International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

Article - e001

Router-Based Zero Trust Network Access Gateway for Secure Work-from-Home Environments: A LITERATURE REVIEW

Ujjwal Patidar[1], **Dr. Sumit Jain**[2]

[1,2] Department of Advance Computing Specialization, SAGE University, Indore

Received: 15/06/2026 **Revision Received**: 01/07/2026 **Accepted**: 09/07/2026

ABSTRACT

The rapid growth of work-from-home and hybrid enterprise operations has exposed the limitations of perimeter-based remote access models, especially virtual private networks that often grant broad network reachability after initial authentication. Zero Trust Architecture addresses this problem by shifting security decisions from network location to continuous verification of users, devices, and requested resources. This paper proposes a router-based Zero Trust Network Access gateway for secure work-from-home environments, in which the edge router functions as a policy enforcement point that authenticates users, evaluates device posture, and grants only application-specific access according to defined security policies. By restricting access to authorized services instead of exposing internal network segments, the proposed model reduces implicit trust, limits lateral movement opportunities, and strengthens protection for distributed users connecting from untrusted home networks. The paper conceptually analyzes the architecture in terms of access control, segmentation, monitoring, and suitability for modern remote work, and argues that router-level ZTNA enforcement offers a practical and scalable approach for improving enterprise remote-access security

Keywords: *Zero Trust Architecture, Zero Trust Network Access, Router-Based Security Gateway, Work-From-Home Security, Remote Access Security, Identity-Aware Access Control, Device Posture Assessment, Least-Privilege Access, Policy Enforcement Point, Network Segmentation.*

1 Introduction

The rapid shift toward hybrid work and work-from-home operating models has transformed how enterprise resources are accessed, but it has also exposed fundamental weaknesses in

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

traditional remote-access security. For many organizations, remote connectivity still relies on perimeter-based assumptions, where a user authenticates once through a virtual private network and then receives logical access to a broader internal network. This approach is increasingly misaligned with modern enterprise conditions, where users operate from unmanaged home environments, applications are distributed across on-premises and cloud platforms, and devices move constantly between trusted and untrusted networks. NIST identifies remote users, bring-your-own-device practices, and cloud-based assets outside enterprise-owned boundaries as key drivers behind the need for Zero Trust Architecture.

Traditional network security models were designed around the concept of a trusted internal zone protected by a hardened perimeter. In this design, anything inside the boundary is often treated as more trustworthy than anything outside it. While this model was workable when users, assets, and applications remained largely within centralized enterprise infrastructure, it becomes less effective when access originates from home networks, personal or mobile devices, and distributed services. Once a remote session is established through a legacy VPN, the user may gain network-level reachability that exceeds the minimum access actually required, thereby increasing exposure if credentials are stolen or endpoints are compromised. NIST's zero trust guidance explicitly reframes this problem by focusing protection on resources rather than network segments and by removing implicit trust based on physical or network location.

Zero Trust Architecture (ZTA) has therefore emerged as a more suitable security model for modern remote access. NIST defines zero trust as an evolving set of cybersecurity paradigms that move defenses away from static, network-based perimeters and instead focus on users, assets, and resources. Under this model, no user or device is trusted by default, even if it is already inside a corporate network. Authentication and authorization are treated as discrete and continuously relevant functions, while trust must be evaluated repeatedly throughout access to protected resources. This represents a major conceptual departure from conventional remote-access systems, where trust is often concentrated at the initial login stage.

A practical implementation of this model in remote work environments is Zero Trust Network Access (ZTNA). ZTNA limits users to application-specific or service-specific access rather than extending full network visibility. In other words, a remote employee should be able to reach only the resource that policy explicitly allows, not an entire subnet or internal zone. This reduces the attack surface, constrains lateral movement, and supports least-privilege access control. The shift from network-wide trust to resource-specific trust is one of the most important operational advantages of zero trust for distributed enterprises.

Within this broader context, the idea of a **router-based Zero Trust Network Access gateway** offers an important architectural direction. Rather than treating the router merely as a packet-forwarding device, the proposed model elevates it into an active policy enforcement point at the network edge. In zero trust terminology, a policy enforcement point (PEP) is the component that applies access decisions to requests for protected resources, while the policy engine and policy administrator contribute to determining whether access should be granted, denied, or revoked. By embedding or integrating these functions around the

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

gateway, the router can validate identity, inspect device posture, consult access policies, and permit traffic only to approved applications or services.

This design is especially relevant for work-from-home environments. Home networks are rarely managed to the same standard as enterprise infrastructure, and remote endpoints may operate under variable security conditions. In such settings, the enterprise cannot safely assume that successful authentication alone is enough to establish trust. A router-based ZTNA gateway addresses this issue by placing access control at the edge, where each request can be mediated according to identity, device state, policy rules, and contextual factors. Such a model supports continuous verification and can adapt access if risk conditions change during an active session.

The objective of this paper is to propose and analyze a router-based ZTNA gateway architecture for secure work-from-home environments. The study focuses on how such a gateway can authenticate users, assess device trust, apply policy-driven authorization, and restrict access to specific enterprise applications rather than exposing internal network segments. The paper also examines how this approach compares conceptually with traditional VPN-based remote access in terms of trust assumptions, segmentation, and resistance to lateral movement.

2 Literature Review

The literature on Zero Trust Architecture (ZTA) has expanded in response to the collapse of the traditional enterprise perimeter. As organizations adopted cloud services, remote work, bring-your-own-device practices, and distributed application hosting, older security models based on fixed network boundaries became less effective. NIST frames zero trust as a direct response to these shifts and defines it as a cybersecurity paradigm that moves defenses away from static network perimeters and toward users, assets, and resources.

A detailed review of the literature shows that current work can be grouped into five main areas: foundational zero trust theory, ZTNA for remote access, implementation-oriented architecture studies, edge- and gateway-centric security models, and research on deployment challenges. Across all of these areas, a common theme appears: security decisions should be made dynamically using identity, device state, policy context, and continuous assessment rather than relying on location-based trust. However, fewer studies directly examine the router or home gateway as the main enforcement point, which leaves a clear opportunity for the present work**.**

2.1 Foundational Zero Trust Literature

The most important foundational literature is NIST SP 800-207, which formalized the modern conceptual model of Zero Trust Architecture. This work established the principle that no user or device should receive trust solely because it is inside a corporate network or located on an enterprise-managed segment. Instead, authentication and authorization must be performed before access to an enterprise resource is granted, and access decisions must be tied to explicit policy evaluation.

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

A major contribution of this literature is that it redefines what needs protection. Earlier security models concentrated on defending network boundaries, but NIST's framework emphasizes the protection of resources themselves, including applications, services, workflows, and data. This is especially relevant to remote-access security because it supports the idea that a user should be allowed to reach only the specific resource required for a task rather than receiving broad network-level connectivity.

The foundational literature also provides the logical components that later studies build upon. NIST identifies elements such as the policy engine, policy administrator, and policy enforcement point, which together enable dynamic access control. These components have become central references in later ZTNA, SASE, and enterprise zero trust implementations. As a result, nearly all serious literature on zero trust traces its conceptual structure back to this NIST model.

2.2 Zero Trust for Remote Access

A second major body of literature focuses on the use of zero trust for remote access. This literature argues that traditional VPNs are insufficient because they often create a trusted tunnel into a wider enterprise network after the user authenticates once. In distributed work environments, where users connect from home networks, public networks, and mixed personal or managed devices, this level of network exposure increases risk. NIST's publications repeatedly identify remote users and non-enterprise environments as major reasons for adopting zero trust.

ZTNA emerged in this literature as the practical remote-access expression of zero trust principles. Instead of exposing internal subnets or entire segments, ZTNA limits access to approved applications or services. This application-centric approach aligns with least privilege, reduces the attack surface, and lowers the chance of lateral movement after compromise. The literature therefore positions ZTNA not simply as a product category, but as a more precise way to operationalize zero trust for remote users.

The literature also emphasizes that remote-access control must account for more than user credentials. Strong ZTNA systems combine identity verification with device posture, contextual awareness, continuous monitoring, and policy-based decisions. This broader understanding of trust is central to the move from "log in once, trust continuously" to "verify continuously, allow conditionally."

2.3 Implementation-Oriented Literature

A third category of literature examines how zero trust can be implemented in real organizations rather than only described conceptually. NIST SP 1800-35 and associated NCCoE materials are especially important here because they move beyond abstract principles and provide practical implementation guidance. NIST explains that a zero-trust architecture enables secure authorized access to enterprise resources distributed across on-premises and multiple cloud environments, and the corresponding implementation work provides 19 example architectures built with commercial off-the-shelf technologies.

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

This implementation-focused literature is valuable because it demonstrates that zero trust is not a single product or one fixed topology. Instead, it can be realized through multiple architectural patterns depending on the organization's environment, applications, identity infrastructure, and deployment constraints. The literature also shows that practical ZTA adoption involves staged integration rather than immediate replacement of all older systems.

Another contribution of implementation literature is its emphasis on real-world scenarios. NIST's guidance includes use cases involving multiple cloud platforms, branch environments, and public Wi-Fi conditions for remote employees. These scenarios are highly relevant to work-from-home security because they reflect the operational complexity of distributed enterprise access rather than assuming a clean, centralized environment.

However, this literature is generally enterprise-wide and vendor-neutral. It offers models, patterns, and deployment choices, but does not focus specifically on whether the router itself can serve as the central zero trust enforcement point in a work-from-home architecture. This leaves room for more specialized research such as the present study.

2.4 Edge and Gateway-Centric Literature

A fourth line of literature examines the movement of security enforcement closer to the network edge. This includes studies and architecture guidance related to SASE, SD-WAN-integrated security, secure service edge, and gateway-based policy control. In these models, identity, inspection, and access enforcement are placed closer to users, branches, or service edges in order to reduce latency, simplify policy distribution, and avoid unnecessary traffic backhauling.

This literature is highly relevant to the proposed study because it shows a broader trend toward distributed enforcement rather than sole dependence on a central perimeter. Edge-centric models support the idea that the first point of network mediation can also become the first point of trust evaluation. In other words, the gateway is no longer just a transport component; it becomes part of the security control plane.

Even so, much of this literature discusses gateways in broad operational terms rather than as the core research object. It commonly describes edge functions in product architecture or implementation terms, but fewer works isolate the router or home edge gateway as the main locus of zero trust policy enforcement for remote users. This is where the present paper can contribute a narrower and more targeted architectural argument.

2.5 Literature on Challenges and Limitations

A fifth major group of literature focuses on the challenges of zero trust deployment. Survey work on ZTA highlights difficulties such as policy complexity, legacy-system integration, identity sprawl, scalability concerns, telemetry overload, usability friction, and the challenge of coordinating multiple security systems into a coherent trust model. These studies are important because they show that zero trust is not only a conceptual improvement but also an operational challenge.

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

One recurring concern in the literature is the complexity of policy definition. Because zero trust decisions depend on identity, device state, resource sensitivity, and context, the policy layer can become difficult to design, audit, and maintain. Another issue is that many enterprises still depend on legacy applications that do not integrate easily with modern identity and posture-aware systems. These limitations directly affect any effort to implement ZTNA, including a router-based model.

2.6 Research Gap

Although the literature strongly supports the principles of zero trust and the use of ZTNA for remote access, a specific research gap remains around router-based enforcement for work-from-home environments. Most foundational studies are conceptual. Most implementation studies are broad and enterprise-wide. Most edge-oriented studies discuss service-edge platforms, SD-WAN appliances, or cloud-delivered enforcement rather than a dedicated router-based gateway as the focal architecture.

This gap matters because work-from-home access introduces a distinct operational context. Users connect from networks that the enterprise does not fully control, devices may shift between compliant and noncompliant states, and applications may be distributed across cloud and on-premises environments. A router-based ZTNA gateway could provide a practical response by combining access brokering, traffic mediation, and policy enforcement at the point where remote access begins. Yet this possibility is not fully developed in the current literature.

The present study therefore builds upon existing work while narrowing the focus to a more specific architectural question: can the router itself function effectively as the zero trust enforcement layer for secure work-from-home access? This question is consistent with zero trust principles, supported by broader implementation trends, and still underexplored enough to justify dedicated study.

Literature area	Main contribution	Limitation relative to this study
Foundational ZTA literature	**Defines zero trust principles, resource-focused protection, and logical components such as policy engine and enforcement point**	**Mostly conceptual, not focused on router-based work-from-home enforcement.**
Remote-access ZTNA literature	**Replaces broad VPN access with application-specific, policy-controlled access for distributed users.**	**Usually discusses generic ZTNA rather than router-level enforcement.**
Implementation literature	**Shows that zero trust can be deployed in multiple practical ways using existing technologies.**	**Focuses on broad enterprise patterns rather than a single router-based architecture.**

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

Literature area	Main contribution	Limitation relative to this study
Edge and gateway-centric literature	Supports moving policy enforcement closer to the user or access edge. nist+1	Often product- or platform-oriented, not a focused academic treatment of router-based ZTNA.

3 Related Work

Research and standards literature on Zero Trust Architecture (ZTA) has grown rapidly as enterprises have moved away from perimeter-centric security toward identity-aware, resource-focused protection models. NIST's foundational work defines zero trust as a cybersecurity paradigm that removes implicit trust based on network location and instead requires explicit authentication and authorization for each instance of resource access. This standards-driven view has strongly influenced later research and industry implementations of Zero Trust Network Access (ZTNA), secure service edge, and segmented remote-access designs.

Most existing work does not treat the home router or edge gateway as the primary object of study. Instead, the literature tends to focus on conceptual zero trust principles, cloud-based enforcement systems, identity-centric access control, and enterprise-wide deployment blueprints. This creates an opportunity for the present study, which examines whether a router-based gateway can serve as a practical zero trust enforcement point for work-from-home environments.

3.1 Foundational Zero Trust Literature

The earliest and most influential related work comes from NIST SP 800-207, which formalized the conceptual model of Zero Trust Architecture. This publication established the core idea that security decisions should center on users, assets, and resources rather than on trusted network boundaries. It also introduced the key logical components of a zero trust system, including the policy engine, policy administrator, and policy enforcement point. These concepts remain central to nearly all later ZTA and ZTNA literature.

A major contribution of this foundational work is its clear separation between access decision-making and network location. In earlier perimeter-driven systems, location inside the enterprise network often implied some level of trust. In contrast, the NIST model treats all access as potentially risky and requires policy-based evaluation before any resource interaction is permitted. This conceptual shift has influenced both academic research and product design across enterprise remote-access technologies.

3.2 Zero Trust for Remote Access

A second stream of related work focuses on remote access and distributed workforces. NIST's zero trust publications repeatedly highlight remote users, bring-your-own-device

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

practices, and cloud-hosted resources as major reasons why legacy network security models are no longer sufficient. This line of work is highly relevant to work-from-home security because it frames remote access not as a temporary exception to enterprise policy, but as a normal operating condition requiring continuous trust evaluation.

The main theme across this literature is that authentication alone is not enough. Remote-access systems must also consider device posture, contextual risk, session monitoring, and resource sensitivity before granting or maintaining access. These requirements align closely with ZTNA, which narrows access to specific applications rather than exposing broad internal connectivity. As a result, related work in this area consistently supports resource-level access control as a more secure alternative to legacy VPN-style connectivity.

3.3 Implementation-Oriented Work

A more recent body of work has moved from abstract zero trust principles toward concrete implementation strategies. NIST SP 1800-35 and the associated NCCoE project provide practical guidance for building zero trust architectures using commercial off-the-shelf technologies. According to NIST, the finalized guidance includes 19 example architectures and captures results and best practices from a multi-vendor effort to demonstrate end-to-end ZTA deployments. This is important related work because it shows that zero trust is no longer only a conceptual framework; it now has multiple validated deployment pattern.

However, these implementation studies are broad and enterprise-oriented. They examine multiple architectural patterns across cloud, on-premises, and hybrid environments, but they do not specifically center the research question on a router-based ZTNA gateway for home users. The present study differs by narrowing the scope to the network edge and asking how policy enforcement can be embedded at the access gateway itself.

3.4 Edge, SASE, and Gateway-Centric Approaches

Another important area of related work involves secure access service edge (SASE), security service edge (SSE), and SD-WAN-integrated ZTNA models. These approaches extend zero trust principles toward distributed enforcement at cloud points of presence, branch gateways, and edge appliances. Current architectural explanations of SASE position ZTNA as one component in a broader inspection and policy framework that may also include secure web gateways, CASB, and SD-WAN routing.

Industry demonstrations also show movement toward placing ZTNA and policy logic closer to the edge. For example, recent gateway-oriented demonstrations describe ZTNA or SSE connectors running directly on SD-WAN appliances to avoid traffic hair pinning when applications reside in branch or distributed environments. This is highly relevant to the proposed study because it supports the practical feasibility of edge-resident access enforcement, even though it is usually presented from a product or architecture perspective rather than a focused academic one.

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

3.5 Research Gap

Although related work has established the value of zero trust, resource-focused protection, and edge-aware security, there is still a noticeable gap in how router-based enforcement is studied for work-from-home scenarios. Most literature either remains conceptual, focuses on cloud-centric identity enforcement, or discusses enterprise deployment patterns at a high level. Fewer works isolate the home or branch gateway as the central research object and analyze its role as a dedicated policy enforcement point for identity-aware and device-aware access control.

This gap matters because work-from-home environments present a distinct mix of challenges: unmanaged local networks, variable endpoint security, distributed applications, and the need to limit lateral exposure without harming usability. A router-based ZTNA gateway directly addresses these conditions by placing policy enforcement where remote connectivity begins. The present paper therefore extends related work by connecting established zero trust theory with a more specific, edge-centered architectural model for home-based access security.

4 Popular Techniques used

Zero Trust Network Access is built from a set of well-established security techniques that replace implicit network trust with explicit, policy-driven verification. NIST defines zero trust around continual evaluation and identifies core architectural elements such as the policy engine, policy administrator, policy decision point, and policy enforcement point. In practical deployments, these ideas are translated into a smaller group of recurring techniques that shape most ZTNA systems.

For this study, the most relevant techniques can be grouped into five major categories: identity-based authentication, device posture assessment, least-privilege access, microsegmentation, and policy enforcement with continuous verification. These five are sufficient to explain how modern ZTNA systems work and to show how the proposed router-based gateway differs from more generic implementations

4.1 Identity-Based Authentication

Identity-based authentication is a foundational technique in zero trust systems because access decisions are tied to the verified identity of the user rather than to network location. This usually involves identity and access management services, single sign-on integration, multi-factor authentication, and sometimes certificate-based methods. NIST emphasizes that authentication and authorization must occur before a session to an enterprise resource is established, which makes identity verification central to ZTNA design.

In conventional ZTNA deployments, identity verification is often handled through a centralized identity provider or cloud access broker. In the proposed router-based model, the same principle is retained, but the router acts as the immediate enforcement layer that consumes identity assertions before allowing traffic toward internal applications. This means identity is not only checked at a remote cloud gateway but also translated directly into edge-level routing and access decisions

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

4.2 Device Posture Assessment

Device posture assessment checks whether the endpoint requesting access satisfies required security conditions, such as patch status, certificate presence, management enrollment, or endpoint protection state. This technique is important because zero trust does not assume that a valid user is safe if the device itself is compromised or unmanaged. NIST's zero trust terminology includes telemetry and supporting information in policy decisions, which makes device health an important input for access control.

In many common ZTNA systems, posture information is collected by endpoint agents or management tools and then consumed by a policy service. In the proposed model, the router-based gateway would use posture results as part of its access control logic before creating a path to an enterprise application. Compared with generic approaches, this creates a more direct connection between endpoint state and edge-network enforcement.

4.3 Least-Privilege Access

Least-privilege access is one of the most popular and important techniques in ZTNA. OWASP describes least privilege as giving the minimum access needed to perform a task, which aligns closely with zero trust's emphasis on protecting resources instead of broadly exposing networks. In remote access, this typically means a user receives access only to a specific application or service, not to an entire subnet or internal segment.

In standard ZTNA implementations, least privilege is often enforced by brokers or proxies that map a user to a small set of approved applications. In the proposed router-based ZTNA gateway, least privilege is enforced at the network edge by forwarding only the traffic associated with explicitly authorized resources. This gives the router a stronger role in translating security policy into actual traffic restriction.

4.4 Microsegmentation

Microsegmentation divides enterprise resources into smaller trust zones so that compromise in one area does not automatically expose others. This technique is widely used in zero trust because it reduces lateral movement and limits the damage caused by stolen credentials or infected endpoints. OWASP's zero trust guidance and NIST's architecture principles both support the idea of narrowing trust boundaries around resources.

In many environments, microsegmentation is implemented using software-defined policy controls, internal firewalls, or service-level segmentation. In the proposed router-based approach, segmentation can also be reflected at the gateway itself by exposing only approved destinations and keeping internal services hidden from general network visibility. This does not replace internal segmentation, but it strengthens it by adding an outer application-aware control point at the edge.

4.5 Policy Enforcement and Continuous Verification

Policy enforcement and continuous verification form the operational core of zero trust. NIST defines the policy enforcement point as the component that enables, monitors, and terminates connections, while the policy engine decides whether access should be granted,

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

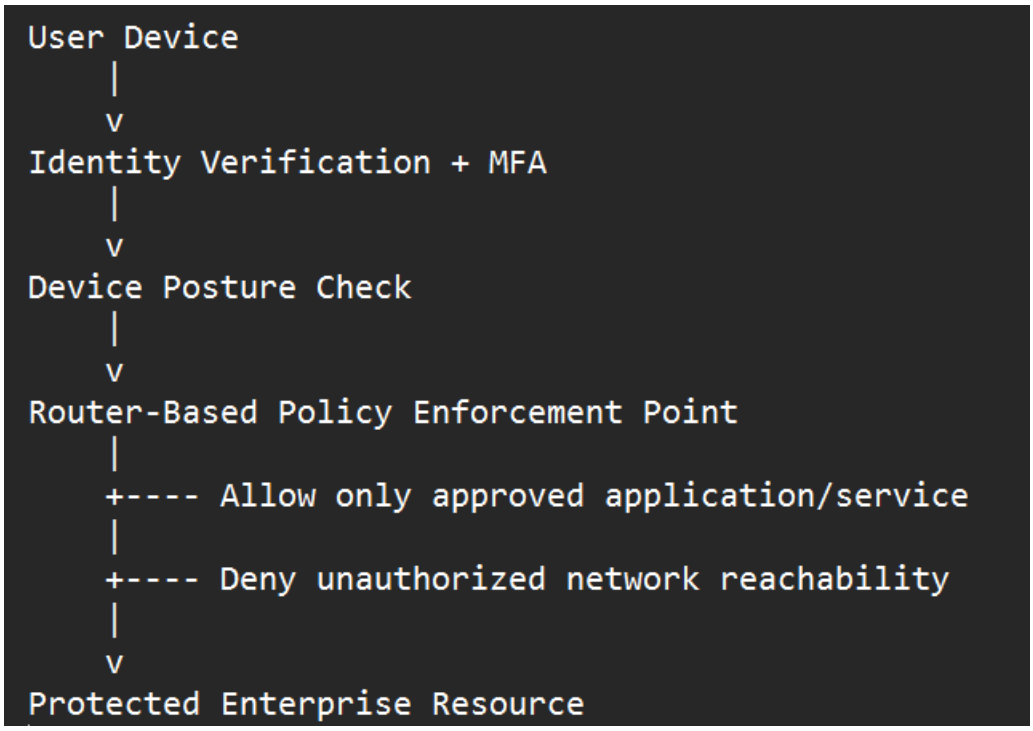
denied, or revoked based on policy and trust information. This makes policy enforcement more dynamic than traditional firewall allow/deny logic because decisions can change during the life of the session.

In common ZTNA architectures, this function may exist in a broker, reverse proxy, cloud edge service, or application gateway. In the proposed router-based model, the router itself acts as the policy enforcement point or hosts that functionality at the edge. This is a key distinction of the study, because it places continuous verification closer to the access path and makes the gateway a central control device rather than only a transport appliance.

Technique	Common ZTNA implementation	Proposed router-based ZTNA model
Identity-based authentication	Verified through IdP, SSO, and MFA before app access is allowed.	Identity is verified similarly, but the router directly enforces the resulting access decision at the edge.
Device posture assessment	Endpoint telemetry is checked by centralized policy systems or brokers.	Posture results are consumed by the router-based gateway before application traffic is forwarded.
Least-privilege access	Users are mapped to specific applications instead of full network tunnels.	The router enforces resource-specific forwarding so only authorized traffic reaches enterprise services.
Microsegmentation	Implemented through internal segmentation, software controls, or service-level isolation.	The router adds an edge-level segmented entry point that hides internal services and reduces exposure.
Policy enforcement and continuous verification	Usually handled by brokers, proxies, or cloud-based gateways.	The router functions as the policy enforcement point, enabling dynamic edge-based access control.

International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

Conceptual Diagram



This diagram shows the main difference between the proposed model and generic remote-access approaches. Instead of giving the user a broad tunnel into the enterprise after authentication, the router-based gateway evaluates identity, device state, and policy first, then permits only the exact approved service path. That makes the edge router an active zero trust control point rather than a passive forwarding node

5 Existing Architecture

The existing architecture for Zero Trust Network Access is typically built around a centralized identity provider, a policy decision layer, and a policy enforcement point that mediates access to protected applications. In practice, a remote user first authenticates through the identity system, the gateway checks posture or context, and then the ZTNA service proxies traffic only to the approved application rather than exposing the full internal network. This is the standard model used in many modern ZTNA deployments and aligns with NIST's zero trust guidance on policy enforcement and continuous verification

5.1 Identity Layer

The identity layer is the first component of the architecture. It usually includes single sign-on, multi-factor authentication, and directory services such as enterprise identity providers. NIST's zero trust model treats authentication and authorization as discrete steps before access is established, so identity is never assumed from network location alone.

International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

5.2 Policy Decision Layer

This layer evaluates whether the access request should be allowed. It checks user identity, device status, and contextual signals, then returns a grant or deny decision. In zero trust terminology, this is the policy engine or policy decision point, which works together with the enforcement point.

5.3 Policy Enforcement Layer

The enforcement layer is where traffic is actually allowed or blocked. In common ZTNA designs, this is a cloud connector, proxy, or service edge that sits between the user and the application. Cisco's ZTNA architecture, for example, describes a service edge acting as a proxy while authentication and posture checks occur before routing traffic to the application.

5.4 Application Access Layer

Instead of exposing the whole private network, the user receives access only to the specific application or service. This app-centric model reduces lateral movement and limits the blast radius if credentials or an endpoint are compromised. That is one of the main reasons ZTNA is preferred over legacy VPN-style remote access.

5.5 Monitoring and Telemetry Layer

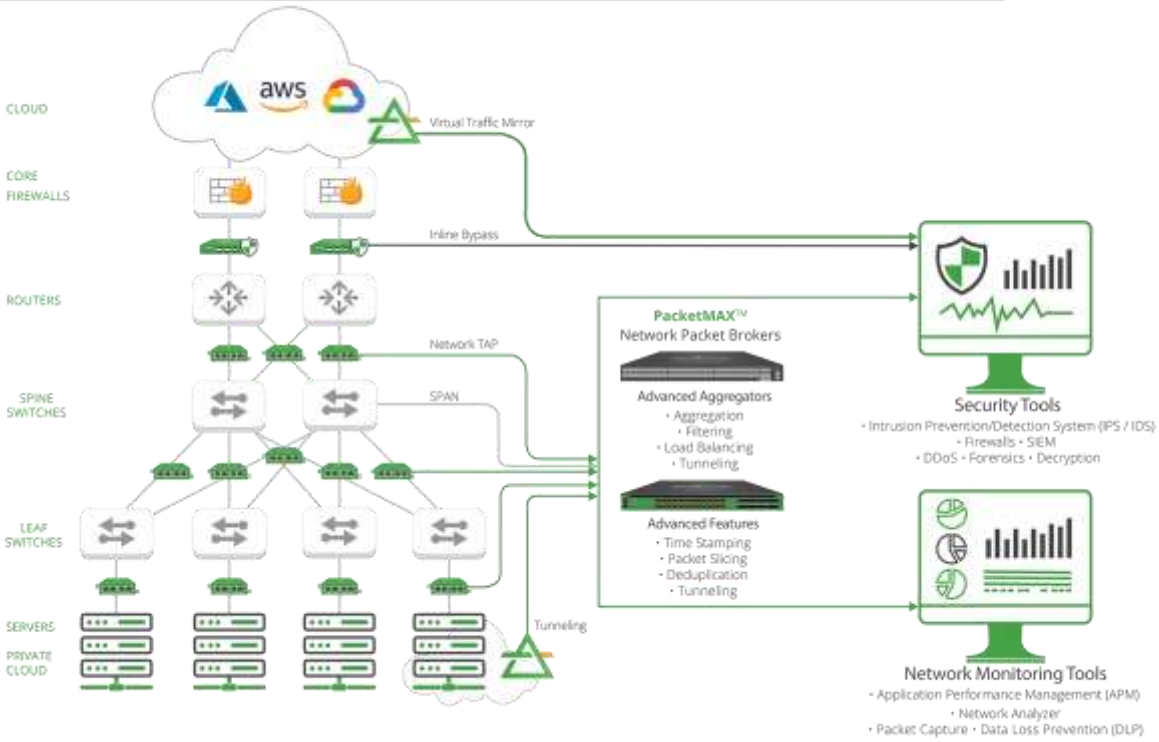
Modern ZTNA architectures also include telemetry, logging, and continuous monitoring. The policy system can keep evaluating session behavior and may revoke access if risk changes during the session. This makes the architecture more adaptive than traditional one-time authentication models.

The existing architecture is usually cloud-proxy centric, while the proposed architecture in your paper is router-centric. In the common model, the ZTNA broker or service edge becomes the main gatekeeper, whereas in your proposed model, the router or gateway itself becomes the enforcement point. This difference is important because it moves security control closer to the user's access point and can reduce dependency on a separate cloud proxy for every decision.

Aspect	Existing ZTNA Architecture	Proposed Router-Based Architecture
Enforcement point	Cloud proxy, broker, or service edge.	Router or gateway at the network edge.
Trust model	Identity and posture are checked before app access.	Same trust model, but enforced directly by the router.
Access scope	Application-specific access	Application-specific access only.

International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

Aspect	Existing ZTNA Architecture	Proposed Router-Based Architecture
	only.	
Traffic path	User → ZTNA cloud/service edge → application.	User → router/gateway → application.
Control location	Mostly outside the local network edge.	Directly at the local edge device.



6 Challenges in Existing and Proposed ZTNA Models

Zero Trust Architecture is effective, but it is not easy to implement because it requires continuous verification, strict policy control, and integration across mixed environments. Recent surveys and implementation guides highlight common challenges such as legacy system compatibility, IAM complexity, policy management, monitoring overload, performance overhead, and user friction.

6.1 Legacy System Compatibility

One of the biggest challenges is integrating zero trust with legacy infrastructure. Many organizations still depend on older applications, static access rules, and systems that were

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

never designed for identity-driven or policy-based access. This makes it difficult to retrofit ZTNA controls without redesigning parts of the environment.

For your proposed router-based model, this means the gateway may have to support older services that cannot speak modern identity protocols cleanly. That can force the design to rely on workarounds, protocol translation, or partial enforcement, which may weaken the purity of the zero trust model.

6.2 Identity and Policy Complexity

Zero trust depends heavily on identity, device posture, and dynamic policy decisions. The challenge is that these policies can become very detailed and difficult to manage, especially when users, devices, and applications change frequently. Research also notes that unclear trust thresholds, weak policy definitions, and accountability gaps in policy engines can reduce the reliability of enforcement.

In your router-based architecture, this becomes a design challenge because the router must interpret policy decisions accurately and consistently. If the policy logic is too complex, the gateway may become hard to administer, harder to audit, and more error-prone in real deployments

6.3 Monitoring and Visibility

A zero-trust system only works well when it has good visibility into users, devices, traffic, and session behavior. Surveys of ZTA implementations point out that large volumes of telemetry, fragmented security tools, and inconsistent visibility across cloud and on-premises resources can create blind spots or alert fatigue.

For a router-based ZTNA gateway, visibility is both a strength and a challenge. The router can see access attempts at the edge, but it still needs clean integration with identity systems, endpoint tools, and logging platforms. Without that integration, the gateway may enforce access mechanically but fail to provide enough context for real security decisions.

6.4 Performance and Scalability

Another major challenge is the performance cost of continuous verification and fine-grained access control. Zero trust often adds authentication steps, telemetry checks, encryption overhead, and policy evaluation latency, all of which can affect user experience if the system is not well optimized. This is especially important for remote users who expect fast and stable access from home networks.

For your proposed design, the router must process policy decisions without becoming a bottleneck. If the gateway is overloaded, users may experience delays, dropped sessions, or unstable access, which could make the system less practical than a traditional VPN in some environments.

6.5 User Experience and Adoption

The final challenge is usability. Zero trust systems can frustrate users if they require too many re-authentication steps, overly strict device checks, or access prompts that interrupt

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

normal work. Literature on ZTA adoption notes that excessive friction can lead users to seek workarounds, which creates new security problems.

This is important for your paper because a router-based ZTNA gateway must balance security and convenience. If the system is too strict, users may resist it; if it is too loose, it loses the benefit of zero trust. The proposed architecture should therefore aim for strong policy enforcement with minimal disruption to legitimate work-from-home activity.

Challenge	Impact on ZTNA	Impact on Router-Based Model
Legacy compatibility	Hard to retrofit modern identity and policy controls into older systems.	Gateway may need protocol translation or exceptions for older services.
Policy complexity	Dynamic rules are difficult to define, maintain, and audit.	Router must execute policy accurately without becoming too complex.
Monitoring visibility	Tool fragmentation can create blind spots and alert overload.	Router must integrate with logging and telemetry systems.
Performance overhead	Continuous checks may add latency and processing cost.	Router may become a bottleneck if not optimized.
User adoption	Too many prompts or checks reduce usability.	Home users may resist if access becomes slow or disruptive.

7 Future Research Directions

Future work on a **router-based Zero Trust Network Access gateway** can extend the current concept in several useful directions. Since the proposed model is still architectural and conceptual, the next research step should focus on validating it through prototype testing, performance analysis, and security evaluation in realistic work-from-home conditions.

7.1 Prototype Implementation

A natural next step is to build a working prototype of the proposed router-based ZTNA gateway. NIST notes that zero trust architectures can be implemented in multiple ways and that some designs protect groups of resources through gateway security devices, which

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

supports the feasibility of treating the router as an enforcement layer. A future prototype could integrate a home or branch router with an identity provider, multi-factor authentication, device-posture checks, and a policy engine so that access to enterprise applications is mediated directly at the edge.

Such a prototype should be designed to test whether the router can reliably perform the functions expected of a policy enforcement point. This includes establishing user sessions, validating identity tokens, consuming device-trust signals, forwarding only authorized application traffic, and logging access decisions for later inspection. NIST's published implementations show that zero trust studies become far more useful when they move from abstract architecture to concrete builds and validated use cases.

Future studies could also compare different implementation choices for the prototype. For example, one prototype may use a software-defined router or virtual appliance, while another may use a dedicated edge router with integrated policy modules. Comparing these variants would help determine whether router-based ZTNA is best realized as a lightweight software gateway, an enterprise branch appliance, or a hybrid design that coordinates local enforcement with a cloud policy service.

7.2 Comparative Performance Evaluation

Another important research direction is comparative performance evaluation. NIST's implementation work emphasizes not only architectural correctness but also tested results across realistic enterprise scenarios, which suggests that future router-based ZTNA studies should measure how the proposed design behaves under load and under normal user activity. A router-based enforcement model should therefore be compared with at least two common alternatives: a traditional VPN-based remote-access model and a cloud-brokered ZTNA model.

Performance evaluation should include standard network and security metrics such as connection setup time, authentication delay, policy-decision latency, application response time, throughput, session stability, and resource utilization on the router or gateway. These metrics would help determine whether moving enforcement to the router adds operational cost or instead reduces latency by keeping decisions closer to the access edge. The analysis should also measure how quickly the system reacts to changing trust conditions, such as posture failure or policy revocation during an active session, because continuous verification is a defining feature of zero trust.

A well-designed comparative study could also test security effectiveness alongside performance. For example, researchers could simulate credential theft, unauthorized device access, or lateral-movement attempts and then compare how each architecture responds. This would provide stronger evidence than a purely conceptual argument, because it would show both the security benefits and the trade-offs of router-based enforcement relative to VPN and broker-centric ZTNA models.

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

7.3 Policy Automation

Another direction is automating policy decisions using contextual signals such as device health, time of access, risk score, and user role. This would make the gateway more adaptive and reduce the need for manual rule updates. Research could also explore whether machine learning or rule-based engines give better access decisions.

7.4 Legacy Application Support

Many organizations still use older applications that are difficult to secure with modern identity systems. Future work can study how the router-based ZTNA gateway handles legacy services, including protocol translation, segmentation wrappers, or proxy-based access. This is important because real enterprise environments rarely consist only of modern applications.

7.5 Security Validation

The architecture should be tested against common attacks such as credential theft, lateral movement, session hijacking, and unauthorized access attempts. Future studies can model how much risk is reduced when access is limited to application-level authorization at the edge. This would help prove whether the design actually improves resilience.

7.6 Scalability and Deployment

Future research should also examine how the proposed architecture behaves in real-world deployment scenarios. NIST's zero trust guidance explicitly uses scenarios that reflect modern enterprise complexity, including distributed resources across on-premises and multiple cloud environments, branch offices, and remote users connecting through public Wi-Fi. These scenarios provide a strong template for evaluating router-based ZTNA in conditions that are closer to operational reality than a simple lab test.

One useful scenario is a work-from-home employee connecting from a managed laptop through a residential router to reach a small set of internal business applications. This can be used to test application-specific access, posture-aware policy enforcement, and the effect of normal household network conditions on latency and session reliability. A second scenario could involve a branch or small office router serving multiple users who need access to a mix of on-premises and cloud-hosted enterprise services, which would help evaluate scalability and policy consistency at the edge.

A third scenario should involve higher-risk conditions, such as access from public Wi-Fi, device noncompliance, or attempts to reach unauthorized resources. NIST specifically includes public Wi-Fi use cases in its implementation guidance, making this a strong reference model for future studies of router-based ZTNA under adverse conditions. Testing in such scenarios would help determine whether the proposed architecture can maintain low trust assumptions without making legitimate access impractical for users.

International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

8 Conclusion

The increasing dependence on work-from-home and hybrid access models has made traditional perimeter-based remote-access security less effective for modern enterprises. NIST's zero trust guidance explains that security should focus on protecting resources rather than trusting users or devices because of their network location, especially in environments with remote users and distributed assets. In this context, Zero Trust Network Access provides a more secure approach by enforcing identity-aware, policy-driven, and application-specific access instead of broad network connectivity**.**

This paper proposed a router-based Zero Trust Network Access gateway as a practical architecture for securing work-from-home environments. The central idea is that the router or gateway should not act only as a packet-forwarding device, but also as a policy enforcement point that validates user identity, checks device posture, applies access policy, and limits communication to authorized enterprise resources. This aligns with NIST's zero trust model, which uses policy decision and enforcement functions to control access dynamically and continuously.

The study also examined the background, conceptual basis, related work, existing architecture, common techniques, and implementation challenges associated with ZTNA. The analysis showed that identity-based authentication, device posture assessment, least-privilege access, microsegmentation, and continuous verification are the major techniques that make ZTNA effective. When these techniques are applied at the router level, the architecture can reduce implicit trust, narrow attack surfaces, and limit lateral movement opportunities for remote users connecting from home networks.

At the same time, the paper identified important practical challenges. These include legacy system compatibility, policy complexity, monitoring integration, performance overhead, and the need to preserve usability for legitimate users. NIST's implementation work shows that zero trust adoption is possible through multiple real-world architectures, but it also confirms that deployment requires careful planning, clear policy design, and strong coordination between identity, endpoint, network, and monitoring systems.

Overall, the proposed router-based ZTNA gateway represents a meaningful architectural extension of existing zero trust principles. It preserves the core idea of continuous verification and resource-specific access while shifting enforcement closer to the network edge, where remote access begins. As enterprises continue to secure distributed users and resources, this approach offers a relevant and practical direction for strengthening remote-access protection in work-from-home environments

References

[1] Deepstrike.io, "Remote Work Security Risks 2025: Protecting Distributed Teams," Oct 2025.

[2] CM-Alliance, "Redefining Secure Remote Work In 2025," Oct 2025.

July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/b7v66f97

[3] Seraphic Security, "Secure Remote Access in 2025: Risks, Protocols & Best Practices," Nov 2025.

[4] Xage Security, "Zero Trust Remote Access Solution - ZTRA," May 2025.

[5] TechTarget, "How to secure a home network for remote workforces," 2020.

[6] CloudThat, "Remote Work Security: Challenges and Solutions for 2025," Mar 2025.

[7] Alkira, "Zero Trust Network Access: Enabling Secure, Scalable Remote Connectivity," May 2025.

[8] Pivit Global, "Implementing Zero Trust Architecture in Remote Work Environments," Mar 2025.

[9] Forcepoint, "What Is Zero Trust Remote Access?," Mar 2025.

[10] Zscaler, "Zero Trust Network Access (ZTNA) – Benefits & Overview," 2024.

[11] InstaSafe, "Secure Remote Access: Safeguarding Networks in 2024," Mar 2025.

[12] Palo Alto Networks, "What Is Zero Trust Network Access (ZTNA)?," 2020.

[13] Fortinet, "ZTNA agentless web-based application access," 2024.

[14] Cloudflare, "What is microsegmentation?," 2024.

[15] TechNewsWorld, "AI Raises the Bar for Home Network Security," Jan 2022.

[16] Cato Networks, "Introducing AI-Driven Policy Management for Better Security," May 2025.

[17] Nano-NTP, "Adaptive AI-Driven Security Framework for Work-from-Home," 2025.

[18] USPTO Patent 11785050, "Security management system for remote working environment," 2023.