SOLUTION OVERVIEW

ARUBA CLEARPASS POLICY MANAGEMENT PLATFORM

Remember when IT was the gatekeeper of everything enterprise and ruled with a combination of strict policies and a fully-contained ecosystem? Those days are long gone.

Today, billions of Wi-Fi-enabled smartphones, tablets and Internet of Things (IoT) devices are pouring into the workplace. Users are armed with more than three devices apiece and each device can have over 40 business and personal apps on it.

The use of IoT devices on wired and wireless networks has also quickly challenged the model of pure IT management. Many of these devices are new technology and will require access from external administration resources.

The expectation is that everything just works and is secure – in the office, at a branch or at home. As IT struggles to maintain control, they need the right set of tools to quickly program the underlying infrastructure on-demand and control network access for any unknown IoT and mobile device, without wasting countless hours and unnecessary resources. With the increasing variety and scale of apps running on the network, they need a common policy framework to move beyond the perimeter-based security model for all things connected.

MOBILITY AND IoT ARE REDEFINING TODAYS SECURITY PERIMETER

The boundaries of IT's domain now extends beyond the four walls of an enterprise. And the goal for organizations is to provide anytime, anywhere connectivity without sacrificing security. How does IT maintain visibility and control without impacting the user experience?

Understanding what devices are being used, how many, where, and which operating systems are supported provide a foundation. Deciding what happens when users and devices connect and when they are not in compliance is the key.

Organizations must plan for existing and unforeseen challenges. It's not realistic to rely on IT and help desk staff to manually intervene whenever a user decides to work remotely or buy a new smartphone.

IT now requires a better way to deploy and secure devices and the network across an environment. Organizations need to adapt to today's evolving devices and their use – whether a smartphone or surveillance camera.

ONE PLACE TO MANAGE ALL THINGS

The Aruba ClearPass Policy Management Platform takes a fresh approach to solving the secuity challenge – one that gives IT a simple way to build a foundation for enterprise-wide policies, strong enforcement, 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 appropriate access privileges – regardless of access method or device ownership.

Policies need to include user roles, device types, available MDM data and certificate status, location, day-of-week, and time-of-day.

ClearPass is the foundation for policy management that includes a contextual database filled with valuable user and device attributes that can be shared. This enables consistent policy enforcement for an end-to-end approach that siloed AAA, NAC, and guest solutions can't deliver.

THE POWER OF CLEARPASS EXCHANGE

CLEARPASS BENEFITS

- Policies and AAA services that support any multivendor wireless, wired, and VPN environment.
- Network privileges based on real-time contextual data – user roles, device types, location, and time-of-day.
- Built-in device profiling that identifies device types and attributes for everything that connects.
- Real-time troubleshooting tools that help solve connectivity and user issues quickly.
- Built-in integration that allows you to build a coordinated defense effort where everything – third-party security solutions like MDM/EMM, firewalls and SIEM tools – works as one solution.
- The latest enhancements to ClearPass 6.6 enable custom profiles to be created to identify and secure IoT devices in real-time, with minimal hands-on IT interaction.
- ClearPass 6.6 supports integration with popular multi-factor authentication platforms such as DUO for any network or application access.

BUILDING A SOLID BASELINE

Tackling mobility starts with managing how users and their devices connect – wired, wireless or VPN – to access corporate resources. User roles, device risk-profiles, and other contextual data provide for granular policies that truly let you offer differentiated access.

ClearPass provides important features that make mobility easy:

- Role-based policy management for users and devices (IT- managed, BYOD, and IoT).
- 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 sharing of resources using Bonjour and DLNA services.
- Complete visibility features – real-time dashboards and post authentication reporting.

To deliver more than legacy AAA, ClearPass lets you leverage user and devices roles, dynamic VLAN and access control list (ACL) enforcement rules, and services that touch everything from identity stores to Aruba and multivendor network infrastructure using standards-based protocols.

The ability to utilize multiple identity stores within one service, including Microsoft Active Directory, LDAP-compliant directories, ODBC-compliant SQL databases, token servers, and internal databases sets ClearPass apart from legacy solutions.

DEVICE PROVISIONING WITHOUT IT INVOLVEMENT

Managing the onboarding of personal devices for BYOD deployments can put a strain on IT and help desk resources, and can create security concerns.

ClearPass Onboard lets users configure devices for use on secure networks all on their own. Unique device certificates even eliminate the need for users to repeatedly enter login credentials throughout the day. That convenience alone is a win. The additional security gained by using certificates is a bonus.

The IT team defines who can onboard devices, the type of devices they can onboard, and how many devices each person can onboard. A 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.

Guest access that's simple and fast

BYOD isn't just about employee devices. It's about any visitor whose device requires network access – wired or wireless. It requires a simple model 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 makes it easy and efficient for employees, receptionists, event coordinators, and other non-IT staff to create temporary network access accounts for any number of guests per day. MAC caching also ensures that guests can easily connect throughout the day without repeatedly entering credentials on the guest portal.

Self-registration takes the task away from employees and lets guests create their own credentials. Login credentials are delivered via printed badges, SMS text, or email. Credentials can be stored in ClearPass for set amounts of time and 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 branded guest portals that are sized for laptops and smaller mobile devices. Customization options exist for ads, news updates, discount offers, and other targeted content.

For regulatory requirements, guest access records make it easy to measure and audit network usage, identify Wi-Fi coverage requirements, and meet corporate and industry compliance mandates.

When device health determines access

During the authorization process, it may be necessary to perform health assessments on specific devices to ensure that they adhere to corporate anti-virus, anti-spyware, and firewall policies. Automation motivates users to perform an anti-virus scan before connecting to the enterprise network.

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 provide extra corporate security:

- Handling of peer-to-peer applications, services, and registry keys.
- Determination of whether USB storage devices or virtual machine instances are allowed.
- Managing the use of bridged network interfaces and disk encryption.

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

Getting more from third-party solutions

ClearPass Exchange lets you automate mobile security using popular third-party security solutions like firewalls, MDM/EMM, and SIEM tools. Leveraging the context intelligence that ClearPass contains allows organizations to ensure that security and visibility is provided at a device, network access, and traffic inspection and threat protection level.

Using a common-language representational state transfer (REST) API and data feeds like syslog, ClearPass Exchange shares context such as user ID, device, location, and authentication state to make smarter decisions – no more complex scripting languages and tedious manual configurations.

ClearPass 6.6 now supports integration with popular multi-factor authentication (MFA) platforms such as DUO for any network or application access. ClearPass offers a MFA challenge to mobile devices as they are onboarded to the existing network infrastructure for the first time and/or as they return for new connections. This MFA challenge can be presented to the end user based on different criteria in order to better satisfy corporate policy requirements: from certain locations, only for select mobile device types, or a select group of users.

With ClearPass Exchange, networks can automatically take corrective actions:

- MDM/EMM data like jailbreak status of a device can determine if it can connect to a network.
- Firewalls can accurately enforce policies based on user, group, and specific device attributes.
- SIEM tools can be setup to capture all authentication data for single dashboard visibility.

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

Access work apps securely from anywhere

Logging in to work apps throughout the day needs to be fast and effortless. The ClearPass Auto Sign-On capability does just that. Instead of a single sign-on, which requires everyone to login once manually to apps, ClearPass Auto Sign-On uses a valid network login to automatically provide users with access to enterprise mobile apps.

Instead of remembering and manually entering passwords for every work app, users only need their network login or a valid certificate on their devices. ClearPass can also be used as your identity provider (IdP) or service provider (SP) where Single Sign-On is utilized.

Bonjour, DLNA and UPnP services

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 finding these devices and sharing between them simple.

For example, a teacher who 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 else can use the display – this keeps students from taking over the display.

Another example is within the healthcare sector – doctors can easily project digital PACS images from their iPads to a larger screen anywhere within a hospital. Patient collaboration just got simpler.

A FOUNDATION FOR SECURITY

Providing a seamless experience for today's #GenMobile and the fast adoption of IoT technologies within the enterprise have created a host of new IT challenges. It takes planning, the right tools, and a strong foundation to secure anytime, anywhere access for mobile and IoT devices.

ClearPass solves these challenges by providing a platform that delivers policy control, workflow automation, and visibility from a single cohesive solution. By capturing and correlating real-time contextual data, ClearPass enables you to define policies that work in any environment – wireless, wired, or VPN.

The latest Aruba ClearPass enhancements also handle emerging network security challenges surrounding adoption of IoT, stronger mobile device and app authentication, and deeper visibility to security incidents. Automated threat protection and intelligent service features ensure that each device is accurately given network access privileges with minimal hands-on IT interaction.

aruba
a Hewlett Packard Enterprise company

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