DATA SHEET

Securing Workload Communications with Cloud Connector

Simple, secure access for workloads to the internet and private applications with a direct-to-cloud architecture.

Advance network communications for the cloud

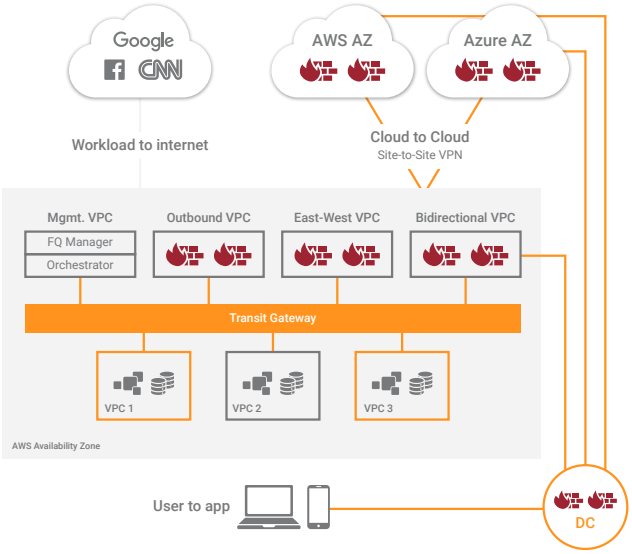
As workloads move to the cloud and users become increasingly mobile, organizations have an urgent and compelling need to transform their networks to ensure business competitiveness. It is no longer feasible to extend legacy networks and apply perimeter-based security using firewalls. For organizations modernizing their infrastructure, ensuring effective workload communications has become a foundational requirement. Cloud Connector from Zscaler has completely re-imagined workload communications to deliver simple, secure access for workloads to the internet and private applications. Unlike legacy network security, Cloud Connector uses a direct-to-cloud architecture, which builds on the proven Zero Trust Exchange platform from Zscaler. Customers gain numerous benefits including better security, simpler operations, more visibility, higher availability, improved performance and lower costs after adopting Cloud Connector to transform their networks.

Workload connectivity challenges with legacy network security

When organizations attempt to connect workloads to the internet or to their other applications in public cloud or data center environments, they face a number of challenges when using legacy network and security architectures, including:

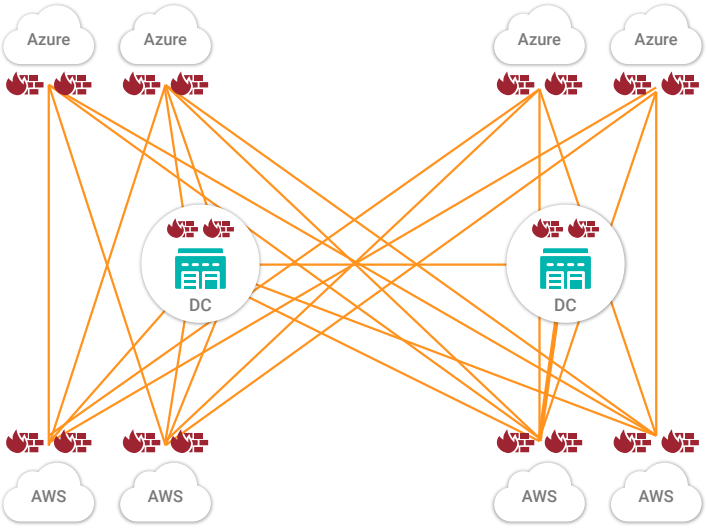
- **Increased risk of lateral threats and internet-based attacks** from using legacy network-centric connectivity solutions such as cloud VPNs, site-to-site VPNs, firewalls or WAN technologies, which overextends a customer's trusted network across the internet to other clouds and on-premise environments to increase network attack surface. A patchwork of security appliances, tools, and non-standard policies increase security risks because of gaps in security coverage that are both known and unknown.
- **Escalating complexity** due to complicated route filtering, multiple network hops, virtual appliances for networking and security, and fragmented policy management from introducing these legacy models to the cloud. Reining in this complexity is a difficult task for security teams as they struggle to enforce standardized workload connectivity and security policy across multi- and hybrid cloud environments.
- **Lack of visibility** across the application connectivity paths creates network and security blind spots. Cloud workloads have become more distributed and environments have increased in scale. Connecting these distributed workloads requires obscure multi-hop networks and "daisy chaining" with multiple network and security appliances. This complex connectivity and a lack of centralized logging, leaves operators blind to application communications.
- **Poor performance and scalability** due to the increasing number of network and security services within public cloud environments, traffic hairpinning and chokepoints for centralized security inspection and control.
- **High costs** due to legacy network security appliances (e.g., firewalls, IPS, routers, and other point products), overprovisioning of network services to compensate for lack of scalability, and increased use of cloud native services such as transit peering.

Legacy: Extend Corporate WAN to the Cloud



Expensive, Operational complexity, Slow user experience,
Poor security due to lateral movement over the WAN

For multi-cloud, complexity and risk grow multi-fold



A mesh of site-to-site VPNs (workforce, partner, devices, customers)
Increased attack surface and risk of lateral threat movement

Corporate network Public Internet

Corporate network

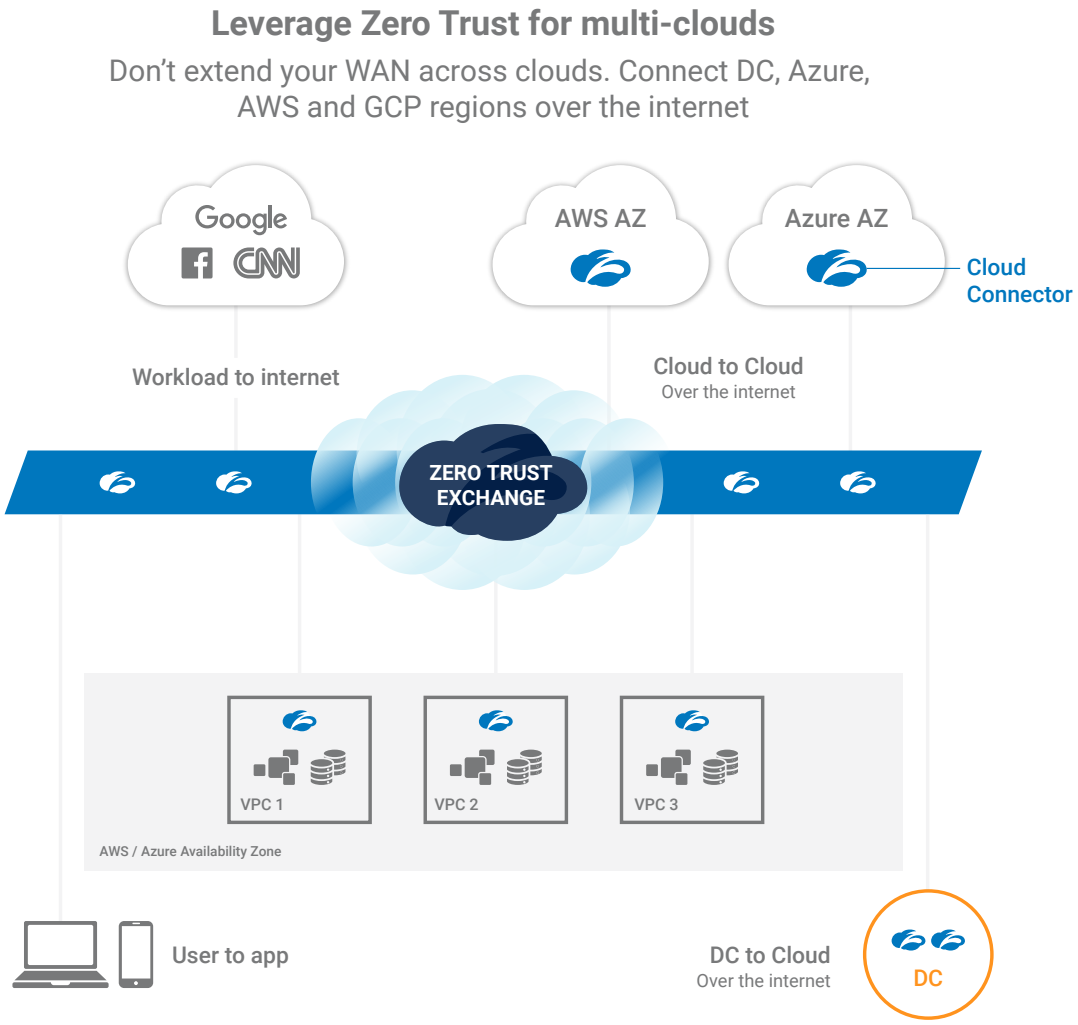
Cloud Connector brings zero trust access for cloud workloads

Cloud Connector provides workloads fast and reliable access to the internet and private applications with a direct-to-cloud architecture, which provides high security and operational simplicity. Cloud Connector eliminates network attack surface by directly connecting workloads to the internet and to private applications using a full proxy architecture. Furthermore, this architecture dramatically simplifies workload communications by eliminating routing, VPNs, transit gateways, transit hubs, firewalls, while allowing for flexible forwarding, and easing policy management by using the proven ZIA and ZPA policy framework.

The direct-to-cloud architecture is only made possible by using the Zero Trust Exchange. Cloud Connector directly forwards all workload communications to the Zero Trust Exchange where either ZIA or ZPA policies can be applied for full security inspection and access identity-based control of workload communications. From the Zero Trust Exchange, the communications are then forwarded to any destination, whether it be the internet or other private applications in a public cloud or an on premises data center. This unique approach provides three key advantages:

- Moves away from network-based VPN connectivity to identity and application-based communication for true, zero trust security
- Eliminates the legacy castle-and-moat architecture without compromising security; no need for legacy products such as Squid proxies, NAT gateways, IPSs and so on
- Provides distributed, scalable connectivity wherever it is needed but centralizes and automates policy management to simplify workload communications

Cloud Connector is well-aligned to help an organization meet its network transformation priorities in several ways. It extends workload-to-workload connectivity, using zero trust principles, across disjointed networks and multiple clouds, including AWS regions, Microsoft Azure, Google Cloud and on-premises data centers. Cloud Connector also delivers secure internet access for workloads in public clouds and data centers. And all these capabilities are delivered via a unified policy plane for traffic forwarding, security and zero trust access across these heterogeneous environments.



Cloud Connector advantages

Simpler deployment, without complicated network configurations. Traditional approaches require complex routing configurations through transit gateways, transit hubs and SNAT which need to be repeated for every VPC and across every cloud. In contrast, all that Cloud Connector needs is a default route to the internet. Policy management for traffic forwarding and security is centralized and standardized in the Zero Trust Exchange regardless of the source or destination of the workload communications.

Full visibility, end to end, with direct-to-cloud connectivity. The old way relies on obscure, multi-hop networking making it very difficult to understand how traffic flows. Moreover, logging is scattered across multiple network products. Because Cloud Connect connects directly to the cloud, operators gain full visibility and control over how workloads communicate. Logging is centralized and streamed in real time. Logs can be exported to a SIEM or a monitoring solution of your choice for correlation and analysis.

Hyper scalability, with no centralized chokepoints. Legacy architectures require all traffic to be funneled through centralized infrastructure, involving transit gateways, hubs and virtual firewalls which lack the elasticity and scale to handle surge throughputs. The modern Zero Trust Exchange architecture, operates at hyperscale across over 150 global data centers, and handles any increase in communications with elastic, horizontal scaling.

High availability without unnecessary replication of services. Existing approaches require a complex availability architecture of multiple firewalls and networking configurations that need to be replicated over multiple zones, regions and clouds. Cloud Connector's direct-to-cloud architecture dramatically simplifies cloud configuration requirements because all the required services are transparently provided in the Zero Trust Exchange, at scale. At the customer's site, automatic failover with N+2 redundancy is provided for forwarding and security.

Reduced costs with streamlined services delivered by the Zero Trust Exchange. Customers no longer have to overprovision services and pay for idle time of firewalls, transit hubs and NAT gateways, replicated across every cloud environment which quickly add up. With Cloud Connector, there are no hidden costs and customers are only billed for consumed security services and not for networking or access. No need to pay for virtual firewalls or proxies in the customer environments.

Cloud Connector unique value

Cloud Connector is built on Zscaler's Zero Trust Exchange, which securely connects users, devices, and apps using business policies over any network and across any cloud, at scale.

- Application workloads are connected directly to each other, independent of the underlying corporate network, VPN or WAN.
- Applications are invisible to the outside world and have no attack surface
- Purpose-built, multi-tenant proxy architecture holds, inspects and enforces policy
- High performance inspection is done by a single-scan and multi-access architecture that is built for scale
- Fine-grained forwarding policy management for internet & non-internet traffic, using Zscaler Internet Access or Zscaler Private Access policies
- Unified, standardized policies across AWS, Azure, Google Cloud and on-premises data centers. This includes managing policy, monitoring traffic, tracking logs

Cloud Connector use cases

Digital transformation

As organizations migrate their applications to the cloud, and build cloud-native applications, the on-premises models for networking and security get broken. Digital transformation necessitates a network transformation, which ushers in a new model for workload communications; a model where workloads communicate with any destination securely and independently from the underlying network. Cloud Connector is purpose built to enable digital transformation.

Workload connectivity without VPNs

Organizations can now directly connect workloads to private applications without extending their WAN or rely on VPNs, which increases network attack surface.

Zero trust mandate

Zero trust assumes that the network has been compromised and can no longer be trusted. In this scenario, Cloud Connector directly connects workloads to the internet or to private applications without connecting networks. Every connection is monitored and logged for audit purposes.

Securing cloud workload access to internet

Workloads can be considered a mirror image of users. Just like users, workloads can be directly connected to the cloud via Zscaler Internet Access and benefit from the same policy framework, security inspection and access control. Virtual firewalls are not required.

Mergers and acquisitions

Merging two disparate networks is incredibly challenging and time-consuming. Problems range from IP overlaps, to routing issues to increased security risk from enlarged network attack surface when two networks are combined. With Cloud Connector, networks do not need to be merged. They can be kept separate and workloads from one environment can surgically connect to private applications in another environment quickly and without disruption.

Branch connectivity

Connecting branch applications to private applications or to the internet has become a lot easier with Branch Connector, which is an on premises version of Cloud Connector. Branch Connector complements SD-WANs and Zscaler partners with all the major SD-WAN vendors.

Capabilities fact sheet

Zero touch provisioning and automated deployment

- Zero touch provisioning with system defined templates for AWS and Azure
- Fully automated deployment (AWS CloudFormation, Azure Resource Manager Templates and Terraform)
- Dynamic discovery of customers Geo-regions, Availability zones, VPC/VNETs
- Built-in SLA monitoring and failover
- Available on AWS and Azure marketplaces

Granular forwarding policy for internet and non-internet traffic

- Options to send the traffic to ZIA, ZPA or Direct (bypassing Zscaler services)
- Flexible traffic selection criteria location, sub-location, location group, 5 tuple or FQDN
- Built-in availability with seamless failover to next available service pop

Unified policy for forwarding and security with Cloud Connector and ZIA

- Locations are created dynamically for the VPCs/VNETs
- Dynamic cloud connector locations are synced into ZIA platform
- Locations created by cloud connectors are like any other existing ZIA location. Any and all security policy can be enabled, including IPS, SSL proxy, url filtering, data protection

Unified zero trust policy for user to servers and server to server

- ZPA delivers a unified policy for user to application and server to server
- Existing ZPA policy is enhanced to include new client type (Cloud Connector) to support server to server connectivity
- Cloud Connector groups created for forwarding traffic in AWS, Azure & Datacenter are synced to the ZPA platform

Unified policies, control and management across AWS, Azure & Branch Connectors

- Cloud delivered centralized dashboard for device health and traffic monitoring
- Filtering available for Azure, AWS & Branch deployments
- Time series for flow count & byte count for ZIA, ZPA, Direct, DNS

Consolidated logging infrastructure for all all types of traffic

- Detailed session logs covering traffic going to ZIA, ZPA and direct (Zscaler bypass)
- All DNS transactions are logged for both public and private DNS
- Fully integrated with NSS infrastructure, existing NSS firewall VM can be used to stream the logs to SIEM

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com