STEALTH™

SAIC®

Exclusive Federal Reseller

Getting to Zero Trust Network Security with Unisys Stealth®

Corresponding to Unisys Stealth® 3.0 and above

White Paper

Table of Contents

Overview

Lax security on internal networks has enabled intruders who breach the perimeter to launch full-scale cyberattacks on strategic assets in the data center. Insider attacks—intentional or otherwise—have also been rising year on year and now constitute a significant percentage of enterprise breaches. The introduction of Bring Your Own Device (BYOD) policies and the extension of data centers to public clouds have blurred enterprise boundaries, making the enterprise more vulnerable to threats. More so than ever, there is a dire need for a more effective and resilient approach that defines access only to authorized users on a need-to-know basis and secures data as it moves within and outside the enterprise.

Forrester's Zero Trust model for information security[1] takes into account the possibility of threats from internal and external sources and aims to protect the organization from these threat vectors.

This paper shares how organizations can utilize Unisys Stealth® to facilitate a Zero Trust network architecture.

'Zero Trust' Model for Network Security and Unisys Stealth

The Zero Trust model was initially proposed by Forrester as an architecture to make security ubiquitous throughout the network and not just at the perimeter. In Zero Trust, all network traffic is untrusted. So all resources must be secured, and access control must be limited and strictly enforced.

Unisys Stealth is an advanced software-defined security solution that uses encryption to enable multiple "secure communities" to share the same network without other groups being able to access – or even see – their workstations and servers. These Communities of Interest (COIs) enable logical segregation and isolation of network data and users without requiring multiple physical networks or inserting additional networking equipment such as firewalls, switches or routers. The key differentiator for Unisys Stealth is identity-based key management for encryption. Stealth™ COI keys are assigned based on user identity or device identity (in case of servers) rather than the IP address. In doing so, access rights are tied to the user, and are not dependent on the network topology.

Stealth integrates with enterprise identity management systems such as Active Directory or LDAP so that the key distribution process is transparent to the user.

Stealth uses FIPS 140-2 compliant algorithms for encryption and key exchange. This makes it suitable for protecting sensitive data-in-motion for mission-critical enterprises. Stealth-enabled devices do not even respond to pings from non-COI members, making them totally cloaked from unauthorized users.

Unlike other security solutions that operate at the application layer, Stealth operates low in the network protocol stack, making it transparent to applications. Stealth operates at the OS level and not the hypervisor level – so Stealth is suitable for securing VMs from other VMs on the same physical server.

[1] No More Chewy Centers: Introducing The Zero Trust Model Of Information Security, Forrester Research, Oct 2014

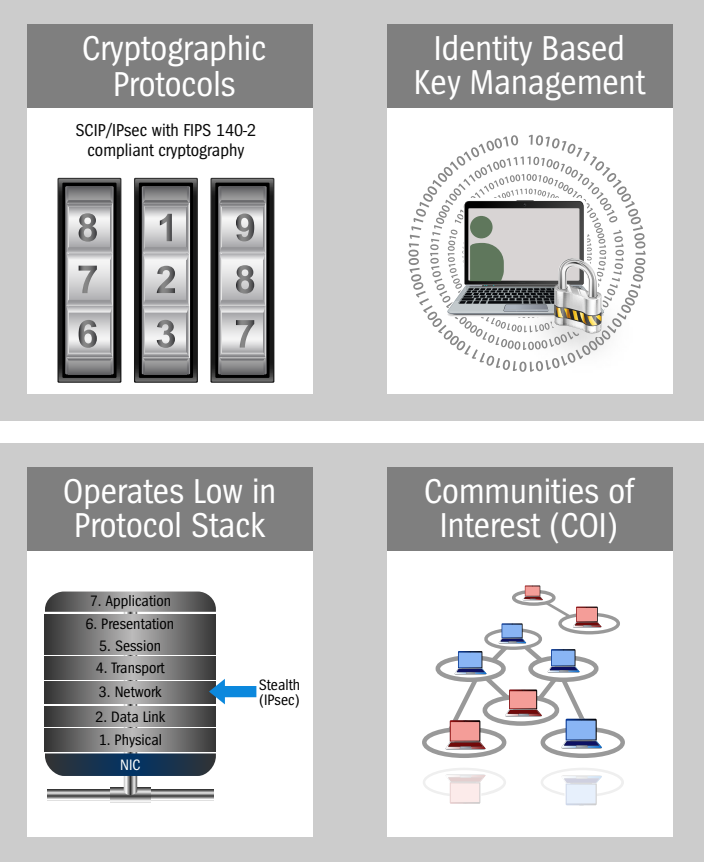

Figure 1: Unisys Stealth Solution Features and Components

Forrester has outlined a number of principles, capabilities, and required technologies in alignment with the Zero Trust security model.

Principles of Zero Trust and Stealth Alignment

Forrester has proposed the following fundamental principles for a Zero Trust network architecture:

Principle 1: Ensure that all resources are accessed securely regardless of location.

In a Zero Trust model, encrypted tunnels should be used for accessing data on both internal and external networks. Internal systems should be protected from insiders much in the same way as external systems are protected on the Internet.

How Stealth facilitates this: Stealth uses FIPS 140-2 compliant encryption to secure data on internal networks. A Stealth-secured system on the internal network can only be accessed through an encrypted tunnel from a user or device belonging to the system's COI. Stealth drops incoming network packets that are not encrypted with matching COI keys.

Unlike traditional VPNs which encrypt data only to the enterprise boundary, Stealth extends this encryption all the way to the server in the datacenter (ref: Fig 2). This is achieved by a component called the Stealth Secure Remote Access (SRA) Gateway, which authenticates incoming connections from remote users, maps them to Communities of Interest based on user identity and creates a Stealth encrypted tunnel for each incoming connection all the way to the destination server in the data center. Therefore, a Stealth-enabled system can only be accessed over an encrypted tunnel, irrespective of whether access is from within the data center or remotely from a PC or mobile device or through a wrapped mobile application.

Principle 2: Adopt a least privilege strategy and strictly enforce access control.

Zero Trust emphasizes proper implementation and enforcement of access control in order to secure restricted resources from unauthorized users.

How Stealth facilitates this: Stealth enforces access control through cryptography. Only users or other servers belonging to a server's COI can access that server. The server will not respond to pings or probes from non-COI members, and is undetectable to all unauthorized users.

COIs are easily defined and managed using the enterprise's identity management system—Active Directory or LDAP. Any access change or addition or deletion of users requires only a change in LDAP/Active Directory—a familiar tool for network administrators.

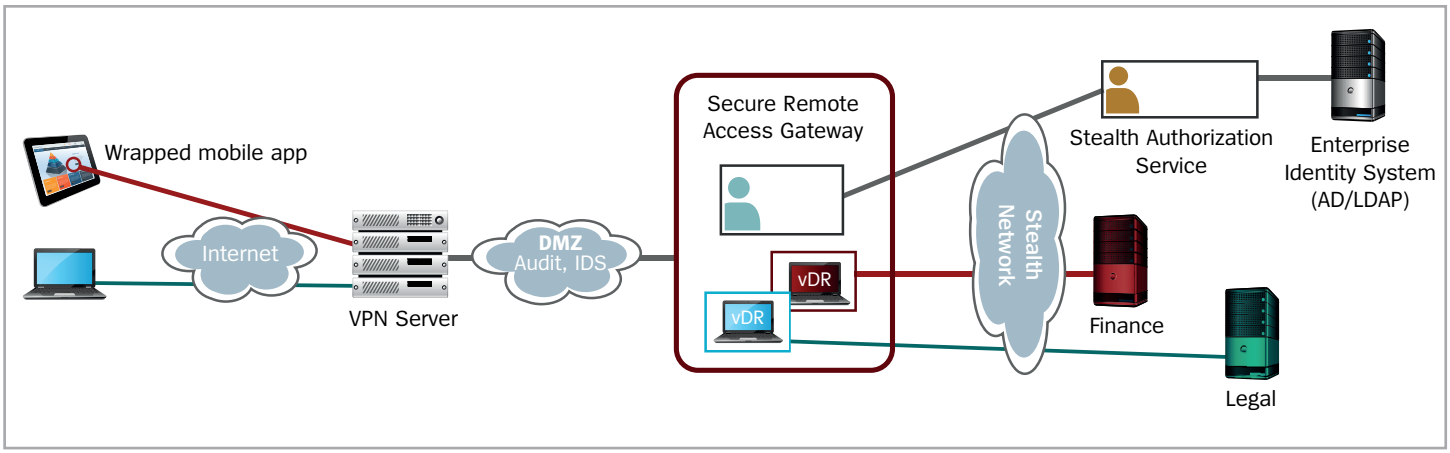

Figure 2: Secure last-mile access with Stealth, regardless of location

Principle 3: Inspect and log all traffic.

Zero Trust advocates two methods of gaining network traffic visibility: inspection and logging.

How Stealth facilitates this: Stealth does not encrypt traffic within the DMZ, to facilitate audit and analysis of incoming data by intrusion detection systems (IDS).

Within the network, Stealth traffic is encrypted and hence the packet contents cannot be inspected by third-party tools without the encryption key. This is by design and is aimed at preventing malicious users from eavesdropping on network data. Traffic can be inspected at endpoints by third-party tools that operate above the network layer.

All network events such as tunnel creation, tunnel termination, COI assignment and other events are logged by Stealth. Stealth supports integration with syslog and Security Information and Event Management (SIEM) tools.

Zero Trust Network Characteristics and Stealth Alignment

According to Forrester, a Zero Trust network should be architected with the following characteristics[2]:

Characteristic 1: Easily managed and segmented for security and compliance.

Stealth alignment: Stealth enables virtual segmentation of the network using cryptographic COIs without insertion of additional network hardware. Stealth can be deployed as an overlay on the existing network without any changes to the topology, making it easier to deploy and manage. The network segments can be easily extended by changing COI membership. COIs are defined by mapping AD/LDAP groups, so any network segment changes can be easily achieved through changes in AD/LDAP. Stealth can be used to reduce the scope for regulatory compliance such as PCI or HIPAA through virtual segmentation of the network, reducing the complexity and cost of maintaining compliance across the environment.

[2] Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Forrester Research, Nov 2012

Characteristic 2: Built with multiple parallelized switching cores.

Stealth alignment: Stealth is agnostic to the underlying network infrastructure–the Stealth agent runs on systems that need to be secured (servers or PCs) with no network changes required. Stealth supports compliance to this characteristic by working with whatever types of switching cores are in use.

Characteristic 3: Centrally managed from a single console.

Stealth alignment: Stealth deployment includes the Stealth Enterprise Manager which offers a single pane of glass interface for configuring and managing a secure network. The Stealth Enterprise Manager provides a web interface and is responsible for registering endpoint devices, authorizing the COI memberships of users, managing licensing, and supporting the Stealth logging functions. Access to the Enterprise Manager portal is restricted to users with specific administrative privileges.

Get to Zero Trust – And More – With Unisys Stealth

Deploying a Zero Trust architecture is crucial to maintain the security of your network. In addition to facilitating a Zero Trust network, Unisys Stealth delivers many additional benefits, leading to reduced complexity and lower cost of deployment and maintenance.

- Unlike other vendors that offer a hardware-based approach to segmentation, Stealth offers software-defined security. Stealth is deployed on your existing network and does not require 'rip-and-replace' of your existing network hardware. This leads to lower costs for deployment, as well as lower operating costs on power, cooling and hardware warranties.
- Stealth, being non-disruptive, can be deployed incrementally on your network, and can scale to secure your entire data center.
- Stealth deployment can also extend to public clouds such as Amazon Web Services (AWS). Unlike other cloud security products, Stealth secures data-in-motion all the way to the destination VM on the public cloud, and not just to the cloud boundary, thus ensuring multi-tenant security on the public cloud.

Unisys Stealth has been cited in Forrester Research's "Market Overview: Network Segmentation Gateways, Q4 2013" as an alternative approach to segment a network for a Zero Trust architecture[3].

In this report, Forrester states *"The Stealth product from Unisys is another offering that takes a unique approach to enforcing Zero Trust principles. Stealth conceals protected endpoints and encrypts data as it moves across Stealth-protected networks. As a data-centric offering, the product is not topologically dependent and can work on many types of networks, potentially opening up opportunities in mobility and cloud security."*

[3] Market Overview: Network Segmentation Gateways, Q4 2013, Forrester Research, Dec 2013

Learn more about how Stealth facilitates a Zero Trust network at www.SAIC.com/stealth and contact us at www.SAIC.com/stealth-contact.

SAIC is the exclusive reseller of Unisys Stealth to the federal government.

For more information visit www.unisys.com

05/20 20-0228