌گیرد و باید بتواند تمامی این ترافیک را بازرسی نماید. بنابراین پیکربندی اشتباه روی دیواره‌آتش می‌تواند دسترسی شبکه را مختل نماید. در این بخش تلاش می‌شود مکانیسم‌های مدیریتی یک دیواره‌آتش سازمانی شرح داده می‌شوند.

- واسط‌های مدیریتی

دیواره‌آتش‌ها به‌طور معمول به‌صورت محلی یا راه دور پیکربندی می‌شوند. برای پیکربندی محلی یک دیواره آتش می‌تواند از طریق اتصال به کنسول یا پورت سریال اقدام نمود. برای مدیریت راه دور نیز می‌توان از طریق واسط گرافیکی و یا Shell راه دور مدیریت را انجام داد.

استفاده از قراردادهایی نظیر Telnet و HTTP برای مدیریت راه دور یک دیواره‌آتش می‌تواند مخاطرات امنیتی مدیریت را بسیار بالا ببرد. در این قراردادها ملاحظات امنیتی لازم نظیر محرمانگی و جامعیت در نظر گرفته نشده است.

- تشخیص هویت و کنترل دسترسی

مستقل از نوع واسط مدیریتی و امنیت کانال ارتباطی آن، تشخیص هویت و کنترل دسترسی از عناصر اصلی مدیریت امن دیواره آتش می‌باشد.. در یک

سازمان ممکن است چندین مدیر شبکه وجود داشته باشد که هر کدام باید بخشی از دیواره آتش را بتوانند مدیریت نمایند. همچنین مدیران مختلف ممکن است سطوح دسترسی متفاوتی در مدیریت دیواره‌آتش در اختیار داشته باشند.

روش معمول تشخیص هویت در دیواره آتش‌ها استفاده از روش username/password است. روش‌های پیشرفته‌تری برای تشخیص هویت نظیر روش‌های مبتنی بر توکن‌های امنیتی نیز برای دیواره آتش‌ها قابل استفاده می‌باشد. برای یکپارچه نمودن مکانیسم‌های تشخیص هویت کاربران مدیریتی در دیواره آتش با مکانیسم‌های موجود در سازمان، از کارگزاران تشخیص هویت نظیر Radius، LDAP و Kerberos نیز می‌توان استفاده نمود. در این شرایط مدیریت کاربران و نگهداری اطلاعات تشخیص هویت آن‌ها توسط کارگزار دیگری در شبکه انجام خواهد شد و دیواره آتش به‌عنوان یک کارفرما، درخواست‌های خود را به آن کارگزار ارسال می‌نماید.

- رویدادنگاری

یکی از روش های اصلی در دیواره آتش رویدادنگاری یا ثبت رخدادها است. به‌طور معمول دیواره آتش‌ها با دسته‌بندی رویدادها، مکانیسم‌هایی را برای تشخیص و ثبت هر رویداد استفاده می‌کنند.

- تحلیل‌گر رویداد

تحلیل‌گر رویداد [1] ابزاری است که اقدام به تحلیل بر روی سطوح مختلف پیغام‌های رویدادنگاری می‌نماید. خروجی‌های آماری نیز از جمله قابلیت‌های این ابزار است.

[1] Log Analyzer

- یکسان‌سازی زمان

زمان برای دیواره آتش‌های مبتنی بر قوانین زمانی، عامل مهمی محسوب می‌شود. یک دیواره آتش باید با تمامی ماشین‌های شبکه همزمان بوده تا در زمان‌های تعریف شده بتواند قواعد را بر روی شبکه و ماشین‌های آن اعمال کند. همچنین در صورت نیاز به رویدادنگاری و گزارش گیری از فعالیت ماشین‌های شبکه لازم است که دیواره آتش با تمامی ماشین‌های شبکه همزمان بوده تا با رخ دادن هر رویداد زمان حقیقی و دقیق آن‌را ثبت کند و برای مدیر گزارش صحیح و دقیقی را تهیه نماید.

- تهیه نسخه پشتیبان

در مورد پیکربندی دیواره‌آتش به عنوان یک ابزار شبکه‌ای تهیه نسخه پشتیبان از اهمیت بالایی برخوردار است. به‌طور کلی پیشنهاد می‌شود قبل از هر تغییری در پیکربندی ابزارهای شبکه‌ای، یک نسخه پشتیبان از پیکربندی جاری تهیه شود. برای این منظور دیواره آتش‌ها امکاناتی را برای تهیه نسخ پشتیبان در اختیار مدیران سامانه قرار می‌دهند.

- نظارت

یکی از امکانات مدیریتی دیواره آتش، نظارت بر ترافیک شبکه و تهیه گزارشات نظارتی برای مدیر سامانه است. به‌طور معمول مدیران شبکه علاقه‌مند به نظارت بر نحوه استفاده از ترافیک شبکه، میزان پهنای باند مصرفی، شناسایی رخدادهای مشکوک و آگاهی از وضعیت‌های بحرانی هستند. دیواره‌آتش‌ها ابزارهای مناسبی برای تهیه تمامی این گزارشات هستند. نوع اعلان به مدیر از طریق پست الکترونیک، رویدادنگاری و یا نمایش پیغام در کنسول قابل پیکربندی است.

دیواره‌آتش‌ها علاوه بر تهیه گزارشات آماری و نظارتی بر شبکه، باید گزارشات نظارتی بر عملکرد سامانه دیواره آتش نیز ارائه نمایند. برای نمونه مدیر سامانه باید از میزان درصد CPU استفاده شده، تعداد اتصالات همزمان، میزان درصد حافظه مصرفی و این چنین موارد اطلاع داشته باشد.

- پیکربندی

مهمترین وظیفه مدیر دیواره آتش، پیکربندی آن است. یکی از نقاط ضعف دیواره‌آتش‌ها این است که عملکرد آن‌ها کاملاً وابسته به پیکربندیی است که مدیر آن تعریف نموده است و معمولاً پیکربندی از پیش تعریف شده‌ای نمی‌توان یافت که قابل اعمال به تمامی شبکه‌ها باشد. پیکربندی یک دیواره‌آتش شامل تنظیم مکانیسم‌های امنیتی مورد نیاز سازمان است.

تعریف سیاست امنیتی در دیواره آتش، حساس‌ترین بخش پیکربندی آن است. در صورتی که سیاست امنیتی تدوین شده‌ای برای پیکربندی دیواره‌آتش وجود نداشته باشد، رویه پیکربندی دیواره آتش در شبکه معمولاً طولانی خواهد شد. به‌طور معمول مدیر دیواره آتش باید تلاش کند سیاست‌های کلان سازمان را در قالب ابزارهای پیکربندی در دیواره آتش پیاده‌سازی نماید.

فصل ۳

معماری و جایگاه دیواره‌آتش در شبکه

مستقل از طراحی و پیاده‌سازی یک دیواره آتش، چگونگی نصب و راه‌اندازی آن یک فرایند پیچیده است. این فرایند کاملاً به ساختار و توپولوژی شبکه بستگی دارد و همین امر بر پیچیدگی فرایند نصب می‌افزاید.

معماری دیواره‌آتش در شبکه

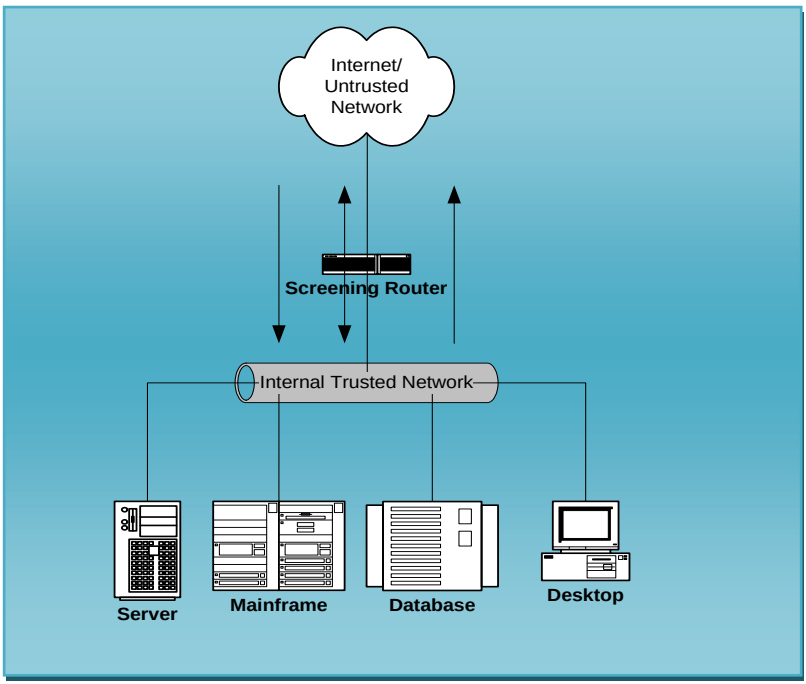
یکی از مهمترین مباحث در انتخاب و به‌کارگیری دیواره آتش‌ها، انتخاب یک معماری مناسب شبکه‌ای با حضور دیواره‌آتش است. به‌عبارت دیگر باید مشخص شود که دیواره‌آتش (ها) در چه نقاطی از شبکه باید قرار گیرند.

به‌طور کلی در طراحی توپولوژی شبکه برای حضور دیواره‌آتش باید اصول زیر مورد توجه قرار گیرد.

- سادگی طرح
- هر ابزاری باید برای اجرای وظیفه خودش استفاده شود
- امنیت در تمامی ابعاد مورد توجه قرار گیرد (اصل دفاع در عمق)
- به حملات داخلی توجه شود

در ادامه معماری‌های موجود برای قرارگیری دیواره آتش در شبکه شرح داده می‌شود. این معماری‌ها به‌ترتیب از لحاظ امنیتی ارائه می‌شوند و معماری‌های نهایی نیازمندی‌های امنیتی بیشتری را پوشش می‌دهند.

برای شرح بهتر معماری‌های دیواره آتش در شبکه، فرض می‌شود یک شبکه با تعدادی کارگزار شبکه، Database، Mainframe و کارفرما وجود دارد. در هر مرحله تعدادی نیازمندی امنیتی برای این شبکه ارائه شده و براساس آن دیواره‌آتش(های) مورد نیاز آن شبکه شرح داده می‌شود. توپولوژی این شبکه بدون حضور دیواره‌آتش در شکل۳ نشان داده شده است. همان‌طور که در این شکل دیده می‌شود، شبکه با استفاده از یک مسیریاب به اینترنت متصل است. این مسیریاب از قابلیت‌های معمول مسیریاب‌ها برای فیلترینگ بسته‌ها نیز برخوردار است.



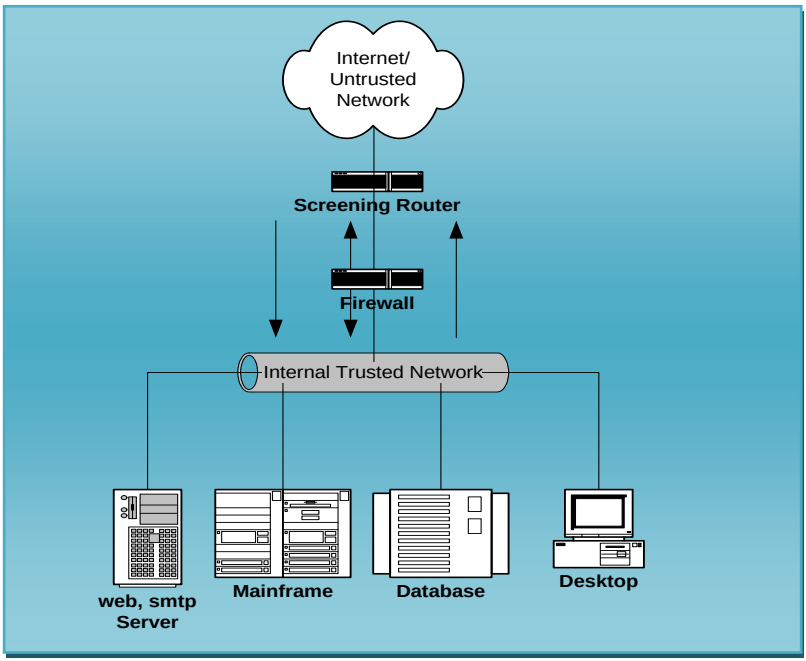
شکل۳ توپولوژی شبکه نمونه بدون حضور دیواره‌آتش

دیواره‌آتش ساده

کنترل‌های اعمال شده توسط مسیریاب برای یک شبکه با حساسیت امنیتی بالا کافی نیست، زیرا مسیریاب‌ها معمولاً کنترل‌های محدودی روی بسته‌ها انجام می‌دهند، قابلیت کنترل حالت‌مند را ندارند و قابلیت‌های امنیتی دیگر را نیز ارائه نمی‌دهند. یکی از چهار اصل ارائه شده برای طراحی دیواره آتش در شبکه، تخصیص وظایف خاص هر ابزار به آن است. بنابراین باید تلاش شود که یک مسیریاب تنها مسئولیت مسیریابی را برعهده داشته باشد، هر چند که می‌توان با پیکربندی لیست‌های کنترلی روی مسیریاب سطح امنیتی را بالاتر برد. با توجه به

این اصل در توپولوژی امن‌تر از یک دیواره آتش برای محافظت شبکه داخلی و کارگزاران از تهدیدات اینترنتی استفاده می‌شود.

در این طرح دیواره آتش ناظر بر کل ترافیک انتقالی بین شبکه داخلی و اینترنت خواهد بود و امکان کنترل کامل روی این دیواره آتش فراهم است. به‌طور کلی در این مدل شبکه به دو ناحیه Trust (شبکه داخلی) و Untrust (شبکه اینترنت) تقسیم می‌شود. عملیات جداسازی این دو ناحیه با حضور دیواره آتش به‌طور کامل انجام می‌شود. بدیهی است در این مدل، کارگزاران و کارفرمایان همگی در ناحیه امنیتی Trust قرار دارند که هیچ کنترلی روی ارتباطات بین آن‌ها وجود ندارد. بدیهی است هر دیواره آتش تنها می‌تواند ترافیک انتقالی بین نواحی مختلف را بازرسی نماید و ترافیک داخل یک ناحیه توسط دیواره آتش قابل بررسی نیست.



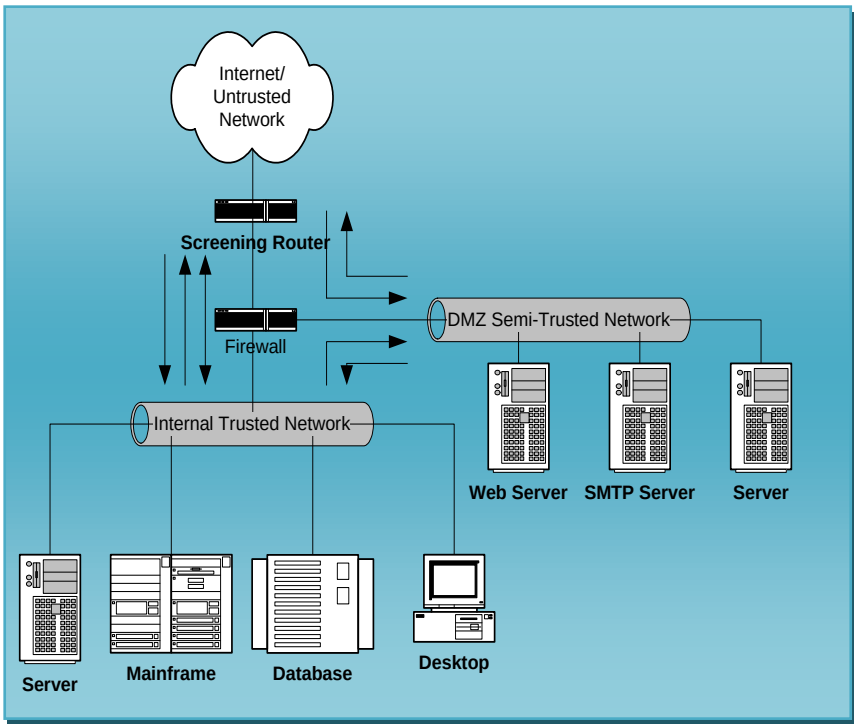
شکل۴ استفاده از یک دیواره‌آتش ساده با دو پورت در شبکه

دیواره‌آتش با چند پورت

در بسیاری از موارد کارگزارانی در شبکه یک سازمان وجود دارند که از لحاظ امنیتی دارای سطح یکسانی نسبت به دیگر کارگزاران و یا کارفرمایان نیستند. برای نمونه برخی از کارگزاران نظیر کارگزار وب، از طریق اینترنت قابل رویت هستند. از طرف دیگر برخی از کارگزاران تنها توسط کاربران داخلی مورد استفاده قرار می‌گیرند. در یک طرح امن شبکه، سطح امنیتی این کارگزاران با یکدیگر متفاوت است.

در صورتی که در یک شبکه برخی از سامانه ها دارای سطح امنیتی مختلفی با سامانه های دیگر باشند، باید آن‌ها را در ناحیه امنیتی جداگانه‌ای قرار داد. به‌عبارت دیگر سامانه هایی که از لحاظ امنیتی در سطح یکسانی قرار دارند در ناحیه امنیتی مشابه‌ای قرار می‌گیرند. با این توضیح در شبکه می‌توان نواحی امنیتی مختلف را طراحی نمود و باید راهکار امنیتی مناسبی برای استفاده از دیواره آتش در بازرسی ترافیک بین این نواحی ارائه نمود. همچنین نیازمندی جداسازی نواحی امنیتی نیز باید پوشش داده شود. یک روش معمول برای برآوردن این نیازمندی‌ها استفاده از دیواره‌آتش با چند پورت می‌باشد که هر پورت بتواند یک ناحیه امنیتی را پشتیبانی نماید. برای نمونه در شکل۵ از یک دیواره آتش با ۳ پورت استفاده شده است که توانایی جداسازی ۳ ناحیه امنیتی Untrust، DMZ و Trust را خواهد داشت.

راه‌حل ارائه شده نیازمندی‌ها، جداسازی نواحی و بازرسی ترافیک بین نواحی را پوشش می‌دهد. نکته قابل توجه این است که در صورتی که به دلیل یک ضعف امنیتی دیواره آتش مورد تهاجم قرار گیرد، تمامی نواحی امنیتی تهدید



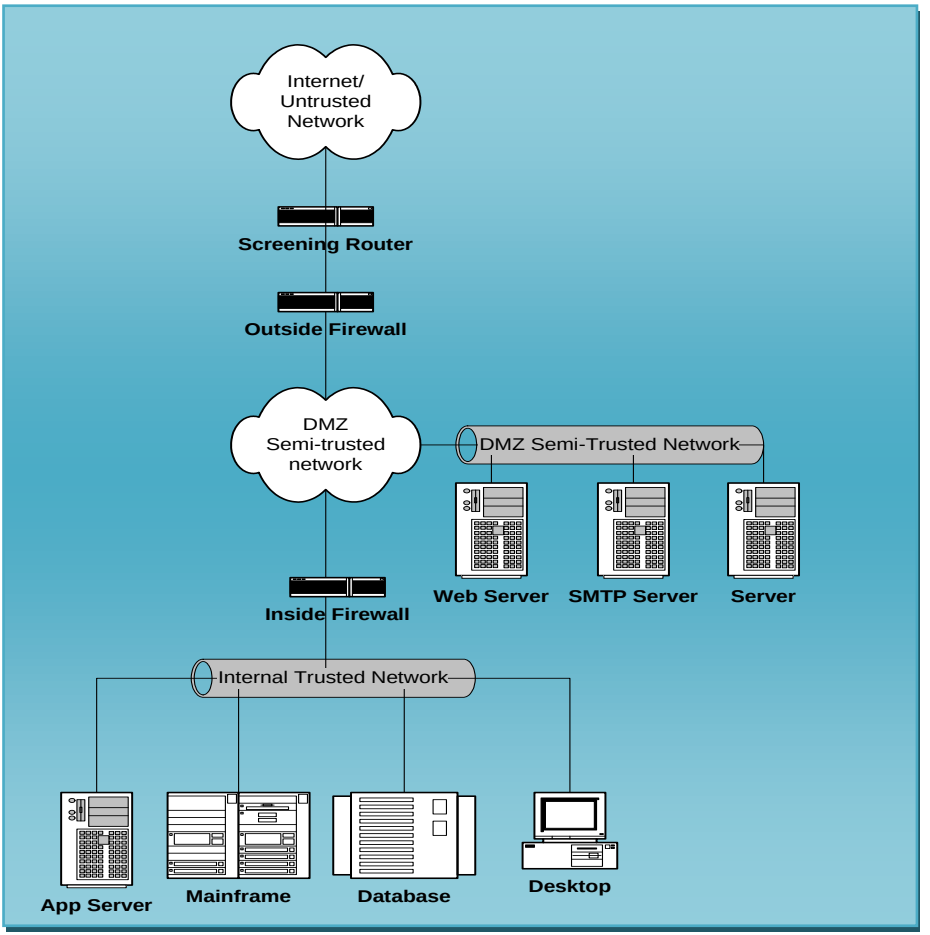
می‌شوند. این در حالی است که حساسیت امنیتی شبکه داخلی نسبت به DMZ بسیار بالاتر است و از طرفی تهدیدات برای ناحیه DMZ نیز بالاتر خواهد بود و همین تهدیدات میزان مخاطره روی دیواره‌آتش را افزایش می‌دهد.

شکل۵ استفاده از یک دیواره‌آتش با چند پورت در شبکه

استفاده از چند دیواره آتش

در توپولوژی ارائه شده در شکل۵ تنها به یک دیواره‌آتش اکتفا شده است. بنابراین در صورتی که این دیواره آتش مورد تهاجم قرار گیرد، کل نواحی امنیتی در خطر خواهند بود. در صورت اختلاف زیاد سطح امنیتی بین نواحی می‌توان از چندین دیواره آتش برای عملیات جداسازی استفاده نمود. در این شرایط با از دست رفتن یک دیواره آتش، تنها تعدادی از نواحی امنیتی که مستقیماً به آن متصل بوده‌اند در خطر خواهند بود و نواحی دیگر هنوز توسط دیواره آتش‌هایی محافظت می‌شوند.

با فرض این که شبکه سازمان دارای ۳ ناحیه اینترنت، DMZ و شبکه داخلی باشد، می‌توان از ایده چند دیواره آتش استفاده نمود. توپولوژی جدید برای این شبکه در شکل ۶ آورده شده است. در این توپولوژی نواحی DMZ و اینترنت (Untrust) توسط یک دیواره آتش دو پورتی و نواحی شبکه داخلی (Trust) و DMZ توسط دیواره آتش دو پورتی دیگری جدا شده‌اند. بنابراین با از دست رفتن دیواره آتش اول ناحیه شبکه داخلی تحت تاثیر قرار نمی‌گیرد.



شکل۶ استفاده از دو دیواره‌آتش با چند پورت در شبکه

ناحیه شبکه داخلی شامل کارگزاران و کارفرمایانی است که از طریق اینترنت رویت نمی‌شوند. این ناحیه در برخی شبکه‌ها می‌تواند به چند ناحیه دیگر تقسیم شود. برای نمونه شبکه داخلی می‌تواند شامل نواحی امنیتی زیر باشد.

- ناحیه کارفرمایان
- ناحیه کارگزاران داخلی
- ناحیه Databaseها
- ناحیه سیستم‌های Mainframe

برای شناخت نواحی امنیتی موجود باید از دو ایده جداسازی ارتباطات و اطلاعات استفاده نمود. همچنین با توجه به درجه حساسیت امنیتی هر سامانه اطلاعاتی می‌توان نواحی امنیتی را شناسایی نمود. بعد از شناسایی این نواحی می‌توان برای جداسازی بین آن‌ها از دیواره‌آتش استفاده نمود. یکی از نکات مهم در این مدل هزینه پیاده‌سازی آن است. معمولاً در شرایطی که حساسیت امنیتی نواحی بسیار بالا باشد، می‌توان از چندین دیواره‌آتش استفاده نمود.

با گسترش تکنولوژی اطلاعات، آسیب‌پذیری‌ها و نقاط ضعف امنیتی بیشتری در سامانه های اطلاعاتی کشف می‌شود و اطلاعات در معرض مخاطرات امنیتی بیشتری قرار می‌گیرد. از این رو فناوری حفاظت از اطلاعات نیز پیچیده‌تر خواهد شد و کنترل‌های امنیتی بیشتری باید در سامانه های اطلاعاتی لحاظ شود.