Combine firewall defense with secure user enrollment

Palo Alto Networks and CommScope RUCKUS® make onboarding easier and firewall control more precise

Highlights of Palo Alto Networks and CommScope RUCKUS integration

- Enroll users and their associated BYOD or IT-owned devices; enroll IoT devices
- Define and enforce firewall polices with per-user, per-device granularity
- Improve the user experience and reduce the burden on IT with easy self-service onboarding
- Trace network traffic back to users and devices to stop attacks based on anomalous patterns
- Easily customize onboarding workflows

Palo Alto Networks is redefining what it means to be secure, including the assurance that work can be done securely anywhere. And these days, "anywhere" covers a lot of territory.

Which is why Palo Alto Networks and CommScope are working together to provide a complete solution that combines firewall policy enforcement with user and device enrollment software.

Working alone, Palo Alto Networks next-generation firewalls can block or allow specific ports and applications, or even specific features within an application. But the firewall applies these policies across all users and devices.

Now IT can use CommScope RUCKUS® Cloudpath® Enrollment Software for secure enrollment of any user and device, including BYOD and IT-owned devices. Not only does Cloudpath identify all of the devices associated with a user, it also associates network traffic with individual users and devices. Because of the integration of RUCKUS Cloudpath and Palo Alto Networks firewalls, IT can define and enforce firewall policies with per-user and per-device granularity. This will enable IT organizations to realize the full potential of their firewall deployments.

PEOPLE AND THINGS SIMPLY EXPECT TO CONNECT

Who—or what—is trying to access networks and resources?

Remote users with mobile devices (IT-owned and BYOD)

Since the pandemic began, more users—particularly home-based users—have been accessing networks from remote locations. Users are also using their own mobile devices, not just IT-owned devices. The sheer volume and diversity of devices requesting network access is creating a complex matrix of security scenarios.

Visitors and guests

Organizations must also accommodate guest access. Guest access scenarios can range from setting up captive portals to authorizing one-time requests.

COMMSCOPE® RUCKUS® paloalto NETWORKS

SOLUTION BRIEF

IT-owned devices

IoT has added yet another dimension to secure access and policy enforcement. IT-owned devices used to mean computers and peripheral equipment like printers. Now IT has to onboard IoT devices, like video surveillance cameras, and extend policies and enforcement to these devices and the traffic they generate.

COMPREHENSIVE AND GRANULAR THREAT PREVENTION

Palo Alto Networks is the leader in global cybersecurity. The company's next-generation firewalls give IT departments more comprehensive and granular control than traditional stateful firewalls. These firewalls provide capabilities like URL filtering, signature-based threat detection, virtual private networks (VPNs), application control and more.

There are several ways the integration of Palo Alto Networks firewalls with RUCKUS Cloudpath can enable IT teams to create security policies that are even more precise and comprehensive.

Tightly control access to applications

With the visibility provided by Cloudpath, IT can assess risk down to the user and device level, and then block individual ports accordingly. For example, IT can allow access to the Facebook news feed for all users but block access to games for some users.

Refine URL filtering policies

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 centers, and allow access for marketing department employees who require this access to do their jobs.

Stop attacks

With the ability to trace network traffic back to users and devices—and see anomalous patterns—IT can stop attacks in progress. For example, the firewall can restrict access to ports for IoT devices, blocking devices that have a high correlation to malware command-and-control callbacks.

Revoke access privileges

IT can use Cloudpath to revoke access for a specific user or device without changing or disrupting security access for other users and devices or making any adjustments to the firewall.

SELF-SERVICE EMPOWERS USERS AND UNBURDENS IT STAFF

Today, strong security must be balanced with a positive user experience and minimal IT involvement. In particular, help desks are usually bombarded with requests from users trying to get through complicated or unsuccessful login procedures. Cloudpath is designed to empower users to onboard themselves with a few simple steps. The result is happier users and a substantial drop in help desk tickets.

Internal users

Cloudpath installs a digital certificate for network authentication. After the initial connection, users don't need to re-enter credentials when they connect again. Users can easily self-provision any device for network access using their existing login credentials.

Guests and visitors

In a few steps, IT can create a portal for guests and visitors to self-register and receive login information via SMS, email or printed voucher. Cloudpath makes it equally easy to customize workflows for individuals and groups of guests, such as setting up a self-service workflow or one that requires permissions from internal sponsors.

Another level of customization is the ability to incorporate social login with Google, Facebook, LinkedIn and other popular identity providers.

BYOD and IT-owned devices

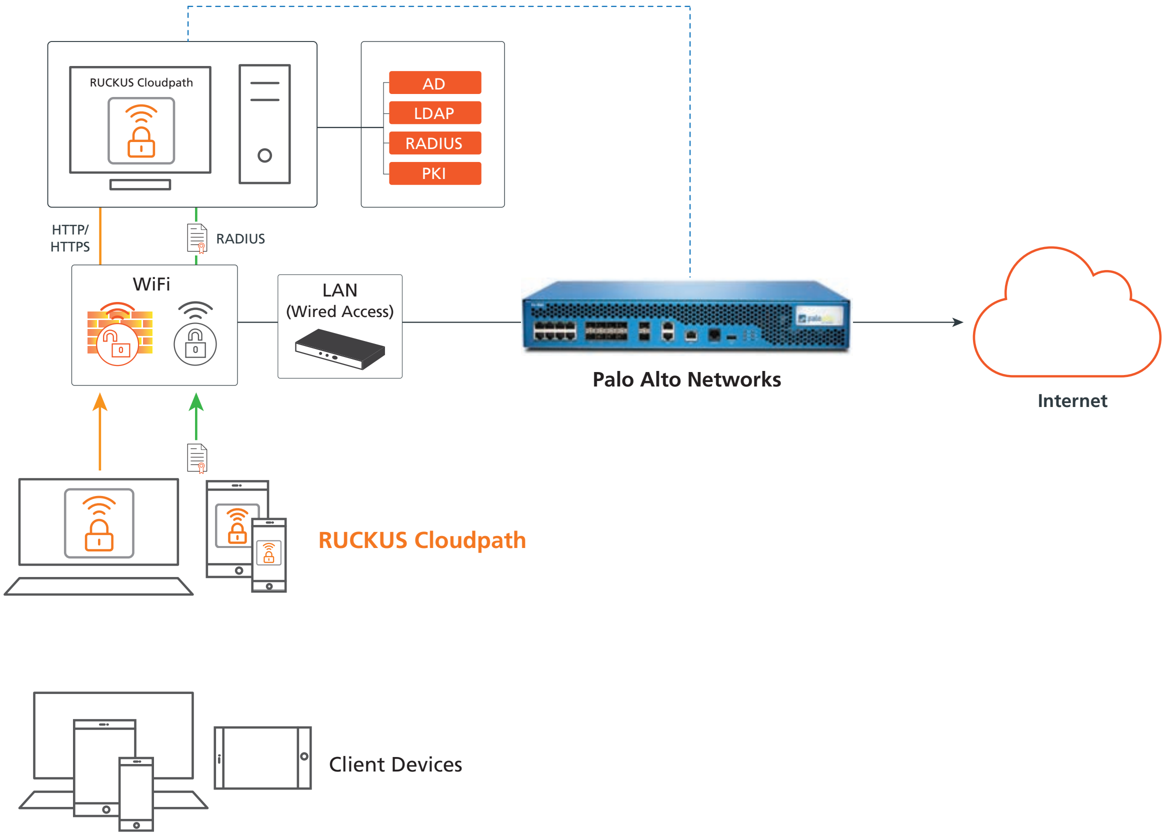
Cloudpath checks the network authorization status of all devices attempting to connect to the network. For devices that are new to the network, Cloudpath lets users onboard approved devices with self-service workflows. Workflows can automatically require users to install specific software during onboarding. A device posture check with remediation ensures that only devices with appropriate security safeguards can access the network. Cloudpath lets returning devices connect seamlessly and securely in a process that is transparent to the user.

COMMSCOPE RUCKUS CLOUDPATH

RUCKUS Cloudpath Enrollment System supports any user, any device, and any network infrastructure. Cloudpath can be deployed as a cloud-based (SaaS) solution or a virtualized on-premises deployment. Network connections are secured with WPA-2 Enterprise via 802.1X authentication.

ABOUT PALO ALTO NETWORKS

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.



RUCKUS Cloudpath Enrollment System delivers secure network access for any device and user on any network.

commscope.com

Visit our website or contact your local CommScope representative for more information.

Unless otherwise noted, all trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of CommScope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to CommScope products or services. CommScope is committed to the highest standards of business integrity and environmental sustainability, with a number of CommScope's facilities across the globe certified in accordance with international standards, including ISO 9001, TL 9000, and ISO 14001. Further information regarding CommScope's commitment can be found at www.commscope.com/corporate-responsibility-and-sustainability.