SAIFE

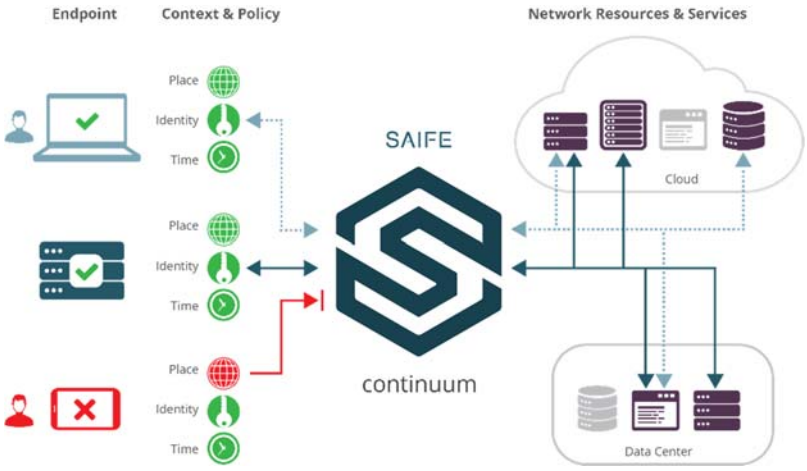
PERIMETER SECURITY RE-INVENTED

The Perimeter Has Moved, Your Defenses Have Not

The concept of a well-defined, locked-down enterprise security perimeter is no longer valid. As applications, people and data have grown more and more distributed and organizations have become increasingly interconnected, the perimeter has moved to wherever those with access to your network are and to whichever internet connected devices they're using. Traditional perimeter-based security defenses that most organizations depend on are proving ineffective as evidenced by ever-growing reports of data breaches and corporate losses from cybercrime. Today, firewalls and VPNs are easily defeated and data encryption alone leaves Internet traffic visible.

A Model for Today's Agile Perimeter

SAIFE® has adapted a Software Defined Perimeter approach that defines access by identity, device profile, context, and authentication method. Access is established to only those applications and resources for which a user is authorized, creating and enforcing agile perimeters in real-time. The entire path from user to application, device to service is secured and network resources are hidden from unauthorized or unauthenticated users. SAIFE's dynamic perimeter overlay (DPO) network creates secure tunnels through the Internet in which the privacy and integrity of all traffic is assured inside a micro-perimeter.



Benefits

Substantially Reduces Attack Surface

Undiscoverable network resources make bad targets. When data sets and services are invisible on the Internet or the internal network, they can't be scanned, they can't be attacked. You Can't Hack What You Can't See.

Significantly Improves Security

SAIFE lowers the chances of successful network-based attacks such as denial-of-service attacks, man-in-the-middle attacks, server vulnerabilities and lateral movement

Lowers Total Cost of Ownership

SAIFE is a software-only solution that can be deployed in a cloud or virtual machine environment, or consumed as a service. There is no hardware to purchase and no hardware to maintain.

Fully Automates Key Management

PKI is complex, hard to implement, and expensive to maintain. SAIFE's centralized key management automatically generates, shares, and destroys keys and certificates from inside your LAN or from across the Internet - all the benefits of PKI with none of the headaches.

Flexible Deployment, Easy to Use

Deployable in public or private clouds, on premise or as a SaaS solution, SAIFE automates centralized key management for rapid provisioning, reducing administrative, management overhead and expense.

The Emerging Software Defined Perimeter

A Software Defined Perimeter overcomes the constraints of traditional tools by effectively creating a dynamic, individualized micro-perimeter for each user based on attributes such as identity, device profile, location, and authentication method. A Software Defined Perimeter approach ensures that all endpoints attempting to access a given resource are authenticated and authorized prior to accessing any resources on the network. All unauthorized network resources are made inaccessible, reducing the attack surface, by hiding network resources from unauthorized or unauthenticated users or assets.

The SAIFE Platform

SAIFE secures the data in transit between devices and the data at rest on devices. SAIFE consists of three components:

- A software interface for endpoint devices, either as a tunneling client (SAIFE Connect), a gateway device (SAIFE Gateway), or a custom application
- Continuum, SAIFE's global, cloud-based routing network
- A management interface, (SAIFE Management Console)

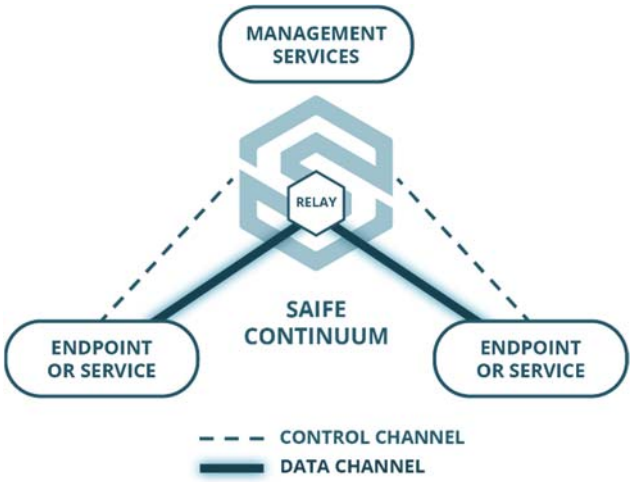
SAIFE Secure Micro-Perimeters

Endpoints attach to Continuum via the SAIFE Connect Client or SAIFE Connect Server. When installed, a unique cryptographic keypair (public and private keys) and certificate signing request (CSR) are generated. The endpoint's identity is established with Continuum by submitting its CSR to Management Services, which validates the endpoint by signing its public certificate. Once downloaded, the public certificate becomes a cryptographic fingerprint that binds the endpoint's identity with its public key.

Communication only occurs between peer endpoints within secure and externally anonymous groups. Secure enclaves are created, edited, and disbanded, either automatically or manually in the Management Interface. When the endpoint is added to an existing secure enclave, the public certificates of other group members are distributed to the endpoint, and the endpoint's public certificate is distributed to the rest of the enclave.

When an endpoint registers its presence with the SAIFE Continuum, Continuum maps the organization's endpoints in real time without sharing or storing IP addresses. The use of public-facing IP addresses is limited to the mapping of endpoints by the Continuum servers; all SAIFE endpoints use their public certificates as a means of identification with one another.

To initiate a secure session, the endpoint and Continuum server mutually authenticate and reserve a packet relay service within the Continuum node. Continuum shares the public facing IP address and port number of the packet relay service (in a secure message) with both endpoints. Both endpoints decrypt the IP address and port number, and use it to create an end-to-end secure tunnel between them.



About SAIFE

SAIFE is re-inventing security for today's agile perimeter. 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 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 3rd party risk. With cloud computing, mobile devices, collaborative networks, and the IoT creating a smarter world that is more aware, more productive – and more vulnerable, our job is keeping it SAIFE.