Mobility Solution Brief

CHALLENGE

Today's mobile devices are becoming constant companions and the platform of choice for many computing tasks. Organizations face a balancing act trying to enable the benefits of mobility without introducing security risks.

SOLUTION

Safely enable mobile devices with Palo Alto Networks™. With the next-generation firewall and GlobalProtect™, organizations can ensure that the use of mobile devices both in and out of the office adhere to security policies.

Get network security, data protection and device management through the Palo Alto Networks next-generation firewall, GlobalProtect and products from technology partnerships.

BENEFITS

Palo Alto Networks enables organizations to consistently enforce network security policies for all users, both internal and external, while providing users with the freedom to choose their own mobile devices. Instead of trying to block mobile devices from the network, the organization can allow users to choose their preferred smart phones and tablets while mitigating risk.

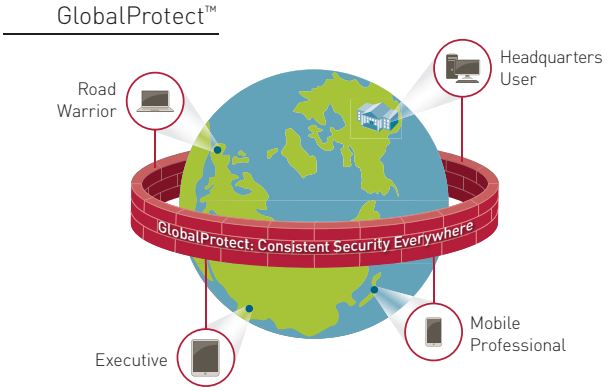
THE LANDSCAPE FOR MOBILITY

In recent years, the landscape for mobile devices changed in a dramatic fashion. No longer being limited in capability and functionality, the modern smart phone and tablet are becoming a constant companion (and in some cases, a replacement) for the traditional laptop. In fact, with more of these devices connecting directly to the network, security teams are facing growing concerns about the limitations of what they can and cannot protect.

Without a strong view of what's happening on the network, many organizations assume a fear-based posture towards mobility. Instead of embracing the positive benefits, security teams attempt to block devices from their network in hopes of recreating the controlled environment that once existed in the past. Such efforts are often limited in scope, and fail to deliver an appropriate balance between what the business needs in terms of security and what users want.

Palo Alto Networks provides a comprehensive network security solution for mobility that enables customers to embrace mobility without sacrificing security. Using the next-generation firewall with GlobalProtect, organizations can extend network security and data protection to mobile devices, including smartphones and tablets. GlobalProtect can automatically connect users to the best available GlobalProtect gateway on a Palo Alto Networks next-generation firewall. As a result, organizations can consistently enforce security policies based on application, user, content and device, regardless of where the user is located. Through the safe enablement of applications, users can access business and productivity tools while enjoying protection from mobile threats to the device and data. By placing the security in the network and leveraging an always-on connection to the next-generation firewall, enterprises can now let employees take full advantage of the mobile device of their choice without security compromises.

In addition, mobile device management (MDM) and data containment products from technology partners complement the Palo Alto Networks mobility solution. With Palo Alto Networks, the adoption of mobility can be done in a manner in accordance to the organization's particular requirements and attitude towards risk.



paloalto NETWORKS
the network security company™

BENEFITS AND LIMITATIONS OF EXISTING APPROACHES

When looking at the landscape for mobile device security, there are a number of approaches that are available. There are container and VDI technologies that isolate data. There are many mobile device management products designed to manage the settings on a device. There are legacy VPN products which were originally designed for the remote access use case scenarios. Each one of these pieces provides an element for a mobility solution, but it's important to understand the role, scope and limitations of what each can do.

Containers and Virtual Desktops Infrastructure

Containers and virtual desktop infrastructure (VDI) provide a method to isolate some data. Containers can partition data on a device in a sandbox. VDI allows users to access a desktop remotely, thus separating the entire desktop from the device itself.

In both cases, there is an implicit assumption that the only sensitive data on the device is in the container/virtual desktop. However, users may use other productivity applications on the device as well, which spreads the sensitive data throughout the device.

Mobile Device Management (MDM)

Provides the means to set mobile device settings and provisioning the device for use. MDM may be considered a baseline requirement for managed devices, but there are additional considerations that one must also add to address security.

Traditional SSL VPN

SSL VPN provides temporary access to corporate networks. However, it does not provide any network security controls, such as ones that enforce appropriate application usage, block undesirable traffic and prevent inappropriate file sharing. As a result, the SSL VPN provides the means for mobile devices to access corporate applications without the measure to protect it.

In addition to the technologies listed above, there are a number of security products designed for network access, such as network access control and wireless network security which are often considered in conjunction with a mobility strategy. There are also stacks of traditional network security products such as the stateful inspection firewall, IPS, and proxies, which are managed in separate contexts and disjointed policies. With a bewildering list of technologies to consider, developing a comprehensive mobile strategy can pose a formidable challenge.

SAFELY ENABLING MOBILE DEVICES

Palo Alto Networks recommends that the proper solution to safely enable mobile devices involves three critical ingredients:

- Protect traffic
- Protect data
- Ensure the device is OK

Through a combination of technologies from Palo Alto Networks and its partnerships, an organization can ensure that only proper devices have access to sensitive information, maintain consistent security throughout the organization, and protect mobile devices from vulnerabilities and malware.

NEXT-GENERATION NETWORK SECURITY WITH AN ALWAYS-ON CONNECTION

The network is the link between enterprise applications, data and users. It provides the obvious location for providing policy enforcement and safe enablement of devices. However, the traditional firewall does not differentiate between users, nor does it identify applications. It simply permits any traffic allowed on a particular network segment to pass as long as it follows basic port-based policy guidelines. Mobility exposed this pre-existing condition, as users were able to access anything they wanted once they were able to get their device on the network. Existing traditional security did not provide the means to provide visibility and control.

Remote users pose a second set of challenges because network security is ephemeral with the traditional VPN. Once the user disconnects from the corporate wireless network or the VPN, the user has a direct path to the Internet without any security in the network traffic path and outside of the jurisdiction of safe practices.

The next-generation firewall paired with GlobalProtect solves both conditions. Instead of treating all network traffic in the same generic manner, the next-generation provides the means to classify traffic by application, user and content. Thus the protection lies within the network, ensuring that policy enforcement is always in place, rather than being dependent upon blocking technologies to keep mobility off. GlobalProtect provides the VPN connection in a manner that's not predicated on temporary connections, but rather an always-on connection to the corporate network, regardless of location. Whether in a hotel room or in the office, the user stays on network with the same enforcement of policy. This approach provides consistency for the protection and safe application enablement provided by the next-generation firewall, regardless of whether the user is in the office or on the road.

All of these technologies work together to provide the foundation for mobile protection that extends to all users. With a strong foundation for network security, an organization can provide a choice in devices with an approach that welcomes change rather than resisting it.

The next-generation firewall provides a number of protections for traffic in order to provide safe enablement. Some of the features include:

- **Application policy:** Ensure that users have access to the proper applications while removing dangerous or risky elements.
- **URL filtering:** Restrict access, by specific web site or categorically, to content that may be inappropriate or unauthorized. For instance, an organization may want to make sure that apps can only be downloaded from authorized app stores, while blocking all others.
- **Malware protection:** The next-generation firewall analyzes traffic for malicious content, providing the means to stop dangerous files before it reaches the user. Many enterprises do not have antivirus clients running on their mobile devices, which only reinforces the importance of stopping malware in the network. The next-generation firewall scans content that endangers mobile platforms, thus providing the device with a blanket of protection that's always in place.
- **Vulnerability protection:** Mobile devices pose a special challenge for organizations in terms of maintaining protection against newly discovered vulnerabilities in the operating system. Due to the vast number of devices in use, and the inconsistent application of operating system updates, it's not easy for an organization to ascertain just how much risk they face against a particular attack. By placing vulnerability protection in the network, the next-generation firewall intercepts an exploit before it reaches the user's device, thus providing protection even in advance of patch installation.

DATA PROTECTION

One of the principal concerns about mobility circles around the risk of corporate data being placed outside of controlled boundaries, namely a mobile device which may or may not be owned by the organization or in applications outside of its control. One approach to solve this challenge is to leverage the always-on connection to extend the boundary of protection to all locations. This concept, the logical perimeter, differs from a physical perimeter in that it does not requirethe user to be on premise to benefit from its protection.

The next-generation firewall includes file and data filtering technology to protect data and applied to all users including ones on mobile devices through GlobalProtect. Data filtering features enable administrators to implement policies that will reduce the risks associated with the transfer of unauthorized files and data.

- **File blocking by type:** Control the flow of a wide range of file types by looking deep within the payload to identify the file type (as opposed to looking only at the file extension).
- **Data filtering:** Control the transfer of sensitive data patterns such as credit card and social security numbers in application content or attachments.
- **File transfer function control:** Control the file transfer functionality within an individual application, allowing application use yet preventing undesired inbound or outbound file transfer.

For organizations with highly sensitive data, and with regulatory and compliance requirements, the implementation of containers or Virtual Desktop Infrastructure (VDI) can isolate such data from the rest of the device. A container takes the approach of using a sandbox on the device to separate certain data from the rest of the device. VDI keeps the application and the data within the data center, and provides access through a client on various platforms. The next-generation firewall can add further protections such as restricting access to the data center to virtual desktops, thus providing access to the application without the risk of placing data on the mobile device itself.

All of the measures above work in conjunction with device management, should it be necessary to remotely wipe a device that's been lost or deprovisioned.

DEVICE MANAGEMENT

Device management plays a role in a mobility solution as it establishes the fundamental profiles that govern device settings and device state. In a nutshell, it provides the means to ensure that the device is appropriate for use in a manner consistent with the organization's policies and to bring it under management. Some of the things that device management controls include settings for passcode requirements, remote wiping and device wiping after a number of failed unlock attempts.

Jailbreaking a mobile device removes code signing requirements An organization can check to see if a device has been jailbroken and use the device state as part of its security policy decisions.

The next-generation firewall pairs with mobile device management products to provide device management. Palo Alto Networks complements device management solutions available from technology partners.

TECHNOLOGY PARTNERSHIPS

Device management solutions are available from technology partners and complement GlobalProtect from Palo Alto Networks.

Guest Wireless Networks

Solutions for guest wireless networks allow an organization to implement a variety of network auth-entication. By providing integration with the next-generation firewall, the identity of the user can be used as a policy condition, thus providing additional granularity to control what a user may do once they have access. An organization can provide safe Internet access to guests while ensuring that only corporate users with GlobalProtect have access to the data center, thus establishing user-based (rather than segment-based) network controls.

Authentication

Some organizations prefer to add additional authentication factors to the process of identifying users. With technology partnerships from companies such as RSA Security, Swivel, SafeNet and NordicEdge, an organization can add additional authentication factors to assert an identity of a user. These methods integrate with GlobalProtect through RADIUS, and complement the range of authentication methods that are natively available.

SUMMARY

Many organizations are reevaluating their mobility strategy in order to address the broad range of smartphones, tablets and laptops that their users want to use. Start your strategy by ensuring that the foundation, the corporate network, is ready to safely enable applications and devices. By using the Palo Alto Networks next-generation firewall, security teams can say yes to what users want without the fear of losing control, and take full advantage of all the benefits that mobile computing can offer.

To find out more about Palo Alto Networks Mobility Solutions, visit: www.paloaltonetworks.com/solutions/mobility

paloalto NETWORKS

the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com