INTEGRATION BRIEF

Palo Alto Networks and Elisity

Expanding the Scope of Identity-Based Security and Bringing Access Layer Visibility to the Network Boundary

Security teams often face the immense challenge of maintaining accurate and scalable firewall policies in environments with constantly shifting assets. Traditional firewall management requires security teams to manually classify and track devices, leading to inefficiencies and security gaps. Elisity removes this burden by continuously discovering and classifying all campus assets within the Elisity-secured architecture and mapping them to highly accurate Policy Groups. Administrators can then selectively push these groups to Palo Alto Networks firewalls or Panorama as Dynamic Address Groups (DAGs), eliminating the need for manual address group updates. By automating asset classification and DAG management, Elisity enables administrators to focus on building and enforcing security policies, rather than maintaining outdated access lists.

The Challenge

Addressing the Complexity of Firewall Policy Management

Managing Firewall Rules at Scale

Security teams face the ongoing challenge of keeping firewall rules updated and relevant as new devices join the network. Traditional firewall address groups require manual tracking and classification of assets, an operationally intensive process that increases the risk of misconfigurations and security gaps. Without an automated way to classify and segment assets, administrators are forced to spend valuable time managing address groups rather than focusing on defining and enforcing security policies.

Lack of Visibility Leads to Security Gaps

In many organizations, static IP-based policies fail to reflect real-time changes in device identity, role, or risk level. This creates blind spots in enforcement and introduces unnecessary complexity when maintaining consistent security postures across multiple sites. IT and security teams need a way to continuously identify, classify, and segment assets without manual intervention, ensuring policies remain aligned with evolving security needs.

The Solution

Automating Asset Classification and DAG Assignments

Elisity eliminates the challenge of manual asset classification by automating the discovery and categorization of all campus-connected assets within the Elisity-secured architecture. By dynamically assigning devices to Policy Groups and selectively propagating them to Palo Alto Networks firewalls or Panorama as Dynamic Address Groups (DAGs), security teams gain precise control over firewall policy enforcement—without the burden of manually maintaining address groups.

Key Benefits

Automate Firewall Policy Management

Eliminate manual updates to firewall address groups and ensure access policies always reflect real-time network conditions.

Zero Trust with Identity-Based Segmentation

Control access between campus resources, cloud workloads, and remote sites dynamically and apply identity-driven policies rather than static IP-based rules.

Unified Segmentation

No more duplicated efforts. Unify device-group assignments across platforms with Elisity's multi-vendor approach. Ensure OT, IoT, IoMT, and IT devices are categorized ubiquitously.

Rapid Deployment, No Network Disruption

Seamless integration into existing Palo Alto Networks environments via API —no re-architecting required.

How it Works

Step 1 - Elisity Discovers and Enriches Asset Data

Elisity discovers assets at the network edge using existing switching infrastructure. Elisity's IdentityGraph builds a real-time inventory of all devices located within the Elisity-secured infrastructure.

- This includes IT, IoT, OT, and IoMT devices, both managed and unmanaged.
- All assets, such as laptops, workstations, corporate assets, and critical infrastructure components, are automatically classified.
- Context is enriched from multiple trusted sources, including CMDBs, EDR, IAM, Custom Databases, and OT security tools, ensuring precise and dynamic asset identification.

Step 2 - Intelligent Policy Group Assignment

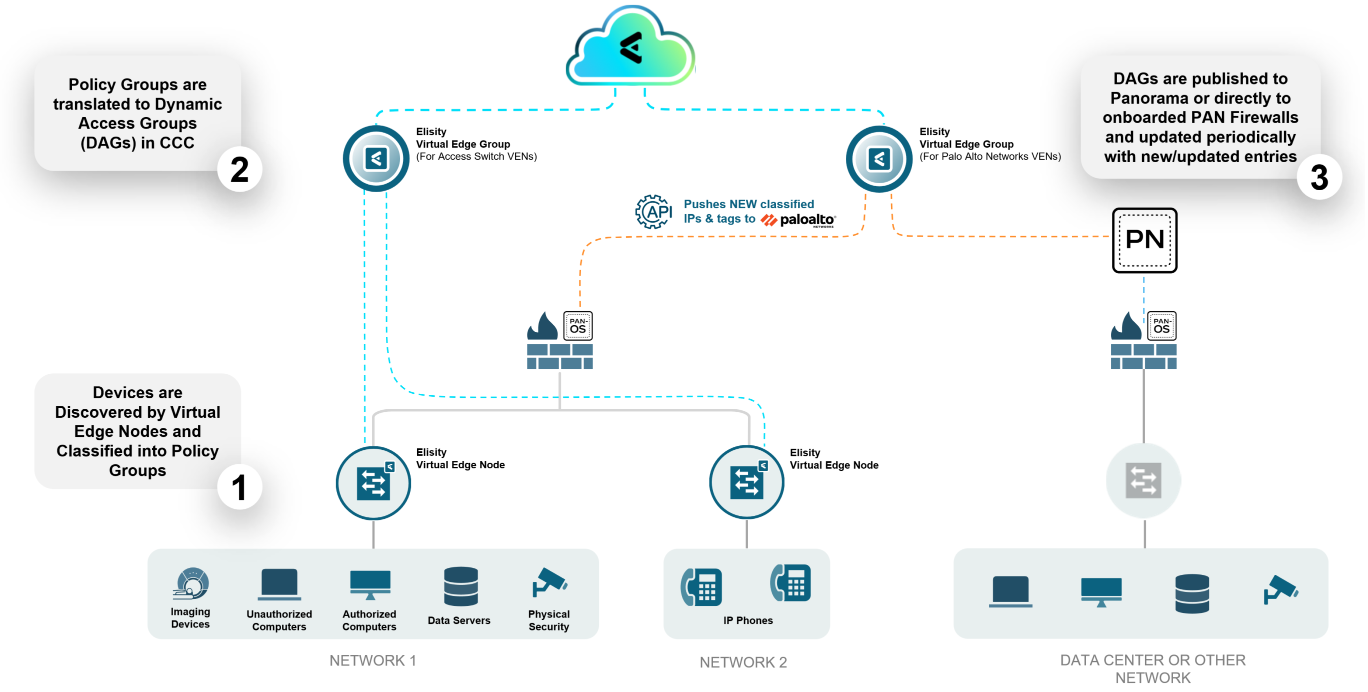
Devices and users are dynamically assigned to Policy Groups based on three primary categories of asset information:

- **Identity:** Elisity leverages Elisity IdentityGraphTM to aggregate identity-related attributes such as Device Type, Class, These attributes provide a granular and real-time understanding of each asset, ensuring that segmentation policies reflect true operational identity rather than static network constructs.
- **Location:** The physical or logical placement of an asset within the network, including proximity to Virtual Edge Nodes, segmentation zones, and dynamic operational boundaries. Elisity ensures that as devices move between segments, policies automatically adjust to maintain proper security enforcement.
- **Trusted Status (Trust Attributes):** Trust Attributes are attributes that verify if an asset is known in system of record (outside of Elisity Native Intelligence) and to what degree these external systems of record agree. Examples include: Known in Palo Alto IoT Security. Known in CrowdStrike, Known in Active Directory, Manually Verified, etc.

Step 3 - Dynamic Address Group (DAG) Synchronization with Palo Alto Networks

- Policy Groups are selectively mapped to DAGs either through Panorama for centralized management, or directly to select onboarded firewalls. These DAGs are then used in firewall policy definitions.
- DAGs are continuously updated based on real-time changes in identity and device context.
- Firewall administrators create security policies between DAGs, ensuring least-privilege access control without manually tracking assets or IP addresses.

Palo Alto Networks + Elisity Overview



Policy Groups are translated to Dynamic Access Groups (DAGs) in CCC 2

DAGs are published to Panorama or directly to onboarded PAN Firewalls and updated periodically with new/updated entries 3

Devices are Discovered by Virtual Edge Nodes and Classified into Policy Groups 1

Extending Firewall Intelligence with Palo Alto Networks IoT Security

Palo Alto Networks IoT Security provides unparalleled asset intelligence and visibility across connected environments. By integrating PAN IoT Security insights into Elisity's Policy Group (PG) match criteria, organizations can **seamlessly incorporate IoT security intelligence into their firewall policy enforcement strategy.**

With this integration, Palo Alto Networks customers can maximize the value of their investments in Next-Generation Firewalls, VM Series Firewalls, and Panorama, ensuring that security policies are not only dynamically managed but also enriched with real-time IoT device intelligence.

How These Integrations Work Together

- Elisity ingests data from IoT Security, among other sources, to classify and segment assets with unmatched precision, giving enhanced confidence in asset classifications.
- Security teams can define Policy Groups using IoT device attributes, and selectively push them as Dynamic Address Groups to specific firewalls or Panorama with flexibility.
- By combining IoT Security, Elisity, and Panorama (or direct integration with NGFW or VM-series firewalls) organizations achieve enhanced Zero Trust enforcement, ensuring that even unmanaged or dynamic assets are properly categorized and protected.

This synchronized approach bridges network visibility with policy automation, allowing enterprises to maintain continuous security posture alignment across their IT, OT, and IoT environments.

Use Case 1: Automated Policy Enforcement for High-Risk or Untrusted Devices

Challenge: Restricting compromised or non-compliant devices without manual intervention is critical to preventing security risks and potential breaches.
How It Works: Elisity continuously monitors devices using integrations with EDR platforms to assess trust attributes such as compliance state and security posture. If a device is identified as high-risk based on predefined compliance checks or security policies, Elisity assigns it to a restricted policy group. Palo Alto Networks Firewall blocks or limits its outbound traffic, preventing unauthorized internet or cloud access.
Example: An employee laptop fails a corporate compliance check (e.g., outdated security patches). Elisity immediately assigns the device to a restricted policy group. The firewall blocks all outbound traffic except for IT support resources, allowing the user to remediate the issue without risking broader exposure.

Use Case 2: Securing Guest Wireless Traffic & Enforcing Least Privilege Access

Challenge: Guest and BYOD devices often connect to corporate Wi-Fi, creating a potential security risk if they have unrestricted access to internal resources.
How It Works: Elisity automatically identifies guest and BYOD devices and assigns them to a guest policy group. Palo Alto Networks Firewall enforces network segmentation, ensuring these devices can only access approved services. Elisity prevents guest devices from reaching corporate assets at the access layer, while PAN FW restricts their North-South traffic.
Example: A visitor connects their laptop to the guest Wi-Fi. Elisity automatically classifies it as a guest device and ensures it can only reach the internet and a company-specific portal for event registration or restricted SaaS apps. No access to internal servers, sensitive data, or employee systems. PAN FW further ensures guests cannot initiate outbound connections to restricted destinations.

About Elisity

Elisity is a leap forward in network segmentation architecture and is leading the enterprise effort to achieve Zero Trust maturity, proactively prevent security risks, and reduce network complexity. Designed to be implemented in days, without downtime during implementation, the platform rapidly discovers every device on an enterprise network and correlates comprehensive device insights into the Elisity IdentityGraph™. This empowers teams with the context needed to automate classification and apply dynamic security policies to any device wherever and whenever it appears on the network. These granular, identity-based security policies are managed in the cloud and enforced across enterprise environments in real-time, even on ephemeral IT/IoT/OT devices, using your existing network switching infrastructure. Founded in 2019, Elisity has a global employee footprint and a growing number of customers in the Fortune 500.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. For more information, visit www.paloaltonetworks.com.