

# HIGHLY SECURE SOLUTION FOR CROSS-NETWORK INTERCONNECTION

## USE CASE

In today's digital era, where business operations are often spread across multiple locations, ensuring secure communication between different companies is not just a luxury but a necessity. With rising cyber threats, companies must proactively protect sensitive data when transmitted over public networks.

Protelion Virtual Private Network is a game-changer when safeguarding communication between offices and/or different companies. By establishing dedicated VPN management centers for each organization, businesses can maintain full control over their security settings, ensuring their data flows securely across both internal and public networks.

This unique approach enhances security while also offering flexibility and scalability – essential for growing businesses. Each company manages its own dedicated VPN infrastructure, allowing for customized configurations that fit specific security needs and operational goals.

## Cross-Network Interconnection Benefits

With the independent Protelion Security Management Center (SMC), each company has full administrative control over its own secured network. This means you can configure firewalls, monitor traffic, and enforce encryption protocols without relying on a third-party service. Customizing your security settings ensures that your company's data is always protected according to your specifications.

Protelion VPN is based on symmetric cryptography, which plays a pivotal role in securing data across the VPN. Symmetric encryption uses pre-shared master keys to establish cross-network interconnection. Compared with other technologies, Protelion's approach is not only faster but also highly efficient for encrypting large volumes of data. The simplicity of symmetric cryptography ensures that sensitive information – such as financial records, proprietary data, and client communications – remains secure while traveling across public networks without compromising on speed or performance.

## Project Specification

Two companies, each managing their own independent Protelion SMC, aim to create a secure, encrypted cross-connection between their networks using Protelion technology. Their goal is to ensure confidentiality, integrity, and seamless integration while retaining full control over their security policies and data exchange methods.

By implementing this approach, the companies can establish a new and common secure, encrypted connection between their teams, information, communication channels, and critical digital resources. This enables safe data exchange, seamless collaboration, and enhanced protection against cyber threats, ensuring that all shared information remains confidential and accessible only to authorized users.

You can connect to an unlimited number of Protelion partner networks based on our technology.

# Implementation

1. Each company should set up its own Protelion Virtual Private Network (VPN), which will be built using independent Protelion Secure Management Center (SMC), Protelion AR Security Gateways, and Protelion AR VPN clients. These core components form the foundation of a private, highly secure network infrastructure and allow cross-connection between two private networks.
2. To set up a partner network connection, create a file in SMC with your Protelion network details. Include the network number, cross-network gateway for connecting to another Protelion network and VPN hosts for linking with the partner network. Share the file securely with protected password and provide it to the partner network administrator.
3. Wait for the partner organization to process the file and provide a response (file). Then, process the response, generate new key sets in Protelion SMC, and update them to your network's VPN hosts.
4. Once the cross-network connection between two Protelion networks is established, you can:
  - Link more VPN devices of your network with partner network devices.
  - Relink VPN devices of your network and partner network devices.
  - Change the cross-network gateway of your network.
  - Provide access to tunneled devices (resources) located behind Protelion AR VPN Gateways.
  - Enable secure communication between users from different companies, such as secure instant messaging, audio and video calls, conferences, file sharing etc.

## Protelion Features

### Customizable Solutions

High flexibility, compatibility, and scalability of the Protelion Security Technology enables customer to create an optimal solution on top of their existing IT infrastructure.

### Protelion VPN Communication Technology

The seamless integration of Protelion VPN Communication Technology allows the creation of hierarchical systems and the establishment of secure, encrypted communication on top of the existing IT infrastructure.

### Certified AES Algorithm

The certified Protelion encryption algorithm protects highly sensitive and critical data. Its security and performance features meet the customer's expectations to the highest level.

### Easy-to-Use Protelion Security

Solutions are designed to be user-friendly, reliable, easy-to-use and compliant with today's General Data Protection Regulations (GDPR), so customers can stay focused on their business.

