Palo Alto Networks Expands Global Reach in Latin America

June 14, 2012

Leading Next-Generation Firewall Company Opens Offices in Brazil and Mexico

Santa Clara, CA , June 14, 2012 Palo Alto Networks™, the network security company, today announced plans to expand its presence throughout Latin America, including opening offices in São Paulo, Brazil and Mexico City, Mexico. The expansion includes additional resources that will include expanded focus on sales, customer support, training, and its partners in Argentina, Brazil, Chile, Colombia, Mexico, and Peru. As Palo Alto Networks further grows its global footprint, the company looks forward to continuing to bring the value of its next generation of network security to its channel partners and customers in these markets.

 "Customer satisfaction is our focus and priority. We take the success of our customers very seriously in how we innovate, develop our products, provide customer support – all to ensure a great experience," said Adam McCord, director of sales for Latin America and the Caribbean, Palo Alto Networks. "Innovation is at the core of everything we do, from being the first company to define and lead the industry's transition from the stateful inspection firewall approach to the Next-Generation Firewall paradigm to continuing to deliver new products and services that benefit customers in unique ways. By expanding our reach and adding offices and resources to these markets, we further extend this commitment to our partners and customers in Latin America."

Latin America Partner Focus

The growing Palo Alto Networks global footprint and continued dedication to its channel translates to new regional partnerships in Latin America as well. As part of its efforts in the region the network security company now includes partners such as Agility Networks, Alsar, NeoSecure and Morphus.

"NeoSecure is always evaluating the best and most innovative solutions to respond to today's complex network security environments and Palo Alto Networks matches up with those needs," says Eduardo Diaz, CEO of NeoSecure. "The competitive advantage of Palo Alto Networks is that unlike existing firewalls, control is based on user, application and content, rather than IP and port number. We are confident that this alliance with Palo Alto Networks will bring to market a disruptive solution."

Solution portfolio

Palo Alto Networks has pioneered the next generation of network security with its innovative platform that allows you to secure your network and safely enable the increasingly complex and rapidly growing number of applications running on your networks. At the core of this platform is our Next-Generation Firewall (NGFW), which delivers visibility and control over application, users, and content within the firewall using a highly optimized hardware and software architecture.

This platform offers you the ability to identify, control, and safely enable applications while inspecting all content for all threats in real time. The Palo Alto Networks NGFW platform can address a broad range of your network security requirements, ranging from the data center to the network perimeter to the far edges of the enterprise, which includes branch offices and mobile devices.

The product portfolio includes:

- PA-5000 Series: Designed to protect data centers, large enterprise Internet gateways, and service provider environments where traffic demands dictate predictable firewall and threat prevention throughput. Tailor-made to provide enterprise firewall protection at throughput speeds of up to 20 Gbps and ideally suited for both datacenter and service provider deployments, the series is powered by more than 40 processors distributed across four functional areas: networking, security, content inspection and management. Reliability and resiliency is delivered by active/active or active/passive high availability; physical separation of data and control plane; and redundant, hot swappable components.
- PA-4000 Series: Suited for high speed Internet gateway deployments within enterprise environments. Designed to provide enterprise firewall protection at throughput speeds of up to 10 Gbps using dedicated processing for networking, security, content inspection and management. Uses a 10 Gbps backplane to smooth the pathway between processors, and the physical separation of data and control plane ensures that management access is always available, irrespective of the traffic load.
- PA-2000 Series: Ideally suited for high speed Internet gateway deployments within large branch offices and medium sized enterprises to ensure network security and threat prevention. Delivers next-generation firewall security using dedicated processing and memory for networking, security, threat prevention, URL filtering and management. And like the PA-4000 series, uses a high speed backplane to smooth the pathway between processors and the separation of data and control plane ensures that management access is always available, irrespective of the traffic load.
- PA-500: delivers next-generation firewall security to Internet gateway deployments within medium to large branch offices and medium sized enterprises. The PA-500 protects enterprise networks using high performance processing and dedicated memory for networking, security, threat prevention, URL filtering and management.
- PA-200: Small and quiet enough to sit on a desk, yet powerful enough to deliver next-generation firewall security to a distributed enterprise office. Extends visibility and control over applications, users and content into enterprise branch

offices.

- WildFire: Delivers protection from targeted and unknown threats by providing the ability to identify malicious behaviors in executable files by running them in a virtual environment and observing their behaviors. This enables Palo Alto Networks to identify malware quickly and accurately, even if the particular sample of malware has never been seen in the wild before. Once a file is determined to be malicious, WildFire automatically generates signatures for both the infecting malware and the resulting command and control traffic. Signatures are delivered with regular security updates to all devices that subscribe to the service to provide automated in-line protection from these highly advanced threats. Your IT team is provided with a wealth of forensics to determine who was targeted, the application used in the delivery and any URLs that played a part in the attack.

For more information on Palo Alto Networks and its products, please visit http://www.paloaltonetworks.com/.