ভার্চুয়াল প্রাইভেট নেটওয়ার্ক যোগাযোগ হাইওয়েতে নিজস্ব রাস্তা

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

বর্তমানে দেখা যায়, বিভিন্ন ব্যাংক বা কর্পোরেট সংস্থার অফিস বিভিন্ন শহরে, এমনকি বিভিন্ন দেশে। এসব লোকাল অফিসকে হেড অফিসের সাথে যুক্ত করতে ইন্টারনেটের সাহায্য নেয়া ছাড়া কোনো পথ খোলা থাকে না। ধরুন, ঢাকাতে কোনো ব্যাংকের অফিস আছে, এখন সিলেটের কোনো লোকাল অফিসের সাথে নেটওয়ার্ক প্রতিষ্ঠা করতে চাচ্ছে। এখন এই ব্যাংকে কোনো অবস্থাতেই তার বা ওয়্যারলেস ইকুইপমেন্ট বসিয়ে নেটওয়ার্ক তৈরি করা কারিগরি ও আর্থিক দিক থেকে ফিজিবল হবে না। তাই এরা অন্য কোনো নেটওয়ার্ক প্রোভাইডারের কাছ থেকে নেটওয়ার্ক ভাড়া নিয়ে থাকে। যখনই থার্ড পার্টি কোনো প্রতিষ্ঠান থেকে নেটওয়ার্ক অবকাঠামো ভাড়া নেয়া হয়, তখনই কিছু নিরাপত্তা ঝুঁকি তৈরি হয়, যেমন : যত ডাটা হেড অফিস থেকে লোকাল অফিসে বা লোকাল অফিস থেকে হেড অফিসে আসবে, সবকিছুই থার্ড পার্টির মাধ্যমে যাবে। ফলে থার্ড পার্টি সেই ডাটা দেখতে, পড়তে ও পরিবর্তন করতে পারবে। এ ধরনের পরিস্থিতিতে ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (ভিপিএন) প্রয়োজনীয় নিরাপত্তা দিতে পারে। ভিপিএনে সব ধরনের তথ্য অ্যানক্রিপশনের মধ্যমে যায়। ফলে কেউ সেই তথ্য দেখে ফেললেও কিছু পড়তে বা বুঝতে পারবে না। ভিপিএন বিভিন্ন অ্যানক্রিপশনের মাধ্যমে এ ধরনের সেবা দিয়ে থাকে। এখানে কয়েকটি জনপ্রিয় প্রটোকল নিয়ে আলোচনা করা হলো।

পিপিটিপি

পিপিটিপি (পয়েন্ট টু পয়েন্ট টানেলিং প্রটোকল) একটি খুবই সাধারণ, হাল্কা ভিপিএন প্রটোকল, যা পিপিপির ওপর ভিত্তি করে মাঝারি গতির সাথে অনলাইনের মৌলিক নিরাপত্তা দেয়। মাইক্রোসফট অন্যান্য প্রযুক্তি কোম্পানির সাথে প্রথম পিপিটিপি তৈরি করে। যেহেতু এটি ছিল প্রথম ভিপিএন প্রটোকল, যা মাইক্রোসফট উইন্ডোজ সমর্থন করত এবং উইন্ডোজ ব্যবহারকারীদের মধ্যে এটি বহুল ব্যবহৃত ভিপিএন পদ্ধতি ছিল।

মোবাইল প্লাটফর্ম (যেমন আইওএস ও অ্যান্ড্রয়িড), মাইক্রোসফট উইন্ডোজের সব সংস্করণ ও অন্যান্য বেশিরভাগ অপারেটিং সিস্টেম (যেমন : ম্যাক, লিনআক্স) পিপিটিপি সমর্থনের জন্য তৈরি করা হয়েছে। পিপিটিপিতে শুধু একটি ইউজারনেম, পাসওয়ার্ড ও সার্ভারের ঠিকানা প্রয়োজন হওয়ায় এটি স্থাপন করা খুব সহজ।

পিপিটিপির অসুবিধা হলো এটি ১২৮ বিট অ্যানক্রিপশন বৈশিষ্ট্য সংবলিত। এটি আসলে অ্যানক্রিপশন বা প্রমাণকরণ বৈশিষ্ট্য বর্ণনা করে না এবং এটি পিপিপির (পয়েন্ট টু পয়েন্ট প্রটোকল) ওপর নির্ভর করে যেহেতু নিরাপত্তা বৈশিষ্ট্য প্রয়োগের জন্য টানেল করা হয়। পিপিটিপি অন্য ভিপিএন প্রটোকলগুলোর ওপর এতটা নির্ভরযোগ্য এবং সুদৃঢ় নয়।

এলটুটিপি

এলটুটিপি একটি অ্যাডভান্স ভিপিএন প্রটোকল। এটি OpenVPN থেকে বেশিমাত্রায় জটিল। কিন্তু যদি আপনি বিশেষভাবে আইওএস বা অ্যান্ড্রয়িড পরিচালনা করেন, তবে এটি হলো পিপিটিপির সুপারিশ করা প্রতিস্থাপন। কার্যক্ষেত্রে মোবাইল যন্ত্রে L2TP/IPSec OpenVPN-এর মতোই নির্ভরযোগ্য এবং সুদৃঢ়।

এটি কনফিগার করা কঠিনতর হতে পারে, যেহেতু এতে অতিরিক্ত প্রমাণাদি লাগে। L2TP/IPsec ২৫৬ বিট অ্যানক্রিপ্ট করে, কিন্তু অতিরিক্ত নিরাপত্তার কারণে পিপিটিপির তুলনায় বেশি সিপিইউ ব্যবহারের প্রয়োজন হয়। এ কারণে এটিকে খুবই নিরাপদ হিসেবে বিবেচনা করা হয়। ২০০০/এক্সপি থেকে পরবর্তী সব উইন্ডোজ, ম্যাক সংস্করণ OSX 10.3+ h L2TP/IPSec সমর্থন করে। বেশিরভাগ আধুনিক মোবাইল প্লাটফর্ম, যেমন আইওএস ও অ্যান্ড্রয়িডেও এটি সমর্থন করে। অর্থাৎ আপনার যন্ত্রে যদি OpenVPN বিদ্যমান না থাকে, তবে L2TP/IPSec একটি চমৎকার পছন্দ।

ওপেনভিপিএন

ওপেনভিপিএন হলো একটি অ্যাডভান্সমুক্ত উৎস ভিপিএন সলিউশন, যা ওপেনভিপিএন টেকনোলজিস কোম্পানি তৈরি করেছে। এটিকে প্রথম ভিপিএন প্রটোকল হিসেবে বিবেচনা করা হয়। ডেস্কটপে ব্যবহারের জন্য এটিকে সবচেয়ে বেশি সুপারিশ করা প্রটোকল হিসেবে বিবেচনা করা হয় এবং এটি তারহীন রাউটার ও ওয়াই-ফাই হটস্পটে এমনকি অনির্ভরযোগ্য নেটওয়ার্কেও খুব দ্রুত এবং সুদৃঢ়।

ওপেনভিপিএন ২৫৬ বিট অ্যানক্রিপশন দেয় এবং এটি অন্য সফটওয়্যারের মতোই স্থাপন করা খুবই সহজ ,যা ইনস্টল এবং চালাতে মিনিটের বেশি সময় নেয় না। উপসংহারে বলা যায়, ওপেনভিপিএন হলো সর্বোত্তম পছন্দ, খুবই দ্রুত ও নির্ভরযোগ্য। একমাত্র সমস্যা হলো কিছু ভিপিএন সেবা মোবাইল যন্ত্র ও ট্যাবলেটের জন্য ওপেনভিপিএন অ্যাপ্লিকেশন দেয় না।

এসএসটিপি

সিকিউর সকেট টানেলিং প্রটোকল বা এসএসটিপি হলো একটি টানেলিং প্রটোকল, যা এসএসএল ভিপিএন ব্যবহার করে, যাতে এইচটিটিপিএসের মাধ্যমে প্রবেশ করা যায় ২০৪৮ বিট নিরাপত্তা ব্যবহার করে। এই কারণে এটিকে সবচেয়ে নিরাপদ পদ্ধতি হিসেবে বিবেচনা করা হয়।

এতে কোনো সফটওয়্যার ইনস্টল করার প্রয়োজন হয় না, কারণ গ্রাহকের অ্যাপ্লিকেশন হিসেবে ওয়েব ব্রাউজার ব্যবহার করে। এসএসটিপি লিনআক্স, রাউটারওএস এবং SEIL-এর জন্য পাওয়া যায়; তারপরও এটি বৃহদার্থে শুধু উইন্ডোজের প্লাটফর্ম। এটি উইন্ডোজ ভিস্তা এসপি১ থেকে শুরু করে অন্য উইন্ডোজ সংস্করণ সমর্থন করে এবং একে একটি সীমাবদ্ধতা হিসেবে বিবেচনা করা হয়। কেননা, এটি অন্য সব বহুল ব্যবহৃত অপারেটিং সিস্টেমকে সমর্থন করে না। এর আরেকটি সীমাবদ্ধতা হলো ধীর সংযোগ।

ওপেনভিপিএন ওভার এসএসএইচ

এই প্রযুক্তি ব্যবহারের কারণে সব ভিপিএন প্রদানকারীর মধ্যে WASEL Pro ভিপিএন হলো নেতৃস্থানীয়। সিকিউর শেল (এসএসএইচ) প্রটোকলে রয়েছে একটি অ্যানক্রিপ্ট করা টানেল, যা এসএসএইচ প্রটোকল সংযোগের মাধ্যমে তৈরি। এসএসএইচ টানেল একটি নেটওয়ার্কের মাধ্যমে অ্যানক্রিপ্ট ছাড়া ট্রাফিককে একটি অ্যানক্রিপ্ট করা চ্যানেলের মাধ্যমে স্থানান্তর করতে পারে। ওপেনভিপিএন প্রটোকলের মতোই এসএসএইচ টানেল ফায়ারওয়ালকে পাশ কাটাতে পারে, যেটি কিছু ইন্টারনেট সেবাকে বাধাগ্রস্ত বা ফিল্টার করে।

কিছু কিছু দেশে আইএসপিগুলো ট্রাফিককে কর্তৃত্ব এবং ফিল্টার করার জন্য স্পর্শকাতর প্রযুক্তি ব্যবহার করে। এই প্রযুক্তিগুলো হলো ডিপিআই (ডিপ প্যাকেট ইনস্পেকশন), যা OpenVPN – L2TP/IPSec এবং সংযোগ আটকে দিতে ব্যবহার হয়, এর ফলে কোনো ব্যবহারকারীকেই নিরাপদ সংযোগ ব্যবহার করতে, কিছু নির্দিষ্ট ভিওআইপি সেবা বা কিছু ওয়েবসাইট, ব্লগ ও সামাজিক নেটওয়ার্ক ব্যবহার করতে দেয় না।

তাই WASEL Pro তার ব্যবহারকারীদের জন্য একটি সম্পূর্ণ নিরাপদ ওপেনভিপিএন সংযোগ দেয়, যা শনাক্ত করা যায় না এবং এর ফলে ওইসব দেশে আইএসপিগুলো বাধা দিতে পারে না এবং এটি ওপেনভিপিএন এবং এসএসএইচ টানেলকে একটি সাধারণ ধাপে একত্রিত করে। এটি আপনাকে ওপেনভিপিএনের মতো একই বৈশিষ্ট্য দেবে কোনো সংযোগ বিচ্ছিন্ন না করে।

সুতরাং বলা যায়, বেশিরভাগ ভিপিএন ব্যবহারকারীদেরকে তাদের ডেস্কটপ কমপিউটারে ওপেনভিপিএন এবং মোবাইল যন্ত্রে L2TP/IPsec ব্যবহার করার পরামর্শ দেয়া হয় কজ

ফিডব্যাক : jabedmorshed@yahoo.com