SAIFE

A NEW PARADIGM FOR SECURING TODAY'S POROUS PERIMETER

INTRODUCTION

Analyst firms warn that traditional network designs pose excessive risk. Legacy network security and monitoring tools were not built for today's interconnected environment...

There is an ongoing struggle in cyber security today to provide secure, trusted access to services and data over the internet and other untrusted networks, both public and private. Despite millions spent on a vast array of security technologies, the problem is getting worse and the incidence of data breaches, ransomware, and denial of service attacks continues to rise. The perimeter is no longer tightly controlled and well understood; it has evolved to wherever users happen to be, on whatever internet-connected device, from whatever free public Wi-Fi network they choose. The perimeter has become more dynamic in response to our increasing reliance on a multitude of devices and cloud services, and as a result it is increasingly porous and vulnerable. Compounding this, today's highly interconnected and complex networks can expose valuable internal services to open internet connections. Analyst firms warn that traditional network designs pose excessive risk. Legacy network security and monitoring tools were not built for today's interconnected environment or its ever-growing attack surface, and are doing a poor job of protecting users and data. SAIFE has created a new paradigm for securing the dynamic, porous perimeter that enables organizations to protect their sensitive information.

THE STATE OF OUR NETWORK IS NOT GOOD.

The network has become a dangerous place due to several factors including misplaced notions of trust, its porous perimeter, insecure and hard-to-manage security tools, PKI shortcomings, a flawed approach to connectivity, untrustworthy internet routing, and broadly-permissive access.

1. No trusted network device identity

The internet was built on the premise of trust. At that time, the concept of an exploit did not exist.

The original internet, as well as corporate LANs, were built on the premise that every device and service should be exposed because devices on the network or inside the perimeter could be trusted. A device's IP address validated that it was on the local network. In reality, it's almost impossible to be sure who is talking based on IP address: ARPs can be spoofed, IPs masqueraded, spoofed or shared, and DNS spoofed or unavailable. Certificate Authority (CA) roots and trust anchors can be spoofed or compromised. Initially, it was believed that credentials were all that were needed for securing applications and systems. For example, anyone on the internal network can see the Human Resources system, but not everyone has credentials for that system or needs to access it. At the time this trust paradigm became the de-facto standard for network security, the concept of an exploit did not exist.

2. No trusted internet routing

The path of traffic flowing across the internet cannot be forced to travel over trusted circuits. As a result, traffic can be intercepted and modified; session negotiation can be brute-forced, credentials compromised, and established sessions hijacked. Even from the public internet, network topology is exposed, revealing points of entry, available services, and connections among cloud, on-premises and third parties. Hackers scanning a network will find the weakest point, start their attack and then move laterally throughout the network. Blind trust in DNS and IP routing tables for session establishment leave the network open to distributed denial of service (DDoS) attacks; because it's not possible to distinguish valid from invalid sources, our networks accept and process all packets including those from bad actors. Denial of service attacks overwhelm compute power and network stacks, causing a disruption in service to legitimate users or customers. Changing and broadcasting notification of a new IP address through DNS means the bad actors get the update as well as the valid users. Consequently, this makes changing an IP difficult when needed, such as when recovering from a DDoS attack.

3. A complex, porous perimeter

Misplaced internet trust and untrustworthy routing issues are compounded by the agility of the perimeter. The multitude of devices and services, both in the cloud and on premises, create an extremely porous perimeter because external applications and devices need to access internal systems and data. This model has long since outgrown the ability of traditional VPN and firewall technology to protect it. We hope that the services themselves, as well as the OS and network stack,

have been implemented securely. We all repeat the mantra of good patch management and endpoint hardening, but it doesn't happen. Endpoints will never be completely hardened, or patched in a timely fashion. Patches are created continuously and installation must be staged to avoid downtime. (The spread of the WannaCry malware was due primarily to poor cyber hygiene; the patch to prevent the infection had been issued long before the advent of the malware itself.) Some systems (e.g. SCADA) and most embedded devices can't be patched. Any vulnerability due to unpatched, poorly-written or poorly-configured applications can be an open door into the network.

We all repeat the mantra of good patch management and endpoint hardening, but it doesn't happen.

Yet we can't avoid the requirement to share sensitive data and services with employees, partners, contractors and vendors, each ideally with their own set of entitlements that limit access to a subset of the network. We resort to placing enterprise systems in a DMZ, often crowded with servers containing enterprise data with no isolation from modern attacks and few barriers against further penetration into the network. DMZ services accept incoming connections from anonymous devices outside the network, consequently offering direct internet visibility but lacking proper perimeter protection.

4. Insecure security solutions and their management burden

Millions of dollars are spent to defend our networks, but the security systems we put in place are themselves difficult to manage and vulnerable. VPNs, firewalls, VLANs and NAC are typically implemented to provide network access in an all-or-nothing fashion, giving authenticated users broad network access. Each tool brings its own set of issues, not the least of which is a huge management burden. For example, implementing VPN connections with third parties can take months of negotiation and often results in more access than is required. This is because they are based on the traditional concept of trusting everyone inside the perimeter. VPNs create and maintain open firewall ports that can be scanned and exploited, increasing the attack surface.

PKI and CAs are fundamental to internet communication, yet PKI is difficult to implement properly and the problems are not trivial.

Firewalls are costly and time-consuming to set up, and firewall rulesets quickly become complex, requiring continuous management as network needs change. This presents a substantial ongoing management burden, which organizations often outsource. When ports are no longer needed they are too often left open, exposing systems no longer being actively patch managed or giving unintended access to a new system through an old firewall rule. Even when firewall pinhole rules are used they still expose the services behind the pinhole, and they too become outdated or orphaned, creating stability issues as well as potential exposure of the entire network.

5. PKI and certificate issues

PKI and CAs are fundamental to internet communication, yet PKI is difficult to implement properly and the problems are not trivial. Even when PKI is set up without errors, it's common for users to ignore

warnings and for applications to fail open. CA roots can be spoofed, misused, or their keys can be compromised – all of which have already happened on root CAs that your existing devices still trust. Trust anchors can be compromised, undermining our assumptions about the strength of public key cryptography altogether. Any compromise in one of the many roots of trust can lead to a catastrophic failure of your entire deployment of endpoints. Due to the complexity, it's common for organizations to forego PKI altogether in favor of less-secure but easier-to-implement shared secret keys. Once deployed, PKI management can be burdensome: Certificate revocation has become one of the biggest problems with PKI. Many CA administrators never revoke certificates, or, if they do, the software does not bother to check. A recent study showed that nearly 1% of revoked certificates are still actively used, and that browsers frequently do not check whether certificates are revoked. Mobile browsers never check. [i]

6. A flawed approach with TLS/IPSec connectivity

Traditional methods of securely authenticating via TLS and IPSec leave a huge, recognizable attack surface. Founded on the legacy view of the internet where anyone can request any service, they follow the "connect, then authenticate" approach. Authentication takes place after initial connectivity has already been established, supporting anonymous introductions via certificates. In addition, both TLS and IPSec require and thus expose the IP address of each side in the cryptographic binding of a session. This makes both sides vulnerable to man-in-the-middle attacks and spoofing at every layer: ARP poisoning, IP spoofing, CA attacks and user spoofing. Weak algorithms also plague TLS and IPSec. During TLS handshakes, it's possible to negotiate a weaker algorithm or modify the session establishment to trick endpoints into using a weaker one. IPSec can be used with pre-shared keys and weak encryption algorithms. Either of these practices can vastly increase the attack surface.

7. Broadly permissive access

The security issues related to broadly-permissive VPN connections cannot be overstated. These connections must exist on the edge of the network, exposed to the internet for incoming connections. VPN servers are typically set up for large swaths of the network, with poor limits on what can be accessed once on the network. Typically, a device connected via a VPN is treated as a trusted device that is sitting on the internal network. This is in part because limiting what is visible to VPN users takes time, care, and effort. Organizations must sometimes stand up multiple VPN servers just to provide multiple permission sets to customize access for individual external users. Any broadly-permissive VPN connection – between your company and another with not-so-stringent security, or between vendors that should have limited access to your network but in fact can see more than they should - becomes a launchpad for any attacker resident on their network into your network.

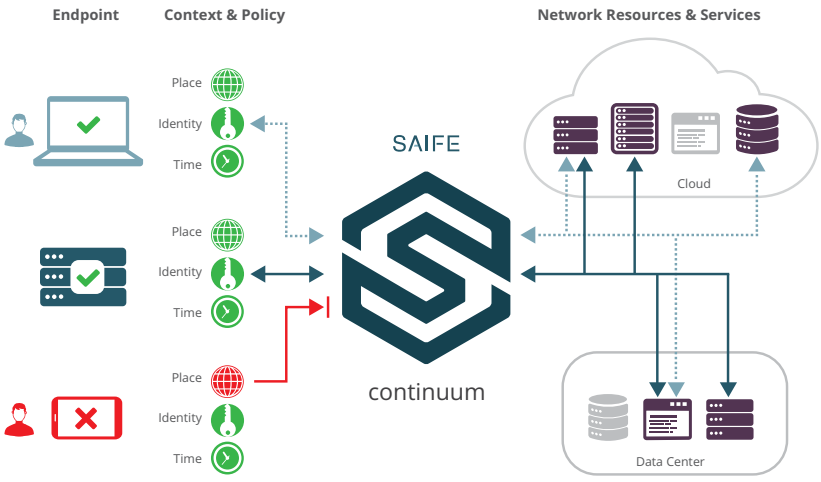
SAIFE ADDRESSES THE CHALLENGE

SAIFE combats the vulnerabilities and risk created by internet openness, the assumption of trust, the increasingly porous network perimeter, and overly-broad access. SAIFE ensures secure identity and secure connectivity, extending control of user access far beyond the traditional perimeter, and all the way down to individual services and applications as they are defined in the existing enterprise identity and entitlement system. SAIFE is built on the principle of a Software Defined Perimeter (SDP) [ii] which defines a set of network-connected participants within a secure computing enclave, restricting access to specific participants and hiding the assets from public visibility, thus reducing the attack surface. This approach has been endorsed by Gartner [iii] and ESG [iv] as one of the leading technologies for 2017 and years to come.

SAIFE combats the vulnerabilities and risk created by internet openness, the assumption of trust, the increasingly porous network perimeter, and overly-broad access

By adopting the concept of a Software Defined Perimeter, SAIFE isolates network services and resources from the internet. SAIFE creates a dynamic, individual micro-perimeter for every endpoint, inside of which the privacy and integrity of all traffic is assured. The entire path from endpoint to service, from user to application, is secured. Network access is defined by identity, device profile, and context, and access is allowed to only those applications and resources for which a user is pre-entitled. An endpoint attempting to access a given resource is authenticated before being connected to the infrastructure, and is then only given access to resources for which a pre-authorized connection has been established. An authorized user sees only the services and resources he/she is entitled to access. Everything else on the network is invisible, precluding access to unauthorized services or lateral movement. To an unauthorized user or

Figure 1 – SAIFE Micro-Perimeterization



would-be attacker, the entire network is hidden. There is no attack surface, there is no target. SAIFE's patented certificate-based Secure Private Session Routing Protocol extends the concept of a Software Defined Perimeter and removes the residual vulnerabilities and attack surface of solutions that strictly adhere to the Cloud Security Alliance SDP definition.

SAIFE PHILOSOPHY AND DESIGN CONSIDERATIONS

SAIFE was designed for the most demanding use case: securing military communication over untrusted networks with well-funded adversaries presumed to control the network equipment and basic identity and routing services. SAIFE trusts neither users nor providers of network accessibility, nor does it require trust in third-party Certificate Authorities to maintain a chain of trust. This zero-trust approach removes reliance on ARP, IP and DNS for identifying and providing routable addresses. SAIFE similarly puts the ownership of certificates into the organization's hands, making each its own CA with seamless and automatic certificate management, distribution and revocation.

SAIFE eliminates anonymous and/or unauthenticated connections (and the resultant attacks) by requiring each connection to be pre-authenticated and pre-authorized.

SAIFE addresses each of the seven issues related to the current state of the network:

1. Trusted Internet Identity

When it comes to sensitive information, an organization knows who its employees are, who its registered customers are, and who its partners are; there is no need for anonymous devices to connect to systems or services. There is no need to expose the vulnerabilities of those systems to the larger network or the internet. SAIFE eliminates anonymous and/or unauthenticated connections (and the resultant attacks) by requiring each connection to be pre-authenticated and pre-authorized. SAIFE avoids the common target of a centralized trust broker by making each endpoint the keeper of the identities of other endpoints and services for which connections are allowed. Endpoints must perform a certificate proof-of-possession for authentication with the SAIFE Continuum (see description below), which registers their presence to accept incoming connections or make outgoing connections. Thus, there is no trust in ARP or IP. DNS is not needed at any stage to discover the network location of an endpoint. An organization is its own Certificate Authority; there is no dependence on outside third-party CAs. Certificates are pinned to an identity (service, server or subnet) and are securely pre-introduced by signed encrypted messages to each endpoint. In addition, SAIFE's open API can be configured so that applications can build on top of device-specific security capabilities, if desired.

Secure Private Session Routing Protocol eliminates the need to rely on untrustworthy DNS and routing over potentially hostile networks, which invites DDoS, MITM, and session hijacking.

2. Trusted Internet Routing

Organizations no longer need to rely on untrustworthy DNS and the routing of traffic over potentially hostile networks, which invites denial-of-service, man-in-the middle, and session hijacking attacks, among others. The SAIFE Secure Private Session Routing Protocol, as described later in this document, is a more secure discovery service than DNS and

is not subject to spoofing or denial-of-service attacks. The SAIFE Secure Private Session Routing Protocol supports only secure algorithms and requires pre-introduction for endpoints to connect. It is not vulnerable to attacks such as spoofing or session hijacking. SAIFE addresses all entities by certificate, and does not require sharing the IP address of each end of a connection with the endpoint on the other side, eliminating the reliance on DNS and untrustworthy routes.

With SAIFE, all network connections appear to terminate within the SAIFE Continuum, which hides network topology and the IP address of every endpoint within the network. Secure routing through the SAIFE Continuum keeps data and keys private from end to end. All endpoints are hidden behind firewalls that block all inbound connections, and that have no publicly-routable IP address (other than the public IP address of the firewall). The firewall address does not need a DNS entry. If the firewall is targeted by a DDoS attack, the IP address can be merely changed; new incoming connections will automatically flow to it – no need to broadcast the change because authorized clients will find it, and attackers will not.

3. Agile Yet Secure Perimeters

The basic premise is simple: You can't hack what you can't see.

Services, devices, and applications no longer need to be exposed to the internet, or to any users that are not authorized to see them. This virtually eliminates the attack surface. The basic premise is simple: *You can't hack what you can't see*. With SAIFE, endpoints (service, server, subnet or device) are no longer visible from the public internet. Instead, they hide behind firewalls that can be set to block all inbound connections, all the time. This eliminates the need to open firewall pinholes that can be exploited, or flooded with packets in a DDoS attack.

SAIFE reduces the risk associated with VPNs, firewalls and DNS by allowing only connections between pre-authenticated endpoints. Bad actors can't take advantage of vulnerabilities because they won't even see the services. Patching becomes much less of an urgency when only trusted, pre-authenticated users and devices are connecting to your systems. SAIFE can also validate the security posture of an endpoint before allowing connection to ensure systems are not exposed to uncontrolled or poorly-provisioned devices.

4. Secure, Manageable Security Solution

There is no need to depend on proper management of firewall rules, VLANs, and VPNs to protect the network against unauthorized and/or unrestricted access. Much of those management costs can be eliminated. SAIFE greatly reduces the management burden, and the security risks, of maintaining defense-in-depth. Rather than relying on firewalls, VPNs, VLANs, and the like to enforce access controls, SAIFE automatically updates entitlements throughout the population of interfaces that need access. Similarly, SAIFE updates entitlements automatically as users, services, servers or subnets are changed or retired from your deployment. The network perimeter becomes

completely dynamic, without incurring additional risk. By leaving internet-facing firewalls in an all-inbound blocked state, SAIFE relieves the management burden of maintaining firewall rules, opening and closing ports when no longer needed, worrying about port scans, managing VLANs, undergoing lengthy negotiations with vendors for VPN access, and much more.

5. PKI and Certificate Issues Resolved

Organizations can leverage PKI without worrying about implementation and management costs. SAIFE makes PKI simpler and more trustworthy, solving the PKI key management/distribution problem. An organization is its own CA for device and user authentication to the SAIFE environment. The SAIFE Deployment Manager (see description below), provides point-and-click management of all endpoints, and serves as the organization's Certificate Authority. All certificates are pinned to specific identities and entitlements; a compromise of any one device has a limited "blast radius", and a defined recovery path that is swift and absolute. The ability to authorize or revoke connections resides exclusively within the SAIFE solution, with no vulnerable centralized key database. This removes the danger of a developer, third-party authority, operating system or app store damaging the chain of trust. No longer are organizations dependent on outside third-party CA's root level, device, developer, store or browser, and there is no vulnerable centralized key database. More information can be found in the "New Clients" and "Groups and Entitlements" sections below.

SAIFE makes PKI simpler and more trustworthy, solving the PKI key management/ distribution problem. An organization is its own CA...

6. A Saner Approach to Connectivity

An organization's security solution no longer needs to announce itself, and all its users, to the public internet. Anonymous devices simply cannot see the network. SAIFE removes the dangerous interface surface area of IPSec or TLS. The SAIFE certificate-based Secure Private Session Routing Protocol skips the anonymous introduction steps that TLS and IPSec/IKE require. Because SAIFE endpoints maintain the identities and certificates of the other services to which they are entitled to connect, SAIFE can go directly to the session key establishment messages. This reduces the attack surface to the math of elliptic curve cryptography itself. There's no man-in-the-middle attack possible from anonymously introduced endpoints. And there is no risk of the next Heartbleed or Poodle attack that exploits TLS protocol vulnerabilities.

Additionally, SAIFE enforces the strongest encryption possible. It's impossible to negotiate a weaker algorithm or modify the session establishment to trick endpoints into using a weaker one, as is possible with IKE and TLS. Key generation and sharing and cryptographic activity occur only at the device level, making backdoors impossible. Within the SAIFE encrypted tunnel, organizations can use their own encryption.

7. **Enforced Fine-Grained Access**

   Organizations no longer need to worry about broadly-permissive network access given to VPN users, partners, or contractors. SAIFE establishes identity at the endpoint or network service level, not at the level of a gateway that sits in front of them. This allows users to segment services – or entire network subnets – behind SAIFE Connect Servers. Having multiple groups enables granular control over what services, servers and subnets a particular endpoint can access: only endpoints sharing membership are allowed access. Addressing via SAIFE certificates tied to endpoints that can be deeply embedded within the network topology enables precise access to specific assets. It limits the blast radius of third-party network compromise. All other services remain invisible.

THE SAIFE PLATFORM

SAIFE is a trust-centric authentication and encryption framework for real-time data connectivity. SAIFE assures trusted routing for any endpoint, across any network, regardless of infrastructure by creating secure tunnels through which the privacy and integrity of all traffic is assured inside a micro-perimeter. SAIFE can be deployed in the public cloud, on private clouds or on-premises, and can be integrated into existing network solutions, creating a closed ecosystem of trust. SAIFE secures enterprise applications, voice, SMS and data from smartphones and tablets, cloud storage, IoT and operational data, and provides the ability to create secure communities of interest.

SAIFE has three principal components:

» **The Continuum is a robust mesh network composed of many Continuum Nodes.** It is a cloud-based, globally distributed, highly resilient overlay network that provides trusted routing over the internet or private networks. Endpoints, hidden behind firewalls that can be set to block all inbound connections, must authenticate to connect to Continuum, which then brokers a trusted connection between those authenticated endpoints. Continuum handles the routing of encrypted data between endpoints based on their certificates and last known location. Continuum itself is a low-value security target: it never has access to sensitive data or key material that is stored in the endpoints. High availability is designed in: if needed, the SAIFE network will heal itself by taking down affected servers and rerouting traffic to unaffected servers.

» **SAIFE-Enabled Endpoints serve as the on-ramps and off-ramps to the Continuum.** They communicate using SAIFE Connect Client software, a physical or virtual SAIFE Gateway appliance (when a software client is infeasible, such as IoT, SCADA, VLAN extensions, etc.) or the SAIFE Open API (for direct integration of applications). SAIFE Connect Clients and applications establish secure communication with the SAIFE Continuum, which validates their security posture, as well as other contextual information such as time-of-day and geolocation, before allowing the

connection. For each connection, Clients generate ephemeral key pairs used for perfect forward secrecy of each session, which in turn generate unique symmetric AES keys for each data session to encrypt data. The lightweight Client software on the endpoint provides the local keystore, encryption, and routing of encrypted data through the Continuum. Local database files employ AES Key Wrap for protection of the sensitive keystore and policy configuration data that persist for the life of the endpoint.

» **The SAIFE Deployment Manager is the configuration and control mechanism for an organization's deployment on Continuum.** It manages the lifecycle of certificates and secure groups. The Deployment Manager interface makes it easy to create logical groupings or secure enclaves, allowing endpoints to communicate with each other if they are in the same groups. This can be done in integration with an enterprise IAM, such as Active Directory, and the enterprise policy model, easily administered through the Deployment Manager. It provisions new endpoints, signs their self-generated certificates, and exchanges those certificates with other endpoint members of the same secure group by introducing them to one another in advance of communication. Once an introduction has been made by the Deployment Manager, an endpoint can request a connection with a certificate that represents a single service, endpoint or subnet within their group for which they have been authorized.

SAIFE IN ACTION

SAIFE secures the network by enforcing a "authenticate then connect" approach, a zero-trust model which requires pre-authentication and pre-authorization of endpoints connecting to services. Authenticated endpoints, services or devices have visibility to only those resources on the network for which allowed connections have been pre-authorized. All other assets are invisible. To a would-be attacker, the entire network is invisible. There is no target, so credential theft and privilege escalation are meaningless. Details on how new clients are enabled and placed in appropriate groups, and how allowed connections are established and revoked follows.

SAIFE secures the network by enforcing a "authenticate then connect" approach, a zero-trust model which requires pre-authentication and pre-authorization of endpoints connecting to services.

New Clients

When a new client is installed, it generates entropy, which it uses to generate a key pair that it self-signs. It introduces itself to the SAIFE Deployment Manager by sending it its public self-signed certificate. The Deployment Manager signs the certificate and returns the CA-signed client certificate and provisioning information to the client. Included is the list certificates of the other endpoints or services that the client can see, effectively creating an individual micro-perimeter encapsulating the endpoint and service that it can access. The new client's signed certificate is shared with other endpoints (with their own micro-perimeters), introducing the new endpoint as a member of the secure group. The endpoint is trusted to see only those services for which it has been pre-authorized, as opposed to completely trusting it to see every resource inside the traditional perimeter.

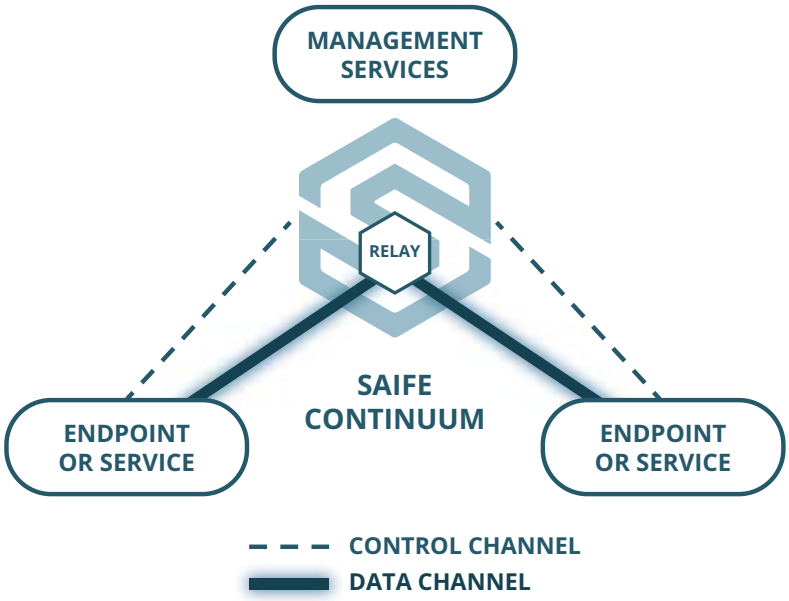
Groups and Entitlements

The SAIFE Deployment Manager's interface allows organizations to place endpoints into secure groups. It then securely shares the certificates of the group's membership with all the clients in the same group. This pre-introduction enables endpoints in the group to make connections with one another. Clients never exchange certificates directly – they are provided with the certificate for the other side of the connection in advance in order to connect. If the membership of a secure group should change, the SAIFE Deployment Manager sends new information to every client, either adding or removing the certificates of the other client endpoints from their local list in memory. This enables or disables their ability to connect. Membership in the groups can be synchronized with an Active Directory group membership for automatic updates. Endpoint management is simple thanks to the Deployment Manager's intuitive GUI and synchronization with Active Directory for automatic updating.

Connections: SAIFE Secure Private Session Routing Protocol

In day-to-day operations, when an endpoint needs to access a service, it establishes a connection to Continuum and authenticates by proving possession of its certificate as well membership in the relevant group, and optionally meeting both context (e.g. location, device, OS, patch level, time of day, AV protection, etc.) and policy requirements. Network services similarly establish and maintain presence with Continuum. The endpoint then sends a connection request to Continuum containing the certificate fingerprint of the target endpoint or service. Continuum assigns a rendezvous point

Figure 2. SAIFE Control and Data Channels



for the pair to directly communicate with each other, providing limited metadata and no visibility of the intended target on the other end. Peer endpoints validate each other to establish a secure end-to-end session and share an encryption key. All data exchanged through the rendezvous point are end-to-end encrypted using only strong algorithms (AES 128 or 256, Elliptic Curve P-384, Diffie-Hellman). All traffic appears to terminate in the cloud (Continuum). Connections are invisible, and traffic is undecipherable.

SAIFE creates and enforces agile perimeters in real time, securing the entire path from user to application, device to service.

SAIFE hides both endpoints of a connection behind all-inbound-blocked firewalls that have permanent DENY-ALL inbound rules, yet still accept incoming connections. A firewall pinhole is never opened. Services will only establish connections from already-authenticated and authorized endpoints. In this way, SAIFE creates and enforces agile perimeters in real time, securing the entire path from user to application, device to service.

Access Revocation

When an endpoint is lost or stolen, or must be removed from a group or the network, access revocation occurs. The process is quick, thorough and painless, without requiring management and distribution of certificate revocation lists. A point revocation is issued to all the clients that shared a secure group with the now-revoked client certificate, effecting an immediate revocation of the endpoint. This also wipes the keystore from the revoked endpoint. Any revoked endpoint attempting to connect to Continuum will be denied access. Even if it could succeed, it would be cryptographically unable to establish a secure session with any other client, as the other clients no longer have the public certificate of the revoked endpoint: the SAIFE Deployment Manager will have already issued each an update that removed the certificate upon the endpoint's revocation.

CONCLUSION

SAIFE eliminates the inherent vulnerabilities of traditional perimeter SAIFE has created a new paradigm for network access and security that extends the concept of a Software Defined Perimeter. SAIFE effectively eliminates the attack surface, so adversaries cannot perform reconnaissance against or directly try to exploit any endpoint or any network service. By pre-authenticating endpoints to Continuum and using only outbound connections, SAIFE hides the endpoints behind stealth outbound-only firewalls. SAIFE uses certificate-based routing over the SAIFE Continuum, making connections invisible and traffic undecipherable. It avoids the issues related to TLS and IPSec/IKE, DNS, VPN, firewalls and other technologies that create or expose vulnerabilities. Fully-automated key management brings the benefits of PKI without its overhead and vulnerabilities. Integrated with IAM (and other security solutions such as SIEM and network monitoring) SAIFE brings a new level of network security to an organization's most sensitive resources and services. SAIFE is an innovative and proven way to provide secure, trusted access to services and data over untrusted networks.

SAIFE has created a new paradigm for network access and security that extends the concept of a Software Defined Perimeter

ABOUT SAIFE

SAIFE eliminates the inherent vulnerabilities of traditional perimeter defenses that cost organizations hundreds of millions of dollars in breach-related losses every year. We are redefining perimeter security, enabling secure, trusted access to services and data sets over untrusted networks, while making those same services and data sets invisible to unauthorized users and would-be attackers. We've extended the concept of a Software Defined Perimeter to create the first solution that enables dynamic, agile, network overlay perimeters that are device, user, and application-centric, and which can span on premise, cloud, mobile devices, and applications. SAIFE protects customers by substantially lowering their attack surface and enables information sharing across untrusted networks to reduce third-party risk.

As the world gets more interconnected, it becomes smarter, more aware, more productive — and more vulnerable, our job is keeping it SAIFE.

Email: **info@SAIFE.io**
Phone: **+1 703.229.5924**
www.SAIFE.io

...

[i] Liu, Yabing et al. *An End-to-End Measurement of Certificate Revocation in the Web's PKI.* University of Maryland, 2015. Retrieved from http://www.cs.umd.edu/~dml/papers/revocations_imc15.pdf.
[ii] Software-Defined Perimeter. Cloud Security Alliance, Dec. 2013. Retrieved from https://downloads.cloudsecurityalliance.org/initiatives/sdp/Software_Defined_Perimeter.pdf
[iii] *Gartner Identifies the Top Technologies for Security in 2017*. June 2017. Gartner. Retrieved from https://www.gartner.com/newsroom/id/3744917
[iv] Oltsik, Jon. *Software-Defined Perimeter Essentials. CSO Magazine*, June 2016. Retrieved from http://www.csoonline.com/article/3077818/security/software-defined-perimeter-sdp-essentials.html

For more information:

Email: **info@SAIFE.io**
Phone: **+1 703.229.5924**
www.SAIFE.io