Zero Trust Compliance for Everyone?

Leveraging cloud-based identity and VPN services to overcome remote use ZTA compliance challenges

Security policy planning for remote work whether agency user or contractor can be complex. Proper planning requires careful consideration of each individual posture. This becomes exponentially more difficult when assessment over time identifies an exhausting number of postures that need to be addressed. This can lead to generalized policy application that is at risk of being too strict or too lenient, adversely impacting productivity or increasing potential compromise. What if there was a way to implement zero trust for remote users that mitigates the challenge with diversity of postures to focus on eliminating policy gaps?

The first step is the selection of ZTA architecture variations to be used to address the challenge of securing the network regardless of resource location. NIST 800-207 outlines two architectures that will influence the remote use case design.

Network Infrastructure and Software Defined Perimeters. The remote resource and the application establish a secure channel using a mesh VPN. This falls under other for the NIST guidelines most closely resembling a cloud virtual network. The mesh VPN is a software overlay on the resource providing secure access. The virtual network provides a policy that defines how the resource interacts with other resources on a resource-by-resource basis. Additionally micro segmentation is presumed to be present to further protect corporate resources. This does not add any additional complexity for resource-to-resource communication as the underlying infrastructure is purposefully obfuscated.

Enhanced Identity Governance. The remote resource, including the VPN service access (also a resource) and the application are registered to the identity provider. The resources establish a secure channel used for communication between the IDP and between themselves. The IDP is cloud hosted providing extensibility regards of remote resource location. As described in NIST 800-207 section 3.1.1, the primary requirement for resource access is based on the access privileges granted to the resource. The design also uses other factors such as asset status, and environmental factors to calculate the final confidence level.

Design Review

Network Infrastructure The challenge with a traditional VPN is that it is a tunnel into the network managed with access to network managed through policy on a VPN gateway. It immediately breaks a ZTA tenet that all data sources and computing services are considered resources.

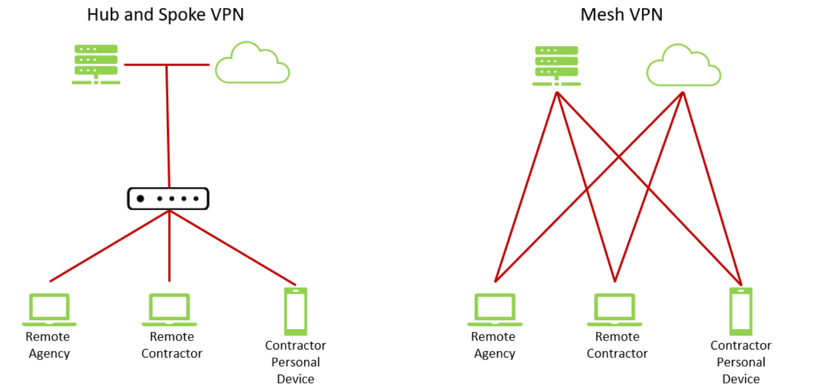


Figure 1. Hub and Spoke VPN vs Mesh VPN

At first review, the remote user with a hub and spoke VPN has the potential to access all resources behind the gateway. This technically looks more secure because the gateway is the only entry point to the network. However, the potential attack surface, the capability to access resources if security is bypassed, is much greater. It requires significant changes to architecture such as arbitrary network segmentation and complex access policies to limit use to specific resources. Furthermore, security is typically implemented with user group access policies to manage complexity. The potential for policy coverage gaps increases significantly.

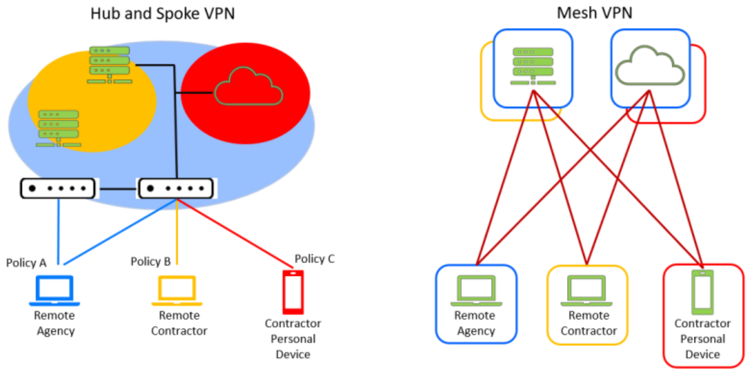


Figure 2. Policy scope Hub and Spoke VPN vs Mesh VPN

Figure two visually represents the attack surface ramifications, especially if the user with access to the full network is compromised. Even if a solid policy is in place to restrict access to assets, users in this architecture still provide the capability for threat actors to exercise discovery and persistence. With the mesh VPN, each device is equal in its implicit deny, is deployed with same software, and is only differentiated by policy for any user as a resource to access any other resource in the network.

Software Defined Perimeter. The software overlay on top of the VPN is what provides the mesh VPN with the ability to manage per resource access. This software overlay has features to do segmentation at a resource level, providing the ability to manage resource to resource access to include routing, DNS directory services, and security access controls. It also creates a process pipeline through its implementation that aligns to identity and application policy decisions to make automation feasible. So, policy actions at the network level become simpler to digest, implement, monitor, and automate per resource.

The software overlay in this design provides seamless integration with identity and application layers. It adds a comprehensive application programming interface (API) to allow for seamless integration with identity and application workflows and policy. This flexibility also drives the software defined integrations for visibility and policy validation that allow for the design to potentially advance the ZTA to an optimal level. The alternative of manually implemented and periodically reviewed layering of enforcement points and gateways on top of legacy applications adds complexity, risk, and latency.

Enhanced Identity Governance. Using enhanced identity governance contributes significantly to addressing the challenges of simplifying the remote use case. Initial access authentication and authorization is managed by the policies defined through planned participation of resources in the mesh VPN. The identity service provider (IDP) is cloud based and is synchronized with the federated authentication for organization affiliated users. Users are presented with an identical workflow to gain access to a privileged resource regardless of where the protected resource exists. The same process is applied whether it is on the organization network, in the cloud as a resource or as a SaaS.

NIST 800-207 calls out use of this model for remote access but warns of the risk involved with granting basic access to the network. This risk is significantly reduced by the mesh VPN software overlay features described in the software defined perimeter section of the publication. This means access through the VPN does not preclude the right to gain even visibility to the resource. Resources can be further protected by utilizing recommendations for a micro segmentation architecture. While it is not called out in the publication, using virtualization to provide segmentation works well in tandem with remote use, especially with organizations that have both privately hosted and cloud hosted applications.

Application, Visibility and Validation to Support Design

Application Enforced Access Control. The design proposed is purpose built to include network and identity polices in the decision-making process to allow access to the application. The application also is responsible for protecting data where a user must pass all security controls to access application hostname/IP. The application though has final say, reviewing policy, identity, and access, to determine whether the user is granted access. Figure three is an example of the high-level call flow that includes the access and identity integration:

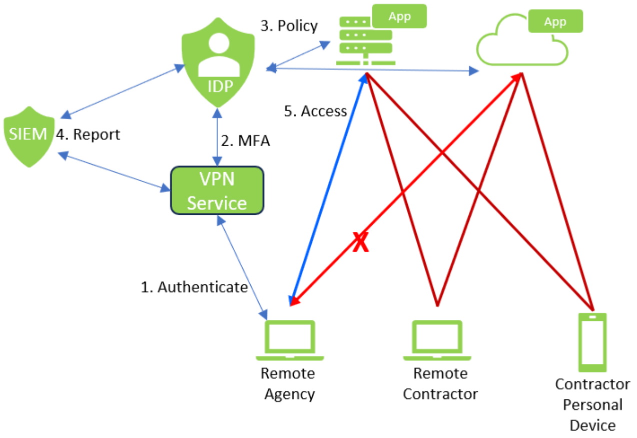
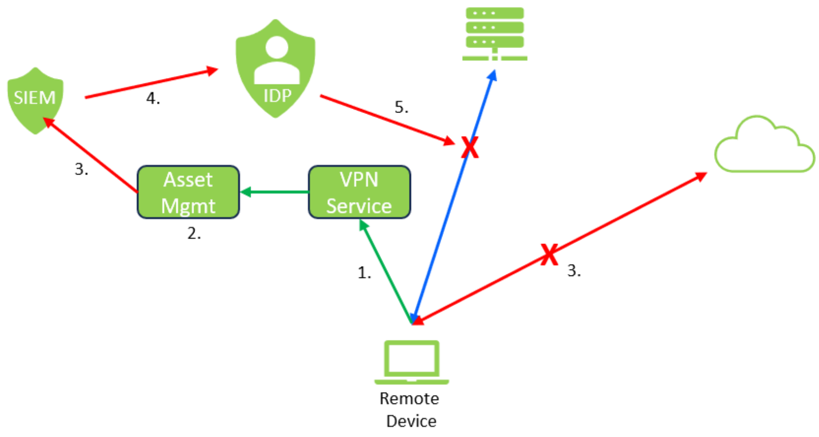


Figure 3. Remote user to resource access control.

The cloud based IDP acts as an arbitrator of policy to connect the resources through multi-factor authentication (MFA). Policy is defined for every resource regardless of resource type. The IDP verifies first through MFA that the remote user is validated and then checks the resource that the VPN service has indicated the remote user has access to. If policy check determines this is true, then the IDP reports to VPN service that the remote user can access the resource and makes the resource available. The user now has access to the applications frontend. Once the user selects a workflow, the application initiates its own access validation against policy for access to resource associated data. The access control mechanism for the design is indiscriminate and exercises the same checks regardless of user or system type authorization. It simplifies deployment by creating a single workflow, differentiated only by policy, regardless of the end device being for the organization, contractor, or personal use.

Visibility and Asset Management for Remote Resources. Visibility is critical for exposing event gaps, especially when implementing automation processes using APIs as described. The design relies heavily on the software defined perimeter and identity to define remote access policy and feed events for analysis. Section 5.4 of ZTA publication calls out challenges with visibility regarding assets that do not belong to the organization. These assets will be unlikely to have the endpoint detection and response (EDR) software agents or other tools used to confirm a device's compliance with policy. This example explores using an agent-based port mirror on a non-organization device to forward traffic to an asset management software that analyzes device traffic for policy compliance:



1. Represents the agent port mirror sending network traffic to asset management service.
2. The asset management service builds a profile and assigns a confidence level from traffic.
3. Remote device uses clear text authentication, event is reported to SIEM with a downgraded confidence level.
4. SIEM reports confidence level change to cloud based IDP.
5. IDP withdraws access to mesh VPN, blocks user and reports action.

Figure 4. Automated mitigation workflow of compromised device

The port mirror on the remote contractor device not only enables a confidence level assessment, but through integration can also exercise automated mitigation leveraging the identity and VPN service APIs.

This application will require that the remote device be accessible on the VPN so the asset management service can analyze the traffic and provide a score. It would be possible in this design to block access to an application until an assessment score is completed.

Continuous Policy Validation. Zero Trust necessitates a complex environment that evolves over time. Validation of these environments requires network test and measurement solutions that support Identity based traffic and policy enforcement interactions to validate environment functionality and performance.

One example is to simulate remote endpoints using a software traffic generator. The traffic generator employs lightweight agents deployed across a variety of environments to realistically model dynamic application traffic, user behavior, and threat vectors at scale. The traffic provides the unique ability to interleave applications and attacks to model user behavior and security breaches. It can be used to evaluate change and efficacy of zero trust policy in security devices for private, cloud and hybrid security device implementations.

Another example is a test tool that integrates with leading SIEM vendors enable end to end validation on how the prevention/detection works and identifies security sensors that may go dark. Bidirectional communication with SIEM tools provides SOC teams with push events that notify them during attack and breach simulations, enabling them to quickly distinguish simulated attacks from non-simulated ones.

NIST 800-207 discussed establishing trust in all the data sources and computing services of the enterprise — irrespective of their location — through secure communication and the validation of access policies. ("A Zero Trust Architecture Model for Access Control in Cloud Native Applications in Multi-Cloud Environments") Test tools can support the validation of access policies, exercising the policies in a way that typically can only be done when address an active threat. Furthermore, testing can be used with continuous automation of ongoing tasks in support of achieving optimal levels as described in zero trust maturity model.

Summary

The following describes how the design aligns to the zero trust tenets:

- **All data sources and computing services are considered resources**. All users, applications and assets in the design are managed regardless of owned or associated.
- **All communication is secured regardless of network location.** Network and all application workflows are encrypted. All remote access, regardless of location, is managed through mesh VPN.
- **Access to individual resources is granted on a per-session basis.** All applications registered with the IDP, with the IDP managing the authentication to access the application. The IDP requires MFA per session request.
- **Access to resources is determined by dynamic policy.** The asset posture is dynamically assessed and scored when the proposal for network discovery is used. This score is communicated to IDP to assess posture prior to granting access.

- **Monitor and measure integrity and posture of all owned and associated assets.** Once again, the proposal for network discovery allows for asset assessment allows then to be extended to associated assets as well.
- **All authentication and authorization are dynamic and strictly enforced prior to access.** IDP integration and asset assessment occurs first and is checked every time a session request occurs. If an access request fails to meet the minimum score, then access is not allowed to the application.
- **Collection as much information as possible about the current state of assets, network, and communications.** The design currently is implemented to support collection of information on access, networks, communications between resources and is capable of much more.

Please reach out to Jarrod Tsukada (jarrod.tsukada@keysight.com) to discuss, ask questions, or provide comments.