Perfecta

Labyrinth White Paper
5/13/2019

DIGITAL FINGERPRINTS THAT LEAD BACK TO YOU

Your organization leaves a digital fingerprint that is traceable and brings risk to your operations by identifying people, infrastructure, networks and locations. Perfecta provides a managed attribution network solution for organizations across the globe, known as Labyrinth, that obscures sensitive operations and protects privacy while ensuring activity logs are preserved for internal auditability and verification.

READ THIS WHITEPAPER TO LEARN:

Your organization's digital fingerprint is at risk.

An individual's digital fingerprint differs from your organization.

STEALTH

AVOID LEAVING TRACES AND AVOID DETECTION

Our Internet activity leaves traces of a digital signature when we operate in cyber space. Various entities, including private companies and government organizations monitor and track Internet activity, in some cases to enhance marketing capabilities and in other cases to detail what information individuals and organizations are researching, which individuals are doing the research and where they are located. Internet research can be sensitive. In legal, investment banking and military organizations, researchers do not want to attract the attention of monitoring entities. For example, law firms explore information related to potential lawsuits and cannot leave digital traces that can be attributed to the firm. Or investment-banking organizations require private avenues for due diligence research in anticipation of financing a start-up or prior to a merger or acquisition. While conducting investigative work, federal and state government agencies have **legitimate needs to cloak their digital signature** so that criminal organizations are not tipped-off to their identity.

When a user visits a website, information can be collected such as the user's IP address, an approximate physical location of the user, the user's time zone and language preference. In addition, the operating system, browser type, software, fonts, audio stack and plug-ins of the user can be determined to provide a digital fingerprint of the user.

Criminal and terrorist organizations have improved their technological capabilities and are intelligent enough to **detect and identify government and military IP addresses** as well.

TOR, I2P & VPN

PARTIAL MEASURES FOR INCOMPLETE COVERAGE

To combat online tracking, anonymity networks like **The Onion Routing (Tor)** and the **Invisible Internet Project (i2p)** have emerged to conceal user identities by removing links between a user's IP address, their digital fingerprint, and their online activities. Additionally, to establish a secure and private online presence, **Virtual Private Networks (VPNs)** are available for use that can provide tunneling and encryption of transmitted data.

While **anonymity networks** and **VPNs** deliver some privacy and security to individuals for their Internet activities such as web browsing and Voice over Internet Protocol (VoIP) for individuals, these solutions have deficiencies when used by organizations. Anonymity networks can be slow and unreliable. And activity logs are inaccessible. While an organization may want to obscure Internet traffic from the entities that are monitoring activity, from a defensibility perspective, an organization often needs to know and be able to audit the cyber activities their employees engage in.

LABYRINTH SYSTEM

MANAGED ATTRIBUTION - PERSONA MANAGEMENT - AUDITABILITY

To address organizational needs for secure and private browsing and messaging, Perfecta developed the patented Labyrinth system. Labyrinth is an advanced and trusted, managed attribution network that utilizes **virtual machines**, **secure VPNs** and **high availability (HA) mesh topologies** to efficiently direct operational Internet traffic while simultaneously providing management of logging and payment transactions. Sensitive searches and messages are secure, yet internally traceable if activities are questioned or challenged and require an auditable defense.

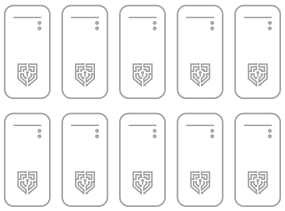
SEPARATING PERSONA

LABYRINTH SEPARATES PERSONA FROM INTERNET ACTIVITY

This is done by changing IP addresses, modifying network signatures, and altering the appearance of language packs, browsers, and operating systems for our customers. In addition, Labyrinth alters the purpose of traffic generated from the end user's system by **blending it with other traffic** coming from the same system.

A NETWORK OF HIGHLY PERFORMANT MESH NETWORKS

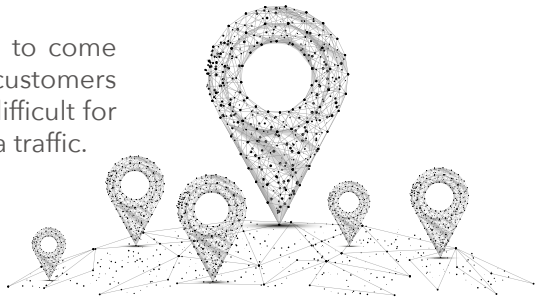
In the Labyrinth system, four legal companies are established for a customer – two in the U.S. and two abroad that are associated with their own configuration of operational transaction servers, log management servers and support servers. Each of the four companies have their own website and registered agent. There are no similarities between the companies, and they are not associated with Perfecta in any way. Each company has separate bank accounts and are configured so that there are no identifiable shared traits including the business information, network, administrative traits, finance or accounting activities.



Each operating company has ten computers, with a mesh architecture of four computers dedicated to operational traffic, a separate mesh of four computers dedicated to log management and two computers designed to handle company transactions and host a company website. Benefits of mesh configurations are **high availability, robustness, security and privacy while insulating the network from failure** at any node. The mesh topology provides an interconnection of multiple computers connected redundantly so that if one node fails the system still functions. Customer bandwidth utilization is maximized by directing operational traffic and log management activities through separate meshes.

ATTRIBUTION TO GEOGRAPHICALLY DIVERSE EXIT NODES

Labyrinth adjusts incoming and outgoing traffic so that it appears to come from different locations via **geographically diverse exit nodes**. Our customers select points of presence (POPs) from around the world, making it difficult for adversaries to determine the network infrastructure behind their data traffic.



This exit node configuration allows researchers, such as analysts, police or military personnel, to conduct research using a trusted, secure system that doesn't attribute back to the organization. Exit nodes are isolated from the mesh and are the associated attribution of web browsing activity.

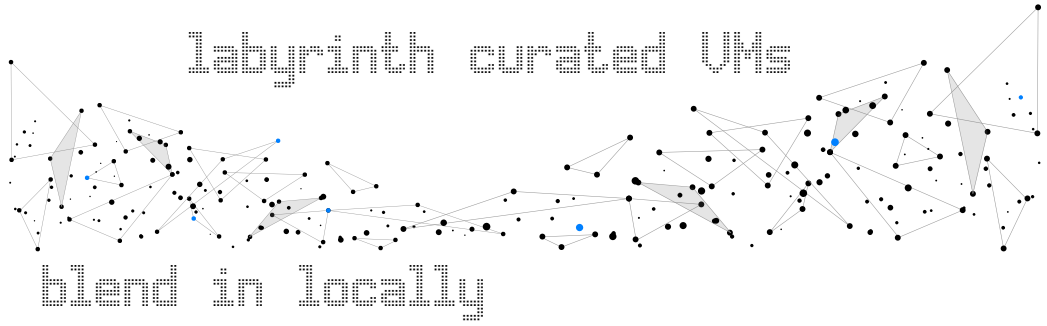
By using our virtual machine nest, customers connect using a web browser, select the type of machine they want to use, and that machine information gets routed out through the appropriate mesh to an exit node. For example, if a user conducts a search on Google, Google will see the IP address and virtual machine (VM) information related to the exit node.

ADVANTAGES OF THE
LABYRINTH ARCHITECTURE

OPERATE ONLINE AND BE UNTRACEABLE TO OUTSIDERS INCLUDING ISPs, GOVERNMENT & HACKERS

Utilizing VPNs for Internet activity allow users to operate online and be untraceable to outsiders such as Internet service providers (ISPs), government entities and hackers. Data is encrypted when using a VPN, essentially creating a tunnel between the network and an exit node in another location. Web browsing and online activities remain anonymous. And our network is built using a mesh topology to ensure high availability while maximizing throughput.

However, the creation of secure VPN using a mesh configuration is technologically complex and can be expensive for an organization to develop internally. **There are numerous advantages to using Perfecta's highly scalable, secure Labyrinth system** that incorporates both VPN and mesh topology to create a matrix of secure network infrastructure.



Flexible Configuration - Our customers often like to modify their fingerprint or switch to different virtual machines. In some regions, governments may restrict access to certain websites, or it may be important to leave a fingerprint that blends in with fingerprints typical in a specific region. We curate numerous virtual machines that our customers can use to blend in to the local area where they are doing research or activity.

The architecture provides for four companies in the U.S. and abroad, and each company can be easily shut down if necessary. We can quickly establish a new company to replace an existing company. In fact, **all infrastructure is disposable based on customer utilization**. Customers can configure the node firewalls on a temporary or permanent basis and specify which log data is monitored.

Exit nodes are often rapidly disassembled as necessary and substituted with replacement nodes.

ACCOUNTABILITY AND COMPLIANCE

Risk Management – While a flexible configuration is important, it is occasionally necessary to respond to questions or challenges regarding Internet activity. Customers often require reporting to another entity or organization. Perfecta logs all activity to support our customer's defense to these challenges. Because we maintain the logs, we can prove our customer did not commit a detrimental act and we provide this defense as part of our service. Perfecta completes all setup, monthly and daily maintenance tasks associated with each company, node and POP in the system.

ADVANTAGES OF THE
LABYRINTH ARCHITECTURE

[CONTINUED]

Flexible Configuration - Risk Management - Secure Network - Customer Control - Internal Traceability
Up-to-date Technology - Experienced Staff - Established Customer Base

Secure Network - Most systems are subject to network attacks and ours is no exception. In response, we developed a proprietary software defined networking (SDN) system to manage the traffic between the meshes in a customer's different companies. Our SDN defends the system using a custom sensor network deployed on all our machines that monitors the systems, the traffic and logon information.

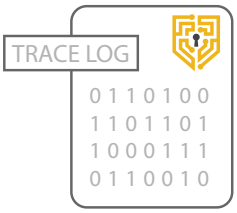
In fact, one customer requested an evaluation of our network by DARPA, who found that the **Perfecta Labyrinth system was secure, satisfying requirements of the DARPA assessment**.

Customer Control - Our customers desire the ability to control their network. In response, we developed the Labyrinth Management Portal (LMP).

LMP is a tool that allows our customers and our customer's users to monitor and control their mesh and exit nodes without relying on the Perfecta network operations center.

Through the LMP, users can turn on and turn off exit nodes, open and close ports, activate and deactivate VPNs, and download log files from any of the systems in their network.

Internal Traceability - Perfecta maintains logs of the system configuration and activity on the network and our customers have access to all their logs. Our customers frequently access and inspect their activity. For example, a customer may need to inspect all activity for the past 60 days. Logs are maintained using a customized Elasticsearch log stack (ELK Stack) in Kibana, an open source log management platform originally built by Amazon. Each customer's activity is maintained in a private, secure ELK Stack system that can be accessed remotely. We also provide files on disk or thumb drive if requested.



Up-to-Date Technology - Perfecta works with our customers to understand changing requirements and then use that knowledge to plan updates and new technical iterations. Several times per year our staff review the architecture and determine what technologies to add or update. For example, data leakages have emerged as an issue for systems using Web RTC (browsers with Real-Time Communications). To combat this threat, Perfecta incorporated a Web RTC proxy to eliminate the vulnerability from our network. In the process, we were able to strengthen our network's capacity to handle video and VoIP traffic, so that customers can send and receive phone calls, video messages and text messages securely through the network.

ADVANTAGES OF THE LABYRINTH ARCHITECTURE

[CONTINUED]

Experienced Staff - Perfecta staff members supporting the Labyrinth system have government security clearances and are based in the United States. Our staff are employees of Perfecta; we do not use contractors. Perfecta engages in regular reviews by third party law firms to ensure the methods we use to deploy and manage systems are legal under the laws of the relevant nations where systems are deployed.

Our networking staff continuously collaborate with the software development team, the internal research team, and participate in networking with other professionals to stay current on the best and most secure technologies. We work with our customers to understand changing requirements and then use that knowledge to plan each technical iteration. Several times per year our staff review the architecture and determine what technologies to add or update.

Established Customer Base - Customers have been using Labyrinth since 2015, including several federal and state government agencies, law firms and investment banks. Our customers help us to continually improve our systems, making them bigger and better each year.

100% RETENTION

Labyrinth is an established system and our customers stay our customers
– we are proud of our 100% customer retention rate.

Perfecta

ABOUT US

For over a decade, Perfecta has been trusted by organizations around the globe as a premier SaaS provider. Perfecta is ISO 9001 certified compliant and recognized as a Commercial Solutions for Classified (CSfC) trusted integrator by the NSA/CSS. Our experienced staff include former members of the U.S. military as well as global experts in voice, video, data streaming and network security.

Check us out at www.perfecta.com.

ISO 9001:2015