InstaSafe
Cloud. Secure. Instant.

NEXT GENERATION SECURE ACCESS

Secure Access or Remote Access solutions are clearly out dated for the millennial business. Ensuring security with seamless connectivity requires secure access products that combine multiple technologies to ensure the modern day attacks are blocked while enabling the adoption of Cloud technologies and BYOD confidently.

THE CHALLENGE

Organisations today have a complex network than ever before due to the changing business requirements. Apart from maintaining the current Data Centre infrastructure technologies, organisations are adopting Cloud services (such as SaaS, IaaS, PaaS etc.) extensively to stay agile and enable business to perform better. The consequences of the required agility and performance has resulted in the hybrid network, where the perimeter has dissolved.

Access control is most commonly performed at the network and protocol layers, and inside the application to handle role based access. However, access control at the network and protocol layer is proven to be ineffective as zero-day attacks pass through hidden with legitimate traffic. Further, in a hybrid network, the ever expanding ingress and egress points are many; making network access control complex, and so in most cases not strictly implemented. Applications hosted in Public Clouds are required to be exposed to the Internet to allow access to all users.

However, to enforce the corporate access control security, organisations generally use IPSec VPN to connect the Pubic Cloud applications to the data centre and then backhaul all user traffic. And this of course, negatively impacts the user access of the applications resulting in lost productivity.

Especially with third party remote access to applications in the cloud and in the data centre; access control and additional security controls (such as encrypted access) requires a complex setup of IPSec VPNs and SSL VPNs with complex routing between them to achieve a decent level of security posture. This is further complicated in case of regulatory compliance requirements to further secure the data being accessed.

Lastly, and very importantly, the devices that connect to the networks are inherently trusted and never verified - to be an authorised device, used by an authorised user. As such, credential theft attacks are successful as the authentication of users is independent of the device being used to connect to the network / application. This gap in verifying the device and the user together helps attackers use the trusted devices to move laterally within the network.

THE INSTASAFE SECURE ACCESS SOLUTION

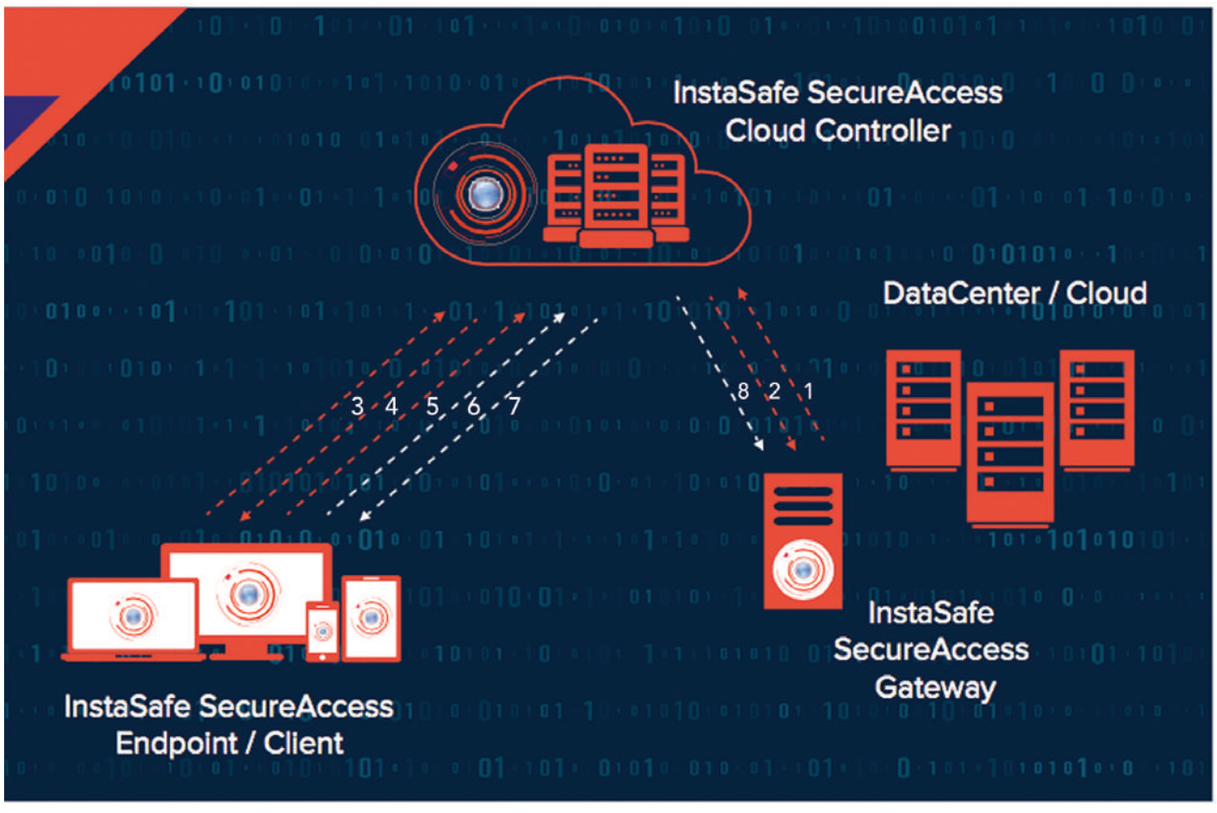
To protect such an elastic and complex setup in an uniform and effective way, organisations need here with zero trust. access control solutions that can verify the trust of every device before the checks on user authenticity. Once the user and the device are verified, dynamic encrypted access should be provided to the applications only on a "need-to-know" basis. This "need-to-know" controlled network is required, first and foremost within the corporate network; and also needs to extend beyond the physical bounds of the corporate (such as for cloud based applications, branch offices, remote workers, business partners etc.),
while being able to manage it centrally and easily. Built for today's networks, InstaSafe Secure Access (SA) solutions secures the hybrid network by authorising the endpoint devices and authenticating users before creating a dynamic / on-demand secure connection(s) from the authorised devices to the protected application(s).

THE TECHNOLOGY

The InstaSafe SA solution brings your public cloud, data center, offices and remote users into one encrypted virtual private cloud network. This effectively makes your public cloud invisible to the internet besides keeping your applications inside the data center also hidden. By using private IP addressing and encrypted communications, the virtual private cloud network is invisible and inaccessible to any other network. Using a Centralized Management Console that we call the Core, you can define granular access rules to ensure that only authorized users with authorized devices can access specific applications within the virtual private cloud network.

The diagram below provides further clarity on the architecture :

1 Gateway device authentication (Certificate, Device ID).
2 Gateway authenticated & available.
3 Endpoint provides device credentials (Certificate, Device ID).
4 Device verified and authenticated. Initiate User Authentication (tied to this device).
5 User Authentication using Password + OTP / Token.
6 User requests access to Application-X.
7 Based on device and User authorization, access allowed. Connect to InstaSafe Gateway.
8 Forward User traffic for Application-X.



In the above steps, the SecureAccess Gateway and the Endpoints connect to the Cloud Controller. The Gateway acts as the entry / exit point to a network – be it a Public Cloud, datacentre or an office and it connects to the InstaSafe Cloud Controller. The Gateway uses mTLS with AES-128 bit encryption to connect to the Cloud Controller along with providing its server fingerprint. With this method, the Gateways are able to defeat common attacks like MITM, connection hijacking and even DoS. Further, the Gateway creates an outbound connection to the Cloud Controller which means that the firewall at the datacentre / office / Public Cloud does not require any inbound ports to be opened therefore making the Gateway and the network behind it invisible to the Internet.

The endpoints agents also connect to the InstaSafe Cloud Controller using mTLS with AES-128 bit encryption and device fingerprint1. The Cloud Controller considers the device authorized only if both the mTLS negotiation is successful and the device fingerprint is found correct. The user authentication stage begins only after successful completion of the device authorization stage. The user is bound to the device, enforcing the user that is mapped to this device to authenticate him/her self through any of the different user authentication mechanisms (such as AD, LDAP or RADIUS). Optionally, SMS OTP factor can be enabled for user authentication over and above the password based authentication.

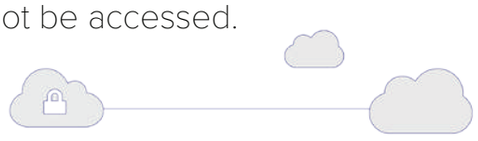
With this process of authentication and authorisation of the endpoints and the Gateway, the following attacks are mitigated:

- Credential Theft – stolen passwords of users do not pose any threat since the password will not work on any unauthorized devices.

- Connection hijacking / MITM – common attacks that target non-technical persons to accept certificate errors leading to MITM attacks are defeated.

- DOS – As the Cloud Controller will not accept connections that do not provide the client certificate and the device fingerprint, DOS attacks are prevented to the Cloud.

- Server exploitation – As there are no inbound firewall rules, the applications / servers are invisible to the internet and so cannot be accessed.



Version control 20062017/VR

SUMMARY

InstaSafe SecureAccess solution solves the access control challenges faced by organisations today using Hybrid networks. The InstaSafe Secure Access solution can interconnect all the Public Cloud deployments, the datacentre, the corporate offices and the employees into one Virtual Private Cloud (VPC) Network. However, it is not an open network and has granular ACLs that allow specific users using only their authorized devices to connect to specific applications that are located anywhere in the VPC Network. With this architecture, organisations are able to simplify the internal access and remote access controls while interconnecting physically disparately located systems.

InstaSafe
Cloud. Secure. Instant.

Did we get you interested?

hello@instasafe.com +91 8880220044 www.instasafe.com
facebook.com/instasafe @instasafe linkedin.com/company/instasafe

Recognitions:

Microsoft Ventures