ENCLAVE

Technology Whitepaper

May 2018

Westgate
CYBER SECURITY

Rapidly build end-to-end encrypted networks.

task or purpose specific
secure, and private
provider agnostic
micro-segmented

Your network **without** Enclave

Expensive

- Network configuration is time consuming.
- Centralisation of bandwidth is expensive.
- Hardware is expensive and takes time to deploy.

Time consuming

- Changing the network introduces operational risk.
- Change management is laborious and error prone.
- Setting up networks distracts from core business, and often halts projects. Working on infrastructure doesn't add value, Its not a differentiator.

Complicated and exposed

- Cryptography and secure networks are hard to get right. Certificates and PKI are expensive, and always-on remote access services expose your network, and leave it vulnerable to attack.

A typical network today is…

Complicated to manage, hard to setup, fragile to operate and resistant to change. Deploying secure networks introduces operational risk, and wastes engineer time on activities that don't add value to the business.

Your network **with** Enclave

Costs less

- Deploy secure networks in seconds, hassle free.
- Connect endpoints directly without centralisation.
- Deploy without changing your existing networks.

Saves time

- Reduce risks with change-free overlay networks.
- Free engineering resource to be strategic and focus on core business activity.
- Migration of devices and endpoints becomes easy.
- Enable features like multicast in Cloud networks.

Reduces complexity and improves security

- Automatic end-to-end encryption.
- Mandatory mutual authentication.
- Enclave networks are invisible, reducing organisational risk and visible surface area.

With Enclave…

Your network becomes a time and cost saving competitive advantage. Spending time building out your network doesn't differentiate you from your competitors; Enclave does.

Enclave dramatically simplifies your network topology and reduces the risks associated with network changes. Rapidly deploy **software defined virtual networks**, without needing to change your underlying infrastructure.

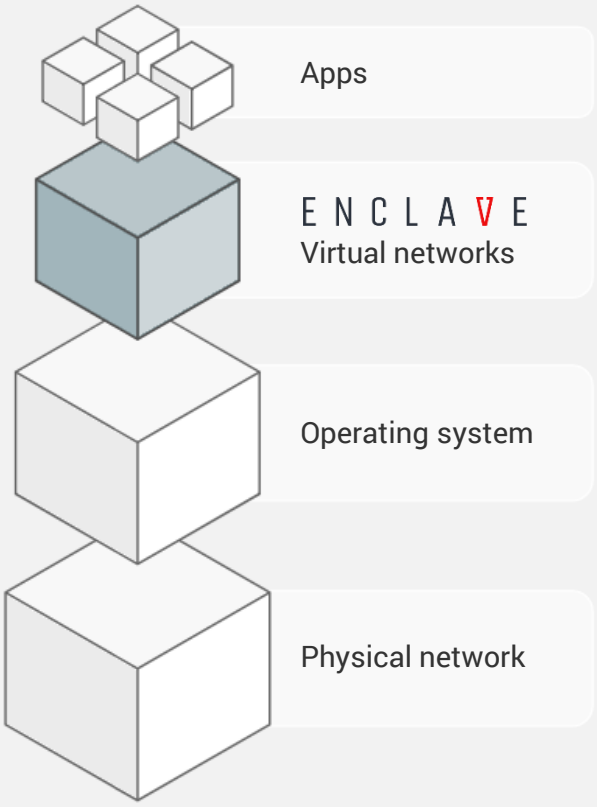
Enclave builds private peer-to-peer connected overlay networks which can be setup or thrown away in seconds, that work everywhere, with automatic end-to-end encryption, and zero changes to your existing network.

Westgate
CYBER SECURITY

Architecture

Enclave makes **introductions** and facilitates **direct connections**.

- Enclave builds overlay networks across groups of devices, virtual machines or containers to form strongly authenticated, and encrypted communities of interest.
- Once installed, Enclave creates a new virtual network interface for each overlay network that system is a member of.
- Each virtual network interface is assigned an IP address so it can communicate with other parties in the same overlay network.
- Existing applications and services send data to one another using their IP addresses assigned in the overlay network.
- In order to communicate, all parties must be part of the same overlay network.
- Enclave locally encrypts all traffic crossing the overlay networks, so your data is secure in transit.
- Overlay networks are fully transparent to existing applications and services.



Certificates and trust

Reliably exchanging public keys is challenging when working with infrastructure and pre-shared keys (PSKs) are both impractical, and extremely insecure.

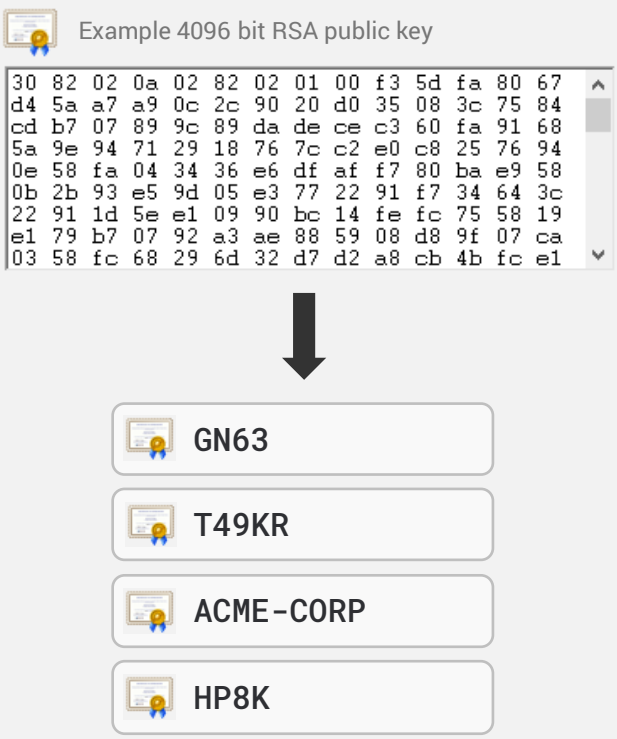
Enclave uses certificates with human friendly names as cryptographic place-holders which can be exchanged instead of the public key itself. Users, administrators and system operators need to exchange the public keys for each of their endpoints, and certificates issued with arbitrary, but short, sharable and human friendly names make this process much more manageable.

Short, sharable, human friendly **names** not long complicated **public keys**.

In effect, Enclave gives users, administrators, and system operators a convenient way to handle public keys without needing to incur the expense and complexity of issuing strongly named certificates to their fleet of servers, devices and IoT endpoints.

By using short, simple, but arbitrary common names, certificates can be issued instantly without end-user interaction and as a machine to machine conversation.

This cuts certificate issuance time down from weeks to seconds and eliminates significant complexity at the same time.



Westgate CYBER SECURITY

Establishing an Enclave

Users exchange **certificate names** and instantly get a **secure, private network**.

1 **Client certificate issued**

Westgate Cyber Security has developed a novel twist on standard public key exchange, allowing client certificates to be issued in real-time to end users and systems for an unbelievably simple user experience.

2 **Mutual authentication**

Cooperating parties exchange the common names of their client certificates. This ensures all parties must mutually authenticate one another before any communication can take place.

3 **Secure enclave established**

Once authenticated, our peer-to-peer technology establishes direct connections, exchanges ephemeral session keys and stands up instantly available virtual private networks between connecting parties.

All parties participating in an Enclave must mutually authenticate one another by exchanging certificate names. This can be done manually, or the process can be centralised and automated using Westgate's Enterprise Dashboard software.

Without mutual consent from all parties, tunnels cannot be established and communication is not possible. Enclave requires at least two party consent in order to establish an Enclave, yet either party may, at any time, change their mind and tear down the connection.

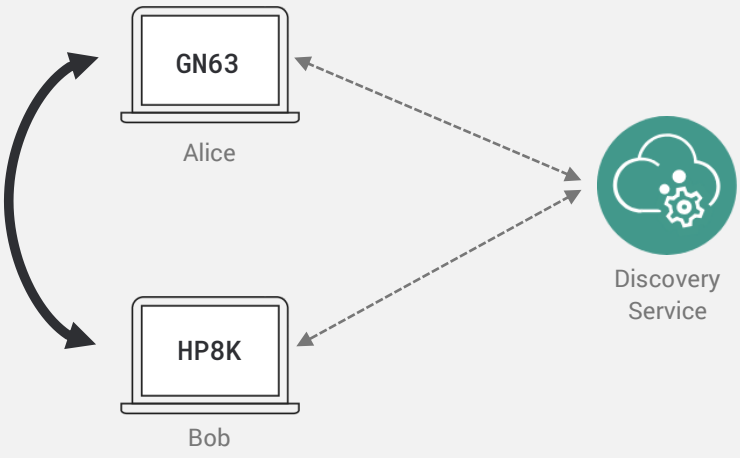
This elasticity makes Enclave especially well suited to ad-hoc, and dynamic situations where secure communication is required at speed, but is equally reliable in long-term deployment scenarios.

How Enclave works

1. Enclave builds a certificate signing request and sends it to the authority, which issues a certificate with a name of its choosing back to the endpoint. The endpoint now possesses an identity (a private key and corresponding certificate).

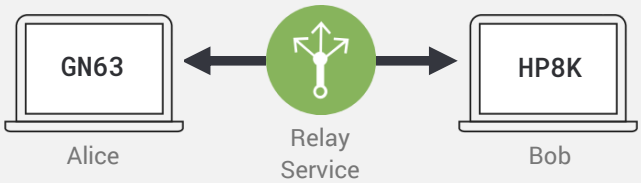
2. Enclave connects to the discovery service from Alice's machine, and requests a connection to **HP8K**. The request is acknowledged, but no connection is established.

3. Bob's machine (owner of the private key corresponding to the certificate **HP8K**) asks for a connection to **GN63**. The Discovery service sees mutual intent and introduces both parties to one another so that they can establish a direct connection. *



* Once connected, both parties use their mutual intent to connect (via exchanged certificate names) and the public keys from each certificate to perform an ephemeral key exchange and agree a shared secret for the encryption cipher

4. If a direct connection is not possible, the Discovery Service selects a geographically optimal relay service and builds a pathway that both parties can use to establish a connection.



Use-cases and industries

Isolation and compliance

Enclave allows customers to safely partition and microsegment their infrastructure into isolated, secure overlay networks that only exist on authorised systems. One customer created two virtual networks with a partner organisation, the first for operational traffic, and a second for failover. Overlay networks create isolated environments, with Enclave working at the network edge to keep traffic between partners, customers, and infrastructure separate and compliant.

Hybrid and multi-cloud deployments

Enclave helps customers securely connect data centre applications to cloud-based compute resources. Enclave adds full end-to-end encryption and highly available networks to secure and segment applications deployed between the private data centre and cloud. Enclave also brings features like multicast support to cloud-vendor networks, allowing customers to take advantage of cloud capabilities and simplify migrations without needing to re-architect legacy applications.

Internet of things

Enclave allows customers to greatly reduce their attack surface area, simplify IT administration and breeze through compliance audits with one simple solution which can enforce security policies at the application layer. Easily, securely and centrally manage systems at distributed remote locations while improving efficiency, and cutting costs by streamlining processes.

Fintech, supply chain, logistics and distributed industry

Enclave allows customers to provide secure remote access with one simple solution. Give contractors secure remote access to industrial systems, and increase team autonomy by leveraging existing infrastructure — no complex and costly traditional solutions required. Customers avoid deploying expensive circuits, and save money by using SDN to connect everything from off-shore rigs, to retail store locations, and PSD2 partners in fintech and banking.

Westgate

CYBER SECURITY

Contact

Email: founders@westgatecyber.com

Telephone: +44 (0)1633 215 545

Website: https://westgatecyber.com

Address: Westgate Cyber Security Ltd
Springboard Business Innovation Centre
Llantarnum Industrial Park
Cwmbran
NP44 3AW
UK