PALO ALTO NETWORKS®

Granular firewall policy definition and enforcement

SOLUTION BRIEF

HIGHLIGHTS

RUCKUS CLOUDPATH™ ENROLLMENT SYSTEM AND PALO ALTO NETWORKS

- Deliver secure network access for BYOD, guest users and IT-owned devices
- Protect your IT environment with comprehensive firewall features
- Enable per-user and per-device firewall policy enforcement

THE CHALLENGE

IT security threats have evolved and so have security safeguards. Traditional stateful firewalls blocked or allowed traffic based on the logical port. Next-generation firewalls include security features that extend well beyond the traditional firewall, including URL filtering, signature-based threat detection, virtual private networks (VPNs), application control and more. IT teams use these features to help boost both productivity and IT security. The term firewall has come to mean this superset of features—a firewall is understood to have these next-gen capabilities.

But even with their tremendous power, next-generation firewalls need a mechanism to identify users and devices for maximum effectiveness in policy definition and enforcement. Without the right technology integration, IT teams fail to realize the full potential of their firewall deployments.

THE SOLUTION

Ruckus Networks and Palo Alto Networks partner to raise the bar on network and data security. IT teams can use Cloudpath Enrollment System to deliver secure network access for BYOD, guest users and IT-owned devices—including IP-enabled IoT devices. Cloudpath software/SaaS features special technology integrations with Palo Alto Networks Next-Generation Firewalls thanks to the two companies' partnership. Customers that use both products gain the ability to identify users and devices on the network and to associate network traffic with those users and devices. They can define and enforce firewall policies with per-user and per-device granularity.

Working alone, the firewall can block or allow specific ports and applications, or even specific features within an application. But it applies these policies across all users and devices in this scenario. With Cloudpath software, firewall policies become much more precise because the firewall becomes aware of who and what devices are generating the traffic.

The firewall can restrict access to ports for IoT devices, blocking those that correlate highly with malware command and control callbacks. It can block ports on a per-employee basis depending on the assessed risk associated with each port. IT can trace network traffic back to users and devices to put a stop to attacks in progress that are characterized by anomalous traffic patterns. They can then use Cloudpath software to revoke access for that user or device.

Using the two products together allows differential enforcement of URL filtering policies for users and groups of users. For example, IT teams can use the firewall to block social media sites for call center workers but allow access for marketing department employees, who require this access to do their jobs. The firewall can control access to applications in a more granular way, too. For example, it can allow access to the Facebook news feed for all users while blocking access to messenger and games for some users.

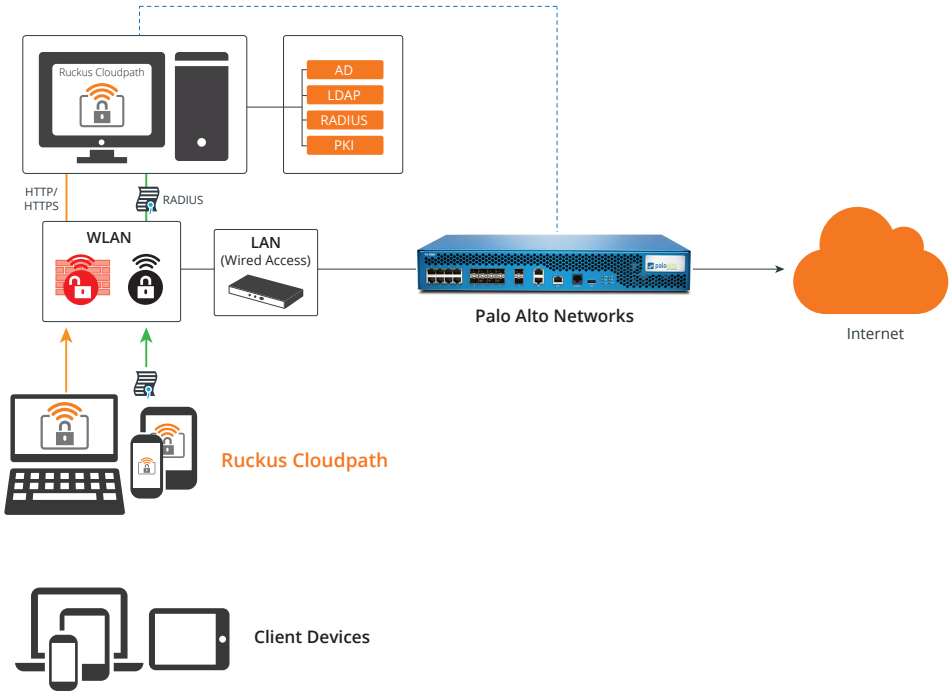
Cloudpath checks the network authorization status of all devices seeking network access. For devices that are new to the network, Cloudpath software lets users onboard approved devices with easy self-service workflows—without IT intervention. The system lets returning devices connect seamlessly and securely in a process that is transparent to the user.

PALO ALTO NETWORKS

Granular firewall policy definition and enforcement

SOLUTION BRIEF

Ruckus Cloudpath Enrollment System and Palo Alto Networks



The Palo Alto Networks next-generation firewall classifies all traffic, including encrypted traffic, based on application, application function, user and content. IT teams can create comprehensive, precise security policies to safely enable applications. Authorized users can run only approved applications, reducing the attack surface for cyber threats.

RUCKUS CLOUDPATH ENROLLMENT SYSTEM

Ruckus Cloudpath Enrollment System is software/SaaS that delivers secure network access to support any user, and any device, on any network. It streamlines network onboarding for BYOD, guest users and IT-owned devices—including IoT devices. The software increases security with powerful encryption for wireless data in transit, access policy management and up-front device posture assessment with remediation. Intuitive self-service workflows deliver a great end-user experience while dramatically reducing helpdesk tickets related to network access. Unlike leading competitors, Cloudpath software offers a choice of cloud-based or virtualized on-premises deployment, built-in multi-tenancy, lower total cost of ownership and superior ease of use.

Find out more at https://www.ruckusnetworks.com/secureaccess.

PALO ALTO NETWORKS NEXT-GENERATION SECURITY PLATFORM

Palo Alto Networks® Next-Generation Security Platform, comprised of 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 its 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.

www.ruckusnetworks.com | 350 West Java Dr., Sunnyvale, CA 94089 USA

RUCKUS™ an ARRIS company