InstaSafe

Zero Trust Scenarios and Use Cases

VPN Replacement/VPN Alternative

VPNs and their issues with regards to securing modern networks, and the amount of unfettered trust that they assign in distributed network scenarios have been discussed at length. In summary:

- Traditional VPNs can only establish a single secure tunnel from the user's device to a VPN server, which permits network traffic to proceed into the private network area.
- VPNs perpetuate a perimeter-based network model, requiring that any distributed resources be connected to the enterprise's core network over a WAN
- This means that malicious actors can easily tap into this core network ad access confidential resources
- Alternatively, they will require users to manually switch VPN connections when they need to access resources in different locations. In contrast, Zero Trust systems will establish multiple secure connections so that users can access resources transparently.

There are multiple considerations to be kept in mind while deciding on candidate VPN Services that can be considered for implementing Zero Trust:

Resources

Organisations need to have a re-look at the number, type, location, and value of the resources that are to be secured. The primary question when assessing the security posture of organisational resources is, how business critical are they? What issues are associated with the current VPN?

Generally, Zero Trust solutions provide better performance than VPNs, especially for distributed resources, wherein applications, databases, and servers exist in multicloud environments. They also can often be deployed to protect resources in locations or environments where the enterprise cannot deploy a VPN entry point, for example, on a third-party network.

If your organisation has a highly distributed or highly dynamic set of resources, there is a necessity to upgrade your current security posture and adopt a Zero Trust approach.

User Experience

It is extremely crucial to keep the end user experience in mind when deploying security controls across your network. As such, before embarking on a VPN Replacement Journey, the following considerations are to be borne in mind:

- Who are the users currently utilizing the VPN, or who need to access these new resources?
- Are the users all remote?
- Are the users composed only of remote employees, or do they also include third party workers?
- Are on-premises users accessing these resources through a separate security model—for example, via firewalls?
- How rapidly was this remote user access solution deployed (and potentially with some known issues or compromises), for example, in response to the pandemic induced work from home shift?

In the event of such cases wherein the scalability and flexibility of the current solution, and their impact on latency and user experience come into question, Zero Trust poses an effective alternative, to overcome the security and operational costs associated with deploying a VPN solution that has been deployed rapidly.

- If there are resources that were deployed recently, it may be the case that only remote VPN users have a secure access pathway and that your organization needs a solution for on-premises users. Zero Trust Solutions like InstaSafe provide a unified answer for secure access by both remote and on premise users
- Zero Trust solutions are designed to secure access for all users to all resources, and at the same time, they can eliminate siloed solutions, such as separate rules and access mechanisms for remote vs. on-premises users
- Zero Trust can allow for what can be called implementation of granular level access policies. This means that Zero Trust policies can be applied incrementally, group by group, or application by application.
- This means that you will be able to decide on a group by group or individual by individual basis, as to who has access to what, without necessarily affecting latency during access

Here, an important consideration is to be aware of the different access tools that your initial sets of users utilize, to avoid imposing unnecessary friction. For example, you likely shouldn't require that a set of end users switch back and forth between their current VPN and your Zero Trust solution throughout their workday. It'd be far better to have a group of users switch over to your Zero Trust solution for all their access needs, combining their current broad VPN-level access with more precise Zero Trust policies for specific resources. This way, they begin to obtain improved security while also obtaining an improved user experience.

Identity Providers

- In some cases, your VPN implementations are not integrated with enterprise identity providers; in these cases, InstaSafe's Zero Trust deployment can quickly deliver considerable value

- By tying remote access user authentication to their enterprise identity provider, security teams eliminate an identity silo that existed within their VPN. This eliminates any work necessary to keep that silo in sync with their primary provider.

- Even if a VPN uses an enterprise IdP, Instasafe's Zero Trust solution will improve on it, by enforcing fine-grained and context-sensitive access policies. Many Zero Trust solutions also support multiple identity providers of different types, so that different user groups can authenticate against different IdPs, or so that legacy systems can be protected by modern authentication protocols. InstaSafe goes one step further, having an inbuilt IDP that helps in creating and managing user groups

- Simply put, a Zero Trust approach not only complements the efficacy of your IDP, but also helps in strengthening identity based access policy implementation. Zero Trust Models integrate seamlessly with IDPs, while also helping in implementation of access policies that restrict access to enterprise applications based on the purpose of each access request, the identity of the user, and the posture of the device being used.

Network Infrastructure

It is extremely important to have a comprehensive understanding of your network topology and understanding data flow before moving forward with an upgradation of existing security postures.

It is often important to first determine whether or not remote users are accessing resources via a single entry point, and which networks these entry points grant access to, and of course, how distributed your network resources are. In addition, it is critical to know what type of remote access policies your current VPN implements.

- Even if a single entry point exists, a Zero trust solution can contribute to increasing productivity and security, by improving stability of the system, and providing better access control

- Organisations that have distributed resources, and distributed workforces requiring access to these resources from multiple Policy Enforcement Points, will find a Zero Trust solution to be the perfect answer for secure access.

Network Infrastructure

VPN replacement and VPN alternative are a common first Zero Trust project, and are an optimal project to get started with. The security and business are clearly lain out, and the functionality of a traditional VPN is generally quite easy for a Zero Trust solution to replace. We do recommend an incremental deployment, with consideration for those user groups who may need to retain both Zero Trust and VPN access for a period of time. These solutions generally can co-exist in harmony on an end-user device, especially as InstaSafe's Zero Trust Solutions are designed for a seamless user experience

3rd Party Access

3rd Party access has long proven to be a security challenge for most organisations, irrespective of their size or the scale of their remote access needs. In the case of highly fragmented organisations with any amount of dependency on third parties, Zero Trust is an effective alternative.

To set the record straight, a third party is any individual or entity that is a non-employee, but requires access to enterprise private resources in order to fulfil obligations of legal agreement between itself and the organisation in question.

Often, these contractual workers are treated, in some ways, as similar to full time workforces. In many cases, they are issued company managed devices, and are a part of the enterprise security and identity management systems. . In some cases, with companies adopting BYOD policies, they may be allowed to use BYOD Devices, which could further loosen the scope for security controls. From a security perspective, they should be managed in the same way as employees, but their access will be very restricted, and their actions closely monitored.

Note that we're excluding full-time contract (non-employee) workers from this scenario; in our experience, these folks are treated much more like regular, full-time employees from an IT perspective. That is, a contract programmer on a 6-month assignment may not be a company employee, but will typically be issued a company-managed device, and be part of the enterprise's identity management system. Simply put, these users require a set of tighter security controls, InstaSafe's Zero Trust principles require that all users be authenticated and their network access be restricted to what is called a need to know basis. Till now, organizations have used VPNs as a remote access tool for third party employees, and of course, VPNs exhibit all their weaknesses for third-party access, including the potential to be exploited for lateral movement attacks. In addition, these third-party users are not employees, so by definition, they're not using devices that are managed by the enterprise. This means that the enterprise cannot mandate or rely on the security posture of that device, which makes it even more important to impose security controls around network access for that device. This can be enabled by a Zero Trust Model.

In addition, a key challenge that security teams face is that in case of BYOD policies, wherein third party vendors will have to use unmanaged devices, security software can't be downloaded. This is where InstaSafe's agentless approach comes in, wherein you will not have to download an agent/application in the vendor's device to manage their access.

We'll now discuss the key considerations to be kept in mind while adopting a Zero Trust Model for Third Party Access

Considerations

Architecture

Third-party access architectures are very similar to existing VPNs; in fact, it's quite likely that third party vendors will be using existing VPN tools to access enterprise applications. In this scenario, it is critical to understand traffic flows, in terms of how and where these people are getting onto the network, and how their network traffic traverses the enterprise to reach requisite resources. Also, the principle of least privilege access needs to be strictly enforced, and the Policy Enforcement Points should prevent unnecessary network access for all users

User Experience

User Experience in the case of third party vendors may be a secondary consideration for organisations. Access for third party vendors may be a temporary or intermittent requirement as well.

In order to deal with the issue of installation of security software, Zero Trust technologies like InstaSafe support the both agent based and agentless, browser based access. More often than not, web based applications are easily accessible with an agentless model. For vendors who need to have agents installed in their devices, but do not want to comply with these requirements, Zero Trust policies can be enforced by hosting a VDI for them, and installing Zero Trust agents in the VDIs.

All in all, while user experience may not be important in this case, a Zero Trust setup may serve to uplift the user experience as compared to VPNs

Recommendations

From a user authentication and authorisation and management perspective, it is recommended that organisations replace their existing VPNs with a Zero Trust system and use the third party's enterprise identity management system for authentication. In addition, it is also recommended that you enforce MFA for these users, each time they attempt to access your resources. This follows the principle of Never Trust, Always Verify followed by Zero trust systems, and the principle of continuous three dimensional risk and trust assessment for your users, and also eliminates the potential for credential sharing by third-party users (which is a common occurrence).

In addition, Zero Trust systems enforce contextual access control, which means each access request is considered separately and authorised, with additional security controls like Geolocation, wherein access is restricted based on the location of the device, and also ensure the enforcement of granular access controls which can restrict privilege for third party vendors to a minimum.

Cloud Migration

Migration of applications and data to the cloud forms a major part of organisations' functioning today. Leveraging the scalability and flexibility of the cloud has become a necessity in the present context, which is why it's important that Zero Trust projects and leaders embrace this and educate their colleagues on the business and application development side about this new approach. Ideally, security teams will have in place a Zero Trust approach and approved components, which will enable application owners to quickly embrace the cloud securely and quickly.

Cloud Migration may be categorised into 4 broad sections:

Forklift Migration: the application is moved from an on-premises physical or virtual environment to an IaaS environment "as is." That is, there are no changes to application logic, topology, or technology. The end result is that the same application is running in a different place. Because this maintains the application's structure and interdependencies, this migration can be faster and simpler, but delivers more limited benefits.

Refactor the Application: The application is migrated to an IaaS environment, but it includes some technical or structural changes, ideally to take advantage of its new cloud platform.

Rewrite the Application: application developers have the opportunity to completely rethink the application architecture, including taking a "radical" approach to embrace modern components such as containers, PaaS, microservices, or NoSQL databases, among others.

Adopt Saas: With this approach, organizations are making the shift from on-prem applications to a cloud-based SaaS application, which essentially represents a wholesale shift in application topology and access controls.

All of the above cloud migration projects are suitable for Zero trust technologies, since they present an opportunity to embrace a security friendly platform. Since Zero Trust technologies are dynamic and context sensitive, they can leverage the APIs presented by cloud technologies

One of the key considerations to be kept in mind is the functionality of a uniform Zero trust tool in multicloud environment. The newly migrated applications will have different network access models as a result of their migration to the cloud. This can disrupt or challenge the end-user experience. Your Zero Trust solution can often eliminate this friction, giving users transparent and secure access to these cloud-based applications while also enforcing dynamic and context-sensitive access policies.

Secure DevOps Access

DevOps teams represents a fresh way of approaching application development, centered on collaboration between siloed software development and operations teams. By using automated toolsets and rapid cycle times, this approach helps organizations dramatically increase their deployment speed.

Let's now look at the DevOps phases, and see how Zero Trust applies to them.

Plan and Code

From a design perspective, this phase is where security teams should collaborate with and educate application developers on their Zero Trust architecture, capabilities, and policy model. Giving application designers this knowledge will help them decide where they can rely on the Zero Trust platform and where they need to take responsibility

Build and Test

As application code proceeds through the build and test phases, this is a natural place for the Zero Trust system to use automated policies that grant access only to the right set of people and tools based on workload attributes.

Release and Deploy

These last steps of the release process will result in the application being placed into production, within a Zero Trust environment with a full set of policy enforcement. That is, all access to application services is controlled by policies, which are only granted to authenticated and authorized subjects

Operate and Monitor

For this phase, Zero Trust will help ensure the stability of the environment, and control any administrative or troubleshooting access to production applications. It'll also provide identity-enriched logs, ensuring that all access is properly associated with authenticated identities.

DevOps is an interesting and relevant use case for Zero Trust because there are so many ways to tie it to, and get value from, Zero Trust. Even basic integration gives security and application development teams the opportunity to balance and share access control approaches and policies. Breaking down this traditional silo helps "bake in" Zero Trust integration throughout the entire application lifecycle.

Digital Transformation and a Shift to Full Zero trust

The most important difference is that going "full Zero Trust" involves a shift in networking philosophy, that of taking all your users "off net" and requiring use of the Zero Trust system to access any enterprise resource. Interestingly, the abrupt COVID-19- driven shift to a predominantly work-from-home user population in early 2020 accelerated many organizations' readiness to make this change. The biggest mind shift associated with this is the realization that the problem to be solved isn't "remote access"—it's just "access." In fact, taking a unified approach to securing all access is what underpins much of the value of a Zero Trust environment. This also reinforces one of the key tenets of the Zero Trust Model, that of not discriminating on the basis of locality and ensuring secure access by all users

InstaSafe ZTAA Features

Core Security Capabilities

Separate path for data and control traffic
ZTNA has a separate data and control plane. A control plane essentially sets up the controls necessary for data to pass from one endpoint to another. Separating the control from the data plane renders protected assets "black," thereby blocking network-based attacks. It also ensures that the customers' data directly flows from the user device to the application without driving it through to the vendor's machines. The method helps to avoid the network latency as well.

Drop all firewall
Drop-All firewall ensures that every data traffic coming to the IP address is dropped. It helps to ensure that no entity in the internet can get to know the presence of the IP address in the network. Each access to the IP needs to be separately enabled as an exception to the drop-all rule at the firewall. In other words, only the authorised IPs/devices (By the controller) can reach the IP addresses hidden by the drop-all firewall.

Single Packet Authorization
When a device is protected by a drop all firewall, there should be a mechanism to reach the device with the right auth data, after which the access can be enabled. This is the task of the Single Packet Authorization.

One a data packet reaches the destination device, which is protected by drop all firewall, the device recognises the dropped packet and validates the same. Once the authentication information is found legitimate, the access to the remote IP will be enabled at the firewall automatically.

Completely hidden from internet but visible to remote users on internet
As explained at the above two features, the drop all firewall completely hides the IT infrastructure completely whereas the Single Packet Authorisation technology enables the seamless access for the legitimate users.

Even the tools such as nmap cannot probe the ports to identify the presence of the devices as each received packet is dropped off.

Least Privilege access on need basis
Every user is given the least possible amount of access, as we can limit the insider threats coming out of each access. It is very important to contain the attacks when a user device is compromised.

It is often during the cyber attack incidents that the malwares and scripts spread within the network and hackers will manually attempt to hack into the possible access points. When we contain the user access to a limited set of applications or devices

MTLS Encryption of traffic
The data travelling between the user device and the application is encrypted with Mutual TLS encryption. The methodology ensures that no device can establish a Man-In-The-Middle attack as the traffic is a mutually established TLS connection.

Applications hosted on DCs and multi-Cloud available at single click on a page
Today applications and servers are spread across multiple cloud and data center environments. The ZTNA platform helps to deliver all the applications to the user at a single UI via the ZTNA-Agent.
The gateways kept at each of the separate networks will share the application and network traffic with the user device directly and the agent collates all of them at a single page on the USER Interface.

Separate encrypted tunnel for each application connection
It is very important to limit each user's access to the organisation's network. The methodology ensures that each connection for each of the users is contained within a specific tunnel. This reduces the insider threats as no user is able to get to know about other users that are using the application or network. Also it helps to contain the external attacks to a small tunnel or a single application. As the hackers visibility will be highly controlled and contained.
The user has to authenticate and get authorized himself at the controller in order to access an application via the gateway. The gateway ports will be visible only to the legitimate users and devices which got validated by the ZTAA Controller.

Automation and Orchestration
NIST and later CSA drew the architecture for Zero Trust. There are many network elements and software elements that need to work together to make it happen effectively. ZTNA has automated and orchestrated each of these elements following the architecture and wrapped with other needs in the access management scenarios such as InstaSafe authentication, Inbuilt IDP and support for L3/L4 and L7 layers of protocols and applications.
The applications can be shared via TCP channel or the VPN channel . VPN gateway configuration can help if there are specific need for exposing a series of IPs or specific ports

Identity & Authentication Capabilities

Inbuilt IDP(Users, groups and management)
InstaSafe ZTNA solution supports integrating with customers' third party IDP solution providers such as AD, Azure AD and has an inbuilt IDP. The inbuilt IDP helps create and manage the users and user groups. Any number of users and groups can be created as per the team structure of the customer. The access to the users and groups can be managed separately based on the privileges via policies.

InstaSafe TOTP Authenticator application
ZTNA is supported by InstaSafe TOTP authenticator. It helps to possess the MFA capability via the mobile app. The solution is a highly user friendly application that can be installed over the Android as well iOS based mobile phones. The user access to the platform can be enabled with a single click at the mobile app.

Support for Third party solution providers such as AD, Azure AD
Today most of the organisations manage their users, groups and policies on a third software such as Active directory and Azure AD. InstaSafe ZTNA can integrate with these solution providers and have the users validated and authorised based on the configurations at these solutions. It's a great advantage to sync the existing solution with ZTNA as it will ease the deployment and adoption.

Multi-Factor authentication via TOTP Apps, SMS, Email
MFA feature of ZTNA is powered by SMS, EMAIL and TOTP providers such as google and Microsoft. InstaSafe authenticator as well can be used to enable the MFA functionality. ZTNA has quick workflows to enable and connect to the existing MFA methodologies for each of the users. Each user account can be configured separately in order to align with one of the selected MFA methods.

Single Sign On for the applications
InstaSafe ZTNA brings out every application and network access on to a single plane. What if we can achieve an automatic login to these applications on a single click at the application icon. The single sign on feature works closely with the SSO enablers such as Google SSO and SAML solution providers

Multi- Factor authentication for the specific Applications
ZTNA agents have all the applications at the single view point on the user interface. There could be a need for specific additional authentication for the critical applications. When the feature is configured, the user will be asked for additional authentication whenever the application is attempted by the ZTNA client user.

ML based Behaviour Authentication
While all the authentication mechanisms focus on validating an information or software element that's present with the user, Machine Learning(ML) focuses on the behaviour of the user. When another user impersonates the original user, the way he types or access could be different. The solution identifies the impersonation of the end user based on the usage of keystrokes and other history based approaches and block access.

Dynamic Authorisation based on Geo-risk and Temporal (Time based) Risk Assessment
The feature enables to control the user access based on working hours and location. As we know, the organisations are being sniffed by the hackers around the globe for information. There are occurrence of password being lost and shared across the public platforms as well. The feature ensures that the access to the user device will be provided only when it adheres to conditions such as location of the device, time of access and security posture of the device

Access Control Capabilities

Managed access control policies
All the access control policies are kept on a single page irrespective of the users, application, network and other elements. Admin can manage the access for each of the applications against users or user groups. The method helps to configure the access policies for the applications belonging to multiple networks at one place.

Granular control of access among user, user groups, devices and applications
The access policies can be defined at a very granular level for each of these elements. Each user, user device, groups or application can be subject to specific rules. The rules define how the access should be established between the users and applications. The network admins can manage the granular level control of each element at the same dashboard.

Control the and limit access based on the device posture(NAC usecases)
When the users are remotely accessing the organisation’s assets, it's important to validate the security posture of each of these user devices separately. The NAC features embedded inside the ZTNA validate the security posture of the user device from various aspects, The validation can be customised for the organisation and the users or groups based on the need.

User DB sync with External Access management solutions
When an organisation is adopting the ZTNA solution it is important to ensure the seamless integration of the existing User management solutions. The IDP integration feature at the ZTNA helps to sync the users, their policies and other elements present at the user database of the IDP solution providers. The continuous sync enables the orchestrated solution to quickly update the changes made at the IDP solutions such as Active directory servers or Azure AD

Control your access at one place by connecting all the application and users
The controller acts as a center for management. The administrator a quick and easy dashboard to manage the entire access for the devices, users, gateways and applications. The container based infrastructure is a highly secured entity that provides the end-to-end management of the access and connection between the network elements.

Application Access Capabilities

Enables access to layer 3 and Layer 4 protocols and related apps
It is the need of the hour for the organisations to share the access for SSH, RDP and other protocols at these layers. In addition to the layer 7 access to the applications, ZTNA supports the protocol level access at layer 3 & 4. Thus admin is able to share direct connectivity to the servers or network at the IP level.

Connect to any App from mobile, desktops and laptops
Each of these end user devices are different in nature, and they behave differently while validating the device posture, prior to establishing the connectivity. ZTNA ensures that each of these devices are separately identified and validated by the ZTNA controller.

Inaccessible from internet, making it Unreachable for DDoS attack
As the ZTNA is protected by features such as drop all firewall and Single packet authorisation, the InstaSafe ZTNA components are completely blackened from the internet. The network packets targeted at the InstaSafe infrastructure will be dropped off by the firewall, and hence no device or tool can reach or probe for the existence of the machine or port.
DDoS attacks need multiple connections getting established by the attackers. The ZTNA infrastructure makes sure that the connectivity to the user device is established only when a device is approaching with a legitimate packet containing the authentication information.

Endpoint security & control Capabilities

Secure posture validation of the user device
As per the zero trust architecture put forward by CSA and NIST, it is important to validate the devices that are requesting access. Both user and device should be validated prior to the access. InstaSafe ZTNA solution ensures that each of the devices are validated against a fixed set of security posture requirements. It can be customised based on the business requirements or the verticals.

Disable Screen capture, Copy/Paste & Clipboard
It is important to ensure the safety and privacy of the data, when an organisation's asset is shared with a remote user.The ZTNA user agent installed at the user device provides the application, device or network access within a container. The container ensures that the user is blocked from copying the content out of the container by blocking or disabling the operations such as Screen capture, Copy/Paste,Screen Recording & Clipboard

Block downloads for sensitive applications
Each of the applications can have its own policies defined at the ZTNA controller.The policies defines whether a user will be allowed to download an application or not. If chosen, the users will not be able to download any data, file or links from the shared application.

Secure workspace on chromium container
The user is presented with a chromium browser based controlled container, when the ZTAA agent is installed at the user device. The user can access each of the applications provided to him at the chromium container. The container supports features such as multiple tabs as the user can access multiple applications this way. The user can be limited to the container in terms of data access and browsing.

Clientless browser access
ZTAA supports browser based clientless access as well. In this method, the user does not need to install the ZTAA agent application. Each of these applications will be directly accessed via the browser as per the policies defined at the ZTAA Controller. As we discussed each of the devices is validated against the predefined posture requirement while connecting to the Zero Trust infrastructure. The validation will be limited to the information that can be grabbed from the browser, while accessing the application in the clientless mode.

Agents for Windows, Linux, Mac, iOS iPhone, and Android
As the organisations are sharing the applications and servers with the users, the users have started accessing them from various operating systems such as Windows, Linux, iOS and Android . ZTNA agents support each of these platforms and operating systems. The separate installable for the devices can be downloaded from the controller UI

Reporting Capabilities - this needs both competitive research & our console research

Security events
Events such invalid login attempts and bruteforce will be identified and logged at the controller panel for ZTAA. It also records the authentication related activities of the user at the page. The customised set of security events will be reported under the event section of the tool in the admin panel as part of the audit functionality. The events help to monitor the suspicious activity and validate them.

Login events and history
The users can login from multiple devices such as mobile, laptop and third party desktops . ZTAA diligently records the access events from each of these devices. The logs can be maintained for a predefined period of time. The information help the auditors to analyse the operations and ensure the secure posture of the system

Live active users
Even Though there are a large number of users it is important to analyse and understand how many users are currently active. This information can help the admins while planning, updating and monitoring the IT infrastructure and its consumptions across different gateways and networks. ZTAA dashboard showcases the live users and their application access logs at any point of time.

Health of the gateways
Gateways are guarding the customer IT infrastructure and applications. The ZTAA controller monitors the health of the gateway and lets the administrator know about it via displaying it on the screen or via alerts. The alerts can be customised and configured as per the need as well.

Alerts
Alerts can be raised for different needs and scenarios. The importance and need for alerts will vary across the industry vectors and companies. The alerts present at the ZTAA can be customised and created as per the specific requirements from the customer.

Application access requests
The applications are shared via different mechanisms. ZTAA audit logs capture the access requests coming from the users to different types of applications across the various types of gateways. The access requests and their status will be recorded for a customisable amount of time.

Integration Capabilities

Integrated SSO and SAML
Single sign-on is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. The single Sign On feature at the ZTAA helps users to directly login to the applications once logged in to the ZTAA client. ZTAA supports the SAML based service providers service to validate the users and allow them to access the applications without additional authentication requirements.

Easy Integration with 3rd party IDPs and own IDP
InstaSafe has created complete user and group management systems along with a large set of features around policies. The IDP is integrated with ZTAA. ZTAA also supports major Identify management solutions such as Active directory servers and Azure AD.

Easy Integration with SIEMs
SIEMs can effectively triage and correlate the data available at network logs. ZTAA can share the audit logs directly with the SIEM servers. The data can be polled from the SIEM servers once configured. The Log streaming services and setup can be modified and revoked dynamically at any point of time.

TOTP Authentication
Time based one time password is a highly secure mode of authentication to any system. ZTAA accepts the TOTP password as a second authentication after the password validation. InstaSafe has made its own Authenticator application named InstaSafe authenticator which is supported by ZTAA. ZTAA also supports major TOTP authenticators such as Google and Microsoft.

Deployment & Scalability Capabilities

Horizontally scalable Gateway and Controller infrastructure
InstaSafe has deployed more than 27000 users within 5 days of time. More resources can be easily attached to the system, as the gateway of the controller is horizontally scalable. The operations can be done by a small team as the operations are supported by highly automated workflows.

Quick adoption method in to the Zero Trust Network
Zero Trust method of implementation is the key aspect of ZTAA. The adoption of Zero trust Application level access can be quickly achieved by the solution. The solutions such as InstaSafe authenticator and integrated IDP help to ensure that a complete access management system gets built by a single vendor avoiding the delays.

Quick and easy 3 step process for the Application access by the user
The user of the ZTAA solution needs to install the ZTAA agent(one time), login to the application, and click on any of the applications that he needs to use. The user is presented with a single page dashboard where all the applications are listed . He can access any of the applications present at the page on a single click

Quick 4 step process for the Application access deployment by admin
It takes just 4 steps for the administrator to enable access for an application:

> Install the gateway and agent at the datacenter,
> Add the identity schema (AD/IDP) for the users
> Add applications to the ZTAA controller
> Define the user/ groups access policies.

Support Capabilities

24/7 and 8/5 support available
InstaSafe support team works for 24 hours on a shift model. The support of 24/7 or 8/5 will be decided based on the options chosen by the customer while signing the deal. The team follows very strict SLAs on first response and takes up the technical issues based on the complexity.

Team monitors alerts generated at customer locations
On a selected alert customers can choose to have InstaSafe monitoring of the health of elements like gateway. As soon as a failure is identified the team can get into action and solve the same during the physical, network or software glitches. The team has access to all the assets shared across the globe and a highly skilled engineering force.

24/7 Customer Support
InstaSafe has a completely automated process of working. The tickets for any of the issues can be raised by just sending an email to support@instasafe.com. The team follows a strict SLA and addresses the issue on priority

InstaSafe
Cloud. Secure. Instant.

Asia's fastest growing cybersecurity company is going global. InstaSafe is your trusted remote access security provider, catering to the remote access need of some the world's largest MNCs

Representative Vendor- Gartner's Market Guide for Zero Trust Network Access- Global

Nikkei Asia Growth Champion- Fastest growing cybersecurity company of Asia

True Zero Trust Model, based on the CSA-NIST architecture

Representative Vendor- IDC's Guide for Software Defined Secure Access

Network and security support experts available around the clock

AWS Advanced Technology Partner

42 Points of Presence with 10 million + endpoints

Customer presence in more than 70 countries

Customers in 120+ countries

The InstaSafe Experience Zero Trust. One Access.

Scalable security that caters to the requirements of enterprises of any size. From onboarding and deployment within 4 days, to 24/7 support, at InstaSafe, we believe in leveraging identity to provide an integrated security experience

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