InstaSafe
Cloud. Secure. Instant.

ZERO TRUST ARCHITECTURE COMPARISON GUIDE

DIRECT ROUTED ZTNA

VS

CLOUD ROUTED ZTNA

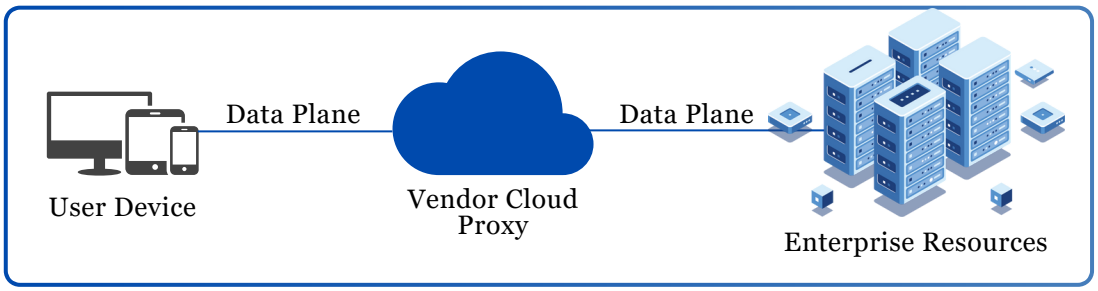
Introduction to Zero Trust Security Model

Traditionally, organizations were focused on implementing security measures at the network perimeter level. The traditional perimeter-based security model assumes everything inside the perimeter is trusted. However with the increased adoption of cloud services, hybrid work environments, and mobile devices augmented with increasing sophistication of cyber threats, perimeter security is no longer adequate.

Zero Trust Access is a perimeter-less security model which ensures right users with right device is accessing authorized enterprise resources with greater visibility and security controls. Zero Trust assumes “Never Trust and Always Verify” be it for internal and external of enterprise network.

Cloud Routed Zero Trust Architecture

In a cloud routed architecture, all the data traffic from user device to enterprise resource is routed through the vendor cloud. Cloud proxy inspects all the user data before routing the traffic to the application server. Cloud proxy contains components of policy engine, policy administrator, and policy enforcement point (PEP).



Disadvantages of Cloud Routed Zero Trust

Cloud routed Zero Trust claims to have more control over the user data against cybersecurity threats but there could be various challenges:

- ***Assumed Trust on Vendor Cloud***: Since all enterprise user data flows through the vendor cloud and all data traffic gets inspected, there could be privacy concerns with enterprise critical data. A vendor managed device shouldn't get the visibility to the data consumed by the users of the organization.

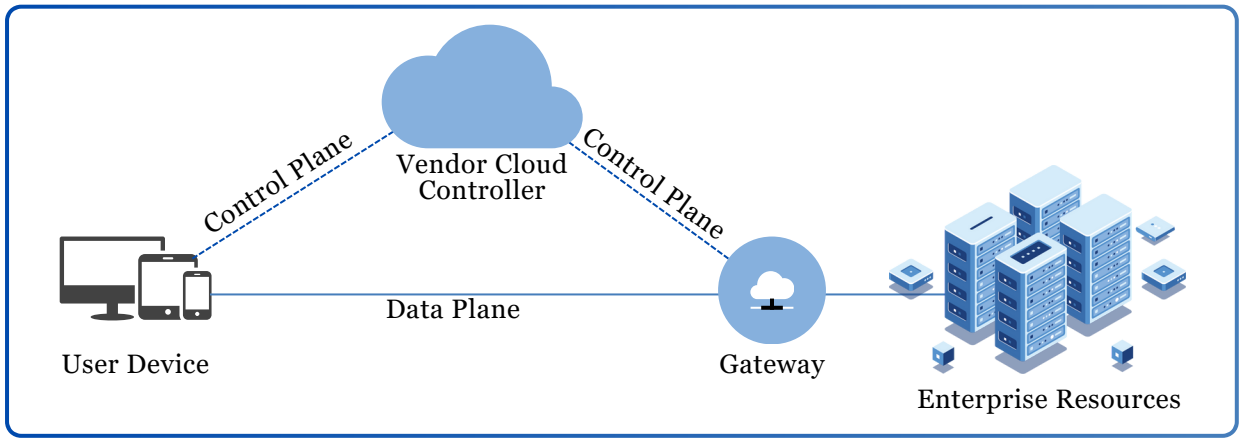
- ***Latency Issues***: Depending on the distance between location of vendor cloud and enterprise server, there could be latency issues associated with vendor cloud bandwidth and availability.

- ***Risk of Supply Chain Attacks***: Once the vendor cloud gets compromised, there arises risk of company data getting compromised.

- ***Hidden/Variable cost of Cloud Services***: Since, all data traffic is routed through the cloud, there could be significant cloud cost that will be added to the annual license cost. With rising cloud cost over the years, subsequent cost of Zero Trust will increase dramatically over the years.

Direct Routed Zero Trust Architecture

In direct routed Zero Trust Architecture, there is a separate Data plane and Control plane. Policy Enginer, Policy administator and Policy Enforcement point are included in Cloud controller. Based on cloud controller directive, secure encrypted tunnel gets established between user device to gateway for data traffic.



Advantages of Direct Routed Zero Trust

There are several advantages of direct routed Zero Trust architecture because of separate data and control plane.

- ***Low Latency***: Because of direct data tunnel established between user device and enterprise resources, there is less latency issues compared to cloud routed architecture.
- ***Flexible Deployment Options***: Both Controller and Gateways can be deployed in hybrid model (On-premise and Public cloud).
- ***Predictable Pricing***: There is no hidden or variable cloud cost associated with this architecture. Customers can be assured of a predictable pricing structure.

The Misunderstood Aspect of Port Opening

When discussing direct-routed ZTNA, the topic of port opening often arises. Port opening, in simple terms, is like selectively opening doors in a building for specific guests. While it may seem risky, it's fundamental to ensuring that the correct data reaches the right place. The process is secured with robust firewalls and authentication protocols, ensuring only authorized traffic passes through these digital doorways. Contrary to common concerns, opening ports is not inherently insecure; it's a controlled and monitored process integral to maintaining a streamlined and secure data flow in direct routing.

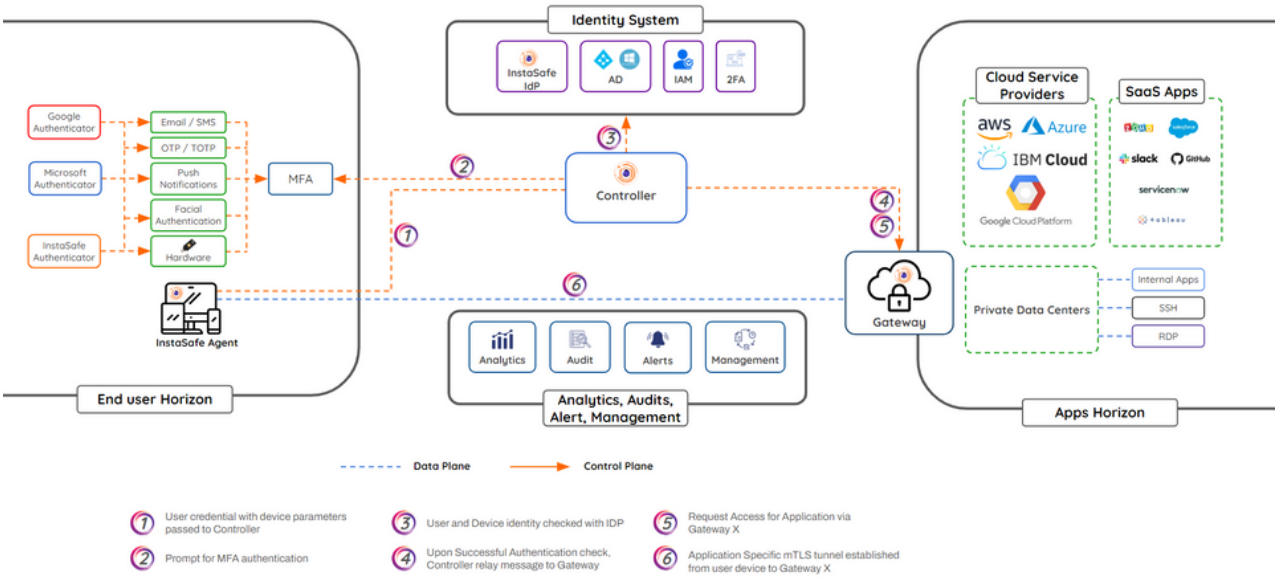
Technical Details

In direct-routed setups, port opening is a crucial aspect of network configuration. It involves configuring network firewalls to allow specific types of network traffic through designated ports, which act as controlled entry and exit points for data, similar to checkpoints.

- ***Purpose and Usage***: Each port is designated for a specific type of service or protocol, such as web servers using port 80 for HTTP traffic. Opening a port means allowing traffic for that particular service.
- ***Security Protocols***: To prevent unauthorized access, strict security protocols are applied, including using secure authentication methods to verify the legitimacy of the traffic and implementing advanced firewall rules that specify which types of traffic are allowed through a port.
- ***Ongoing Management***: Regular monitoring and updating of port configurations are essential to address evolving security threats, which includes closing unused ports, updating firewall rules, and auditing traffic for suspicious activity.

InstaSafe Direct Routed based Zero Trust Architecture

InstaSafe Zero Trust architecture is based on Cloud Security Alliance - Software Defined Perimeter (SDP) based architecture.



InstaSafe Zero Trust Architecture featuring Split Plane Architecture (Data plane and Control plane)

InstaSafe Zero Trust Architecure has three component - ZT Agent, ZT Controller and ZT Gateway. ZT agent is installed on the user device which helps in device authentication. Controller is the policy engine which authenticates user and grants least privilege access as per user roles. Gateway resides on the edge of corporate DC and protected with a Drop All Firewall.

InstaSafe Zero Trust architecture supports L3/L4 and L7 layers of protocols. InstaSafe Zero Trust provide support for integration with customers' third party IDP solution providers such as AD, Azure AD and includes an inbuilt IDP, which helps create and manage the users and user groups.

InstaSafe Zero Trust also enables single sign on functionality for all web based applications. InstaSafe has its own Multi Factor Authenticator which supports OTP, T-OTP, Biometrics, Hardware Token, Passwordless, and Form based authentication.

Conclusion

Choosing between direct-routed and cloud-routed ZTNA depends on an organization's specific needs, capabilities, and security priorities. Direct routing offers a faster, more controlled path, ideal for those who prioritize these aspects and are equipped to manage their network infrastructure. The decision isn't just about the route your data takes; it's about selecting the path that aligns best with your organization's vision of network security and efficiency.

About InstaSafe

InstaSafe's mission is to secure enterprises from the abuse of excessive trust and privilege access. We empower organizations across to globe in preparing their security infrastructure for digital transformation in a cloud-dominated world. Recognized by Gartner as one of the top representative vendors providing Zero Trust Security, InstaSafe Secure Access, InstaSafe Zero Trust Application Access, and InstaSafe Authenticator follow the vision that trust can never be an entitlement, to offer securely enhanced and rapid access of enterprise applications to users situated anywhere across the globe. We secure 500,000 endpoints for more than 150 customers, spread across 5 continents, with our 100% cloud-delivered solutions, ensuring that our offerings are in line with our mission of being Cloud, Secure, and Instant.

Problems? Talk to us

Let's talk more about how InstaSafe can empower your remote workforce through transformational and seamless security.

sales@instasafe.com

www.instasafe.com

You can connect us at:

/instasafe /instasafe /instasafe /instasafeZT