IdentityConnect™ for Palo Alto Networks

Making Next-Gen Firewalls Smarter through Contextual Intelligence™

Highlights

- Ability to assign policies based on contextual intelligence attributes (identity, device type, location, time, ownership, and security compliance) for AD domain managed, personally-owned (BYOD), guest, and non-browser network devices.
- Single Sign-On (SSO) support for secure wireless 802.1X-WPA2E and AD domain authentication mechanisms which eliminates the need to repeatedly prompt users with a captive log-in portal page to gain identity.
- Authentication persistence offers a one-time or periodic authentication policy that prevents the user from experiencing frequent log-in portal prompts as they traverse or reconnect to the network.
- Flexible annual and multi-year subscription pricing; no additional upfront charges
- Real-time and historical contextual intelligence-based reporting
- Easy-to-deploy and supported by a cloud managed service
- Enhances investment in Palo Alto Networks technology

impulse

The ability to determine and take action based on device-specific attributes in context (such as user identity, device type, location, ownership, and security posture) is a fundamental requirement for addressing regulatory compliance, security forensics, trending analyses, and data access management.

The BYOD Management Challenge

The Bring Your Own Device (BYOD) phenomenon has introduced a major blind spot for next-generation firewall providers when it comes to associating user identity to non-AD domain managed devices. This includes employees, students, faculty, guests, and contractors who require access to network resources using their personally-owned mobile devices.

Additionally, the ever increasing mobility trend results in frequent IP address reassignments as users move from one wireless network zone to another. These constant changes also limit the ability to successfully track AD Domain managed devices, creating another visibility blind spot. Therefore, the IP address is no longer an acceptable mechanism for monitoring and controlling user activity for BYOD, guest and AD domain managed devices.

Organizations need a cost-effective solution that can associate a device's attributes with its IP address in real-time to enable next-generation firewall, web content, and bandwidth policies by user identity (group), device type, and ownership (whether a device is corporate- or personally-liable).

IdentityConnect™ for Palo Alto Networks

IdentityConnect™ is a software plug-in for USER-ID™ that enables Palo Alto Networks (in conjunction with App-ID™ and Content-ID™) to assign more granular device policies based on Contextual Intelligence™ information, which includes user identity (group), device type, location, time, ownership (liability), and security compliance for all devices on the network (wired, wireless, VPN).

IdentityConnect is a purpose-built, annual subscription-based, cloud managed service offering that enables identity-based policy management of AD domain managed, personally-owned (BYOD), guest, and non-browser network devices at a fraction of the cost of homegrown or complex NAC alternatives.

Common Use Cases

- Assign **application-aware firewall access privileges** based on user group (executive, human resources, sales, faculty, student, vendor, guest); ownership (corporate or personally liable); device type (laptop, iPad, mobile phone); location (HQ, remote office, dormitory, public Wi-Fi, library); and time (weekdays only, after-school hours) **per device**.
- Assign **web content access policies** by user identity group (VIP, faculty, student, or guest).
- Assign **bandwidth policies** based on user role, device type, ownership, location, and time **per device**.
- Assign **aggregate data consumption policies** for all devices associated with **a user**.

"Gartner recommends that organizations [should] begin the transformation to context-aware and adaptive security infrastructure now as they replace static security infrastructure, such as firewalls, and web security gateway and endpoint protection platforms."

Neil MacDonald
Vice President and Fellow,
Gartner Research

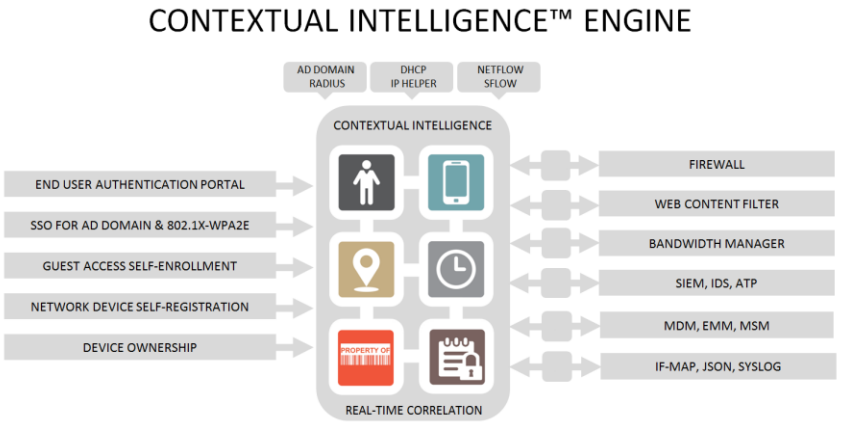
End User Self-Service Portals

IdentityConnect integrates with Palo Alto Network's redirection portal technology to provide the following End User Self-Service Portals:

- **User Authentication Portal** – Captures user identity, AD/LDAP group membership, and ownership for users that have existing organization directory credentials (username and password)
- **Guest Access Self-Enrollment Portal** – Assigns identity and role to guests users based on their function (guest, vendor, contractor)
- **Network Device Self-Registration Portal** – Associates identity and role with non-browser network devices (gaming, media, printers)

Contextual Intelligence™ Publishing and Reporting

IdentityConnect collects and correlates information from a variety of network and directory sources, and publishes contextual intelligence information that enables real-time identity-based firewall, web content URL filter, and bandwidth/data consumption policies. IdentityConnect includes a Reporting Dashboard that provides real-time and historical contextual intelligence visibility for compliance reporting, trending and forensic analysis.



IdentityConnect also provides real-time contextual intelligence data to other third-party security management systems such as SIEM, IDS, and Advanced Threat Protection providers to enhance their ability to identify and track managed and non-managed (BYOD) devices in real-time as they traverse the network. This enhanced visibility equates to more accurate and timely security decisions and control.

Managed Support Services

All Impulse products come with an industry exclusive and comprehensive maintenance program. This includes 24x7x365 system monitoring; problem determination and resolution technical support; daily remote backups and device type profiling updates; and application of no-charge maintenance and software version upgrades.

Impulse | Experience the Freedom.
Impulse is the leading provider of Contextual Intelligence™ and access control solutions in support of BYOD-friendly enterprises. Impulse securely and efficiently automates BYOD by combining our real-time, context-aware and simplified architecture, remote managed support services and customer-centric business philosophy to enable customer freedom. Our customers know this as the Impulse Experience. The security of more than four million endpoints is entrusted to Impulse. Visit www.impulse.com