SAIFE CONNECT

The on-ramp and off-ramp to SAIFE Continuum

SAIFE® enables endpoints and network services to communicate securely over untrusted networks. Over Continuum, SAIFE's global, cloud-based routing network, the privacy and integrity of all traffic is assured, even on compromised devices and untrusted or exploited networks. SAIFE Connect products are the ingress and egress points to Continuum for network services, data sets, and endpoints, and create secure tunnels for encrypted data sharing over the Internet with always-on connectivity to private networks.

Whether connecting an enterprise's remote devices to its private network, establishing server-to-server communications, or enabling remote access to a virtual private cloud, SAIFE Connect provides a secure, encrypted, hidden channel for data in transit.

SAIFE Connect products perform:

Authentication. Connect authenticates with Continuum and with other endpoints by establishing the endpoint's identity with Continuum and registering its presence. This enables Continuum to map all endpoints in real time without sharing or storing IP addresses.

Authorization. Connect grants and limits access to other endpoints and services. Continuum pushes a table of authorized connections and their associated public certificates, which Connect maintains and uses to grant or deny access. Only authenticated, pre-authorized connections are granted.

Key Generation and Key Exchange. Connect generates an endpoint's unique cryptographic key pair and stores the public certificate generated by Continuum management services. The public certificate serves as a cryptographic fingerprint, binding the endpoint's identity with its public key.

Encryption and Decryption. Connect enables end-to-end encryption across Continuum. Encryption and decryption only occur locally. Connect encrypts data using the public key of the intended recipient and decrypts messages received with its private key.

SAIFE Connect Client

The SAIFE Connect Client is an easy to install client application available for Windows, Linux, OS X and Android devices. Connect quickly and easily extends a network's secure perimeter to remote devices and remote servers enabling secure data exchange over private or public networks.

Whether protecting employee BYOD devices or server-to-server connections between remote sites, the SAIFE Connect Client works seamlessly, protecting valuable data in transit by making it invisible to potential attackers.

Connect Client Supported Platforms

Platform	Minimum Platform Version
Windows®	Windows 7 & 10 (64-bit versions only)
Android™	5.0+
OS X® (macOS)	10.8
Linux®	Red Hat® Enterprise Linux/CentOS 6.6

SAIFE Gateway

The SAIFE Gateway is a plug and play hardware appliance that enables endpoints and network devices to be easily connected to Continuum via a network cable. With four RJ45 jacks, Gateway can be used to provide up to four cryptographically isolated, independently routed tunnels. The SAIFE Management Console is used to specify the traffic to be routed to each port. Gateway is easy to configure via a simple web interface and manage through the SAIFE Management Console.

- Secure legacy devices and platforms for which no SAIFE Connect Client is available. Gateway can easily protect and extend the life of costly, older equipment.
- Secure devices without having to install or modify software. Gateway can be used to secure devices without the need for costly and time consuming re-certification.
- Secure Industrial IoT and OT devices, making them undiscoverable by unauthorized users and would be attackers.

SAIFE Gateway Specification

CPU	4 core Intel® Atom™ C2558 CPU, 2.4 GHz
Dimensions	1.5" high x 6.8" deep x 7" wide
Weight	1lb. 4oz
Ports	6x RJ-45, 2x USB 2.0, 1 Mini-USB Serial Console Port
Power	External ITE P/S AC/DC 100-240V, 50-60 Hz, 12V 4.16A
Ambient temperature	Fanless operation from 0°C to 40°C
Ethernet	High-performance 10/100/1000 Ethernet controller; IEEE 802.3/802.3u-compliant

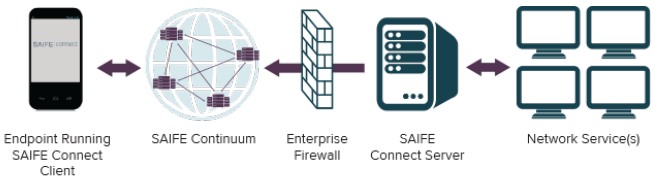
SAIFE Connect Server

SAIFE Connect Server is an aggregator for connecting multiple SAIFE Connect Clients on the same local network to Continuum. SAIFE Connect Server creates an independent tunnel for each client.

SAIFE Connect Server works within the existing infrastructure and can be deployed on a physical server on premise or a virtual server in the cloud.

SAIFE SDK

The SAIFE SDK can be used to enable applications and services to connect directly to SAIFE Continuum. By including the SAIFE Endpoint Library within an application, peer endpoints can securely communicate over SAIFE Continuum. The SAIFE Endpoint Library supports Android, iOS, OS X (mac OS) and Linux.



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.