Mancala Networks: making "Bring Your Own Device" initiatives (BYOD) manageable

Enterprises, public institutions and managed service providers are increasingly challenged to ensure network security and regulatory compliance in an environment where an ever increasing number and variety of user provisioned prosumer devices are accessing corporate network resources. Who is responsible for which device? What resources should be available to which class of device? For better or worse, this challenge isn't ready to subside. As a point of reference, Apple sold more than 1 million iPhone 4s on the first day of availability!

According to Gartner, 75% of enterprises have policies related to employee provisioned devices, some as simple as "they are not allowed" in an attempt to avoid the problems raised. Nearly 100% of the time, this avoidance strategy fails. The reason for this is that these policies typically remain largely limited to a couple of paragraphs in the employee handbook with no real-time enforcement mechanisms in the network itself. Enterprises are routinely surprised by the fact that, in spite of paper based policies stating the contrary, there are at least 30% more devices connected to their network at any given time than are documented and controlled in their CMDB, the delta being mostly employee provisioned smartphones. Most IT organizations configure their WLAN to implement WPA2-enterprise authentication. While this is a secure configuration, it does not take users long to discover that the same username/password combination that they enter on their corporate PC will also get their Apple iOS and Android devices authenticated to the corporate network. While incredibly useful for the employee, this creates difficulties for the IT organization, as the employee-owned devices may have security vulnerabilities that do not apply to IT-supplied PCs with locked-down configurations.

The key questions to be addressed are :

1. How to distinguish between David Jones on his corporate PC, as opposed to Mr. Jones on his personal smartphone, and

2. How to adapt network policies for devices that are not controlled or configured by IT, but owned by the employee.

Beyond having visibility of who is connected with what device, it is important to automate the provisioning and monitoring processes to avoid overwhelming the IT helpdesk.

Mancala Networks enables enterprises to boost security without sacrificing flexibility and to transition their policies from static paper to dynamic, real-time control for mobile device access control.

The Mancala Network Controller provides an integrated management and control solution providing the tools necessary to regain control over BYOD deployments:

1 Hybrid device fingerprinting and real-time inventory technology provides an accurate identification of device type; thereby allowing precise control and management of mobile devices on the enterprise network (WLAN & LAN).

2 An integrated, onboard captive portal enables the automation of device configuration and network enrollment; thereby enabling device specific authentication to be applied in parallel to user specific authentication. (David Jones using his corporate PC vs. David Jones using his tablet).

3 Building on these starting blocks, additional features of the Mancala Network Controller deliver continuous improvements in agility and security to the network manager, supporting a network driven by business needs, not vendor technology.

Key BYOD challenges for IT organizations

User provisioned devices provide a wide variety of new challenges to IT organizations.

Mean time to get online

The first challenge is getting the devices connected. In spite of the easy to use nature of most modern mobile devices, many end users are not technically savvy and require assistance getting the devices connected or with performance and application centric issues once online. The additional headaches and workload generated by employee provisioned devices cannot be ignored by IT groups.

Knowing who and what is online

While many employees may solicit the helpdesk for assistance to get online, a not insignificant number figure out that entering their standard network credentials gets them online. For the 30% or so who fall into this category, IT has no tools to know that they have connected an unauthorized device. At most, we know that “Mr. Jones” is connected. We don’t know whether Mr Jones is connected on his personal tablet, on his smartphone or on his PC. Without tools to provide visibility into who is connected where with what device, network management costs for user provisioned mobile devices can quickly become unsustainable.

Securing mobile devices that are, well, mobile

In addition, securing an employee device differs from securing an IT supplied PC. Unless specifically configured, the devices are always “live”. For example, no password is required for access and stored data is, in general, unencrypted. Credentials are cached on the device so that when the corporate WLAN is detected the device connects “automagically”. As a result, there is no guarantee that it is Mr. Jones who is using Mr. Jones’ GalaxyTab tablet and a misplaced or stolen device, configured for WLAN/LAN access can be used by an attacker to access sensitive data.

Incorporating BYOD into capacity planning

Employee owned, prosumer devices consume IT resources including bandwidth and IP addresses. Understanding the scope of employee owned device usage enables IT organizations to better plan for capacity increases and prioritizing traffic.

Context awareness and device identification

The key driver behind all of the challenges described above is the lack of context aware control - monitoring and limiting the behavior of employee owned devices. In other words, the ability to identify the type of device connecting to the network. Is it an iPhone? ...a Windows PC? ...a printer? Has the user authenticated? Is it a corporate PC or an employee smartphone? Knowing the answer to this question in real-time enables us to apply device centric, “context aware” policies.

Some enterprises have tried to work around this issue by creating separate Guest and Employee SSIDs and “requiring” that employee owned devices used the Guest VLAN that has access limited to general internet access. Guest networks are perfect for (as its name suggests) guests that require a time limited access to external internet resources. In fact, the Mancala Network Controller comes with an onboard captive portal to easily implement multiple forms of guest access - click through terms of use based access, sponsored access and time limited use. However, this means that employees using their personal devices for valid business reasons are quickly burdened by additional cumbersome configuration requirements like using a VPN to access internal corporate resources.

It is nearly always simpler and therefore better to enable personal devices to access the corporate network directly. As discussed earlier, without strict, network based context aware controls, a corporate policy “requiring” employe owned devices to access the guest network is nearly impossible to enforce.

The Mancala Network Controller solves this conundrum by facilitating standard authentication mechanisms, but also adds an additional layer of policy control based on device type. Built-in, hybrid device fingerprinting technology enables the Network Controller to recognize the unique signatures of mobile devices as they authenticate and perform initial network protocol dialogs (RADIUS, DHCP, DNS, ARP, etc.) Devices are automatically classified by type (PC, Router, PDA, Printer, IP camera, Sensor, etc.). This enables the Network Controller to immediately recognize that it is Mr. Jones using his personal tablet instead of Mr. Jones using his corporate PC and to apply appropriate policies in real-time.

This real-time inventory capability enables IT administrators to see all corporate and employee owned devices on the network at any given time, along with the type of device and its owner.

The network event driven, hybrid device fingerprinting automatically identifies and classifies iOS (iPhones, iPads), Blackberry, Android, Windows, Linux and other operating systems for smartphones and tablets.

Once a device is classified, the Mancala Network Controller provides a wide variety of policy enforcement options and access control capabilities. By configuring these various options, the network architect can limit access to sensitive corporate resources.

To illustrate using our previous example, from his corporate PC, David Jones may be able to access email, internal web resources, HR resources and financial resources. From his personal smartphone and tablet, he may be restricted from HR and financial resource access.

Device on-ramping

In order to keep BYOD initiatives from exploding IT helpdesk costs, organizations need to take a controlled approach to provisioning network access for employee owned devices. The Mancala Network Controller's flexible architecture enables multiple device enrollment and provisioning scenarios. For the purpose of this white paper, we'll focus on the most common variation.

Typically, an employee owned device connects to the LAN or WLAN. It is detected as an unknown device and automatically provided temporary quarantined network access to enable provisioning of the device. The device is redirected to a specific "employee owned device" provisioning page hosted on the Network Controller's captive portal. The employee enters his/her credentials to authenticate the user which are validated against the existing authentication infrastructure (Active Directory, LDAP). In parallel, the Network Controller has fingerprinted the device, identifying it as an unknown iOS device. As a result, it classifies it as an employee owned device.

At this point, the user is either presented with the information required to configure the device for network access. Once the device's profile has been updated, it is allowed network access.

Conclusion

Many CIOs face irresistible pressure to implement enable the usage of personal mobile devices on the corporate network. Only a year ago, analysts and consultants were recommending options for standardizing on a single platform and discussing the relative merits of iOS vs. Blackberry vs. Android. Today, nearly all of them recognize that the battle for standardization on a corporate platform is lost and that solutions must be found to make the network infrastructure more open while maintaining security and control. The Mancala Network Controller enables enterprises, institutions and managed service providers to control the explosion in both the number and type of connected devices as well as the ever increasing mobility of end users.

For more information, please consult www.mancalanetworks.com

Mancala Network Controller - Enterprise network control and management solution

Built from a patented and award winning technology, the Network Controller's innovation lies in its capability to not only monitor network control flows, but to also leverage that information to increase network security and management flexibility.

The Network Controller is installed in the local network as a natural complement to routers, switches and firewalls already in place. It interfaces with the network control services (DNS, DHCP, RADIUS, SIP). Easily integrated into existing network infrastructure and solutions, it detects connected devices and users in real-time, analyses their behavior and acts automatically to optimize network security. It brings an unequaled combination of visibility and control to enterprise network environments.

The Network Controller is available in a range of software editions adapted to the specific needs of each vertical market : Enterprises, Systems Integrators, and Managed Service Providers. Optionally, the software solution may be preloaded onto a range of physical appliances.