SOLUTION OVERVIEW

THE CLEARPASS ACCESS MANAGEMENT SYSTEM™

Remember when IT was the gatekeeper of everything enterprise and it ruled the network with a combination of strict policies, purpose-built devices, and a fully-contained technology ecosystem. Those days are long gone.

Today, billions of Wi-Fi-enabled smartphones and tablets are pouring onto enterprise networks. Users are armed with more than three devices apiece and each contains over 40 business and personal apps.

In fact users have far more latitude – freely connecting their *own* smartphones and tablets to the enterprise network and downloading the apps of *their* choice. The expectation is that the mobility experience will be the same in the office as it is at home – everything just works.

Consequently, IT is struggling to stay in control.

MOBILITY IS REDEFINING THE MISSION

The boundaries of enterprise IT's domain now extend beyond the infrastructure and demand that a reliable user experience is provided without sacrificing security and control for this new generation of users.

However, big challenges remain. How does IT maintain visibility and control how mobile devices are given access? Where devices are being used, how many per user and which operating systems supported? What happens when device profiles change or become jailbroken or lost?

IT organizations must also contend with some formidable provisioning challenges. It's not realistic to rely on already-strapped IT helpdesks to manually configure access and security settings on every mobile device across the entire organization.

Another challenge is the ability to effectively use mobile device management (MDM) technology to not only safeguard company data but enforce network access policies. MDM and policy management must work together.

Until now, IT addressed this problem with multiple, disparate systems that did not exchange data between them – network access control, mobile device management, guest management, and Auto Sign-On solutions – and manually tried to tie them all together. Every system was another touch point.

Unfortunately, stringing together a multitude of loosely integrated point-products can lead to more complexity, higher costs and compromised security controls. This approach also fails to streamline and automate time-consuming configuration and helpdesk tasks.

Now IT organizations are the ones demanding a better way to deploy and secure mobility across the environment.

ONE PLACE TO MANAGE ALL THINGS MOBILE

The ClearPass Access Management System from Aruba Networks® takes a fresh approach to solving the mobility challenge – one that gives IT a simpler way to build a foundation that supports enterprise-wide policies, strong security and an enhanced user experience.

From this single ClearPass policy and AAA platform, contextual data is leveraged across the network to ensure that users and devices are granted the right access privileges. For contextual data, we leverage user roles, device types, available MDM data, Auto Sign-On privileges, location, day of week and time-of-day.

With ClearPass, IT can centrally manage network policies, automatically configure devices and distribute security certificates, admit guest users, assess device health, and even share information with third party solutions – through a single pane of glass, on any network and without changing your current infrastructure.

Equally compelling, ClearPass automates many of the time-consuming tasks that the IT helpdesk had to manually perform.

THE CLEARPASS ADVANTAGE

Policy

- Policies and AAA services work across the enterprise in any multivendor environment.
- Network and application access privileges are automatically extended to users and devices via contextual data – user roles, device types, location and time-of-day.

Workflow automation

- Users configure their own devices with proper security and authentication settings without IT helpdesk assistance.
- Users register their own devices – such as projectors, printers and Apple TVs – by simply filling-out an online form.

Visibility

- Built-in device profiling identifies devices connected to the network and controls access based on device type and ownership.
- Real-time troubleshooting tools solve connectivity issues without having to review lengthy log databases.

The upside for IT organizations that adopt ClearPass and Aruba's integrated approach is the ability to phase-in required functionality. For starters, IT can eliminate the complexity associated with integrating dissimilar, siloed point-products by building a foundation for policy and AAA, and providing guest access, MDM integration and BYOD services.

Finally, for a crystal-clear picture of whom and what is connecting to your network, ClearPass provides the all-important visibility and reporting needed to implement controls based on users' mobility habits – when they connect and where.

FOUNDATIONAL MOBILITY SERVICES

Building a solid baseline

Mobility starts with knowing how users and their devices connect – wired, wireless or VPN – and access corporate resources. User roles and device risk-profiles are just a few criteria that must be considered when determining differentiated access policies.

The *ClearPass Policy Manager* makes network policy definition and enforcement simple by controlling every aspect of user and device connectivity from a single platform. Performing comprehensive authentication and enforcement also happens without changing the existing infrastructure.

ClearPass provides important features that make mobility easy:

- Role-based policy management for users and devices – IT-managed and BYOD.
- Enterprise-grade AAA, including RADIUS/TACACS+, 802.1X and non-802.1X services.
- A full suite of customizable captive portal options for guest access, BYOD, and the sharing of resources using Bonjour and DLNA services.
- Discovery and categorization of devices with detailed profiling information.

A wide range of network-based policies are enforced by ClearPass, including dynamic role-based access enforcement, VLAN and access control list (ACL) assignments, and bandwidth prioritization using application-aware quality of service (QoS).

ClearPass is also capable of leveraging multiple identity stores within one service, including Microsoft Active Directory, LDAP-compliant directories, ODBC-compliant SQL databases, token servers and internal databases.

The use of multiple identity stores enables IT to manage and enforce policies across multiple domains where autonomous departments exist or organizations have recently merged. Identity stores can also be utilized to authenticate users and authorize the use of resources.

The resulting platform provides the foundation to address today's evolving mobility requirements – delivered from a single, extensible platform with dynamic capabilities that grow and adapt to changing business needs.

SECURITY FOR MOBILE DEVICES

Device configuration without IT involvement

ClearPass Onboard allows users to self-configure and secure their own mobile devices. It accomplishes this by redirecting unknown devices through a simple configuration process that's easy for users of all technical ability.

Users simply enter their login credentials to get started and all security settings and a unique certificate is pushed to the device with no helpdesk assistance. The unique certificate is then used for authentication which eliminates the need to repeated type-in login credentials on small mobile device screens. In return, IT collects valuable data for policy and troubleshooting.

ClearPass also lets IT define who can onboard devices, the type of devices they can onboard, and how many devices each person can onboard. The built-in certificate authority lets IT support personal devices more quickly as an internal PKI and subsequent IT resources are not required.

Furthermore, easy-to-use search and menu-driven capabilities ensure the rapid revocation and deletion of certificates for specific mobile devices if a user leaves an organization or the mobile device is lost or stolen.

Visitor management without IT involvement

BYOD isn't just about employee devices. It's about any visitor whose device requires network access – wired or wireless. It requires an integrated solution that automates and simplifies the provisioning of network access for guests, but also provides expansive security features that keep enterprise traffic separate from guest traffic.

ClearPass Guest capabilities make it easy and efficient for employees, receptionists, event coordinators and other non-IT staff to create temporary network access accounts for hundreds of thousands of visitors. MAC caching also ensures that guests can easily connect throughout the day without repeatedly entering credentials on the guest portal.

Guests can also self-register for network access. Once registered, ClearPass delivers login credentials to users via print, SMS text or email. Visitor credentials are stored in ClearPass and accounts can be set to expire automatically after a specific number of hours or days.

ClearPass also enhances the guest experience by enabling organizations to create a branded look and feel on captive portals. You can post customized ads, news updates, discount offers, and other targeted content to create a unique experience for all guests.

With ClearPass, IT has complete visibility into each visitor's network access activities, which makes it effortless to measure and audit network usage, identify Wi-Fi coverage requirements, and meet corporate and industry compliance mandates.

When device health determines access

As a standard networking practice, AAA services can ensure that users and devices accurately authenticate and get access to the right resources. AAA services are also instrumental in logging session data to assist the IT helpdesk in resolving incidents and performing audits.

During this authorization process, some devices can be accurately identified but might be subject to additional scrutiny to ensure that they adhere to corporate anti-virus, anti-spyware and firewall policies.

ClearPass OnGuard features built-in NAC and network access protection (NAP) capabilities that perform posture-based health checks. This eliminates vulnerabilities across a wide range of computer operating systems and versions.

ClearPass also provides advanced health checks that strengthen corporate security posture:

- Specify how to handle peer-to-peer applications, services and registry keys.
- Determine whether USB storage devices or virtual machine instances are allowed.
- Decide if bridged network interfaces are permitted.

Whether using persistent or dissolvable health checks, ClearPass can centrally identify compliant endpoints on wireless, wired and VPN infrastructures.

GETTING MORE FROM THIRD-PARTY SOLUTIONS

ClearPass Exchange lets you automate workflows for everyday IT tasks. So your users have an intuitive mobile experience, without the ongoing manual reconfiguration required to make systems work together. With ClearPass Exchange, you can leverage all the mobility intelligence of ClearPass to enhance security and business workflows.

Now it's possible to interface with SEIM tools and include user, device and location visibility in security events. Or interact with helpdesk tools by automatically creating and populating a helpdesk ticket with information about the user, their device and their location in the event of an authentication failure.

ClearPass Exchange is the glue that makes everything work seamlessly and lets you customize new workflows. Using common-language representational state transfer (REST) APIs and data feeds like syslog, ClearPass Exchange shares context such as user ID, device, location, and authentication state with web-based systems. No more complex scripting languages and tedious manual configurations.

Complex integration made simple

ClearPass Exchange makes integration with existing systems a snap by incorporating RESTful programming instead of complex SOAP or XML scripts. Common-language commands enable rapid program builds that integrate ClearPass with virtually any web-based system. And you can do it yourself.

Completing the MDM puzzle

With ClearPass Exchange, networks can automatically quarantine or take other corrective actions when MDM systems report policy violations, such as jailbroken devices.

ClearPass polls MDM systems for a variety of device information:

- Device manufacturer and model.
- Encryption status.
- Blacklisted and whitelisted applications.
- Jailbroken status.

Network events can also prompt ClearPass Exchange to take action on the device by triggering actions through MDM. For example, if a user fails network authentication multiple times, ClearPass can trigger a notification message directly to the device.

Whether you're using AirWatch, Citrix, JAMF, MaaS360, MobileIron or SOTI, ClearPass has you covered.

Mobilize your IT

Add mobility to your IT workflows by pushing network intelligence to web-services such as Twilio, ServiceNow, and Nearbuy/RetailNext. The result is improved automation and less time spent on manual IT tasks. Just imagine what else your IT department can do now that the mobility infrastructure is communicating with your security and business systems.

MOBILITY MADE SIMPLE

Connect to the network and your work apps are good to go

#GenMobile uses an app for every task. So getting in and out of work apps throughout the day needs to be fast and effortless. The ClearPass Auto Sign-On capability does just that, making it infinitely easier to access work apps on mobile devices.

Instead of a single sign-on which requires everyone to login once manually to apps, the ClearPass Auto Sign-On feature uses your network login and automatically authenticates users to enterprise mobile apps so they can get right to work.

Instead of remembering and manually entering passwords for every work app, users only need their network login or a valid certificate on their devices.

If you're using identity stores like Active Directory, LDAP, and local and SQL databases to restrict who can do what on your network, then now you can extend those same role-driven policies to automatically authenticate users to their work apps. ClearPass securely mediates which users can reach which apps.

ClearPass can be used as your SSO identity provider (IdP) or it can be deployed in-line with Ping, Okta and other identity management engines for Auto Sign-On. This makes it simple and secure for users to access SAML-based app like Box, Salesforce.com and Google that are inside and outside your firewall.

Bonjour, DLNA and UPnP services for all

Projectors, TVs, printers and other media appliances that use DLNA/UPnP or Apple AirPlay and AirPrint, can be shared between users across your Aruba Wi-Fi infrastructure.

ClearPass makes these services mobile-device friendly by limiting the list of shared devices that a user sees on their tablet or smartphone based on the relevance of each user's role and location as well as the time of day.

For example, a teacher that wants to display a presentation from a tablet will only see an available display in their classroom. They will not see devices on the other side of the campus. They can also use the portal to choose who can also use the display – which keeps students from taking over the display.

Or doctors can project digital PACS images from their iPads to a larger screen anywhere within a hospital.

IT can register each device, but user-initiated device registration is a resourceful and inexpensive way for employees, or students and teachers, to share information contained on their mobile devices. And the benefits of doing so extend across a variety of industries and vertical markets.

MOBILITY SOLVED

Providing a seamless mobility experience for today's #GenMobile users has created a host of new challenges for IT. ClearPass solves these challenges by providing a platform that delivers visibility, policy control and workflow automation in one cohesive solution. By capturing and correlating real-time contextual data about the mobile environment, ClearPass enables you to define policies that are relevant for #GenMobile.

From one foundational platform, ClearPass lets IT manage network policies, deploy AAA services, configure and secure personal devices, connect guest users, assess device health – even streamline how mobile apps are accessed.

The automation of workflows eliminates a wide range of time-consuming tasks that can overwhelm IT helpdesks. Even troubleshooting tasks are simplified due to better visibility and interaction with third-party security and business workflow solutions.

ClearPass provides a cost-effective solution that can be deployed on any network and requires no changes to your current infrastructure. It is simply the best way to rollout and manage mobility as the #GenMobile workforce connects to enterprise networks.

aruba NETWORKS

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com