



MULTICLOUD CONNECTIVITY AND SECURITY WITH A DIGITAL EDGE CONTROL FRAMEWORK

EQUINIX WHITE PAPER



Introduction.....	3
Digital disruption creates security challenges	4
IOA® and DECF	6
Access control and segmentation security control function.....	8
Common deployment scenarios.....	10
Summary	13

INTRODUCTION

Technology and infrastructure transformation are already changing modern business, critical strategies and support of new business initiatives. The adoption of social, mobile, analytics and cloud technologies—with measurable business value outcomes—are all driving new enterprise strategies and tech transformation initiatives. This transformation is due, in part, to the explosion of a more autonomous, intelligent edge, where the focus is shifting to edge computing and managing the architecture of applications and data from the cloud to the edge.

Beyond that, the convergence of multiple clouds demands a natural extension of corporate boundaries for today's digital business to where users and data reside. Those boundaries are where companies can manage real-time engagement with customers. It's where social, mobile, analytics and cloud technologies engage together and where on-demand insights enabled by the big data explosion will need to be enabled and managed. Where these worlds meet is the new “digital edge.”

IT-led growth and opportunity are driving enterprises to evolve their architectures

As a result of these trends, IT-led growth and opportunity are driving enterprises to evolve their architectures. To successfully make this transition, organizations are realizing they need a digital edge strategy that places strategic control points next to users, clouds and networks. Enterprises that evolve their architectures toward this digital edge need effective security and privacy safeguards at the front ends of both their internet and internal worlds. They also need to own the security of their applications and data and maintain company and government compliance regulations.

DIGITAL DISRUPTION CREATES SECURITY CHALLENGES

To deliver security and privacy safeguards, enterprises need to implement similar controls that have previously existed onsite or in an enterprise's private domain, but do so in a cloud-oriented approach to establish a strong security posture at all levels of the architecture. A new set of security guardrails and a "trust nothing" (i.e., zero-trust) model are required to protect enterprises as this transformation takes place. These new security guardrails must be implemented in a neutral location, with proximity to users, data and content, with high availability and reliability.

To accomplish these objectives, a security strategy that safeguards the enterprise at the edge must include:

- Awareness and visibility into ingress and egress traffic that traverses the network as well as traffic within the enterprise environment
- Integrated control and management of that traffic via policy enforcement
- Placement of and access to key data

Each of these requirements is discussed below.

a. Awareness and visibility

Historically, an application was a single piece of software running on a data center server or user PC. But today's applications are more likely to be distributed combinations of interconnected and automated components from multiple sources or vendors. These applications are deployed in a central or regional colocation data center, a cloud service infrastructure and/or across a multicloud environment and within SaaS-based services.

These application components, and the continuous interactions among them, have become quite complex over time. As a result, they require dynamic and adaptable approaches to traffic monitoring, along with algorithms that yield security insight, detect intrusion and automate effective responses when threats are detected. This leads to the need to monitor, log and evaluate all traffic across network segments, cloud services and applications as well as within the enterprise perimeter, which is a new requirement for the IT architecture.

By deploying distributed monitoring capabilities and automated event processing at the edge, enterprises will be able to meet this requirement. They will see all traffic traveling across network segments, cloud services and applications, and within the enterprise. This will enable them to identify security threats that can then be acted on in real time.

b. Integrated controls and management

Converting the visibility into relevant action is critical. This takes place through the enforcement of ubiquitous security policies across all enterprise domains, including on-premises capabilities, SaaS applications, cloud workloads and network services. It is important to point out that, while an unlimited number of new security policies can be created, consistently enforcing them throughout the organization is not so easy—especially since much of the data and user activity to which organizations need to apply those policies is outside of their security perimeter and is not visible. It may be known that incidents are occurring, but there is no broad enforcement capability (other than manual processes) to identify and stop them. As digital transformation drives more SaaS application and cloud workload usage, consistent policy design and enforcement across these new domains is critical.

Enterprises need to place their security policies at the edge, as enforcement needs to take place in real time and at the closest point to where most attacks are likely to be initiated. Along with improved performance and scalability when applying these controls, security policies can then be adjusted, also in real time, for the constantly changing nature of enterprise applications.

c. Data placement and access controls

The center of data gravity is moving. Large-scale enterprise data (structured or unstructured, at rest and in transit) is now not just within a centralized corporate data center or in the cloud. Enterprises are now placing data at the edge—where it is generated—to keep it closer to the users and applications of that data.

Movement of this data to the edge requires careful design. Beyond ensuring proper management and distribution of this data, considerations need to be given to data security and privacy. Architects need to design solutions that mask data from potential exposure and ensure proper access controls to that data. Sensitive data should be moved to the edge with encryption in place, as well as access controls to ensure only authorized users and systems have access to that data.

Interconnection Oriented Architecture® (IOA®) and Digital Edge Control Framework (DECF)

To meet the security challenges mentioned above, enterprises should consider evolving their architectures by deploying new enterprise hubs and connecting to clouds. Places with rapid and abundant interconnection possibilities are used as the foundations of these architectures. This interconnected approach is termed an “Interconnection Oriented Architecture,” which includes a set of reference designs, best practices, use cases and roadmaps into an architecture framework that enterprises can use to embark on their transformation.

The evolution of the digital edge into an IOA also mandates a new architectural construct around security that meets challenges of awareness and visibility, integrated controls and management, and data placement and access controls. This architectural construct needs to include a set of security capabilities or control functions that provide traffic visibility, data management and control, and simplified policy enforcement across all domains while establishing a command point in a zero-trust security model.

Equinix is terming this architectural construct a Digital Edge Control Framework (DECF). The DECF contains a roadmap to implement security control functions based on digital transformation best practices and all of the functions and capabilities necessary for an enterprise to support cloud resiliency, agility and controls across multiple public cloud providers, SaaS providers, network service providers and on-premises deployments. DECF enables enterprises to establish distributed visibility and control of data at the cloud edge, segment and provide boundary controls of cloud traffic, and help solve regulation, sovereignty and compliance issues. The DECF also acts as a fallback position in the case of a breach, and enterprises will build up their transformed infrastructure around neutral points of connectivity (what Equinix calls Performance Hub™). Controls within the DECF will also be located or connected at these hubs.

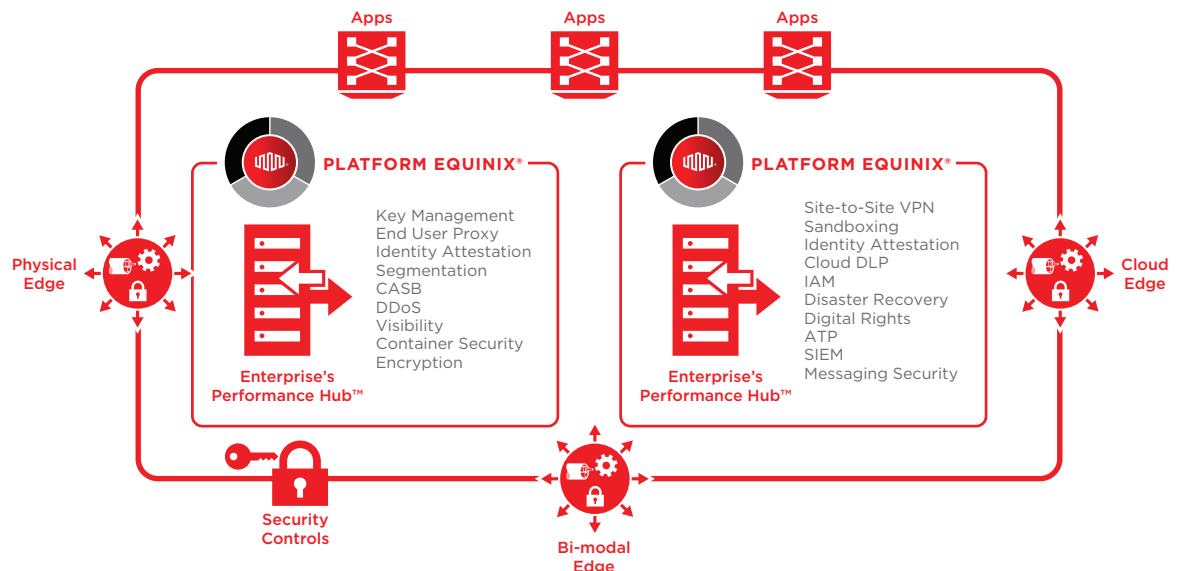


Figure 1: High-level schematic of IOA and DECF architectures

The roadmap for an enterprise digital transformation typically starts with deploying network security functions to strategic interconnection control points and relocating content and services to colocation facilities. The enterprise does this by choosing physically secure locations closest to its users and data, aggregating connectivity and driving traffic through a newly established checkpoint. At this zero-trust checkpoint, the enterprise should consider implementing specific security control functions that establish a security perimeter, segment the network, enable secure message exchange and establish access controls.

Next, the enterprise will typically consider integrating multiple clouds and data controls by implementing a common identity and encryption strategy, privately storing sensitive data and encryption keys and integrating security controls with application infrastructure. To accomplish this, the enterprise can implement security control functions for cloud-agnostic key management systems (KMS), Distributed Denial of Service (DDoS) detection and mitigation, identity and access management (IAM), security information and event management (SIEM), data loss prevention, data encryption, inbound/outbound security proxy and digital rights management. Equinix is working to provide best practices and best-in-breed solutions to enable enterprises to deliver these controls at the edge.

Lastly, the enterprise should consider enabling full digital business by scaling globally and building trust through dynamic user and entity behavior analytics; unifying security and risk metrics across ecosystems; service chaining and workflow optimization; and automating security threat detection and response.

The premise behind the proposed strategy is not only to explore newer, or next-generation, security control functions (which are now designed for multicloud integration), but also to implement these control functions in a way that is designed for continuous change.

Equinix has partnered with Palo Alto Networks to perform functional testing for one of the security control functions of the DECF and the fundamental aspects of zero-trust: access control and segmentation.

ACCESS CONTROL AND SEGMENTATION

SECURITY CONTROL FUNCTION

It is well-established that access control and segmentation is an effective strategy for improving an enterprise's security posture and reducing risk. When implementing this for traditional networks, the Palo Alto Networks Next Generation Firewall (NGFW), in combination with Equinix Cloud Exchange Fabric™ (ECX Fabric™), provides the ability to apply multiple levels of separation based on network topology (zones) and application.

As enterprises move workloads to the cloud and begin using SaaS applications, they need to consider how to re-segment their network to include these new workloads and applications. As this re-segmentation takes place, the enterprise needs to:

1. Ensure these new segments are incorporated into its existing infrastructure
2. Place NGFWs performing the segmentation at the digital edge, within Equinix Performance Hubs

To create new segments for cloud workloads and SaaS applications, the enterprise must move beyond the traditional, broadly defined trusted and untrusted segments it has previously constructed and apply new security policies. To accomplish this, the enterprise needs to implement security zones.

Security zones take traditional network segmentation one step further, allowing an enterprise to move beyond the traditional trusted and untrusted concepts toward a more logical approach based on the specific enterprise environment. As Palo Alto Networks defines it, "security zones are a set of interfaces that can be used to control and monitor inter-zone communications, control management access into, out of, and within a zone, and enforce data confidentiality and integrity rules for data within and to/from a zone." These zones are normally configured in a zero-trust model, which means that the default permissions are to deny access to systems (based on application and user identity), unless expressly permitted otherwise.

Applying the concept of security zones to the cloud, an enterprise environment might be broken down as shown below:

- A public cloud zone with access to workloads and services in cloud service providers such as AWS, Azure, Google Cloud, etc., with multiple vNETs or VPCs coming back through Performance Hubs—where these clouds come together
- An SaaS zone with access to services such as email and collaboration services like Office 365, customer relationship management services, corporate expense services and much more. A Cloud Access Security Broker (CASB), sitting between the NGFW and cloud services, provides visibility of traffic and user controls to set policy context on how corporate users can access those applications. Some SaaS applications may only be reachable via the internet, while others can be accessed exclusively via private connectivity or a combination of the two
- One or more DMZs which separate the internal network from the internet and other untrusted networks
 - Internet-facing services are placed within the DMZ, including web, mail, DNS FTP and sometimes VoIP
 - Branch offices are often connected via a DMZ in situations where they need their own internet access but also access to internal corporate resources
- An Extranet zone (sometimes part of the DMZ), which enables external partners and stakeholders to access the content and functions of an intranet
- An internet zone, which only permits inbound access to the DMZ zone(s), but never to the other zones
- A separate zone for management and operations, which will include functions such as bastion hosts, jump systems, monitoring servers and patching update systems. This zone can reach everything inside the perimeter
- Remote and corporate user access. These users typically have access to not only the internet, but to an SaaS zone, cloud service providers and internal corporate resources

An example of these zones being configured for access control purposes: When layered on top of an SaaS security zone, the Palo Alto Networks NGFW can be configured with a policy such as “allow Box” for all corporate users based on active directory membership.

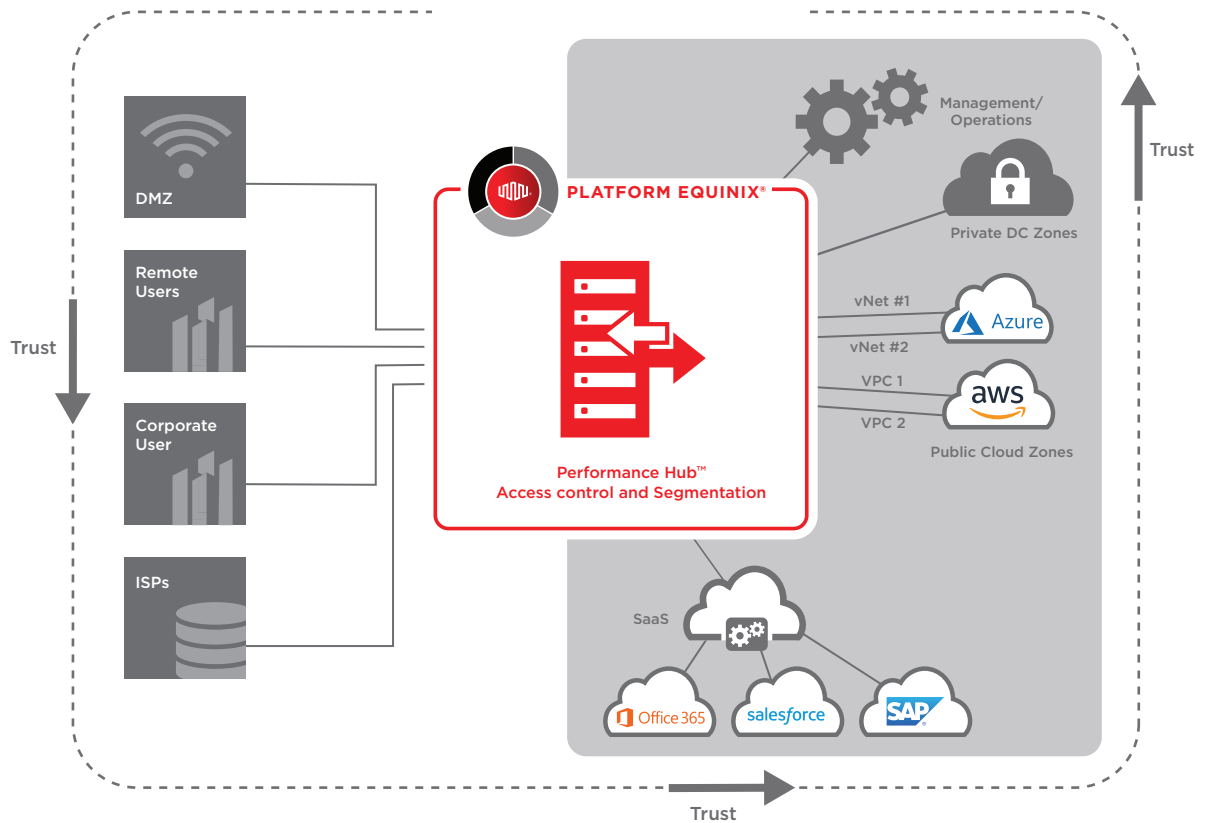


Figure 2: Multiple zones at the edge at different trust levels

COMMON DEPLOYMENT SCENARIOS

There are many different ways in which customers can leverage the DECF architecture to simplify connectivity while improving security. The three most common scenarios observed and validated by Palo Alto Networks and Equinix are outlined below.

a. Hybrid cloud connectivity using virtualized NGFWs

In this scenario, a pair of VM-Series virtualized NGFWs is deployed on AWS. This acts as both an IPsec VPN termination and a security policy enforcement point for all traffic flowing over AWS Direct Connect via ECX Fabric. As new workloads are added, BGP is used to distribute the traffic and the VPC route table is automatically adjusted to ensure traffic is secured. This scenario can also be deployed on Azure and Google Cloud Platform.

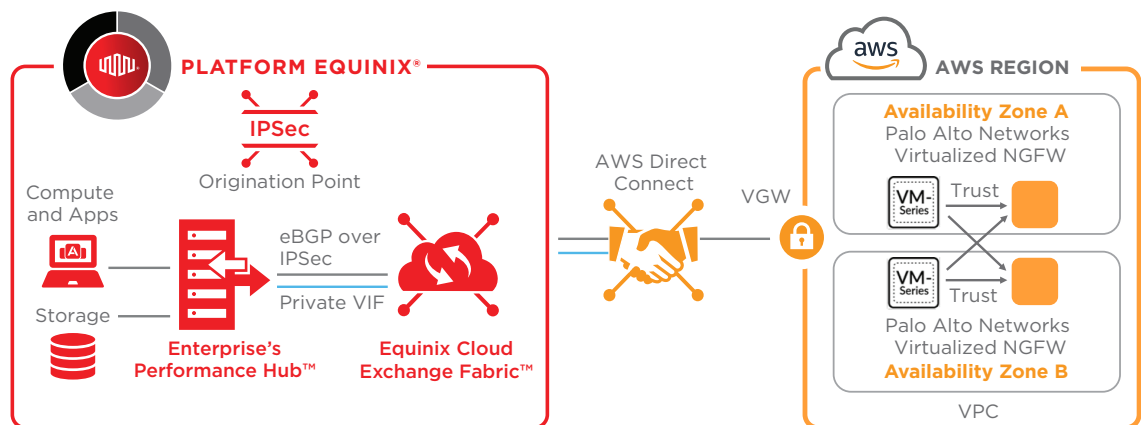


Figure 3: Hybrid cloud connectivity using Palo Alto Networks virtualized NGFWs

b. Hybrid cloud connectivity using physical NGFW appliances

In this deployment scenario, customers who are using dedicated cloud provider connections such as AWS Direct Connect, Azure Express Route and Google Cloud Interconnect (via ECX Fabric) can terminate those connections on a pair of Palo Alto Networks next-generation firewalls within an Equinix Performance Hub. Using physical implementations to secure hybrid-cloud environments has several advantages:

- **Control:** The customer has more control over its cloud environment as it owns the hardware and manages it fully
- **Performance:** High-speed lines can terminate directly on a high-performance firewall, minimizing or eliminating performance bottlenecks
- **Cost-effectively scaling security:** Customers have chosen this option because they have a large-scale cloud deployment and using a single pair of firewalls provides protection now and into the future as the deployment grows

This deployment scenario has been validated jointly by Palo Alto Networks and Equinix, where a pair of Palo Alto Networks NGFWs was deployed in an Equinix Performance Hub acting as a termination point for AWS Direct Connect. Traffic is distributed using BGP between each VPC VGW and the firewall appliances over AWS Direct Connect. This scenario can also be deployed on Azure and Google Cloud Platform.

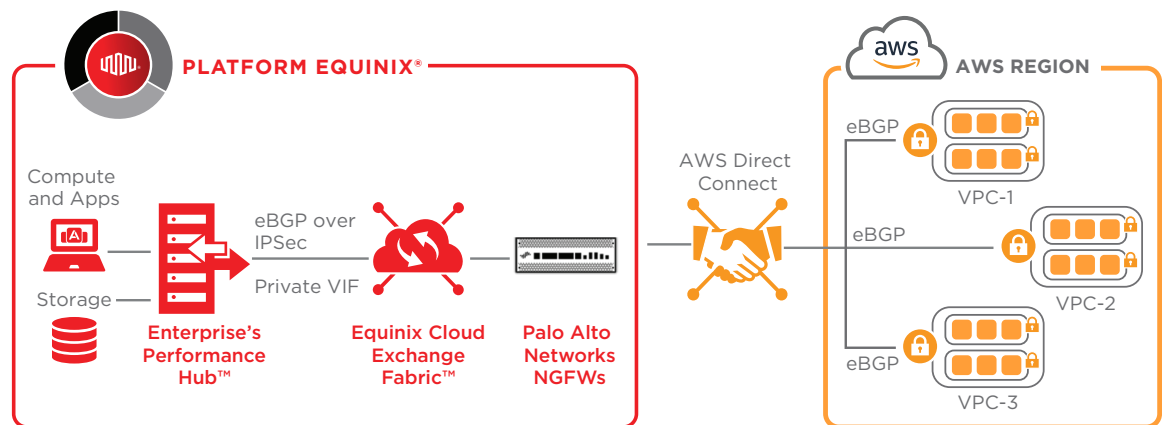


Figure 4: Hybrid cloud connectivity using physical Palo Alto Networks NGFW appliances

c. Hybrid cloud connectivity using a transit VPC

A transit VPC is a more cloud-centric approach to securing AWS deployments with many VPCs and/or accounts. A transit VPC takes a shared services approach to security and connectivity using a hub-and-spoke architecture. The hub houses IPsec VPN connectivity and VM-Series for security, along with other common services, and the spoke VPCs house workloads.

All traffic flowing to and from the spoke VPCs, across AWS Direct Connect (via ECX Fabric), will “transit” the hub VPC where it is protected from threats by the VM-Series. The transit VPC architecture is more cost-effective and easier to manage than alternative approaches of using a firewall in every VPC or backhauling traffic to the corporate firewall. Additionally, this approach allows organizations to protect a broad range of traffic flows including inbound/outbound from corporate and the internet, as well as east-west traffic between VPCs.

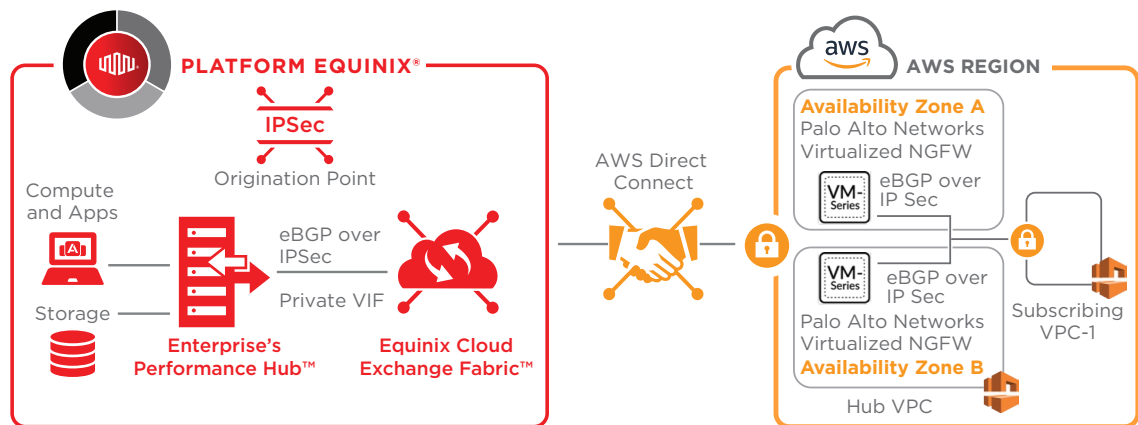


Figure 5: Hybrid cloud connectivity using a transit VPC with VM-series virtualized NGFWs

SUMMARY

Enterprises are establishing a new digital edge due to the adoption of hybrid and multicloud architectures. As a result, they need to collect, process and store data closer to creators and consumers. This has resulted in new security paradigms that need to be considered allowing for control, visibility and segmentation of cloud resources while enabling cloud agility.

The Digital Edge Control Framework has emerged as the architectural layer necessary to implement security control functions applicable to hybrid and/or multicloud environment(s). One of the first security control functions enterprises need to architect is access control and segmentation in order to create new security zones to account for cloud workloads and SaaS services. In working with Palo Alto Networks and Equinix, an enterprise customer has a set of best practices and recommendations on how to segment its networks and provide connectivity to cloud service providers in this new architecture.

Please contact your Palo Alto Networks Systems Engineer and/or Equinix Global Solutions Architect™ if you are interested in discussing the solutions outlined in this white paper or if you are in the process of designing a hybrid or multicloud strategy.



Corporate HQ

Equinix, Inc.
One Lagoon Drive
Redwood City, CA 94065
USA

Main: +1.650.598.6000
Email: info@equinix.com

EMEA

Equinix (EMEA) BV
Rembrandt Tower
Amstelplein 1
1096 HA Amsterdam
Netherlands

Main: +31.20.754.0305
Email: info@eu.equinix.com

Asia-Pacific

Equinix Hong Kong Limited
Units 6501-04A & 6507-08, 65/F
International Commerce Centre
1 Austin Road West
Kowloon, Hong Kong

Main: +852.2970.7788
Email: info@ap.equinix.com

Palo Alto Networks

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
USA

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

About Equinix

Equinix, Inc. (Nasdaq: EQIX) connects the world's leading businesses to their customers, employees and partners inside the most-interconnected data centers. In 52 markets across five continents, Equinix is where companies come together to realize new opportunities and accelerate their business, IT and cloud strategies. In a digital economy where enterprise business models are increasingly interdependent, interconnection is essential to success. Equinix operates the only global interconnection platform, sparking new opportunities that are only possible when companies come together.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks and mobile devices.