UNISYS

Mission-Critical Mobile Security: A Stronger, Sensible Approach

An Overview of Unisys Stealth for Mobile

By Rob Johnson

White Paper

Table of Contents

Abstract	4
Introduction	4
Unisys Stealth for Mobile Architecture	4
Architectural Components	5
Component Interfaces	6
Bring Your Own Device (BYOD) Enablement	7
Interoperability and the Future	7
Conclusion	7

Abstract

The BYOD (Bring Your Own Device) trend is fast gaining acceptance in organizations bringing with it benefits of enhanced productivity, cost-effectiveness and increased employee satisfaction. However, the risks associated with connecting employee-owned devices to corporate networks continue to remain a major cause for concern among corporate security professionals. Instances of personal mobile devices corrupted by malware and intercepted by hackers and eavesdroppers are now a regular occurrence. As enterprises consider how to confidently embrace "Bring Your Own Device" (BYOD) and safely empower mobile users to securely engage with the enterprise, it is only natural that executives are under pressure to adopt an innovative security approach that protects the entire work environment.

This paper shares a unique, innovative approach to help organizations address today's mobile security vulnerabilities and the security risks associated with BYOD. It impresses the importance of protecting mission-critical data from the data center all the way to the mobile device. Moreover, it highlights the need for a reliable mobile security solution that follows the user and one that is not limited to the device.

Introduction

The exponential growth in smartphone usage indicates that the mobile-era of the Internet has arrived and is here to stay. In today's highly connected environment, mobile devices are used, not just for staying in touch, but also to conduct banking transactions, pay bills, view credit statements, shop online, the list is endless. However, every one of these activities, whether business related, or personal, represents a real risk to our identities, bank accounts, and corporate assets.

Research shows there has been a drastic rise in the incidence of malware targeting mobile devices.

- Mobile malware samples grew by 614% from 2012 to 2013[1] according to a sample by Juniper Networks
- In early 2013, McAfee Labs researchers counted 36,699 mobile malware samples; astounding figures, considering only 792 samples were recorded in all of 2011[2]
- At the end of the second quarter in 2013, McAfee recorded over 147 million samples in their malware "zoo"[3]

While the frequency of malware attacks shows no signs of slowing down, enterprises are now facing the alarming reality of people bringing these devices inside the corporate perimeter. The trend to "Bring Your Own Device" (BYOD) is viewed as a benefit by some because it means employees are subsidizing the cost of a highly mobile and more productive workforce. Corporate security professionals, however, are struggling to enable the secure use of BYOD, because it means re-architecting their entire security infrastructure.

Despite the advancements in mobile security, organizations are wary of BYOD because typical security solutions are restricted to protecting the device, leaving doors open to numerous threats. Clearly, the current security solutions are not reliable, which means employees continue to work in an unsecure environment. Protecting sensitive corporate data from hackers and cyber criminals calls for an innovative approach - one that mitigates internal as well as external threats and creates a safe path for movement of data. Unisys takes a radical approach to mobile security by protecting mission-critical data from within and outside the perimeter of your organization.

With Unisys Stealth™ for Mobile, security begins in the data center and extends all the way out to mobile devices, protecting sensitive corporate data as it traverses along the entire path.

Unisys Stealth for Mobile Architecture

Architectural Overview

Despite the risk of malware attacks, one cannot create and deploy protocol-level security technologies like Unisys Stealth to mobile platforms. However, the Unisys unique security solution connects mobile apps and devices to the edge of a Stealth-enabled network, where they are each represented as a unique and independent Stealth endpoint. How is this done?

OS-native or third-party connectivity software is used to establish IPsec tunnels among mobile apps and devices and Stealth for Mobile software at the edge of the enterprise. If this meets the required security profile, then device-level VPN client software can be used. Within the enterprise, the mobile device appears as a Stealth endpoint. This method, which is similar to traditional remote access methods, provides a communication path for malware on the device to access the enterprise.

[1] Juniper Networks Third Annual Mobile Threats Report
[2] McAfee research – "Mobile Malware Growth Continuing in 2013"
[3] McAfee Threats Report: Second Quarter 2013

Alternatively, Stealth for Mobile can also use an application wrapping technique that helps secure specific mobile applications from hackers and eavesdroppers. This technique turns each wrapped app into an IPsec endpoint, making the specific app a Stealth endpoint within the enterprise.

Using these methods, Stealth for Mobile extends the core attributes of Stealth out to individual applications running on mobile phones and tablets. Today, Stealth for Mobile-enabled apps can:

- Go "dark" inside the enterprise network, just as Stealth-enabled workstations or servers.
- Authorize users as members of appropriate Communities of Interest (COI) based on their identities.
- Help secure traffic within the enterprise and across the Internet as it flows to and from Stealth-enabled apps.

Architectural Components

Figure 1 shows the components that make up the Stealth for Mobile solution.

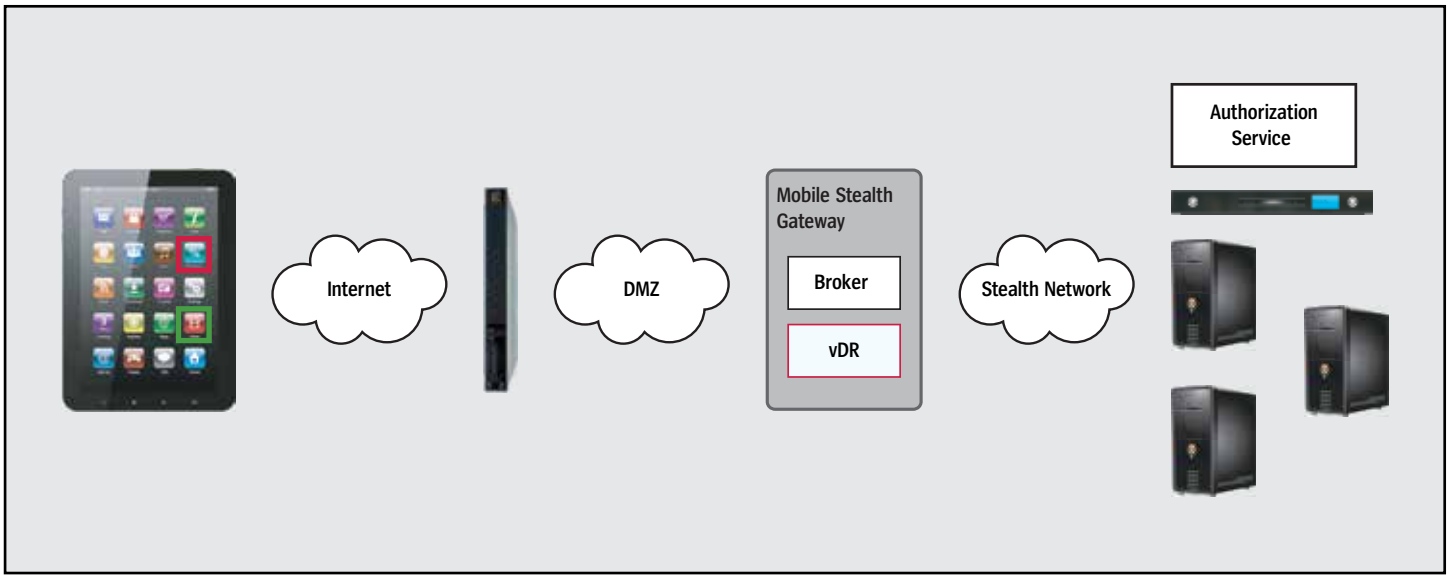

Figure 1 – Unisys Stealth for Mobile Components

Moving from left to right in the figure, the components of the architecture are:

- **Wrapped applications** – The mobile device features two apps within borders (one is red and the other green). These apps have been modified with a wrapper, which among other functions, turns them into independent IPsec endpoints. The Mocana Mobile Application Protection (MAP) technology is one such wrapper.
- **VPN Gateway** – The vertical appliance to the right of the mobile device is a standard, off-the-shelf IPsec VPN gateway.
- **DMZ** – This network can contain any network security functions that are required. For example, firewalls, intrusion detection/prevention, etc. In the simplest case, the DMZ can be a single wire (or virtual wire if running in a hypervisor). Besides functioning as a DMZ, this network allows for lawful interception of traffic, if required.
- **Mobile Stealth Software** – This is a Linux system running a Unisys-supplied OS image and the Stealth for Mobile software components. The Mobile Stealth Software is distributed as a .ISO image, which can be deployed either to a bare metal server, or as a virtual machine within a hypervisor. The subcomponents of the Mobile Stealth Software include the following:
  - *Broker* – This module is responsible for interacting with the VPN Gateway, and as an intermediary in the user authentication process between the VPN Gateway and the Stealth Authorization Service. The Broker also manages (instantiates, authorizes, monitors, and terminates) Virtual Device Relays within the Mobile Stealth Gateway.
  - *Virtual Device Relay (vDR)* – vDRs are authorized Stealth endpoints that represent the individual mobile devices or wrapped apps within the Stealth Network. They are low-overhead, fully isolated containers that hold the Stealth and IP protocol stacks. vDRs are not VMs – they do not contain an OS or any applications. They are simply protocol stacks that relay clear-text traffic to/from the VPN Gateway as Stealth traffic from/to the enterprise Stealth network.

- **Stealth Network** – This is the Stealth-enabled portion of the enterprise's intranet.
- **Authorization Service** – This is the standard Stealth Authorization Service (AuthSvc). The AuthSvc must be running at least a minimum software level (2.5.532).
- **Stealth Appliance** – This is a standard Stealth appliance that licenses the Broker.
- **Servers** – The servers depicted on the right are Stealth-enabled.

Component Interfaces

Figure 2 expands on Figure 1 by showing the interfaces between the components. The interfaces are described below.

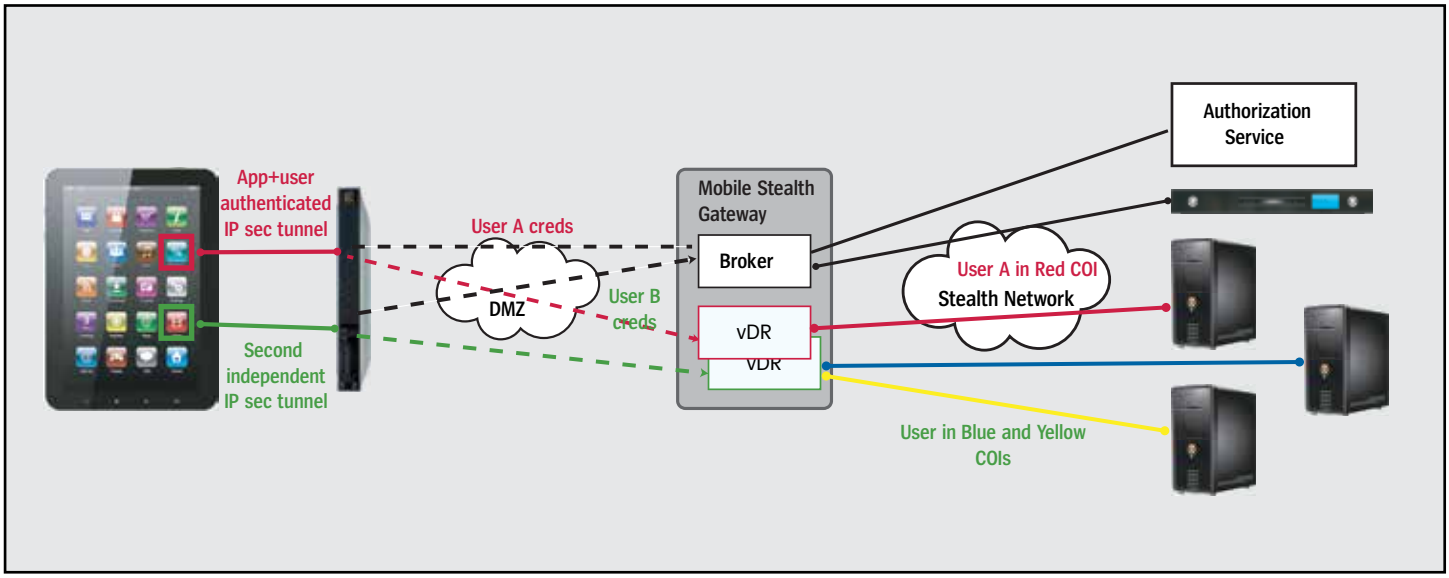

Figure 2 – Architectural Interfaces

The various lines (from left to right) represent interfaces between the components. "Ball-ended" lines represent encrypted tunnels (either IPsec or Stealth), "dashed" lines represent clear-text communications, and the solid line between the Broker and AuthSvc is dependent on the local configuration.

- **Wrapped App <-> VPN Gateway** – The lines (one red and one green) represent independent IPsec tunnels.
- **VPN Gateway <-> Broker** – Authentication requests containing user credentials and their responses are passed from the VPN Gateway to the Broker via the RADIUS protocol. Additionally, some configuration, monitoring, and control messages are passed between the Broker and VPN Gateway. Although represented as clear-text in the figure, the RADIUS and management messages, in fact, are encrypted. The Broker also controls some aspects of the VPN Gateway, e.g. clearing IPsec tunnels, via an SSH connection.
- **VPN Gateway <-> vDR** – Clear-text data traffic is routed between the termination point of an IPsec tunnel and its corresponding vDR. The VPN Gateway is configured to route all traffic to the Mobile Stealth Gateway, and the traffic is then routed internally to/from the correct vDR.
- **Broker <-> Authorization Service** – Stealth-standard authentication/authorization requests and responses are sent between the Broker and the AuthSvc.
- **Broker <-> Stealth Appliance** – Stealth-standard licensing/logging tunnel is established by the Broker, which consumes a Server license.
- **vDR <-> Server** – Being Stealth endpoints, the vDRs' communication with other Stealth endpoints on the enterprise's network is protected. In Stealth for Mobile release 1.0, only IPv4 (i.e. MLSTP) datacenter segmentation use cases are supported.

Bring Your Own Device (BYOD) Enablement

Most enterprises have separate wireless networks for guests that allow unmanaged devices access to the Internet, but restrict access to the intranet. By simply connecting to one of the guest networks, employees can access the same set of Stealth-enabled resources from their mobile devices, irrespective of where they are. Whenever a connection is established, the device is allowed to access an Internet-facing Stealth for Mobile access point. This also gives IT a single mobile access point to control, monitor, and manage, while keeping their guest networks completely firewalled off their intranet.

Interoperability and the Future

Stealth for Mobile has an open architecture and is designed to support the integration of different mobile platforms and VPN Gateway. The solution will continue to mature as Stealth for Network Security (DiM) evolves toward IPv6 and IPsec-based communications. Currently, the Stealth for Mobile 1.0 is qualified with Cisco AnyConnect VPN client and Mocana MAP-wrapped applications on iOS and Android, which are connected through a Cisco ASA 5500 series VPN Gateway. But there are many other configurations, some off-the-shelf and custom connectivity components that may be compatible with Stealth for Mobile over time.

The Stealth for Mobile documentation specifies the IPsec profile that an endpoint device or app must satisfy to connect to the Cisco ASA VPN Gateway. Any device-level VPN or app-wrapping product (e.g. iOS7 per-App VPN) that meets these specifications will be able to leverage the Stealth for mobile solution.

Conclusion

The Unisys Stealth for Mobile architecture provides an end-to-end, mobile app to server solution for integration of mobile users into Stealth-enabled enterprises. Release 1.0 enables Mocana MAP-wrapped mobile applications and Cisco AnyConnect VPN clients access to Stealth-enabled resources through commodity Cisco ASA 5500 series VPN Gateways. The Mobile Stealth Gateway preserves the key attributes of Stealth for Network Security on behalf of mobile users for both remote and BYOD use cases.

For more information visit www.unisys.com

Printed in the United States of America 01/14 14-0051