ফায়ারওয়াল

কমপিউটার ও নেটওয়ার্কের নিরাপত্তা বেষ্টনী

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

ফায়ারওয়াল শব্দটির সাথে আমরা কম-বেশি সবাই পরিচিত। এটি বাইরের আক্রমণ থেকে এক বা একাধিক কমপিউটারকে রক্ষা করার জন্য হার্ডওয়্যার আর সফটওয়্যারের মিলিত সমন্বয়ে কাজ করে। যদিও ফায়ারওয়ালের সবচেয়ে বেশি ব্যবহার লোকাল এরিয়া নেটওয়ার্কের ক্ষেত্রে, তবে এখন এটি ক্লায়েন্ট কমপিউটারেও ব্যবহার হয়। তথ্য রক্ষাই এর মূল কাজ। এই বিশেষ নিরাপত্তা ব্যবস্থায় এক নেটওয়ার্ক থেকে আরেক নেটওয়ার্কে ডাটা প্রবাহ নিয়ন্ত্রণ করা যায়। দুই নেটওয়ার্কের মাঝে এই ফায়ারওয়াল থাকে। যাতে এক নেটওয়ার্ক থেকে আরেক নেটওয়ার্কে কোনো ডাটা পরিবাহিত হলে সেটিকে অবশ্যই ফায়ারওয়াল অতিক্রম করতে হয়। ফায়ারওয়াল তার নিয়ম অনুসারে সেই ডাটা নিরীক্ষা করে দেখে, যে ডাটার ওই গন্তব্যে যাওয়ার অনুমতি আছে। তা না হলে সেটিকে ওখানেই আটকে রাখে বা পরিত্যাগ করে।

ফায়ারওয়ালযুক্ত ডিভাইসগুলো তুলনামূলকভাবে বেশি সুরক্ষিত। কেননা, সেসব ডিভাইসের ক্ষেত্রে ফায়ারওয়ালের নিয়মগুলোই আসলে নির্ধারণ করে দেয়, কোন ট্রাফিক বা ডাটাগুলো ডিভাইসের সাথে যোগাযোগ করতে পারবে এবং কোনগুলো পারবে না।

কমপিউটারে যে কারণে ফায়ারওয়াল যুক্ত করা থাকে

বেশিরভাগ মানুষই এখন তাদের ঘরে রাউটার ব্যবহার করে থাকে, যাতে তারা তাদের বিভিন্ন ডিভাইসে ইন্টারনেট শেয়ার করতে পারে। যাই হোক, আগে এমন একটা সময় ছিল যখন মানুষ ইন্টারনেটে যুক্ত হওয়ার জন্য তাদের ডিভাইসটিকে সরাসরি ইথারনেট ক্যাবল অথবা ডিসিএল মডেমের সাথে যুক্ত করত। যেগুলো ইন্টারনেটের সাথে সরাসরি যুক্ত, সেগুলোর সাধারণত publicly addressable IP থাকে। অন্য কথায়, যেকোনো মানুষ ইন্টারনেট থেকে ওইসব কমপিউটারকে অ্যাক্সেস করতে পারবে। যে ধরনের নেটওয়ার্ক সার্ভিসই আপনি publicly addressable IP কমপিউটারে ব্যবহার করেন না কেন, উইন্ডোজের ফাইল ও প্রিন্টার শেয়ার সার্ভিস, রিমোট ডেস্কটপ এবং অন্যান্য ফিচার– এসবই অন্য কোনো ইন্টারনেট ব্যবহারকারী ইন্টারনেটের মাধ্যমে অ্যাক্সেস করতে পারবেন।

উইন্ডোজের ক্ষেত্রে অরিজিনাল উইন্ডোজ এক্সপিতে বিল্টইন ফায়ারওয়াল ছিল না। লোকাল নেটওয়ার্কের বিভিন্ন সুবিধার জন্য তখন উইন্ডোজ এক্সপিতে ছিল না কোনো ফায়ারওয়াল এবং কমপিউটার সরাসরিই ইন্টারনেটের সাথে যুক্ত হতে পারত। যার ফলে সে সময় উইন্ডোজ এক্সপি ব্যবহারকারীদেরকে বড় ধরনের বিপর্যয়ের মুখোমুখি হতে হয়েছিল। ইন্টারনেটে যুক্ত হওয়ার কয়েক মিনিটের মধ্যেই কমপিউটারগুলো বিভিন্ন ধরনের ম্যালওয়্যার ও ভাইরাসে আক্রান্ত হতে থাকে। যার পরিপ্রেক্ষিতে সূচনা হয় 'The Windows Firewall'-এর। এটি সর্বপ্রথম উইন্ডোজ এক্সপি সার্ভিসপ্যাক ২-এর সাথে বিল্টইনভাবে রিলিজ হয়।

বিল্টইন ফায়ারওয়ালের মাধ্যমে ওইসব নেটওয়ার্ক সার্ভিসগুলো বন্ধ হয়ে যায় এবং সব ধরনের ইন্টারনেট কানেকশন রিসিভ করার পরিবর্তে ফায়ারওয়াল সিস্টেম সব কানেকশন ড্রপ করতে শুরু করে, সেগুলো কি না নির্দিষ্টভাবে রিসিভ করার ক্ষেত্রে কনফিগার করা থাকে।

এটিই পরবর্তী সময়ে অন্যান্য ইন্টারনেট ব্যবহারকারীকে আরেকজনের কমপিউটারে অনিয়ন্ত্রিত অ্যাক্সেস প্রতিরোধ করতে থাকে। শুধু তাই নয়, আপনার লোকাল নেটওয়ার্কের অন্যান্য কমপিউটার থেকে আসা নেটওয়ার্ক সার্ভিসের অ্যাক্সেসও কন্ট্রোল করে ফায়ারওয়াল। এর জন্যই যখন আপনি অজ্ঞাত কোনো একটি নেটওয়ার্কের সাথে যুক্ত হন, এটি আপনাকে জিজ্ঞেস করে– এটি কোন ধরনের নেটওয়ার্ক? যদি আপনি হোম নেটওয়ার্কের সাথে যুক্ত থাকেন, তাহলে ফায়ারওয়াল ওইসব সার্ভিসের জন্য কমপিউটার অ্যাক্সেস করার অনুমতি দেবে এবং যদি পাবলিক নেটওয়ার্কের সাথে যুক্ত থাকেন, তাহলে ফায়ারওয়াল ওইসব সার্ভিসকে কমপিউটার অ্যাক্সেস করার অনুমতি দেবে না।

এমনকি যদি কোনো নেটওয়ার্ক সার্ভিস ইন্টারনেটের সাথে যুক্ত নাও থাকে, তারপরও এটি সম্ভব যে সেই সার্ভিসের নিজের মধ্যেই কিছু সিকিউরিটি ত্রুটি রয়েছে এবং এ ধরনের ত্রুটির জন্য বিশেষভাবে ক্রাফটেড রিকোয়েস্ট যেকোনো ধরনের আক্রমণকারীকে কমপিউটারে যত্রতত্র ধরনের কোড রান করাতে অনুমতি দেবে। ফায়ারওয়াল এ ধরনের ইনকামিং সংযোগগুলোকে ওইসব সম্ভাব্য ভঙ্গুর সার্ভিসগুলোতে পৌঁছানোর হাত থেকে প্রতিরোধ করে।

আরও ফায়ারওয়াল ফাংশন

ফায়ারওয়াল একটি নেটওয়ার্ক (যেমন– ইন্টারনেট) এবং কমপিউটার (অথবা লোকাল নেটওয়ার্ক) মাঝে থেকে কমপিউটারগুলোকে (অথবা লোকাল নেটওয়ার্ক) যত্রতত্র অ্যাক্সেসের হাত থেকে রক্ষা করে। হোম ব্যবহারকারীদের জন্য ফায়ারওয়ালের প্রধান সিকিউরিটির উদ্দেশ্য হচ্ছে অপ্রত্যাশিত ইনকামিং নেটওয়ার্ক ট্রাফিক প্রতিরোধ করা। কিন্তু ফায়ারওয়ালের থেকেও বেশি কিছু করতে সক্ষম। কারণ, ফায়ারওয়াল দুটি নেটওয়ার্কের মাঝে থেকে কাজ করে এবং সব ধরনের ইনকামিং ও আউটগোয়িং ট্রাফিকগুলোকে অ্যানালাইসিস করতে পারে এবং সিদ্ধান্ত নিতে পারে এদের সাথে কী করতে হবে। যেমন– একটি ফায়ারওয়ালকে এভাবেও কনফিগার করা যায়, যেখানে এটি শুধু নির্দিষ্ট কিছু ধরনের আউটগোয়িং ট্রাফিক ব্লক করে রাখবে অথবা সন্দেহজনক ট্রাফিক বা ডাটাগুলোকে কেটে বাদ দেবে।

একটি ফায়ারওয়ালের বিভিন্ন ধরনের নিয়ম থাকতে পারে, যেগুলো কি না নির্দিষ্ট ধরনের কিছু ডাটা টাইপ বাইপাস করার অনুমতি দেবে অথবা অনুমতি দেবে না। যেমন– ফায়ারওয়ালটিকে এমনভাবেও কনফিগার করা যেতে পারে, যেখানে এটি শুধু নির্দিষ্ট সার্ভারে কানেকশনের অনুমতি পাবে ও অন্যান্য কানেকশন রিকোয়েস্ট ড্রপ করবে।

মজার বিষয় হচ্ছে, ফায়ারওয়াল যেকোনো কিছু হতে পারে। হতে পারে আপনার ল্যাপটপে রান হতে থাকা ছোট একটি সফটওয়্যার, যেমন– উইন্ডোজ ফায়ারওয়াল, আবার হতে পারে ডেডিকেটেড হার্ডওয়্যার ফায়ারওয়াল (কর্পোরেট নেটওয়ার্কের ক্ষেত্রে)। এ ধরনের কর্পোরেট ফায়ারওয়াল আউটগোয়িং সব ট্রাফিক অ্যানালাইসিস করতে পারে, যাতে নেটওয়ার্কের মাধ্যমে কোনো ধরনের ম্যালওয়্যার যোগাযোগ করতে না পারে। এছাড়া কর্মীদের জন্য বরাদ্দ নেটওয়ার্ক মনিটর ও ট্রাফিক ফিল্টার করার জন্যও এটি ব্যবহার করা হয়। যেমন– ফায়ারওয়ালকে এমনভাবেও কনফিগার করা যেতে পারে, যাতে শুধু ইন্টারনেট ব্রাউজ করা যাবে, ডাউনলোড করা যাবে না ইন্টারনেট অ্যাপ্লিকেশন।

রাউটারের NAT (Network Address Translation) ফিচারের কারণে এটি আসলে হার্ডওয়্যার ফায়ারওয়াল হিসেবে কাজ করে এবং অপ্রত্যাশিত কোনো নেটওয়ার্ককে আপনার কমপিউটার বা অন্য কোনো ডিভাইসে (যা আপনার রাউটারের সাথে যুক্ত) পৌঁছাতে দেয় না।

এছাড়া বিভিন্ন ধরনের অপারেটিং সিস্টেম ও রাউটারে Access Control List-এর মাধ্যমে ফায়ারওয়াল কনফিগার করা হয়। মূলত এই ব্যবস্থার মাধ্যমে বিভিন্ন আইপি অ্যাড্রেস ও পোর্ট নম্বরকে প্রবেশের অধিকার দেয়া হয় বা প্রবেশের অধিকার রোধ করা হয়।

আমরা ইচ্ছা করলে নিজের কমপিউটার বা নেটওয়ার্ক ডিভাইসে নিজেদের মতো করে ফায়ারওয়াল কনফিগার করে নিতে পারি কজ

ফিডব্যাক : jabedmorshed@yahoo.com