PALO ALTO NETWORKS

Greater Visibility and Control of User Traffic on the Network

Ruckus™ Simply Better Wireless.

SOLUTION BRIEF

HIGHTLIGHTS

RUCKUS CLOUDPATH AND PALO ALTO NETWORKS

- Integrate critical user identity information
- Certificate access to the network
- Incorporate employee BYOD access
- Detect and prevent cyber threats at every endpoint across the organization
- Enforce granular policies
- API or RADIUS accounting based

THE CHALLENGE

Today's IT organizations are seeing a myriad of wired and wireless threats upon their networks. With more users bringing their own devises with potential for vulnerable authentication methods and rampant identity compromise, IT security analyst have seen a rise in cyber threats. Today's environment of point solutions has resulted in limited security visibility, lack of correlation of alarms and threats and slow manual responses. IT organizations are looking to identify and detect threats from sources ranging from mobile devices, incidents at the internet edge, between devices data center

THE SOLUTION

Ruckus Wireless and Palo Alto Networks have partnered to provide a security and policy management platform that enables the IT organization to protect their Wi-Fi network by easily and definitively securing users wired and wireless devices seamless without using unsecure passwords. Enterprise IT departments can now securely onboard employee owned mobile devices and experience cost benefits resulting from employee Bring Your Own Device (BYOD) trends—while maintaining security.

With the integrated solution of Ruckus Cloudpath and Palo Alto Networks, joint customers can benefit for greater visibility and control of user traffic on the network. With easy to use certificate based encrypted connection, coupled with granular traffic policing, customers benefit from greater visibility and control on the user traffic. With this integration, Ruckus Cloudpath which assumes the role of AAA + PKI in addition to other elements in the network can provide user identity information like username, IP address, mac address etc. to Palo Alto Networks Next Generation Firewall (NGFW) which enables Palo Alto Networks to identify each session and tag it to a particular user thereby enabling more granular control of the traffic"

Organizations can now integrate their business policies in the form of easy-to-understand network security rules. Ruckus Cloudpath Enrollment System (ES) and Palo Alto Networks NGFW share user and device information to monitor and enforce application usage policies on smartphones, tablets, laptops and other corporate computing resources.

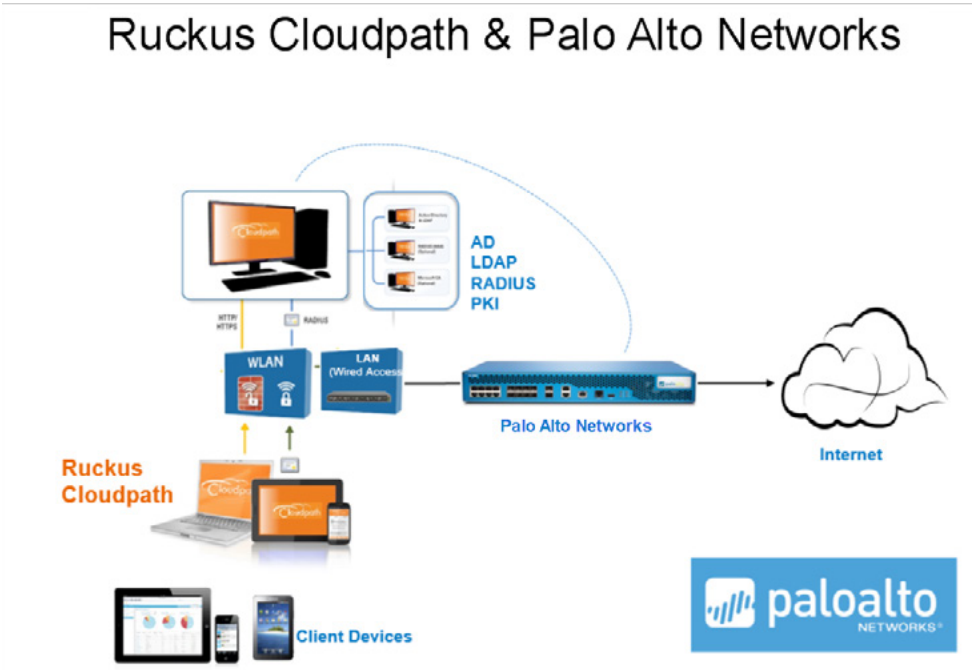
Ruckus Cloudpath software integrates with Palo Alto Networks NGFW to enable the appropriate level of role based security when accessing Wi-Fi networks. Ruckus Cloudpath checks the network authorization status of all network access requests, whether BYOD or IT issued. For devices that are new to the network, Ruckus Cloudpath on-boards all approved devices. Returning devices, which have been previously on-boarded and have not had their credentials removed or revoked, will be connected seamlessly and securely.

Palo Alto Networks platform enables visibility and control within the organization's network. Palo Alto Networks next-generation firewall classifies all traffic, including encrypted traffic, based on application, application function, user and content. Business IT organization can create comprehensive, precise security policies, resulting in safe enablement of applications. This lets only authorized users run sanctioned applications, greatly reducing the surface area of cyber-attacks across the organization.

PALO ALTO NETWORKS

Greater Visibility and Control of User Traffic on the Network

SOLUTION BRIEF



RUCKUS CLOUDPATH SECURITY AND MANAGEMENT PLATFORM

Ruckus Cloudpath Enrollment System (ES) software is a security and policy management platform that enables any IT organization to protect the network by easily and definitively securing users and their wired and wireless devices—while freeing those users and IT itself from the tyranny of passwords. Available cloud-managed or as a virtual instance and priced per user, Cloudpath software lets IT do with one system what usually requires many, while easily and automatically integrating with existing access and network security infrastructure. Ruckus Cloudpath software consolidates and simplifies the deployment of multiple services that are typically disparate and complex to manage: Certificate Management, Policy Management and Device Enablement.

PALO ALTO NETWORKS NEXT GENERATION SECURITY PLATFORM

Palo Alto Networks® Next-Generation Security Platform, comprised of our Next-Generation Firewall, Threat Intelligence Cloud, and Advanced Endpoint Protection, uses an innovative traffic classification engine that provides full context by identifying all traffic by application, user and content. Palo Alto Networks URL Filtering provides protections, synchronized across the attack lifecycle, with the latest threat intelligence on phishing, malware, and undesired content through our cloud-based URL categorization. By combining network, cloud and endpoint security with advanced threat intelligence in a natively integrated security platform, Palo Alto Networks safely enables all applications and delivers highly automated, preventive protection against cyber threats at all stages in the attack lifecycle, without compromising performance.
Find out more at www.paloaltonetworks.com.

Ruckus
Simply Better Wireless.

ruckuswireless.com
Ruckus Wireless, Inc. | 350 West Java Drive | Sunnyvale, CA 94089 USA | T: (650) 265-4200 | F: (408) 738-2065