VIAVI Solutions

White Paper

Dimensioning Enterprise Cloud Platforms for Bring Your Own Devices (BYOD)

BYOD Device Emulation and Policy Analysis

Enterprise Policy Management for BYOD

Enterprises are making use of the fact that their employees are using personal computing devices which are far more advanced than that which would be allocated by their own IT departments.

A number of advantages can be associated with allowing the employee to use their own smart-phone or tablet computing device in the work place - Bring Your Own Device (BYOD). The first real advantage is the increase in productivity. The second advantage is the zero cost associated with the maintenance and technical support of the BYOD.

On the opposite side of the coin, BYOD brings with it a new set of security challenges. Enterprise's must maintain the high level of protection around sensitive corporate data, while enabling network access to the BYOD. Additional consideration must be made for the extra network loads associated with the number of guest devices attaching to the network, which will vary on a daily basis.

BYOD means scaling resources

A fundamental challenge to implementing BYOD is the need to scale existing infrastructure and security. However, with the rapid expansion in virtualization techniques and virtualization of network functions, the challenge of scale can easily be met, through the use of cloud managed platforms. Through the use of software defined networks (SDN) and network function virtualization (NFV) enterprises can with ease deliver secure network infrastructure at minimal costs.

Enterprises now have the flexibility to offload the BYOD to virtual network segments, with the ability to manage guest devices based on the device type and the applications running on the device. The agility of virtualization and NFV/SDN enables enterprises to quickly adopt and meet the demand of varying load on a daily basis.

Securing virtual network and infrastructure for BYOD

For enterprise the challenge is to maintain a high level of security whilst enabling access. A tight security policy will dictate that each BYOD is correctly identified and mapped to a resource accordingly.

Security policies are implemented based on information contained in each layer of the BYOD's stack. Policing no longer solely relies on the information associated with Layer 2 and Layer 3 but also includes information that is contained in the application - Layer 7.

Policy settings are using stateful per flow analysis of each BYOD attempting to access the network. For example by using HTTP protocol headers, information can be gathered which will enable better referencing of the device type, operating system version and software on the device.

For example the following tables below highlight the level of detail which can be collected from the HTTP protocol header. On quick inspection of the table, it's possible to clearly identify the device types. This simple procedure is used to assess the threat level associated with device. Network administrators can now effectively push the traffic originating on the device to a network segment, it deems suitable based on the policy settings.

This stateful approach to managing devices enables enterprises manage access and network privileges on a per BYOD device - type, OS version or even browser version.

Example BYOD HTTP header information	
Android	
User-Agent	Mozilla/5.0 (Linux; U; Android 2.2; en-us; ADR6300 Build/FRF91) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1\r\n
Accept	text/html, application/xhtml+xml, */*
Accept-Language	en-US
Accept-Charset	utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
Connection	keep-alive\r\n
Host	devimages.apple.com
Accept-Encoding	gzip, deflate iPad OS 5.0
iPad OS 5.0	
User-Agent	AppleCoreMedia/1.0.0.9A334 (iPad; U; CPU OS 5_0 like Mac OS X; en_us)
Accept	text/html, application/xhtml+xml, */*
Accept-Language	en-US
Accept-Charset	utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
Connection	keep-alive\r\n
Host	devimages.apple.com
Accept-Encoding	Identity
iPhone	
User-Agent	Mozilla/5.0 (iPhone; U; CPU like Mac OS X; en) AppleWebKit/420+ (KHTML, like Gecko) Version/3.0 Mobile/1C25 Safari/419.3
Accept	text/html, application/xhtml+xml, */*
Accept-Language	en-US
Accept-Charset	utf-8, iso-8859-1, utf-16, *;q=0.7\r\n
Connection	keep-alive\r\n
Host	devimages.apple.com
Accept-Encoding	gzip, deflate

Implementing a correctly dimensioned cloud platform for BYOD

BYOD device and per flow management

Once the underlining virtual infrastructure and relevant network security policies are in place, the challenge is to then dimension the virtual infrastructure functionality and the ability to scale ensuring a robust and reliable deployment of the cloud managed platform.

A part of correctly dimensioning a cloud managed platform for BYOD is to ensure that the security settings and policy updates that occur on a regular basis do not impact services. These regular updates will require regular appraisal ensuring there is no lapse in security. The need for regular or repeatable dimensioning highlights the need for an emulation and performance measurement solution.

Furthermore, the underlining principles of BYOD emphasizes the need for the ability to assess security on a per device, per application flow basis. This represents unique devices attempting network connection. As the security policies are focused on higher levels of the Internet protocol stack, there is a need for stateful application flow emulation.

TeraVM precision dimensioning of cloud platforms for BYOD

TeraVM enables validation of services running in either physical or virtual platforms and is deployable as a virtual network function on a cloud managed platform. TeraVM provides emulation of device types and applications, with the ability to analyze the performance of each of the emulated flows on an individual application flow basis with dedicated performance metrics for data, voice and video.

TeraVM's per flow architecture with real time analysis provides the granularity necessary to determine if services are reliable in a cloud managed architecture, but more importantly can be used ephemerally throughout the lifecycle of the cloud managed platform ensuring updates to the security policies and upgrades on the platform are robust and reliable.

A further benefit of using a stateful emulation tool such as TeraVM, is the ability to reliably repeat functional verification of security policies with a consistent set of BYOD use cases. A key benefit for enterprise users of TeraVM is the considerable time saved to automate repeatable dimensioning assessments on the BYOD cloud network, with minimal configurations and/or management of actual physical devices connecting to the cloud.

Furthermore, TeraVM enables performance analysis of many protocols running over secure VPNs or unsecure connections using either IPv4 and/or IPv6 address assignments.

Other advantages of using TeraVM; is the ability to grow the dimensioning network function, in a pay as you grow manner. Delivering the necessary scale of stateful application flows required to assess the elasticity or limitations of the configured virtual network architectures.

TeraVM is supported on all major Hypervisors - ESXi, Hyper-V, KVM and Xen, plus can be deployed to cloud services such as Amazon or launched in OpenStack enabling further cost savings to the enterprise.

TeraVM stateful application flows

TeraVM emulates as close to real the actual BYOD attempting connection with the enterprise's private network or public cloud infrastructure with real stateful application flows. TeraVM enables users emulate the layer 2 and layer 3 properties of the BYOD. In addition, TeraVM facilitates the option of basic authentication mechanisms, in which the TeraVM emulated BYOD may authenticate with a peer using EAP MD5 with simple username/ password authentication.

The advantage of emulation is the ability to quickly scale to thousands of BYODs, each with unique characteristics.

An example onboarding scheme for a guest BYOD could be dependent on the media access control address (MAC) i.e. if MAC address = 00:33:33:33:AA:AA and the user of the guest BYOD presents the correct authentication details e.g. username and password, then the guest BYOD may be granted access to a dedicated network segment.

For example the visitor on the enterprise network may be granted privileges to use a limited network container enabling the guest access the world wide web.

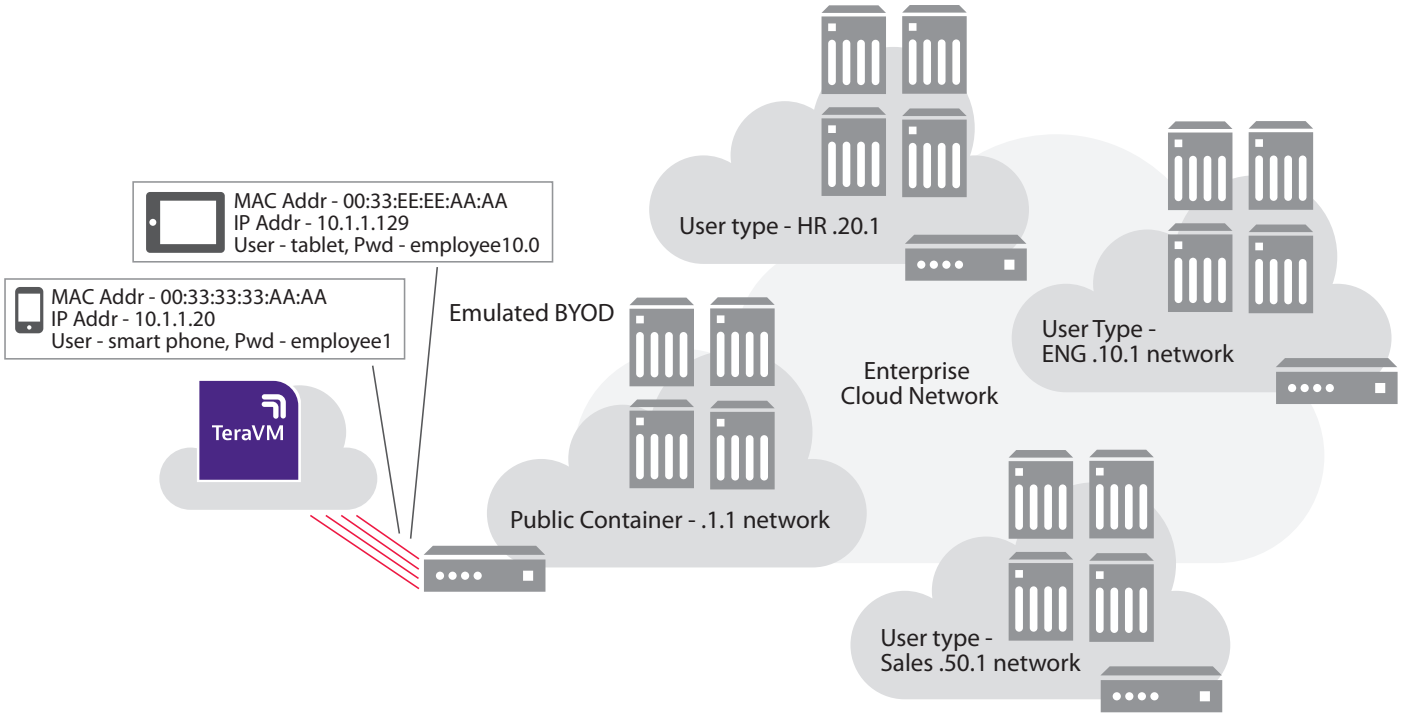

Figure 1: TeraVM emulating BYOD devices and applications

Assessing guest privilege and policies

As network administrators grow the cloud platform for BOYD access, it becomes even more important to assess the capability (and vulnerability threat) of the complete BYOD policy management implementation.

For example, in figure 1 above once the guest has access to the inside or the public container, the BYOD characteristics are again assessed e.g. log on to a virtual VPN gateway server webpage, using your employee credentials.

The VPN gateway may include HTTP transaction header assessment enabling automated policy management decisions based on the device and application details. Essentially this means a device threat level is established, dependent on the device type, OS type and browser version. In the case where the BYOD validated as authorized, the BYOD instance is allocated a dedicated IP address using DHCP. This enables the network administrator apply network segmentation.

The use of various protocols such as EAP-MD5, DHCP and HTTP further highlights the need for stateful traffic emulation, for the enterprise this means less resource wastage and more importantly time efficiency when it comes to validation of BYOD access policies.

Validating the resiliency of the security policy engine requires network administrators to consider the normal and abnormal. What if a device has a unique OS version, or indeed the access login has additional header parameters?

This is further justification to using TeraVM, TeraVM's per flow substitution functionality makes it possible to generate requests with unique details including using malformed header data (fuzzing) or even varying the legitimate data such as version numbering.

Using the sample device data in section 1.2 above, a genuine validation technique is to vary the emulated BYOD characteristics on each connection attempt to the BYOD network. This implies that the HTTP header properties per connection will be different.

TeraVM is the only solution available today that provides such unique capability. The TeraVM substitution element will iterate through a serious of defined substitutions, for example, "OS-Ver-{NUM:1.0-5.0/i}" will iterate through a number series ranging from 1 to 5. This could be representative of different browser versions running on the BYOD i.e. version/1, version/2, version/3, etc.

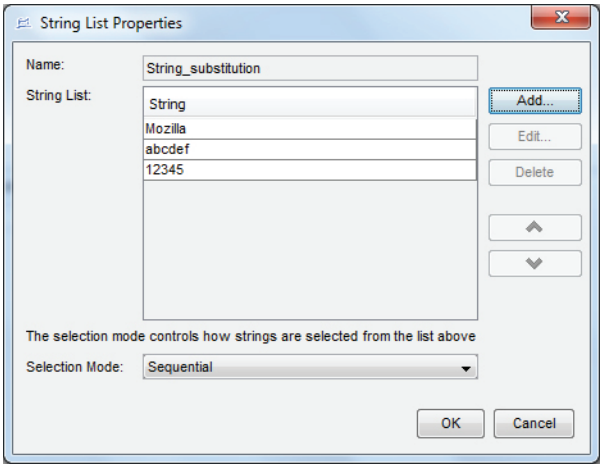

Figure 2 Sample malformed BYOD header manipulation in TeraVM

Alternatively, TeraVM's string substitution element "{STR:String_substitution}" enables the users define a list of elements which include normal/legal parameters and malformed parameters. This simple technique validates the BYOD policy manager's ability to detect when a device that was known as good and had authorized access, is now rogue and should not have access.

Once the basic security policy engine has been exercised, users of TeraVM can begin to validate robustness and resiliency of the cloud managed platform to serve thousands of devices in order to verify the clouds scalability.

Further dimensioning requirements include validating the quality of experience associated with using the BYOD to determine connectivity with real application servers or even virtual services. Basic dimensioning will include latency and throughput. However, if BYOD policies enables device quarantine further validation is required on the server application which may be launched into the virtual quarantine container, the aim should be to determine that there is minimal disruption for the BYOD end user.

An additional example of disruption could be contraction on the BYOD cloud managed security platform. Take a simple scenario - a HR manager is updating records after 6pm. As the number of guest BYODs dissipate, the cloud managed platform may be administered to contract the number of running virtual network functions or virtual machines to a base core number.

As highlighted in figure 3 below, the only noticeable impact on the hard working HR manager, should be a lower quality of experience, in that the service took longer than normal to complete. But in terms of enterprise network administration this shows that there is no service outage. Enabling further cost savings in the enterprise by reducing operational expenditure (OPEX savings).

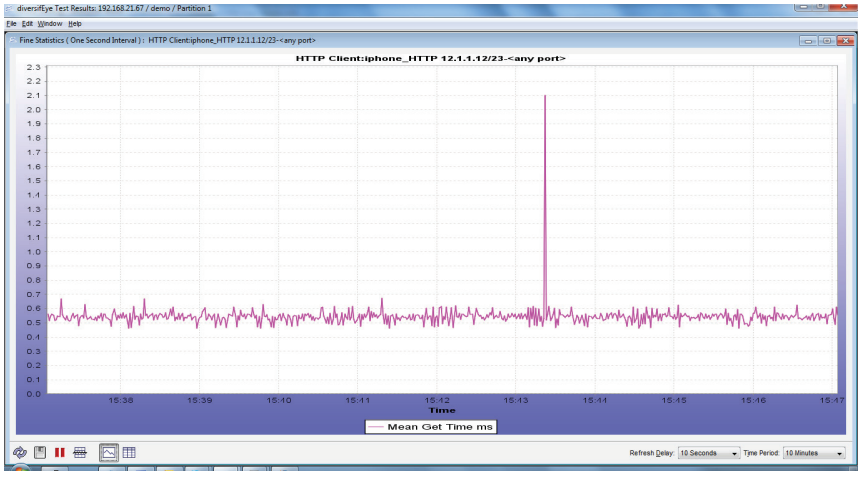

Figure 3: Service disruption on the cloud managed platform

TeraVM enabling effective and efficient BYOD deployments

TeraVM overview

TeraVM is a virtualized IP service validation solution that can emulate and assess performance on millions of unique application flows. TeraVM provides comprehensive performance analysis on each and every application flow with the ability to easily pinpoint and isolate problems flows. TeraVM is deployed on any industry standard hardware (e.g. Cisco, Dell, HP, IBM) running any major hypervisor (e.g. VMware ESXI, Hyper-V, KVM) and can be used in cloud services such as Amazon and OpenStack.

TeraVM facilitating enterprise to deliver cost effective and robust cloud managed platforms for BYOD

BYOD is the future of how enterprises will conduct business, an era in which the employee brings their own computing equipment to work. Enterprises are capitalizing on this phenomenon by allowing the employee to use the smart device in the work place.

By combining virtualization techniques, virtual network functions (VNF) and software defined networks (SDN), never before has it been easier and more cost effective to deliver scaled infrastructure to meet the growing demand for BYOD in a secure manner.

Using TeraVM, enterprise have the confidence to continually expand and update the network infrastructure required for BYOD by continually validating and dimensioning the reliability and robustness of the cloud managed platform and the security mechanisms used for BYOD management. However, more importantly enterprises continue to use TeraVM for continual assessment of security policy performance and threat resiliency throughout the lifecycle of the cloud managed platform.

An important factor of dimensioning any cloud managed platform for BYOD is the ability to emulate and measure performance on each and every device on a per application basis. Per flow delivers the necessary precision to ensure each and every individual BYOD device and flow is managed correctly.

TeraVM is the only solution available today that offers enterprises the ability to validate both security and services running as part of the cloud managed platform. TeraVM is helping enterprise to implement greater cost savings, by ensuring enterprises have the correct infrastructure and operational plans in place.

VIAVI Solutions

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

cloudplatform-byod-wp-wir-nse-ae
30187432 900 0918