International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Integration of CCNA-Level Security with Cloud-Based Networks

Kalpna Vats , Anjali Kaushik , Vaishali Munjal , Anisha
Assistant Professor,
Electronics and Communication Engineering
NGF College of Engineering and Technology

Abstract- — The current paper seeks to present an in-depth analysis pertaining to the integration of CCNA security concepts with contemporary cloud computing networks. Over the years, enterprise networks have undergone a transition from traditional on-premises networks to cloud computing networks. As such, the traditional security concepts studied in the Cisco Certified Network Associate (CCNA) program need to be updated to incorporate the complexities inherent in cloud computing networks. Based on an in-depth analysis of recent developments in the field from 2021 to 2026, the paper seeks to examine the possibility of integrating traditional CCNA security concepts such as Access Control Lists (ACLs), Virtual Private Networks (VPNs), Port Security, and Hardening with contemporary cloud computing networks. A Hybrid Security Integration Framework (HSIF) is proposed as a means of integrating traditional CCNA security concepts with cloud computing networks. From the analysis, it is evident that more than 55% of enterprises currently use multiple cloud providers, while 24% are planning to adopt cloud firewalls as their main solution in the next two years. The adoption of Security Service Edge (SSE) and Secure Access Service Edge (SASE) solutions can be considered a development of CCNA security concepts into cloud technology. By comparing them through four analytical dimensions, it is evident that integration involves both technical and organizational adaptation through DevSecOps practices.

Keyword: CCNA security, cloud networks, hybrid cloud, network security, VPN, SASE, zero trust, firewall, IPsec, access control lists.

I. INTRODUCTION

The landscape of networks over the last decade or so has seen tremendous change. No longer is it true that enterprise networks are comprised of data centers, offices, and other enterprise locations connected by a wide area network. Today, we see public cloud providers (AWS, Azure, Google Cloud), private clouds, SaaS, and a workforce that can connect from anywhere. This change in network infrastructure has dramatically changed the security needs of network professionals and, by extension, the importance of fundamental certifications like the CCNA. The CCNA, especially with regard to the security aspects of the current CCNA 200-301 certification, provides network professionals with a fundamental knowledge of network security concepts, from access control lists (ACLs) for filtering network traffic, IPsec VPNs for secure connectivity, port security for access layer security, and hardening network devices with password policies and secure management protocols. These concepts, though relevant, must be extended beyond the traditional enterprise edge.

Current industry research shows that there is a decisive shift in organizational priorities. According to AlgoSec's 2026 State of Network Security report, security is considered the most important factor in cloud platform selection for 54.7% of all organizations, while nearly a quarter (24%) of all organizations plan to focus mainly on cloud firewalls over the next two years. This is a general shift away from hardware-centric security solutions towards cloud-centric solutions, driven by the increasing use of hybrid architectures, distributed applications, and AI-driven traffic patterns.

The integration challenge is quite formidable. Hybrid networks, which connect on-premise networks to cloud environments using various tools such as VPNs, direct connects, and network security groups, have created visibility gaps and policy inconsistencies. Threat actors take advantage of these gaps, using exploits that chain multiple environments together while security teams struggle to deal with tool sprawl and monitoring challenges. The average data breach cost is now over $10 million in the United States.

This paper discusses how CCNA security principles can be integrated with cloud-based networks to address these challenges. It outlines a framework to extend traditional security concepts to hybrid environments, discusses current industry trends, and provides practical advice for network professionals navigating these changes.

The rest of the paper is structured as follows. In Section 2, a literature survey of CCNA security and cloud networking integration research is provided. In Section 3, the methodology for the proposed Hybrid Security Integration Framework is discussed. In Section 4, analysis and discussion are provided along with four figures and a table. Finally, in Section 5, the conclusion is drawn.

II. LITERATURE SURVEY

2.1 CCNA Security Fundamentals

The current CCNA 200-301 certification includes security-related topics as an integral part of the curriculum, as opposed to a specific security certification track. Based on the current guidelines for the CCNA 200-301 certification exam, the fundamental security-related topics include identifying common attack types (DDoS, man-in-the-middle, malware), access control list configuration, hardening of network devices using password policies and SSH, port security configuration, and VPN technologies including IPsec site-to-site VPNs [1].
The CCNA certification curriculum includes fundamental topics for network configuration, which are essential for network professionals. These include extending access control lists for specific types of traffic, configuring 802.1X authentication with RADIUS servers, switchport security configuration, and configuring IPsec VPNs with proper phase negotiation. These are fundamental topics for network professionals, regardless of the network deployment environment [2].

The study resources for CCNA certification, based on GitHub, include specific study resources for network security, which are divided into specific modules for port security, authentication protocols, VPNs, and troubleshooting methodologies. This is an ideal approach for developing competent network security professionals, as it follows industry standards for learning network security.

2.2 Cloud Network Security Evolution

The adoption and migration to cloud-based networks have increased exponentially. The AlgoSec 2026 report surveyed more than 500 security experts from 28 nations and states that organizations are moving from initial cloud adoption to consolidation and policy control in hybrid environments [3].
Some of the findings from this report include:

- 65% have already adjusted security strategies due to AI-powered attacks
- 24% are planning to migrate primarily to cloud firewalls within two years
- 54.7% rate security as a primary consideration in selecting a cloud platform
- SD-WAN is still a priority for organizations; Cisco leads with a 30.7% market share compared to Fortinet's 31%
- SASE adoption is ongoing; only 27.5% have yet to adopt a solution, down from 40% in 2024

These trends suggest that security in cloud-native environments is becoming mainstream; however, this migration presents a variety of challenges in policy and operational management [4].

2.3 Hybrid Network Security Challenges

According to Fidelis Security, the analysis of the hybrid network environment reveals the following critical challenges facing organizations in the integration of on-premises and cloud infrastructures:

- Fragmented visibility across the hybrid environment causes 30% of breaches costing over $5 million
- Inconsistency in security policies across multiple clouds causes 32% misconfiguration rates
- 60% of the security analysts' time is spent on triaging duplicate alerts from fragmented tools
- Cloud auto-scaling creates assets faster than the patch cycle can keep up
- Unawareness of the shared responsibility model causes critical gaps

According to the Verizon DBIR 2025, third-party vulnerabilities are observed in 25% of breaches, with the number doubled compared to the previous year, with attacks on unsecured hybrid cloud networks.

2.4 VPN and Connectivity Integration

Site-to-site IPsec VPNs are still an essential element in the connectivity of hybrid networks. This technology enables the communication of geographically dispersed networks such as head offices, branch offices, data centers, and cloud virtual private clouds (VPCs), thus enabling them to communicate as if they were in the same private network [5].

Cloud providers have adopted these standards. According to the documentation provided by Tencent Cloud, it is possible to integrate direct connect and VPN connections for redundant hybrid connectivity through Cloud Connect Network (CCN), thus enabling the automatic failover between the primary and replica links. This is an example of the implementation of CCNA VPN concepts in the cloud [6].

2.5 Emerging Security Architectures

Cisco Secure Access is an example of the convergence of traditional security services into a cloud-based service. It is a converged cloud Security Service Edge (SSE) solution that offers Zero Trust Network Access (ZTNA), VPN as a Service (VPNaaS), Firewall as a Service (FWaaS), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Data Loss Prevention (DLP) as a service from a unified console [7].

It is the solution to the hybrid work problem, as it allows the same security policies to be applied anywhere, anytime, on any device, from a centralized console. It is the evolution of the traditional CCNA security concepts, including ACLs, VPNs, and firewalls, into the cloud [8].

2.6 Automation and DevSecOps

The CCNA program is also introducing concepts of automation in their curriculum, as they realize that manual configuration is not possible in cloud computing. Python scripting using netmiko for batch ACL configuration and Ansible playbooks for pushing standardized security policies [10].

Industry studies have also confirmed that integrating security into CI/CD pipelines, infrastructure as code, and DevOps is critical for keeping up with the scale of the hybrid cloud environment. Pre-commit scanning for Terraform templates and automated remediation for vulnerabilities help prevent misconfigurations [9].

2.7 Synthesis and Research Gaps

The literature indicates a trend in the following areas: CCNA security concepts established in the past remain relevant but need to be modified to accommodate cloud and hybrid environments. Some of the findings include: VPN technologies are extended to cloud VPC connectivity; concepts of ACLs evolve to cloud security groups and network ACLs; device hardening evolves to cloud posture management; and consistent policy enforcement is enabled through cloud and hybrid environments with the aid of automation and DevSecOps integration.

Gaps in the research: there is a need for the mapping of CCNA skills to cloud security roles; there is a need to consider public sector and regulated industry constraints; and there is a need for the development of a validated framework for the design of hybrid security architectures.

III. METHODOLOGY:

Based on the literature synthesis, this paper proposes the Hybrid Security Integration Framework (HSIF) to map CCNA security concepts to cloud-based network environments.

3.1 Theoretical Foundations

The Hybrid Security Integration Framework is founded on three theoretical underpinnings. First, defense-in-depth security, which is a fundamental concept of traditional network security, is applied to cloud computing environments through security controls that address network, identity, and application security.

Second, zero trust architecture, where continuous verification is conducted irrespective of location, provides the link between CCNA security, which is traditionally based on network periphery, and cloud computing environments.

Third, infrastructure-as-code, which is a software-defined concept, acknowledges that security configurations in cloud computing environments have version control, thus requiring automation skills, not just CLI skills.

3.2 Framework Components

The Hybrid Security Integration Framework comprises four analytical layers mapping traditional CCNA security domains to cloud controls.

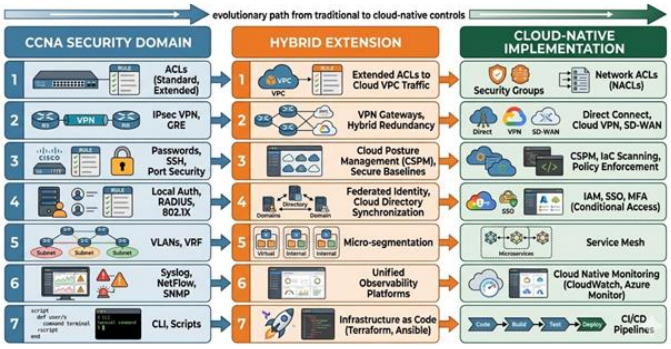

Figure 1: Hybrid Security Integration Framework (HSIF)

3.3 Analytical Dimensions

The framework will allow for a systematic evaluation of the four aspects of the cloud migration:

- Security Controls: The mapping of traditional security controls like ACLs and firewall rules to cloud technologies like Security Groups, Network ACLs, and Cloud Firewalls

- Identity Management: The migration of local authentication and RADIUS to federated identity, SSO, and MFA
- Network Segmentation: The evolution of VLAN segmentation to microsegmentation and service mesh technologies

Monitoring and Compliance: The integration of syslog/SNMP/NetFlow with cloud technologies

IV. RESULT ANALYSIS AND DISCUSSION

This section presents analytical findings regarding integration of CCNA security with cloud-based networks, organized around four illustrative figures and a comparative evaluation table.

4.1 CCNA Security Domain Mapping to Cloud Controls

The foundational security concepts from CCNA certification map directly to cloud-native equivalents, though implementation mechanisms differ significantly.

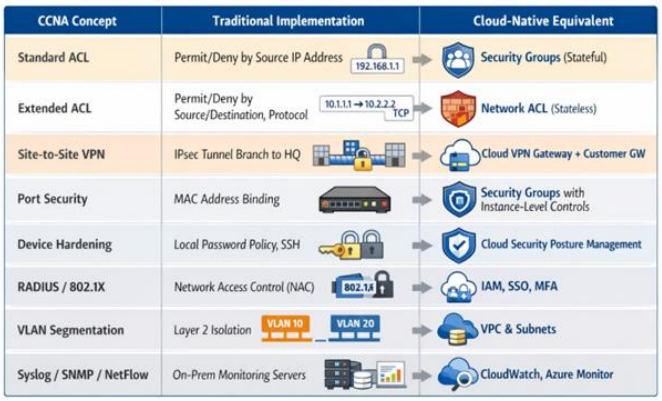

Figure 2: CCNA Security Domain Mapping to Cloud Controls

Figure 2 shows that the conceptual knowledge learned through CCNA certification is highly relevant. Understanding ACL logic, such as permit/deny statements, source/destination matching, protocol filtering, etc., is directly applicable to configuring cloud security groups and network ACLs. However, there is a fundamental difference between security groups, which operate in a "stateful" mode, automatically permitting return traffic, while traditional extended ACLs and cloud network ACLs operate in a "stateless" mode, where all rules have to be manually defined to accommodate both directions of traffic.

IPsec VPNs, too, have direct relevance to cloud VPNs. When configuring a site-to-site VPN between a remote site network and AWS VPC, the same parameters have to be negotiated: encryption type, hashing, Diffie-Hellman group, etc. However, the CCNA-trained engineer is aware of these fundamental parameters, even if the interface looks different.

4.2 Industry Adoption Trends for Cloud Security

Recent survey data reveals accelerating adoption of cloud-native security controls and architectural shifts toward unified platforms.

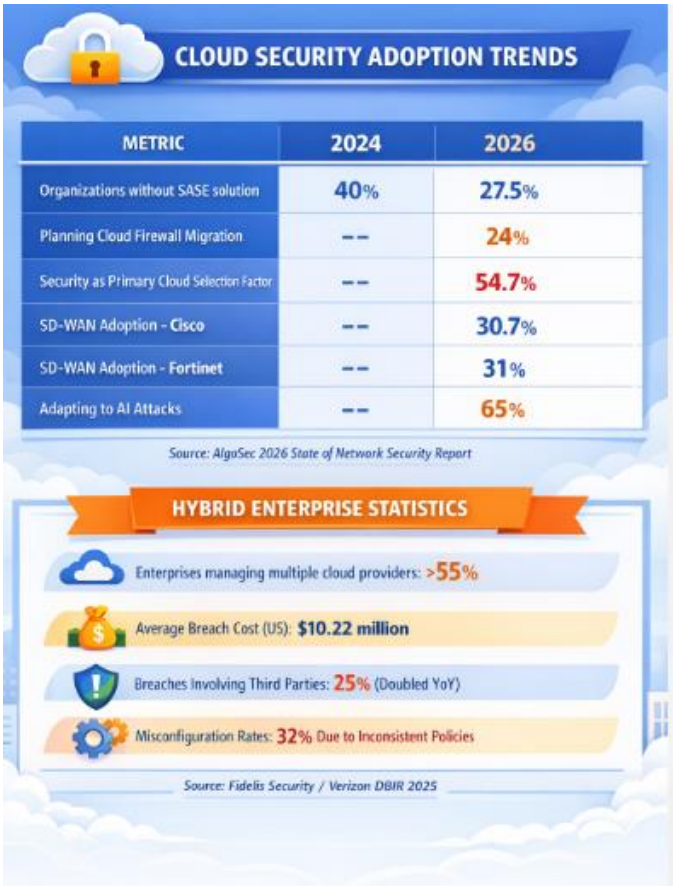

Figure 3: Cloud Security Adoption Trends (2024-2026)

In Figure 3, the speed at which organizations have adopted cloud security models is evident. The decrease in the number of organizations without SASE solutions from 40% to 27.5% in two years is a clear indication that the mainstream is embracing converged security platforms. The number of organizations planning to migrate their cloud firewalls in the next two years is a clear indication that there is a high need for

professionals who are knowledgeable about traditional firewall concepts as well as cloud firewalls.

The emergence of security as the most important factor in selecting a cloud platform (54.7%) is a clear indication that organizations are selecting cloud platforms based on their ability to deliver effective security solutions.

4.3 Site-to-Site VPN Integration Architectures

IPsec VPNs remain fundamental to hybrid network connectivity, with cloud providers offering robust integration options.

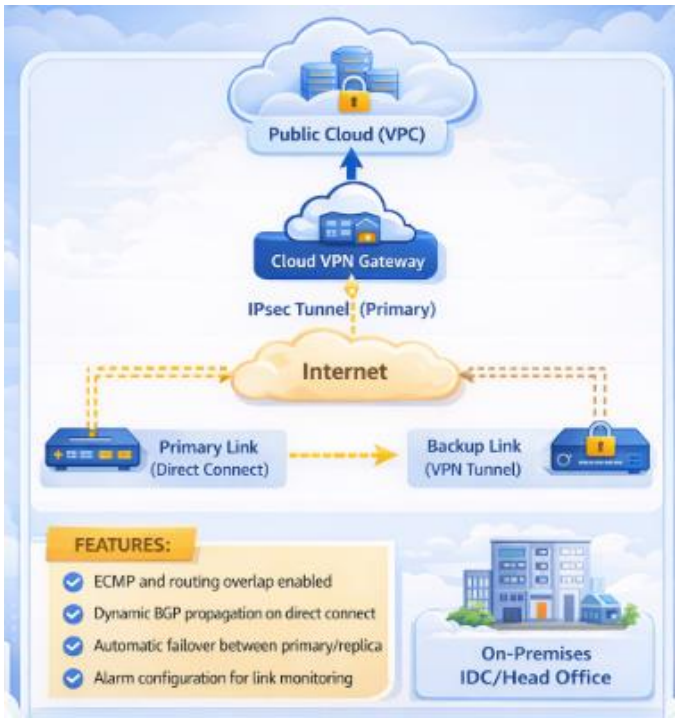

Figure 4: Hybrid VPN Connectivity Architecture

Figure 4 shows the extension of the basic concepts learned in CCNA in relation to the architecture of the cloud. The IPsec tunnel, as expected, needs the same parameter negotiations as in traditional site-to-site VPNs, connecting the on-premises gateway with the cloud VPN gateway. The architecture, however, adds complexity with redundancy in the design, including the direct connect link with failover capability using the VPN backup, as well as the use of cloud routing protocols. For CCNA professionals, the learning curve in relation to the architecture of the cloud involves understanding the concepts of VPC routing tables, internet gateway, virtual private gateway, as well as customer gateway resources, with the underlying IPsec concepts remaining the same.

4.4 SASE/SSE Architecture Evolution

Secure Access Service Edge (SASE) and Security Service Edge (SSE) represent the convergence of networking and security functions into cloud-delivered platforms.

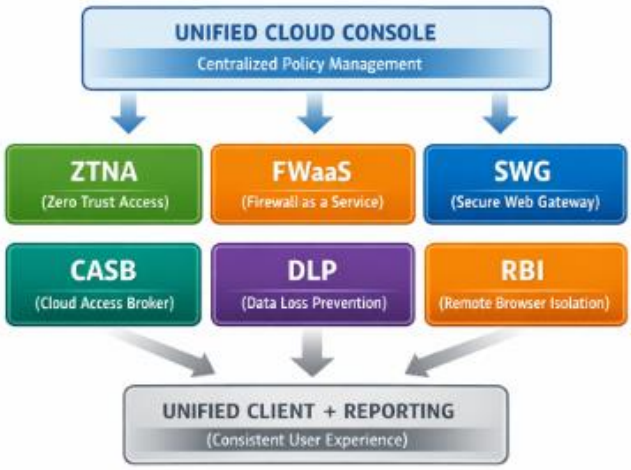

Figure 5: Cisco Secure Access SSE Architecture

Figure 5 illustrates how security products have evolved to security platforms. To CCNA-trained professionals, this is the natural extension of multiple security services, such as firewalls, VPNs, and web security, all being delivered as a single cloud-based security service. Understanding how these security services operate individually is essential to understanding how these services operate together.

4.5 Comparative Analysis of Integration Approaches

Table 1 presents a comprehensive comparative analysis of approaches to integrating CCNA security with cloud-based networks.

Table 1: Comparative Analysis of Security Integration Approaches

Integration Approach	Key Mechanisms	Cloud Implementation	CCNA Skills Required	Organizational Impact	Challenges

Extended Perimeter	IPsec VPNs, cloud gateways	Cloud VPN (AWS VPN, Azure VPN Gateway, Google Cloud VPN)	IPsec configuration, routing protocols, ACLs	Moderate; extends existing practices	Latency, bandwidth constraints, single point of failure
Cloud-Native Controls	Security groups, network ACLs, cloud firewalls	AWS Security Groups, Azure NSG, cloud WAF	ACL logic, protocol understanding, stateful vs stateless	High; requires new tooling and skills	Multi-cloud policy inconsistency, learning curve
SASE/SSE Platforms	Converged cloud-delivered security	Cisco Secure Access, Zscaler, Netskope	Foundational security concepts, policy design	Transformational; consolidates tools	Vendor lock-in, migration complexity
DevSecOps Integration	IaC, CI/CD pipelines, automated scanning	Terraform, CloudFormation, Checkov, tfsec	Scripting, automation mindset, security fundamentals	Cultural shift; requires development collaboration	Skill gaps, toolchain complexity
Hybrid Redundancy	Primary direct connect + backup VPN	Cloud CCN, multi-link failover	BGP, route prioritization, tunnel configuration	Moderate; enhances reliability	Configuration complexity, cost

Analysis of Comparative Dimensions:
Extended Perimeter is the simplest integration, where VPN concepts are extended to connect on-premises networks with cloud VPCs. CCNA concepts are directly applicable, but it is unlikely that the full potential of cloud technologies can be exploited with this approach.

- Cloud-Native Controls - CCNA concepts must be more substantially adapted. Security groups are similar to ACLs but with stateful functionality, while network ACLs are similar to traditional extended ACLs. The learning curve is more substantial, as it requires an understanding of cloud console interfaces and API-driven configuration.
- SASE/SSE Platforms - This requires architectural change, where instead of extending the network perimeter, security is delivered from the cloud, closer to the user or application. CCNA professionals must understand the delivery of traditional functions, such as a firewall, VPN, and web security, as a cloud service.
- DevSecOps Integration - This integration focuses on the importance of automation. When infrastructure is treated as code, security configurations must also be defined as a code, with automated scanning. This requires programming skills with Python or HCL, as well as security knowledge.
- Hybrid Redundancy - This approach combines traditional and cloud technologies for high availability. Primary connectivity is achieved with Direct Connect, with VPN as a backup.

V. CONCLUSION

This paper has presented a comprehensive analysis of how CCNA-level security principles can be integrated into cloud-based networks, building on recent industry research to introduce the Hybrid Security Integration Framework.

Several key findings have been identified through this analysis.

Firstly, it has been shown that CCNA security principles are of critical importance to cloud-based networks, albeit in a modified format.

Secondly, it has been identified that there is a growing trend towards cloud-based networks, which is expected to accelerate in the near future as 24% of organizations are planning to migrate their cloud firewalls in the near future, while 54.7% of organizations prioritize security as a factor in cloud platform selection.

Thirdly, it has been identified that hybrid networks pose a new challenge to network professionals, which exceeds the scope of traditional CCNA-level knowledge.

Lastly, it has been identified that VPN technology remains a critical component of hybrid networks, building on traditional CCNA-level knowledge to include more sophisticated features such as redundancy and routing .

Fifth, SASE/SSE represents the evolution of security functions into cloud-delivered models. For CCNA professionals, it is critical for professional development to understand the delivery of traditional functions as integrated cloud services.

Sixth, there is a growing importance of automation and DevSecOps. Manual configuration is no longer feasible for cloud computing; instead, infrastructure as code and CI/CD integration must become a new skillset.

Several implications for practice can be drawn from the above discussion. For network professionals, CCNA certification is useful but must be combined with knowledge of cloud computing, particularly AWS/Azure networking, security groups, and infrastructure as code. For organizations, integration of cloud computing with traditional IT is critical, which requires investing in both technology and human resources. For educators, CCNA certification must be combined with learning modules on cloud networking, with a focus on conceptual transferability.

Shortcomings of this review: The rate of change may outpace literature, there may be limited coverage of cloud provider implementations, and there is a lack of long-term studies on hybrid security effectiveness. Future research: Long-term studies of security effectiveness in hybrid environments, comparisons of security capabilities between cloud providers, and creation of assessment tools to measure hybrid security maturity levels.

As AlgoSec's Chief Product Officer, Eran Shiff, noted, "We're not only seeing a shift from risk reduction to risk optimization, but also from experimentation to optimization, where companies are not only adopting cloud security solutions, but also optimizing their use to ensure maximum effectiveness." For those with CCNA knowledge, there is both challenge and opportunity: "CCNA knowledge is still relevant, but its application is changing to accommodate the increasing complexity of hybrid environments."

REFERENCES

1. AlgoSec, "AI, hybrid cloud spur security shift to consolidation," SecurityBrief Asia, Feb. 6, 2026. [Online]. Available: https://securitybrief.asia/story/ai-hybrid-cloud-spur-security-shift-to-consolidation
2. Fidelis Security, "Hybrid Network Security Challenges Risks and Best Practices 2026," ThreatGeek, Feb. 5, 2026. [Online]. Available: https://fidelissecurity.com/threatgeek/network-security/hybrid-network-security/
3. Cisco Systems, "Cisco Secure Access Hands-On Lab," Cisco Security Workshop, Jan. 22, 2026. [Online]. Available: https://www2.ciscosecurityworkshop.com/workshop-events/list-all-workshops/cisco-secure-access/01-22-2026-cisco-secure-access-hands-on-lab
4. SPOTO, "CCNA安全考试涉及哪些内容？一文了解," SPOTO Blog, Aug. 19, 2025. [Online]. Available: https://www.spoto.net/ccna/11177.html
5. West Valley College, "CIST 204: Enterprise Networking, Security, and Automation," *West Valley College Catalog 2025-2026*. [Online]. Available: https://www.westvalley.edu/catalog/courses/computer-science/cist204.html
6. R. Roadmvn, "CCNA-Complete-Study-Guide," GitHub Repository, Feb. 20, 2026. [Online]. Available: https://github.com/Roadmvn/CCNA-Complete-Study-Guide
7. R. ullah, "How to Set Up a Site-to-Site IPsec VPN for Secure Network Communication," LinkedIn, Nov. 8, 2025. [Online]. Available: https://www.linkedin.com/posts/rafi-ullah-b00816248_what-is-site-to-site-ipsec-vpn-activity-7392931214468386816-D8da
8. Tencent Cloud, "Connect via Direct Connect or VPN Connection to Interconnect the Primary and Replica Links for Redundant Communication (Auto-Switch)," Tencent Cloud Documentation, Nov. 13, 2025. [Online]. Available: https://www.tencentcloud.com/document/product/1037/60449

9. CBT Nuggets, "Big changes are coming to Cisco certs in 2026," LinkedIn, 2026. [Online]. Available: https://www.linkedin.com/posts/cbt-nuggets_ciscocerts-ccnp-ccna-activity-7341956783130689536-0wrQ
10. S. Sridharan, "Digital-only bank licences are redundant," Financial Express, Feb. 2026. [Online]. Available: https://www.financialexpress.com/opinion/digital-only-bank-licences-are-redundant/4149719/