FIREWALL DEFENSE ENHANCEMENTS FOR THE MOBILE ENTERPRISE

Check Point and Aruba ClearPass extend traditional perimeter defense for today's mobile workforce

Mobility has quickly changed the notion of fixed perimeter security. Enterprise users are no longer confined to office buildings with desktop clients connected to Ethernet ports for access. As user behavior has changed, security for the enterprise has also had to shift to a more granular approach that includes the identity of the user, device, and location context.

As many attacks now target both the intranet and the perimeter, the importance of traditional perimeter security solutions is shifting. Hackers have capitalized on the BYOD phenomenon by targeting users, who may have unsecure devices with suspect apps on the network, and may be unaware of the security implications.

The result of risky BYOD user behavior is another driver — most high profile breaches have occurred due to users bringing unsecure devices into the enterprise. In the past, virtually all breaches came from outside the network, but this shift targets the weakest link in the security chain and requires a new way to enable actionable enforcement to contain threats. A defense based on Adaptive Trust.

Contextual information collected via Aruba ClearPass can be exchanged with third party perimeter hardware, such as Check Point firewalls, to allow for granular firewall policies based on user, group, device type, and location context. Security must adapt to how users and businesses work today.

CHECK POINT FIREWALLS WITHIN AN ADAPTIVE TRUST DEFENSE

The granular user, device, and location information, along with contextual policies defined by IT, are passed from ClearPass to Check Point next generation firewalls (see Figure 1), IPS, Anti-bot, as well as Check Point's sandboxing tools that allow organizations to determine extended perimeter security threats and take immediate remediation action such as blocking a device, blocking traffic, blocking malware, etc.

For example, if a user attempts to connect to a network with a personal non-IT issued device, ClearPass will collect granular information about the user and the device. This detailed information is then passed along to Check Point's firewall. At this point, the firewall will either allow or deny appropriate traffic types and then log the information. If there is any traffic or policy out of order, the user and device can be quarantined from the network.

ATTRIBUTES COLLECTED BY CLEARPASS FROM THE USER AND THEN SHARED WITH CHECK POINT FIREWALLS	
Feature	**Firewall**
Source IP	✔
Username	✔
Dynamically calculated User Role	✔
Domain	✔
Device Type	✔
Machine OS	✔
Machine Name	✔
Health/Posture	

Integration is supported with ClearPass Policy Manager 6.6 or later and Check Point R80.xx. Previous versions of R77.xx are supported with Check Point HotFixes.

Although user name attributes are gathered from the firewall through an identity store like active directory, guest and visitor information can only be passed through from the policy vendor that would gather this type of information from onboarding these types of users.

When roles are passed at authentication from the policy manager, the device type, user profile, and location information is dynamically passed to the firewall to ensure no policy is circumvented through a change in the user's posture, whether it be an expired device OS, user type, or other changes.

With Check Point, not only can these policies allow for a holistic threat defense from both within and outside of the network, but Check Point can protect against additional cybersecurity threats such as:

- Known and unknown malware, zero-day exploits, and other advanced threats
- Blocking and quarantine of users and devices from within and outside of the network
- Remediate compromised or vulnerable devices
- Enforce policies based on user, application, or location information
- Secure work documents outside the network
- Non-employee devices connecting to the internal network

ARUBA CLEARPASS OVERVIEW

The ClearPass policy engine adds security at the user or device level. Contextual data, – user location, roles, device-type, device-OS and endpoint health or posture – can be obtained without IT involvement. Self-service onboarding or guest access capabilities that are built into the system can also provide useful context that can be shared with Check Point. This increased level of contextual information enhances visibility and allows the enterprise security perimeter and associated policies to extend to wherever the end user and device may roam.
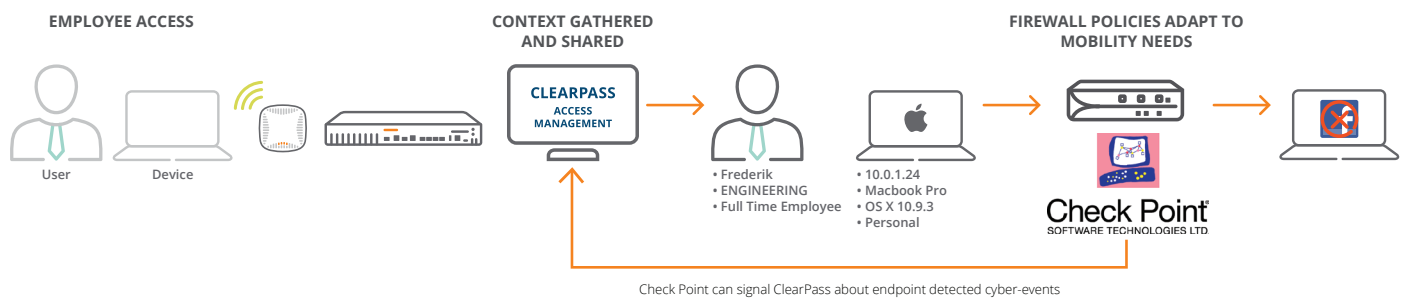
DATA EXCHANGED WITH OTHER NETWORK TOOLS

figure 1.0_113015_checkpoint-soa

a Hewlett Packard Enterprise company

Contact Us   Share