



EQUINIX

ACCESS CONTROL AND SEGMENTATION IN AN INTERCONNECTION ORIENTED ARCHITECTURE™

DISTRIBUTED SECURITY SOLUTION BRIEF

CONTROL FUNCTION SERIES

ACCESS CONTROL & SEGMENTATION

Executive overview

Enterprises seeking to realize the full potential of the cloud are on a cloud transformation journey that requires shifting infrastructure from a siloed and fixed state to one that is agile and dynamic. The **IOA® Playbook** offers a compelling strategy for how to do this with Equinix Performance Hub® on Platform Equinix®. By establishing a hybrid or multicloud architecture at one or more platform colocation sites, legacy private data centers can connect to multiple public clouds and SaaS providers supporting multiple network segments (e.g., VLANs). Security functions, including access controls and network segmentation, can be distributed to solve scale and integration challenges, as seen in the **Distributed Security Digital Edge Playbook**.

Access control and segmentation

Controlling network access and segmentation is a well-defined practice. However, as data, applications and users become more distributed, multiple clouds for workload and SaaS-based IT application delivery are needed. As a result, visibility suffers and traffic transiting high-risk boundaries between enterprises and clouds becomes more vulnerable. Ultimately, the enterprise network becomes untrustworthy. To mitigate—or better, eliminate—these effects, network segmentation and access controls must be enhanced and security zones established, particularly for cloud and SaaS applications.

Network Access Control and Segmentation (AC&S) is a class of security controls that inspects network traffic attributes and selectively permits, denies, routes, switches or rewrites header parameters based on criteria in a defined policy set. Examples of these capabilities are commonly found in next-generation firewalls (NGFW) and network devices such as routers and switches, and host-based firewall systems.

In a distributed environment, basic AC&S principles including traffic inspection and the establishment of “zero-trust” zones are still viable. However, they must be strengthened with:

- **New security zones** accounting for cloud and SaaS applications.
- **A distributed fabric architecture** comprised of directly connected colocation hubs with visibility into all enterprise traffic to and from users and clouds. These hubs become extensions of the corporate network, with segmentation and access controls tailored to each region's compliance and application needs.

AC&S is one of the first control functions that customers tend to design and implement when architecting for digital business. The shift to the digital edge requires placing strategic control points beside users, clouds and networks. This can be achieved by establishing Performance Hubs within Equinix International Business Exchange™ (IBX®) data centers on Platform Equinix.

Focus areas

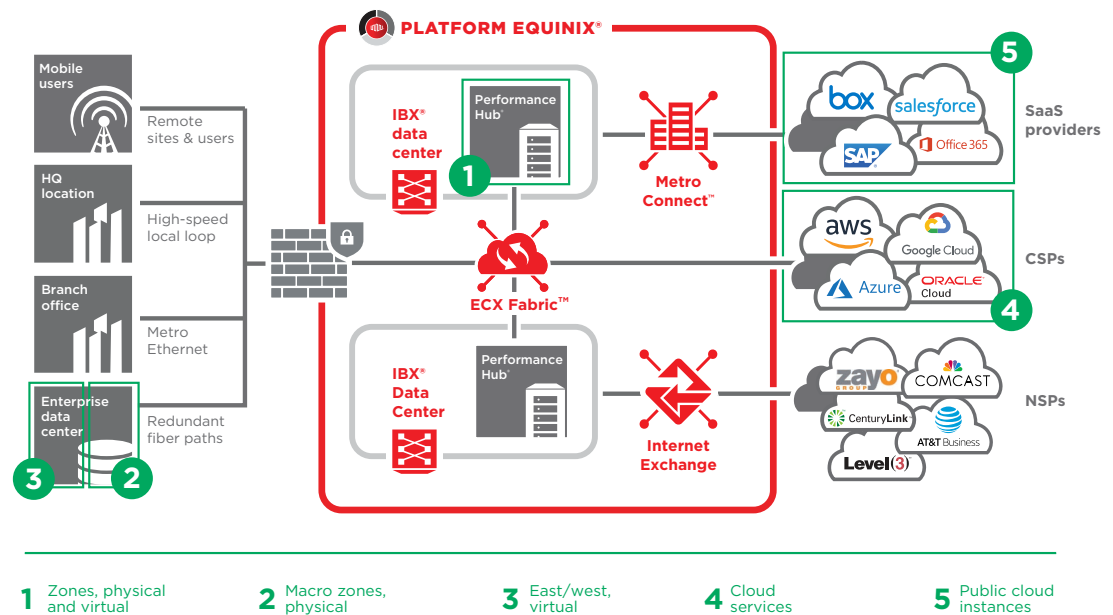
Applying the concept of security zones to the cloud, an enterprise environment might focus on the following five areas for NGFW control:

1. Performance Hub control points.
2. Legacy, private data center facilities.
3. Public clouds.
4. SaaS services.
5. Cloud services.

Interconnection Oriented Architecture®

As cloud computing accelerates, data centers must keep pace by providing flexible infrastructure that offers sufficient computing capacity and secure storage. Interconnection Oriented Architecture, or IOA, is a transformative approach to connecting people, locations, clouds and data. Essentially, it offers a roadmap to re-architecting the network for digitization.

The image below depicts a hybrid multicloud architecture in which AC&S is applied to the five areas listed above within an interconnected architecture:



The Performance Hub, located at the network edge, generally serves as the outer security perimeter, where the network is commonly segmented into security zones. This is the ideal location for an AC&S implementation—not only because it's where various points intersect, but also because low latency between zones improves performance.

An IOA strategy recommends creating an inspection zone with control points (described in step two of the IOA Security Blueprint) that examines traffic flows locally—as opposed to backhauling traffic to a centralized location. In this zone, interactions are scanned for flaws as applications and business processes become more distributed, granular, mobile and automated.

This configuration enables policies to be applied to traffic that is flowing between security zones. The AC&S function enforces local policy between these security zones. NGFWs, including network devices that implement an access control list (ACL), are commonly used to segment security zones and further enforce policy, creating the boundary control and inspection zones described in steps one and two of the Security Design Pattern.

Applied security zones

Common examples of applied security zones include the public internet, a company's demilitarized zone (DMZ), vendor and partner DMZs, remote users, and corporate internal systems and users. Some security zones may extend back to certain app-processing and data store layers, as well as application group zones, within legacy private data centers. Others may extend back to corporate offices, such as the corporate LAN user zone. Management or operations zones often extend back as well.

Security zones may be created within a Performance Hub that overlays virtual network segments defined in a public cloud service provider (CSP) environment (e.g., VPC, VNet, VCN, etc.). One possible design requires CSP network segment traffic to return to the colocation control point for inspection before continuing to the destination segment in the same or a different CSP environment. While cost and performance implications must be weighed, this architecture delivers a control point that standardizes security control functions, including AC&S policy enforcement and operations, across a distributed architecture comprised of one or more CSPs.

SaaS applications and virtual machines

Many architectures will have both SaaS applications and virtual machine (VM) farms deployed within an Equinix Performance Hub. Segmentation may be used to separate traffic to and from SaaS providers and/or VM farms to ensure policies are enforced between different SaaS applications and virtual applications running within the hub. One or more security zones may be created and can include a combination of SaaS services and virtual applications, depending on the policies required.

In some cases, VM farms may be protected by virtual firewall functionality enabled on virtual switches in each host. AC&S provides visibility of east-west traffic on a given host or between hosts, allowing traffic to be inspected and policy enforced within the virtual environment. The traffic need not be sent out to the physical network to be inspected and then returned to the virtual environment—often referred to as “hair-pinning” or “trombone-routing.”

Some approaches may also enforce micro-segmentation and access control at a VM's virtual switch network interface controller (NIC). The Performance Hub in the colocation center allows access control within the colocation node, serving as the enterprise's extension of the data center and preserving the ability to segment within and across the two sites. This connection is segmented by VLANs, so that security zones that exist in both the legacy data center and the colocation node can be maintained simultaneously.

For example, a firewall could forward data flows associated with a specific security zone to the legacy data center via an interface bound to a VLAN. This VLAN maintains the separation of traffic between the security zone and other zones. At the legacy data center, a firewall could receive the flows on an interface associated with the security zone, inspect it and then forward it on. In this way, security zones can be extended between legacy and edge facilities. A company may implement similar security zone extensions for zones destined for corporate campuses/offices in the region. Such zones may include corporate LAN users or zones designated for management/ops.

In addition to the security zones shared with the Performance Hub at the edge, the legacy data center may have zones that live only in the data center. Examples include zones for app-processing servers, data stores and more.

As seen with VM farms housed in a Performance Hub at the edge, VM farms in a legacy data center location may employ a virtual firewall, as described above, to gain visibility and control of data flows traveling to/from the VM farm. Micro-segmentation enforced down to the VM level allows security policies to be tied directly to applications.

For virtual instances running in CSP environments, micro-segmentation and policy enforcement can be achieved using artificial intelligence (agents) technology that learns and automates procedures and processes. With agents running in the OS/kernel of every virtual instance, a controller distributes the access control policy to each agent, and enforcement occurs on the instance itself. This approach provides east-west visibility and policy enforcement for all traffic inside a CSP virtual network segment, as well as between segments. This cloud-neutral approach can be deployed regardless of where the instance runs, whether in a public or private cloud or a legacy or colocation facility.

Cloud access security broker

For SaaS services, AC&S may be achieved using a cloud access security broker (CASB) system. First, a CASB reveals which SaaS providers are being accessed by the user population, whether authorized or not (revealing shadow IT). Second, a CASB permits security policies to control end-user access to and from cloud services and applications, including applying fine-grained control over operations users can perform within each cloud service/app, and the data they can access, post and edit. Additional CASB security features will be covered in a forthcoming control function brief dedicated to CASBs.

When a CASB is implemented as a physical device, it is commonly placed in its own security zone within a Performance Hub. This is particularly true when situated inline with forward and/or reverse proxy enabled, such that end-user traffic bound for cloud services flows through it. When a CASB is implemented as a cloud service itself (assuming end-user traffic is being engineered through the Performance Hub control point), an Equinix Cloud Exchange Fabric™ connection to the service can significantly improve performance for end users.

Element managers

Element managers are either physical appliances or software on a customer-controlled host. Situating element managers in a Performance Hub provides the lowest latency and highest availability to reach the AC&S enforcing elements.

Commonly, element managers are situated in a management/ops security zone. Log servers for these element managers (e.g., RESTful API queries, Syslog, SNMP, etc.) may also be placed within a Performance Hub, enabling real-time analysis to be quickly performed locally or via cloud analytics services.

Conclusion

As data is increasingly distributed to multiple digital edge locations, the traditional, centralized data center model becomes obsolete, unable to provide the security controls needed for digital business. New IT infrastructure and security paradigms allow for control, visibility and segmentation of cloud resources and enable cloud agility. An IOA approach to AC&S is necessary to ensure security control functions apply to hybrid multicloud environments.

Where to get help:

For more information on how AC&S applies in your environment, please contact your local account team.

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
65/F International Commerce Center
1 Austin Road West
Kowloon, Hong Kong

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

About Equinix

Equinix, Inc. (Nasdaq: EQIX) connects the world's leading businesses to their customers, employees and partners inside the most-interconnected data centers. On this global platform for digital business, companies come together across more than

50 markets on five continents to reach everywhere, interconnect everyone and integrate everything they need to create their digital futures.