Public Sector

At-A-Glance

Solving for the 'Bring your own Device' demand in Government organizations

Bring Your Own Device (BYOD) is not new to government organizations. Some people have been bringing their own computer or laptop to work for years. What has changed is how many personal devices people want to bring to work, that a majority of those devices are wireless, and that people are increasingly bringing more than one personal device to work. To further complicate things, laptops, smartphones, and tablets have become an extension of our persona and get changed or upgraded more frequently than devices issued by an organization.

Public Sector organizations are facing increasing pressure to accommodate a growing number of employees, contractors, and constituents expecting to be constantly connected regardless of who owns the device. The network has become a utility that must dynamically adjust in real-time to an exponentially growing and disparate number of devices and applications that demand immediate and secure connectivity. Gone are the days of static capacity planning, as we have entered a new era of 'flash-traffic" where users with multiple devices using multiple applications can congregate anywhere and anytime for a meeting or where the latest release of a new tablet can instantly spike the new devices demanding access to and capacity from your network.

Additionally, governments have unique guest access challenges:

- Contractors requiring access to government network resources
- Cross-department access and information sharing (first responders)
- Key executives demanding access to government networks using personal devices

Public Sector IT cannot 'just say no' to BYOD. It has already begun and it can't be stopped.

The Challenges

SCALABILITY: How can you easily accommodate in real-time the explosion of new devices and applications anxious to operate on your network?

SECURITY: How can you easily secure and determine who, what, when, where, how and how many users and devices access your network?

MANAGEABILITY: How can you easily manage users, devices, and their policy no matter how they connect or where they are located on your network?

The Assumptions

DEVICES: 3+ network devices per user will be commonplace within 2 to 3 years

CONNECTIVITY: 2 out of 3 new network devices attaching to your network in the next 2 to 5 years will be wireless only

PROVISIONING: Personal devices will need to be re-provisioned more frequently (because of personal use) than organization provided devices

The Solution

A Cisco BYOD solution makes "saying yes" to BYOD easy. Simply, securely connected.

The foundation of a Cisco BYOD solution is a Unified Access Network crafted from the broadest portfolio of Routers. Switches, WLAN Controllers, WLAN Access Points, and VPN Technology available in the industry today - resulting in improved economics and unprecedented flexibility and scalability.

The security for a Cisco BYOD solution is coordinated by Cisco's Identity Services Engine (ISE) the industry's only single box offering that combines Authentication, Authorization, and Accounting (AAA) along with Profiling, Posturing, and Provisioning for wired, wireless, and vpn network elements – unifying and simplifying BYOD policy creation and management while delivering unprecedented flexibility and scalability. The ISE also provides Guest and Visitor Management capability, empowering employees to sponsor visitor access in a simplified interface with complete auditing and accountability of the guest.

Public Sector

The management for a Cisco BYOD solution is provided by Cisco's Prime Network Control System (NCS) the industry's only wired and wireless management offering that correlates user identity with policy through a "single pane of glass view" – unifying and simplifying BYOD user, device, and application monitoring, control, and troubleshooting.

- Easier deployment
- Improved performance
- Simplified policy controls
- Uncomplicated user experience streaming video from anywhere

How it works

The most prevalent use case that IT departments need to solve for is the one where an employee brings their own personal device into the company and seeks to gain network access.

- Employee brings both an agency issued laptop and a personal tablet into the office.
- The employee connects both devices to the network using a single service set identifier (SSID).
- Behind the scenes and completely unaware to the user:
  - The network uses 802.1x Extensible Authentication Protocol (EAP) authentication.
  - The Cisco ISE uses a number of device fingerprinting variables to accurately identify the device as a corporate or personal asset.
  - An appropriate policy is determined using a combination of criteria such as who the user is, what device is being used, the location and time, and so on.
  - The Cisco ISE then enforces the policy by placing each device on an appropriate VLAN while the device remains connected on the same SSID.
- The Cisco Wireless LAN Controller grants access to resources as appropriate based on policy.

Cisco's BYOD solution: Simply, securely connected. For more information, please visit our mobility for government page on Cisco.com.

Figure 1 User experience

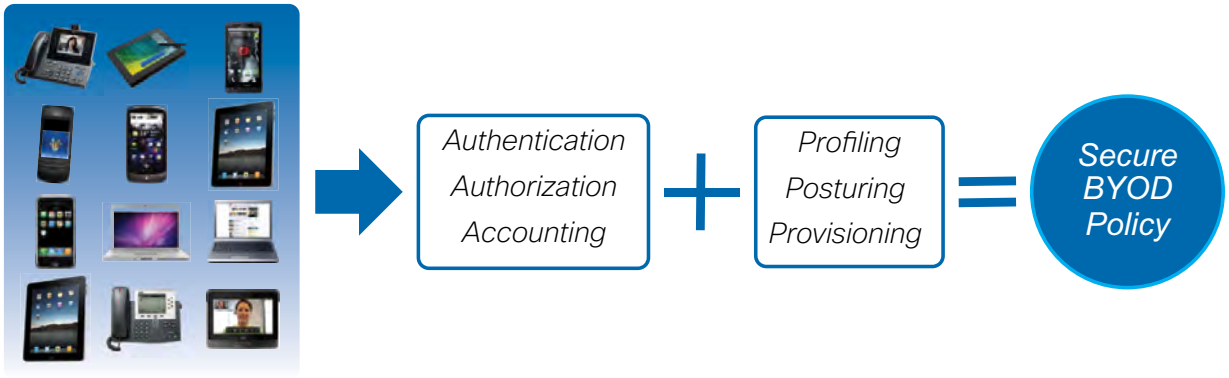

Figure 2 How it works