Secure Host-Specific Site-to-Site IPsec VPN

A PROJECT REPORT

Submitted by

REG. NUMBER	NAME
BL.SC.U4AIE24252	Surya Pramod
BL.SC.U4AIE24248	S.Santhosh
BL.SC.U4AIE24235	K.C.S Varshith

in partial fulfillment for the award of the degree
0f

BACHELOR OF TECHNOLOGY
IN

"Computer Science and Engineering (AIE)"

AMRITA SCHOOL OF COMPUTING, BANGALORE

AMRITA VISHWA VIDYAPEETHAM

Abstract :

Consequently, it has become crucial to have secure communication over public networks due to the ever-growing number of cyber threats and unauthorized access attempts. Virtual Private Networks allow for secure traffic encryption, routing them across extended private networks over public infrastructure. IPsec-based VPNs can enable strong encryption with tunneling mechanisms to securely exchange data between headquarters, remote offices, partners, and cloud-hosted resources.

This project will design a secure host-specific site-to-site IPsec VPN connection between two organizations, MyCo and TheirCo, where only certain hosts (System-A and System-C) are communicating. Compared to traditional VPNs, this solution allows only specified hosts into the network by using ACL-based traffic filtering and ISAKMP policies. The solution meets data confidentiality, integrity, authentication, and high availability through redundant WAN links and Port-Channel aggregation.

The implemented design puts into limelight various real enterprise practices, including crypto mappings, IKE security negotiations, dual WAN connectivity, and controlled traffic policies. This project will show how organizations can operate securely over the public Internet without relying on dedicated leased lines while maintaining strict access control and high reliability.

Introduction :

Modern enterprise networks require secure communications across distributed departments and partner organizations. Organisations need to ensure that their communication channels remain confidential and interception-resistant, given the frequency of sensitive data traveling on public infrastructure. Traditional leased lines offer security but are expensive and not scalable; VPNs have thus been widely adopted as a means of achieving secure communications at lower cost.

This makes IPsec VPN technology strong for security in data exchange, encrypting traffic between endpoints with robust security protocols, flexible deployment options, scalable configurations, and seamless integration with existing network architectures. With the constant evolution of threats, an enterprising trend towards adopting selective, policy-based VPN configurations adds fine-grained access control at the level of individual users or hosts.

A Site-to-Site Host-Specific IPsec VPN is established in this project to securely connect a machine in the network of MyCo, System-A, to the corresponding host in the facility of TheirCo, System-C. The solution restricts the flow of traffic from both ends with access policies, ensuring that no other internal systems can either send or receive any traffic across the VPN tunnel. This approach supports the principle of least privilege and allows for highly controlled inter-organization communication.

Problem Statement :

Organizations often need to exchange business-critical data between departments or with partner companies operating in different geographical locations. Whenever such communications occur over the Internet, they are at high risk of eavesdropping, tampering, spoofing, and unauthorized access. If not properly encrypted and authenticated, such transmissions pose a significant operational and financial risk.

Many VPN implementations connect entire networks, but this wide access creates a larger attack surface and unnecessary trust relationships. If any device is compromised on either side of the network, it could gain potential access to services or data across the tunnel. This violates the principles of zero-trust and complicates security management.

It follows that there is a need to design a host-specific, restricted VPN solution that would ensure only authorized devices are allowed to exchange information across networks. The project aims to implement strong encryption, selective traffic filtering, and high availability through redundant WAN connectivity to establish a secure and reliable connection between the two organizations.

Literature Survey :

Several works in literature review the importance of securing a communication over an untrusted network. Initial VPN research efforts concentrated on tunneling protocols like L2TP, GRE, and PPTP, which emphasized the need for ensuring confidentiality but were without strong mechanisms for authentication and encryption. Later, IPsec was adopted as the industry standard, with various authors proving its superiority due to the layered security provided and mandatory cryptographic enforcement.

IETF studies also investigated the efficiency of IKE-Internet Key Exchange, studying various phases of IKE and how these affect the negotiation speed, network performance, and security strength. Demonstrated was that the kind of encryption suite chosen, like AES-256, would highly influence the resilience of a tunnel in service from brute-force attacks. The findings helped to support the adoption of strong digital protection based on AES.

Recent research work also focuses on selective VPN routing using policy-based filtering, host-level restrictions, and microsegmentation. This research emphasizes that fine-grained traffic control reduces exposure in case of internal breaches and aligns with zero-trust networking models. The present project follows this principle by implementing ACL-based host authentication to enforce restrictive access across the VPN.

Proposed System :

The proposed system provides a secure IPsec site-to-site VPN tunnel between MyCo and TheirCo while allowing communication exclusively between System-A and System-C. This will be fulfilled by Crypto Maps, ISAKMP policies, and Access Control Lists that match only the authorized host IP pairs. The approach aligns with segmented security, ensuring minimal exposure and controlled connectivity.

The tunnel implements AES-256 encryption with Pre-Shared Key authentication to ensure confidentiality and integrity. Secure peer negotiation is done through ISAKMP in Phase-1, while Phase-2 involves the use of IPsec protocols to encapsulate data packets. In this way, any kind of traffic not matching the ACL policies defined will be denied, prohibiting unauthorized hosts from communicating through the tunnel.

The proposed solution also enhances reliability with dual WAN links along with routing using administrative distance. In case any of the ISP links fails, routing automatically shifts over to the backup connection and maintains continuous tunnel connectivity. It is reinforced by Port-Channel aggregation between routers and switches, ensuring network-level failover and increased throughput.

System Model Diagram Description

VPN Logical Architecture :

This architecture consists of two enterprise locations connected through the Internet, with their routers performing IPsec encryption and decryption at both ends. Each router applies a Crypto Map, which defines VPN peers, ACL rules, and transform sets. System-A and System-C are behind their respective routers and are the only devices whose traffic is routed through the VPN tunnel.

WAN Redundancy Model :

Two serial links, one primary and one backup, connect each router to the ISP using administrative distance to select the primary path. If the primary link fails, routing automatically shifts to the secondary line without manual intervention. This setup prevents loss of connectivity and ensures stable access between organizations.

LAN Architecture :

Port-Channel configurations combine multiple physical Ethernet links between routers and switches into one logical interface. This enhances reliability by preventing an outage if any one Ethernet cable or port fails.

Technology Used

IPsec- Internet Protocol Security

The VPN technology that resides at the core of this project is IPsec. It ensures data confidentiality, integrity, and authentication by using protocols such as ESP and AH. Strong cryptographic suites like AES-256 ensure that encrypted data remains computationally infeasible to intercept or tamper with.

ISAKMP / IKE

ISAKMP manages the secure negotiation of cryptographic keys between VPN endpoints. Phase-1 establishes a secure channel, while Phase-2 negotiates the Transform sets to be used for encrypted data transport. Pre-shared keys are a simple, yet secure authentication procedure suitable for private site-to-site interconnections.

Access Control Lists

ACLs apply selective traffic controls by considering source and destination IP addresses. In this context, they are going to ensure that only System-A and System-C can create VPN-bound traffic to prevent lateral movement and enforce micro-segmented access.

Implementation Details:
Step 1 - Configure ISAKMP and Phase-1 Parameters

ISAKMP policies are defined on both routers that define authentication, key exchange mechanisms, hashing algorithms, and encryption strength. AES-256 is chosen because it is robust and widely accepted in the industry. There must be matching configurations on both routers for negotiation to occur.

Step 2 – Define IPsec Transform Set for Phase-2

A transform set defines how the packets will be encapsulated in transit and specifies parameters such as encryption protocol, which is ESP. It defines the actual method by which the data is protected while the tunnel is active.

Step 3 - Create ACLs for Host-Specific Filtering

The purpose of ACLs is to permit only the authorized traffic in between System-A MyCo and System-C TheirCo, filtering out all other traffic. This will ensure that no additional devices from either side can access the partner network.

Step 4 – Link ACLs to Crypto Map

The Crypto Map combines ISAKMP negotiation, ACLs, and transform sets into a workable encryption policy. It also identifies the remote peer using their public-facing WAN IP address. This map is then applied to the outbound interface on both routers.

Step 5 - Configure Dual WAN Paths

Two serial connections are made to the ISP with different administrative distances. The router favors the lower distance route but automatically switches over in case of failure of the primary link. It ensures the high availability of VPN connectivity.

Step 6 - Implementing the port-channel between router and switch

Multiple Ethernet links are aggregated to form a logical Port-Channel, increasing throughput and redundancy at the LAN edge. A single link failure does not bring down the logical channel.

Components Used :

Routers Cisco

Routers act as VPN gateways to implement IPsec negotiation, encryption, and routing. They manage WAN connections, host security policies, and continuous tunnel monitoring.

Cisco Switches

These switches provide connectivity over the LAN and take part in Port-Channel configurations for increased reliability and bandwidth. They ensure stable communication between routers and end-host systems.

End Systems Operators

System-A and System-C are typical enterprise devices such as desktops or servers operating behind their respective routers. They are the only systems that are allowed to exchange data across the tunnel.

Results and Analysis

This will establish an IPsec VPN between the two organizations, ensuring that encrypted traffic flows only between System-A and System-C. Packet inspection confirmed that traffic belonging to any other hosts was denied, demonstrating effective host-level segmentation. AES-256 provided strong cryptographic assurance against unauthorized access.

WAN redundancy greatly improved network resiliency. Simulated link failures demonstrated automated rerouting via the backup link with very minimal packet loss and without any need for manual configuration. The Port-Channel configuration ensured uninterrupted device connectivity even during switch or cable outages.

Overall, the solution proved that a secure, selective, and high-availability VPN connection is deployable without using expensive leased circuits. The implementation is consistent with modern security principles, such as zero trust, least privilege, and network segmentation.

Conclusion :

The project has successfully deployed a secure host-specific IPsec site-to-site VPN between partner organizations based on the standard Cisco networking technologies. The solution showed how enterprises can selectively share sensitive information across open networks without exposing their entire infrastructures. Encryption, ACL filtering, and controlled ISAKMP policies secure high confidentiality, integrity, and authentication. Redundancy features such as dual WAN and Port-Channel aggregation were employed to increase the system's availability and fault tolerance. Even under link failures or network fluctuations, the communication channel remained stable and operational.

Such resiliency is necessary in real-world industrial scenarios since losses are counted in terms of money and delays in operations. Implementation also demonstrated that enterprise security need not be expensive, nor must it be based on complex or proprietary systems. Organisations can ensure distributed operations result in scalable and secure communications by using widely accepted protocols for networking and open deployment standards.

Future Scope :

Integration in the future could be made with next-generation security models, such as SD-WAN, which allows dynamic intelligent routing across multiple WAN links. This will further enhance efficiency, reducing the operational cost while keeping connectivity encrypted. In addition, authentication based on digital certificates can be implemented to replace Pre-Shared Keys for a more robust identity management mechanism. Certificate Authorities would automate key renewal and decrease the administrative workload for large-scale deployments.

Further enhancement of overall trust and resilience might be obtained by multi-factor authentication for VPN endpoints. Real-time intrusion detection and centralized SIEM monitoring can also be integrated into the existing framework. This would ensure better anomaly detection, logging, and automated response, keeping the VPN safe from emerging threats and sophisticated attacks.

References:

[1] D. Felsch, M. Grothe, J. Schwenk, A. Czubak, and M. Szymanek, "The dangers of key reuse: Practical attacks on IPsec IKE," in *Proc. USENIX Security Symposium*, 2018.

[2] A. Herzberg and H. Shulman, "Stealth MITM DoS attacks on secure channels," *Journal of Cryptographic Engineering*, 2010.

[3] O. Alia, A. Huang, H. Luo, O. Amer, M. Pistoia, and C. Lim, "100 Gbps quantum-safe IPsec VPN tunnels," in *Proc. Optical Fiber Communications Conference*, 2024.

[4] F. Hauser, M. Häberle, M. Schmidt, and M. Menth, "P4-IPsec: Site-to-site and host-to-site VPN in P4-based SDN," in *Proc. IEEE/IFIP Network Operations and Management Symposium*, 2019.

[5] A. Marwa, M. Baameur, and N. Ghoualmi, "Enhancing IPSec security using a safer and efficient IKE protocol," *Journal of Information Security Research*, vol. 4, 2013.

[6] Z. Da-yuan, "Implementation and performance evaluation of IPSec VPN," *International Journal of Computer Applications*, vol. 29, no. 2, 2005.

[7] G. T. Jucha, "Security and performance impact of cryptographic and hashing algorithms in site-to-site VPNs," M.S. Thesis, University of West London, 2025.

[8] A. Ahmim et al., "ESIKE: An efficient and secure Internet Key Exchange protocol," *International Journal of Computer Networks*, 2021.

[9] K. S. Munasinghe and S. A. Shahrestani, "Evaluation of IPsec VPN over wireless infrastructure," in *Proc. Australian Telecommunication Networks and Applications Conference (ATNAC)*, 2004.

[10] K. Ghanem et al., "Security vs bandwidth: Performance comparison between IPsec and OpenVPN in smart grids," in *Proc. International Symposium on Networks, Computers and Communications*, 2022.