Application Note

Context-aware security for the mobile enterprise

Unified Access solution integration with Palo Alto Networks

Alcatel·Lucent Enterprise

Introduction

Mobility has redefined the boundaries of the enterprise. Organizations provide their workers with an array of devices to perform their jobs more efficiently both at the office and away from it. At the same time, employees, partners, contractors and visitors are bringing personally owned devices into the workplace. Users today demand access to the resources that they need inside and outside the organization from both corporate and personal devices.

Enterprises desire to embrace mobility and promote an anywhere, anytime, any device culture that improves productivity and fosters innovation to derive a competitive advantage. On the flipside, however, this trend introduces security challenges for IT. Traditional approaches to enterprise security have focused on protecting the network infrastructure from external attacks with no or little understanding of the user: Internal users are trusted without distinction across roles, devices, applications, time of day or location. Traditional port- and protocol-level policies are coarse and fail to incorporate this bigger picture. As a result, these mechanisms are inadequate for today's mobile workforce.

This application note shows how these challenges can be overcome by sharing user-context metadata and leveraging it at security policy enforcement points throughout the network.

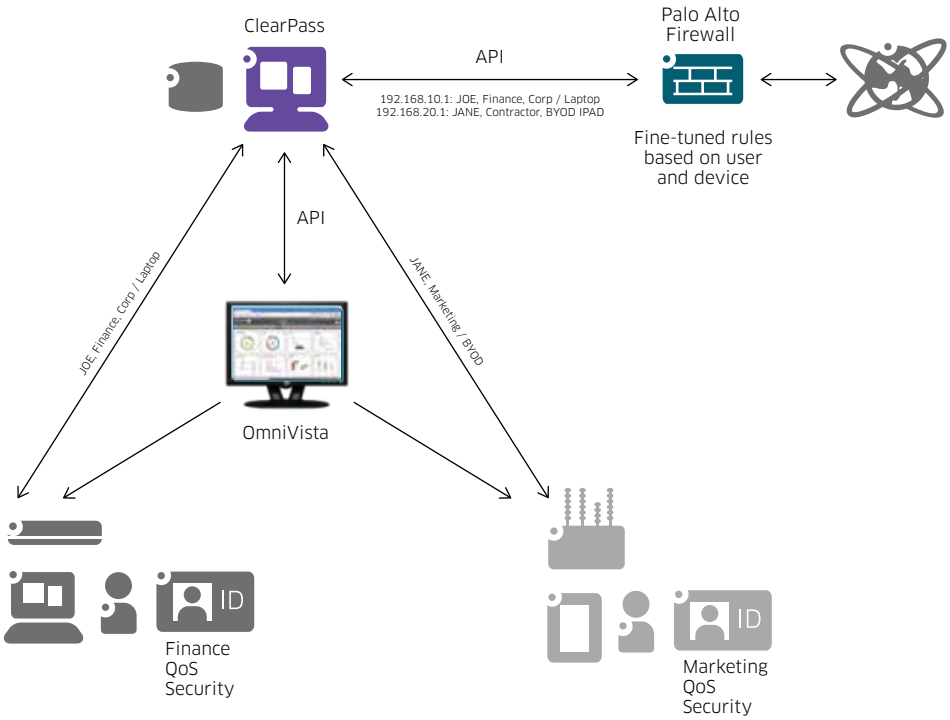
Delivering end-to-end context-aware security

To respond to these challenges, we have integrated our Unified Access solution with Palo Alto Networks® (PAN) Next-Generation Firewall. With Alcatel-Lucent Unified Access, users and devices are authenticated, profiled and checked before any access is allowed to either the wired or the wireless network. Granular access policies are then selected and applied based on the connection's context – user, device, location, application, date or time. Access policies set privileges over network resources and applications as well as service levels.

By integrating our Unified Access solution with the PAN firewall, this user-context metadata (IP address, device type, user role) is shared, enabling fine-grained, context-based policies to be seamlessly applied at the firewall. When applications are launched, the firewall monitors for policy violations based on who and what is connected to the infrastructure. Applications can then be controlled accordingly or blocked if there's no legitimate use for them.

The diagram below depicts the solution components and the interfacing between the Unified Access solution and the PAN firewall.

Figure 1: User context sharing



Alcatel-Lucent OmniVista® 2500 Network Management System (NMS) offers unified management using a single pane of glass for the entire wired and wireless network and significantly simplifies network operations. It includes all the tools needed to provision, monitor, analyze and troubleshoot the network. OmniVista 2500 NMS consistently configures access policies and user profiles across LAN and WLAN alike in a single touch.

The Aruba ClearPass Policy Management System™ (ClearPass) provides a common set of network services, policy framework, authentication scheme and a single authorization database that applies to users accessing the network, both wired and wireless.

The Palo Alto Networks firewall offers a complete set of capabilities to establish the perimeter security, including:

- Enforcing security policies across all users, devices, applications, and locations regardless of port, encryption (SSL or SSH) or evasive techniques employed
- Blocking a range of known threats, including exploits, malware and spyware, across all ports, regardless of common threat evasion tactics employed
- Limiting the unauthorized transfer of files and sensitive data, and control non-work-related web surfing
- Identifying unknown malware, analyze it based on hundreds of malicious behaviours, and then automatically create and deliver protection

Examples

Here are two examples, both based on Figure 1, illustrating how the user context metadata is leveraged both at the Unified Access layer and at the firewall to enforce fine-grained policies as defined by the organization.

Joe is an employee in the Finance department and connects his corporate laptop to the network through an Ethernet cable.

Joe's identity and device are authenticated before he can access the network. Joe's corporate laptop has been issued and provided with a certificate by IT, and it is compliant with endpoint security policies which include limited operating system privileges as well as automated antivirus and software updates. Because of this, the Unified Access policies allow Joe to access a range of corporate resources appropriate to his role from this corporate laptop. These policies are selected by ClearPass on the basis of his identity and device and are enforced at the Alcatel-Lucent OmniSwitch® LAN switch. Through the application programming interface (API), ClearPass shares this user-context metadata with the PAN firewall. With this knowledge, the firewall applies policies that protect Joe from a range of threats but also prevents leakage of sensitive data that he has access to.

Jane is a contractor and accesses the network wirelessly from a non-corporate bring-your-own-device (BYOD) iPad.

Through a self-service process, Jane's iPad has been provisioned with a certificate that authenticates the device's access to the network, but no further health checks or posture assessment are done on her device. Because of this, Unified Access policies restrict Jane's access to just a small subset of the corporate resources. Similarly, these policies are selected by ClearPass on the basis of her role and device and enforced on the Alcatel-Lucent OmniAccess® WLAN. Through the API, ClearPass again shares this user-context metadata with the PAN firewall. With this information, the firewall applies policies that protect Jane from a range of threats but at the same time allow her to share non-sensitive data with her own organization in order to perform her duties.

Benefits

Benefits of this holistic approach to security include:

- Proactive security: Identity is established prior to granting access to wired or wireless network services.
- Threat prevention: Identifies known and unknown malware, breaking the lifecycle of advanced, targeted attacks on computers and mobile devices.
- Granular policies: Fine-grained control extends to wired and wireless bandwidth, location-based services, and device types – not just IP addresses and port numbers.
- Unprecedented visibility: IT gains unprecedented visibility into how its networks and applications are being used and by whom. This data can be used for a diverse range of tasks, including resource planning, support staffing and security threat management.
- Internet of things: The benefits above also accrue to devices without user interfaces, including office equipment, medical monitors and industrial controls. A combination of active and passive methods enables the network to profile these devices and apply policies accordingly without any user intervention.

Conclusion

Mobility has transformed the traditional boundaries of the enterprise rendering static security mechanisms ineffective: The premise that the point of connection can be correlated to the level of trust is no longer valid. Protecting at the perimeter is not enough to provide end-to-end security; it is also necessary to add protection from the inside. And this is what Alcatel-Lucent Unified Access offers: Nobody is trusted – all users must be authenticated and authorized before gaining network access.

Furthermore, in today's mobile enterprise, trust and privileges must be dynamically assessed and granted not only on the basis of identity but also device type, ownership and status, among other factors. It is therefore necessary for the different security elements to have real-time knowledge of this user context.

Alcatel-Lucent Unified Access includes a single repository of user-context metadata that can be leveraged across the network to select the security policies that apply in a given situation. This context metadata drives network access control (NAC), profiles, policies and service levels at the Unified Access layer as well as rules at the Palo Alto Networks Next-Generation Firewall.

With this integration, we have teamed up with Palo Alto Networks to address the security challenges of the mobile enterprise, enforcing fine-grained policies that fit the user, the device and other contextual situation throughout the network.

Alcatel·Lucent
Enterprise