aruba
a Hewlett Packard Enterprise company

EXECUTIVE OVERVIEW

MOBILITY AND THE NEW FACE OF SECURITY THREATS

Back when enterprise security meant blocking off the perimeter of your network to ward off external threats, things were relatively simple for IT. As long as the perimeter was secure, the bad stuff stayed out. An entire industry formed to secure the network based on ports and protocols. Over time, next-generation services evolved to inspect actual packets going into and out of the network, and the industry went from a static to a dynamic approach. For the most part, perimeter security was made better, but the idea was still to focus on threats from the outside.

Things started to change with the explosion of mobile devices — as users went mobile, they started bringing potential threats inside the network. Estimates vary, but one can safely say that the vast majority (>90%) of enterprise security breaches are now based on attacks initiated via unsecured user devices, loss of sensitive data on these devices, and risky end user behavior.

This is drastically altering the security landscape and has changed the way C-level executives think of the perimeter, as these threats can create negative publicity that possibly costs them their jobs. To protect the enterprise network and its resources, organizations must adapt to the way GenMobile works — starting from inside the perimeter. By leveraging known, contextual data that can be trusted — a person's role inside an organization, the devices and apps they use, and their location — policies can be created to fortify the network. We call this approach Adaptive Trust Defense and it essentially turns legacy perimeter security inside out.

EMBRACING SECURE WI-FI

As companies adopt a mobile-first strategy that relies on Wi-Fi replacing the wired network, Wi-Fi vendors primarily differentiate on capacity and throughput. While bandwidth is important, the new mobile threat vector is increasingly concerning. IT must consider stronger security features and integration with best of breed security solutions like policy management, MDM, and firewalls when choosing a Wi-Fi vendor.

The reality is, the goal for a security-centric IT staff is now to evaluate wireless infrastructure solutions from a comprehensive security perspective. Some key security attributes that IT must now consider for securing the perimeter-less network:

- Role-based enforcement capabilities
- Integrated support of external policy management/RADIUS services
- Website and app blocking
- Stateful firewall traffic inspection
- Blacklisting of unauthorized devices
- Protection against man-in-the-middle attacks
- Client fingerprinting for device context and visibility
- User and device role-based enforcement
- Secure Guest — keeping corporate devices off the guest network

Role-based enforcement allows IT to assign different access privileges without creating additional SSIDs or VLANS. And IT can easily create policies that block users from accessing sensitive content, based on their role, device, or location. For example, contractors can be given access to proprietary documents while in the office, but blocked when they are remote.

Device visibility enables IT to allow or contain specific devices or known vulnerable OS versions from accessing the network. Using device attributes also allows IT to permit access from a laptop, but possibly limit access from a smartphone from remote locations. Wi-Fi equipment must now contain collaborative workflows with external security tools for IT to benefit from these capabilities.

THE NEXT GENERATION OF NAC

Network Access Control (NAC) used to just mean simple endpoint health checks to determine security posture, force updates, or remediate as necessary. As today's mobile workforce has changed security requirements, NAC has evolved to offer simplified onboarding, user profiling, managed guest access, and policy management to resolve security gaps without overwhelming IT resources.

Evolving endpoint security requires an Adaptive Trust Defense, which includes policy management and integration with third party security solutions that exist in the network or are being explored, like MDM/EMM, next-generation firewalls, and identity management solutions. It's no longer feasible to deploy point products that work independently of each other.

COLLABORATIVE POLICY MANAGEMENT

Aruba ClearPass sits in the middle of your security components to take in and distribute valuable context with existing multi-vendor security solutions. The combined solution delivers a comprehensive set of end-to-end visibility and protections that strengthen existing security architectures. ClearPass handles all authentications and authorization transactions using role-based user and device context that is not available within traditional perimeter security tools.

Now user identities can include roles, location, device types, and access methods, to allow for differentiated privileges based on accurate and granular login data. Executives are easily differentiated from staff, IT-managed devices from BYOD, and more importantly, this contextual data can be shared with firewalls, IPS/IDS, and MDM/EMM solutions. In most cases, these other security solutions can also share data with ClearPass.

For example, MDM solutions can share jailbreak status or data about devices that contain blacklisted apps with ClearPass, to ensure only devices that meet security standards are permitted to connect to a Wi-Fi network.

ENFORCEMENT THAT GOES BEYOND WIRELESS

For comprehensive security, role-based awareness goes beyond just the wireless network. The same principles like profiling and role-based enforcement are applied to the entire network, regardless of device ownership or type. A laptop or a printer are easily differentiated and given proper network access regardless of where a port is located.

The Adaptive Trust approach distributes the granular contextual user information to the entire wired and wireless network in real-time, enhancing the traditional model of static port configuration based on ports or VLANS on the wired network.

The contextual data collected by ClearPass ensures that user data on a wired or wireless network will be usable for IT to enforce real-time policy changes as needed. This is more adaptive than static user profile data typically fed to the firewall from traditional identity stores. Guest and visitor information is typically not even in these directories, leaving a vulnerability that only a policy engine can fix.

CONNECTING IT AND YOUR USER COMMUNITY

IT resources and labor can be saved using managed end-user self-provisioning and predefined policies — end users self-onboard via a simple web-based workflow and ClearPass does the rest, including pushing certificates onto the device. In addition, secure guest access and employee onboarding becomes a seamless and secure approach by leveraging ClearPass services.

The ClearPass policy engine can allow for benefits outside of the realm of the security team as well. By defining roles based on the user and type of application being performed, QoS policies can be created and automatically pushed to Wi-Fi and wired infrastructure. For example, Wi-Fi infrastructure services can enforce that social media apps are accessible by marketing groups and not for sales, where SFDC access would be a priority.

IT or network security managers also need the ability to enforce end users' rogue devices to maintain required security posture and business goals, like in highly regulated environments such as healthcare, where encrypted storage, and segmented traffic are a must. Another example is in the education vertical — districts may require user-based enforcement, where teachers can access different material than students, or where certain applications are bandwidth constrained.

ClearPass benefits both end users and IT managers by enabling end users to feed context into the policy engine seamlessly when onboarding or authenticating, and IT managers can rest assured knowing the appropriate attributes allow for granular enforcement across all existing network security solutions.

SUMMARY

Today's highly mobile workforce requires an Adaptive Trust Defense that brings together all relevant security components for securing a mobile environment. Wireless and wired infrastructures, while fast and dedicated to moving traffic, require context and internal and external security resources to work together to ensure that users can work as needed, securely, regardless of location or device.

By seamlessly tying together granular contextual information from devices, to policy engine, to traffic protection, enterprises can be assured that their networks are designed with the next generation of network vulnerabilities in mind.

Learn more about ClearPass and Adaptive Trust Defense visit www.arubanetworks.com

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