Dimension Data Cloud
Technical Security Overview

The Dimension Data Managed Cloud Platform (MCP) provides a secure and scalable cloud computing platform with a network-centric design with multiple layers of security for delivery of Compute-as-a-Service (CaaS).

Using our network-centric model and a Defense-in-Depth security architecture approach, the Dimension Data MCP allows clients to create dedicated layer-2 networks and control communication into and out of these networks. Virtual server resources can be quickly brought online and taken offline, allowing for elasticity in resources consumed and costs borne by clients.

This technical white paper is intended to answer questions regarding how security is maintained in our multi-tenanted and dynamic environment. It includes direct statements on how the MCP solution is secured, as well as more direct questions likely to be asked. Lastly, we provide guidance on good security practices for clients using the MCP solution.
Security overview

The Dimension Data Managed Cloud Platform™ (MCP) is our platform for the delivery of public and private enterprise-class cloud services. The MCP provides a secure environment for clients to operate their information systems, built from the network up using dedicated physical networks and enterprise grade security controls on best of breed hardware and software, with full N+1 resiliency across the entire stack.

At the core of the MCP is the Dimension Data CloudControl™ orchestration and management interface. Clients perform all cloud management activities via the web user interface or application programming interface (API). The CloudControl orchestration systems strictly control the actions taken by clients, ensuring that all management requests only affect the systems managed by that client.

Permanent protection

Dimension Data performs 24x7 security monitoring and management of all CloudControl systems, ensuring security of all clients is maintained. The CloudControl systems are protected by multiple layers of security including Intrusion prevention and denial of service (DoS) protection. Penetration tests are also performed against the CloudControl systems by external testing firms, to ensure that there are no remotely exploitable vulnerabilities in the management systems.

Multi-tenanting protection

Each MCP client is allocated its own networks and virtual servers and clients are segmented from other clients using enterprise grade network segmentation. The Dimension Data CloudControl management systems ensure that clients cannot access networks and systems owned by other clients, and CloudControl presents no ability to bypass the management interface.

By enforcing multi-tenanting separation in the orchestration layer, clients are prevented from exploiting the underlying control systems or making any configuration changes which could negatively affect other clients.

Client security tools

Each client has the ability to fully manage all access to their networks, restricting or allowing all communication at the IP and port level. Further, Dimension Data CloudControl allows clients to create multiple administrative user accounts, with each account granted granular control over cloud networks and virtual server systems. Using this capability, clients can enact common criteria role separation to ensure that no single administrator can change the configuration of virtual servers and virtual networks.

In order to manage the operating systems and applications of virtual servers, each client is provided with a secure IPSec-based VPN which allows them secure IP access to their cloud networks so that they can access their virtual servers without exposing them to the Internet.

The CloudControl systems are protected by multiple layers of security including Intrusion prevention and denial of service (DoS) protection.
MCP product comparisons
The Dimension Data MCP allows clients to select from any of the following options, and also mix the options together for a tailored solution.
• Public Cloud
• Hosted Private Cloud
• Private Cloud
All MCP offerings are built and operate using the same architecture and are managed using the same underlying CloudControl management infrastructure.

Public and Hosted Private Cloud
Of these options, both Public Cloud and Hosted Private Cloud use infrastructure which is located within a Dimension Data data centre. In a Public environment, cloud networks and cloud servers are deployed onto shared, multi-tenanted network, compute, and storage infrastructure with separate, client-specific layer 2 networks and customisable firewalls. In a Hosted Private Cloud CaaS environment, the compute and storage infrastructure elements are dedicated to the client’s cloud servers and cloud networks. This provides additional security risk management advantages and allows clients to customise their overall CPU, memory and storage performance.

Private Cloud
The private cloud MCP offering takes the full complement of MCP infrastructure and locates this within a client’s own data centre (or data centre selected by the client). The system behaves and is managed identically to the Public and Hosted Private MCP offerings, however all resources are dedicated to the client and run within the client’s own facility.
As the private cloud solution is located on client premises, Dimension Data cannot provide service level agreements for physical security, reliability of Internet services, power or cooling.

MCP security architecture

Resiliency
All systems within the Dimension Data Managed Cloud Platform are full resilient, using an N+1 resiliency model. This resiliency is applied to the datacentre physical power and cooling, all network equipment, all virtual server hosting systems, all storage systems, and all components of the CloudControl management environment.

Compliance
The Dimension Data MCP solution meets a number of compliance standards and is regularly audited for its compliance with SSAE-16, and European Safe Harbour requirements. Within the North America geographical region, Dimension Data also maintains PCI DSS Level 1 service provider compliance in its Managed Hosting environment for clients processing or handling payment card data.
Each Dimension Data data centre which hosts MCP systems also meets or exceeds the Uptime Institute’s Tier-3 data centre standards.

Secure facilities
Physical security
All Dimension Data facilities hosting MCP equipment are secured locations which are permanently manned by on-site guards with CCTV cameras covering the entire centre. Multi-factor biometric authentication is required for access inside the datacentre, and the MCP equipment is further segmented again within a locked cage environment, also monitored by CCTV cameras.

Power and environment
Each data centre is protected against environmental failures through the use of redundant UPS systems, backup power generation and resilient cooling configured in an N+1 redundancy configuration.

Fire detection and suppression
All MCP data centres use multi-zoned, dry pipe, water-based fire suppression systems. The air is automatically sampled for evidence of fire to provide time to generate fire and safety alarms before fire suppression pipes are pressurised with water. If a fire occurs, water discharge is restricted to the areas within the datacentre where a fire alarm location has been triggered.

Flood control and earthquake
All MCP data centres are built above sea level with no basement areas and there are dedicated pump rooms for drainage of any water ingress. Exterior walls include moisture barriers, and moisture detection systems are in place to detect slow water ingress. All facilities meet or exceed their local requirements for seismic building codes.

Configuration management and software lifecycle management
All changes to the Dimension Data MCP environment are strictly controlled. Changes cannot occur without them passing through a workflow change control process, which requires signoff by multiple authorised personnel.
Updates to the MCP environment are applied regularly, and must pass through multiple testing phases. All changes to the MCP CloudControl systems include automatic deployment to dedicated test MCP environments which complete multiple passes of functionality and performance testing before being accepted and committed for deployment.
In addition to the above, changes are pre-scheduled and follow an implementation and test plan that measures the success, or failure, of a new code or infrastructure deployment. Back-out procedures, in the case of failure, are documented as part of the change plan.

The Dimension Data MCP is regularly audited for its compliance with SSAE-16 and European Safe Harbour requirements.
CloudControl
At its core, the Dimension Data MCP solution is built around our CloudControl management technology. The CloudControl systems are the interface point between clients and the MCP network, server and storage control systems, providing the assurance of secure separation between clients hosted within the MCP solution.

The full suite of CloudControl systems performs the orchestration of server, storage and network resources, controlling the segmentation between servers and networks on the infrastructure used to create the multi-tenant environment. As such, the security of this environment is paramount to providing a secure environment to all MCP clients.

CloudControl security
The Dimension Data MCP cloud management systems reside on dedicated network and server infrastructure, separate to the infrastructure used to host client networks and servers. All CloudControl systems are penetration-tested by external security assessment firms; testing occurs regularly and after every major functionality change. The CloudControl systems are also subject to rigorous software patching cycles.

Network traffic within the CloudControl environment (Public and Hosted Private CaaS only) is also monitored by both network intrusion detection systems and host-based intrusion detection systems, providing round the clock monitoring of each MCP. The Dimension Data Security Operations Centre performs 24x7 management and monitoring of all MCPs around the world, reacting to any abnormal events in real time.

CloudControl resiliency
All CloudControl management systems are hosted on separate network and server hardware to client systems. N+1 resiliency is applied to all CloudControl devices, allowing for multiple device failures with no impact to the accessibility of CloudControl or the performance of the management interfaces.

CloudControl management interface
All client access to cloud management settings is performed via CloudControl using either the web management interface or the CloudControl API. Both methods use SSL encryption with 128-bit keys for security, and all requests made to the CloudControl interfaces are assessed and enacted only if the requested changes are for resources owned by the client. The CloudControl interfaces also restrict clients to actions which are necessary for management of their cloud networks and virtual servers. No direct access is provided to the underlying systems, providing all MCP clients with the assurance that their cloud networks and systems are protected against configuration settings which could affect their performance, security and availability.

No other access method is provided to clients, ensuring that it is not possible to directly attack or affect the cloud network and virtual server hosting technology.

Figure 2
CloudControl network traffic encryption
All CloudControl operations are encrypted using HTTPS between clients and the CloudControl web servers. Transmission encryption is performed using the RC4 encryption algorithm over the TLS protocol, with 128-bit keys. The CloudControl web infrastructure uses a 2048-bit digital certificate for authentication of the web server and encryption of the RC4 initialisation vector keys.

Remote access
Clients can also access their MCP cloud networks using the CloudControl remote access VPN. This service allows administrators to authenticate using their MCP account, and connect either using a web-based SSL VPN portal or a locally installed Cisco VPN client. Both clients use RC4 128 bit encryption over HTTPS and can be used to communicate with servers inside the client’s cloud networks via the IP protocol.

Each VPN client is allocated an IP address which is granted explicit rights to connect to its MCP cloud networks, and logically appears to be one IP hop away from their servers.

Client cloud networks
The first building block for MCP clients is one or more cloud networks. Each cloud network created by clients is a physical layer-2 VLAN created as a security context on a Cisco switch with a private IP network address allocated to it. No software emulation of VLANs is performed in the MCP environment; all network controls are enacted by dedicated network equipment.

Denial of service protection
Client Cloud networks in any Dimension Data MCP environment (public or Hosted Private cloud only) are protected against performance implications caused by network denial of service attacks. Traffic entering and leaving cloud networks destined for the Internet are constantly monitored for DoS behaviour and attacks are blocked when detected. If another client’s network is under DDoS attack, that client network will be segmented to ensure that all remaining clients are not affected.

Network access controls
Every cloud network is protected by ACLs which define what IP traffic may enter and leave the network. Inbound access to cloud networks from the Internet is disabled by default, ensuring a default security posture. Outbound access from cloud networks to the Internet is enabled by default. All ACLs are fully stateful and include deep packet inspection for support of complex protocols.

The ACLs for each cloud network are fully under the control of clients and can be used to provide strict or open access to and from each cloud network. ACLs can be applied to allow/deny access on both inbound as well as outbound traffic.

Cloud network IP addressing
Every cloud network created by clients is allocated a /24 IP subnet within the 10.X.X.X IP address range, and a small block of publicly reachable IP addresses. Additional blocks of public IP addresses can be added to each cloud network.

Network address translation (NAT)
By default, the first public IP address is used for outbound access using Source NAT. Clients can then create static NAT rules to perform a one-to-one mapping between a public IP address and the private IP address of a server located in the cloud network. This static mapping will force all outbound traffic from that server to use the selected public IP address, and will redirect any inbound connections to that public IP address to the selected private IP address. Clients also can create Virtual IP (VIP) rules to allow more complex IP mapping scenarios, including load balancing and port translation.

Cloud network resiliency
The Dimension Data MCP uses N+1 resilient Cisco enterprise grade switching and routing infrastructure with multiple hardware modules in each switch for resiliency of IP routing, access controls and server load balancing. Failures of any management, network or security modules within a switch, or failure of an entire switch, do not affect the accessibility or performance of client cloud networks.

All network equipment is connected together using multiple physical network paths, with each path providing enough bandwidth to service MCP operations in the event of a failure. All physical server hardware is connected to redundant core switches with redundant security blades providing Layer-2 isolation and network functions.

Each cloud network created by clients is a physical layer-2 VLAN created as a security context on a Cisco switch infrastructure.
Client virtual servers

**Virtual server hosts**
The Dimension Data MCP virtual server hosting solution uses VMware ESX hosts to host client virtual servers. All management of VMware ESX functionality is performed by the CloudControl management systems or Dimension Data personnel, with no VMware management interfaces exposed.

**Virtual server images**
Virtual servers created by clients are based on either operating system (OS) virtual images created by Dimension Data or OVF images imported by the client. These images include the necessary tools to allow for pre-build configuration settings to be applied to them as part of the initial server creation process. Only the necessary software or OS components are included in the OS images, and clients are free to further remove any components they deem not required for each server once a VM has been built.

**Virtual server (ESX) host resiliency**
All ESX servers use multiple physical network cards, and connect to the redundant core switches. Link bonding and LACP is used to provide zero downtime in the event of a network failure. All storage used by the ESX hosts is provided by EMC SAN storage systems, with multiple host bus adapters installed in each ESX host, with multiple connections to the SAN array.
All ESX hosts are clustered in an N+1 resiliency model, providing for protection against hardware failure due to CPU, memory or motherboard faults. Failover to another ESX host for client virtual servers is automatic, with the servers being automatically re-started. Any affected virtual servers are offline for the time it takes for them to be restarted.

**Virtual server resource dedication**
Clients with either the Private or Hosted Private MCP are provided dedicated resilient ESX server clusters for their own use. Public MCP clients share ESX server resources with other clients within the same MCP data centre.

**Server administrator passwords**
Clients are asked to provide a root/administrator password for their servers just before they are created. This password is briefly stored on the virtual server operating system disk for the purposes of automated build and startup, after which it is erased with no record of the password kept by Dimension Data.

**Console access**
To maintain the security of the MCP multi-tenant environment, console access is not currently permitted. All communication with virtual servers must be via an IP connection (RDP for Windows, SSH for Linux). For security reasons, Dimension Data recommends clients only connect to these protocols using the VPN and avoid exposing these protocols to the Internet.

**Operating system vulnerability management**
All operating system images created by Dimension Data are periodically patched, with the operating system security patches installed. When clients bring up a new server, that server will start operating with those patches installed. After this point it becomes the client's responsibility to maintain patching of the operating systems and any applications installed on their virtual servers.
For clients without the desire or skills to manage their virtual server operating systems, Dimension Data offers Tech Ops, a suite of server management offerings that provides system monitoring (CPU, disk, etc.), server administration, and OS support and patch management, including security patching.

**Operating system security settings**
All operating system images created by Dimension Data are configured with the basic required components to perform common Internet services roles (such as web servers), and allow clients to add their own desired functionality using the relevant package management tools for the operating system used.
Once an image is customised, clients can clone the image and use it as their new base operating system image for new virtual machines. This allows clients to create their own secure SOE within the MCP environment.

The Dimension Data MCP virtual server hosting solution uses VMware ESX hosts to host client virtual servers.
Local storage

All client virtual servers are provisioned with an initial 'operating system' disk which is a VMDK file hosted on the MCP SAN storage systems. Clients can deploy an additional 14 disks (maximum 250GB per disk) to each virtual server, with a maximum locally attached storage size of 10 Terabytes across all disks.

Storage resiliency

All locally attached disks for virtual servers are located on highly resilient EMC SAN storage using multiple physical disks arranged in RAID arrays, which are presented to virtual servers as locally attached SCSI disks. Dimension Data manages all physical disk maintenance for clients, ensuring that any physical disk failures are invisible to clients and do not create service outages.

Storage encryption

Dimension Data does not encrypt client storage; such an offering would mean that Dimension Data would need knowledge of the encryption keys for deployment of the service on our storage infrastructure.

When encryption at rest is desired for specific risk mitigation or compliance circumstances, Dimension Data recommends that clients enable encryption of data using tools within their virtual servers or within the applications themselves.

For clients with a high level of concern, systems with the most highly sensitive information can be located outside of the Dimension Data MCP environment and linked via a secure tunnel.

Hybrid NAS storage

MCP clients which require storage which is shared across multiple virtual servers can use the Dimension Data Hybrid NAS solution. The Hybrid NAS solution is located within the same data centre as the MCP infrastructure but outside the control of the CloudControl management systems and is requested by directly contacting Dimension Data to enable this functionality.

Hybrid NAS resiliency

The Hybrid NAS solution is hosted on N+1 resilient storage appliances with multiple controllers and disk trays configured in resilient RAID arrays. Failure of NAS controllers or disks is invisible to clients with no downtime or performance degradation.

Hybrid NAS security

Each NAS client is allocated their own dedicated vFiler instance with access restricted to their cloud networks. Access to the NAS is restricted at deployment time to the cloud networks the client requests; this can be all, or some of the clients cloud networks. Any client which grants access to the NAS from all their client networks can further restrict this access using custom ACLs.

The Hybrid NAS deployment does not implement user-based security and is designed to serve as shared storage for server workloads rather than user-based file and print services.

Auditing and monitoring

Dimension Data’s CloudControl software audits all administrator activities performed by clients and allows each client to download copies of these logs in CSV format. Any action taken by a client through the CloudControl web interface or API is fully monitored and the results of those actions are also captured within the audit trail. The audit trail captures the full content of each command entered and the details of any changes made as part of the change.

The audit trail itself can be access via the API, allowing clients to automatically monitor all administrator activity on their MCP accounts, and import these into log management systems or incident management systems.

Activities logged

The MCP administrator logs include details of any commands issued from the CloudControl web interface or the API. Most functions also log both the command request and the actual implementation of that request by the CloudControl software. Activity logs are retained for one year and are available for download from the web-based user interface or API.

Access to administrator logs

To maintain security against tampering of the administrator logs, once a log entry has been created, clients cannot remove the log entries. Copies of the administrator logs can be downloaded by any sub-admin accounts which have the ‘Report’ access role.
User management

**Primary administrator**
All MCP clients start with a primary administrator account. This account maintains full access to all cloud networks and servers for the client, and can create sub-administrator roles with more granular permissions to create and edit network, server or storage resources.

**Sub administrators**
The primary administrator can create sub-administrators and grant these specific permissions only to create and edit the cloud network, server and storage resources. This reduces the likelihood of accidental or malicious removal of resources, and allows for accurate auditing of administrator activities.

**Access roles**
Sub administrator accounts can be granted one or more security roles, those being ‘network’, ‘server’, ‘create image’, and ‘reports’. If no role is chosen, the user will have only ‘read-only’ access. They can view networks, servers, and images, but cannot deploy, modify, or delete them.

The network role allows the user to utilise any of the network functions, allowing them to create new networks, delete networks, or modify existing ones (such as adding/removing firewall rules).

The server role allows the user to deploy servers, modify the characteristics of servers, or delete servers. They can take any action on the server function except to create a customer image.

The create image role allows the user to create customer images from any deployed server.

The reports role allows the user to view reports functions available on the ‘reports’ tab. Customers requiring more granular access control can leverage their own identity management infrastructure and web portals with controlled access to pre-configured API scripting to control what actions a user can perform.

**Data sovereignty**
MCP clients have a choice of in which ‘hub’ region their accounts are created. As such, all clients have full control over the region where servers and storage resides, and can explicitly choose to use multiple regions or a single region.

**Geographical failover**
To enable clients to implement resiliency against failure of access to an entire Dimension Data MCP region, clients can choose to have cloud networks and servers located in multiple geographical locations, and can create ACL rules to allow direct IP communication between their geographically separated cloud networks.

Clients are responsible for implementing the failover solution; Dimension Data recommends the use of global load balancer technology to perform the monitoring of their servers and enacting of the failover event. As part of Dimension Data’s Tech Ops managed service, we are able to help clients configure, deploy and monitor failover solutions.
Frequently asked questions

Can I install my own network security device?
The Dimension Data MCP solution does not support the installation of layer-2 transparent devices. Clients cannot bring their own hardware devices to either the Public or Hosted Private cloud solutions; however clients with their own private cloud deployment can install network security devices inside their data centre ‘upstream’ of the MCP equipment. In supported geographies, clients may connect via private a layer-2 connection using our Customer Private Network Connection service. All clients are free to install any software agent on their servers; therefore the functionality offered by traditional layer-2 transparent devices can be performed using tools such as host-based IPS and firewall protection.

Are virtual appliances supported?
Dimension Data MCP supports the importation of OVF images; however, we do not support the importation of OVA format images. Each virtual image requires some amount of automated system preparation by the CloudControl infrastructure, which may not be possible on many appliance virtual machines. In addition, many virtual machine appliances require direct console access (either during installation or permanently) which is not currently supported by the Dimension Data MCP solution.

Can I install my own hypervisor security controls?
To ensure that no client can negatively affect the performance or security of any other client, there is no access to any hypervisor functionality, and clients cannot install or use hypervisor security controls such as VMware vCloud Networking and Security. Dimension Data maintains strict control over the hypervisor to ensure the highest security is provided to all clients.

Does Dimension Data utilise any VMware hypervisor security controls?
The Dimension Data MCP solution uses dedicated network security devices from Cisco systems for all network security. No network security functions are performed via software emulation which could affect the performance of virtual server systems.

Does Dimension Data monitor my audit logs for suspicious activity?
No, due to the wide variety of client needs, Dimension Data does not assume what administrative tasks for each client are normal or abnormal. However, Dimension Data monitors the CloudControl portal to detect attacks made against it, which may result in clients being alerted that their accounts are being targeted.

Can Dimension Data monitor my systems for accessibility?
Dimension Data does not monitor client servers. However, server start and stop events are included in administrator logs and can be used to detect a manually initiated server shutdown from within the administrator user interface.

For clients without the desire or skills to monitor their virtual server operating systems, Dimension Data offers a suite of server management offerings under the ‘TechOps’ service, which provides system monitoring (CPU, disk, etc.), server administration, and OS support and patch management, including security patch management.

Can I increase the network security between my cloud networks?
Clients are able to fully control the ACLs which define what IP traffic can enter and exit each of their networks. Each client cloud network is a dedicated VLAN which reaches all other networks (including the CloudControl remote access VPN) by passing through a Cisco security module. By default, all IP traffic is permitted between a clients’ remote access VPN and all their cloud networks. The inbound ACL for each cloud network can be configured to restrict this traffic.

Can I restrict communication between my servers within a network?
The Dimension Data MCP solution does not provide the capability to perform within-VLAN filtering. Clients can configure and install any IP filtering solution on their virtual servers, which provides the same functionality. Any communication between servers on other client cloud networks can be controlled using ACLs.

Can I monitor all VLAN traffic on my networks?
The Dimension Data MCP solution does not allow for monitoring of traffic on client networks using packet sniffers. All servers located in client cloud networks can only see IP traffic destined to them and IP broadcast traffic for their VLAN. To ensure that clients cannot attempt to ‘break out’ of the hypervisor and view traffic destined for other client networks, promiscuous mode has been disabled in the hypervisor and cannot be used by any client.

Are my servers backed up?
All virtual server storage (including operating system drives) are stored on resilient EMC SAN storage arrays. Virtual machine backup solutions are available in certain geographies. Clients are free to manually or programmatically (via the API) clone their virtual servers. These clones are labelled as ‘client images’ and can be used to re-deploy a server in the event of failure or server corruption.

Note that clone images may be stored on the same physical storage array as the source virtual machine. For the greatest resiliency, clone images should be exported out of the MCP environment and/or copied to a different MCP location if the client has access to multiple regions.

What happens if an ESX server fails?
The Dimension Data MCP has been built for resiliency. VM hosting ESX servers are configured in clusters with the cluster consisting of actively used ESX hosts and standby servers. Every ESX server uses a combination of bonded NICs, resilient SAN arrays, multiple paths to the SAN, and redundant power supplies.

Client virtual machines are only active on one ESX chassis at any given time. If an ESX server fails, all virtual machines on that chassis will fail. Each virtual machine will then be automatically re-started on another ESX server in the cluster, resulting in a few minutes downtime while the virtual servers are moved and restarted. For added resiliency, clients can use Dimension Data’s Server Anti-Affinity rules to deploy virtual servers on different physical servers.
Can I customise my server operating system settings before creating new virtual servers?

Clients can create their own custom operating system images of server operating systems. To do so, the client must start up a fresh virtual machine from one of the supplied images from Dimension Data or import their own image. Custom settings can be applied to this image, and it can then be configured as a custom image to create new virtual servers from.

Any custom images are not maintained by Dimension Data; if a client does not maintain patching of the operating system for custom images, new virtual machines based off the image may be insecure.

How can I defend against downtime caused a virtual server failure?

If an application hosted on a virtual server fails due to software-based issues outside of Dimension Data’s control, resiliency can be created by deploying multiple servers with the same applications installed, and using load balancing configured within the client’s cloud network. For added resiliency, clients can use Dimension Data’s Server Anti-Affinity rules to deploy virtual servers on different physical servers.

Are complex protocols such as FTP supported, given that NAT is a requirement for external access?

All ACLs are fully stateful and include deep packet inspection which supports the following complex protocols:

- FTP
- DNS
- CMP
- SCCP
- RTSP
- ILS
- SIP

Can I get log entries for ACL rule hits?

The Dimension Data MCP does not currently allow for monitoring of ACL rule hits. If connection logs to servers are desired, this functionality can be deployed by using software tools on a client’s virtual server operating systems, such as host-based firewalls and web server logs.

How do I create Tier-2/Tier-3/Intranet networks?

By default, all MCP cloud networks are configured the same. To make a network unreachable from the Internet permanently so that any accidental NAT changes do not expose systems, clients can delete the default Inbound allow ACLs and replace these with new ACLs which are more restrictive, allowing access only from their other cloud networks.

Access from these networks to the Internet can also be controlled by editing the Outbound ACL, allowing clients to block or restrict all outbound Internet connectivity and connectivity to all other cloud networks.

Can I communicate with other MCP clients from my cloud networks?

If both parties involved in the connection use ACL entries which permit the traffic between the private IP addresses of their own cloud networks, the communication is permitted. This is possible between any Public and Private Hosted MCP cloud network regardless of the source and destination MCP data centre, allowing true private and secure global communication.

All communication between Dimension Data MCP data centres is encrypted using IPsec tunnels using Triple DES 168-bit three-key encryption. Authentication of the encrypted tunnels is made using multiple site-specific pre-shared keys which are managed out of band by Dimension Data. PKI authentication is not used for the encrypted tunnels to reduce the attack surface of the authentication method.

Can I communicate with my own data centre using a site-to-site VPN?

Dimension Data does not currently offer a managed site-to-site VPN service for clients; however virtual servers within cloud networks can be configured as VPN gateways. Clients are able to add routes to their virtual servers which direct all traffic to their own data centre via such a gateway. Clients can purchase a Managed Hosting solution from Dimension Data, which allows for hosting of dedicated physical servers within Dimension Data data centres. Servers hosted in such a manner are able to reach client MCP cloud networks using direct IP routing configured by Dimension Data. In some circumstances, double NAT may be required if there are IP address conflicts between a client’s IP networks and those used within their MCP cloud networks as allocated by Dimension Data. In supported geographies, clients may connect via private a layer-2 connection using using our Customer Private Network Connection service.

Can I change the IP addresses of my virtual servers?

Virtual servers are deployed with private IP address pre-assigned by the CloudControl software. Clients can then control the mapping of this private IP to public IPs on the cloud network via NAT or VIP. Clients can also change the private IP address of their servers but this is not recommended as the CloudControl software will be unaware of the change and changes outside the private IP range will stop the server from being able to access other networks. Additional secondary IP addresses can be added to servers; however these cannot be used to communicate outside of the cloud network where the server resides unless clients create a dedicated IPsec or L2TP tunnel to other networks and servers.

Is IPv6 supported?

Native IPv6 is not currently offered by Dimension Data for cloud networks, but clients are free to use any IPv6 tunnelling technology on virtual servers to reach external IPv6 networks. ACLs which grant access to a client’s chosen IPv6 gateway device on the Internet may be required if they have blocked outbound access from their cloud networks.
The most powerful user account for any MCP client is the primary administrator account. Access to this account should be restricted and it should not be used for daily MCP management operations.

Can I remove the outbound source NAT from my cloud networks?
No, the outbound source NAT rules are not alterable by clients. To block outbound access, clients can edit the default outbound ACL for their cloud networks to stop connections to external networks.

Can I remove the public IP addresses from my cloud networks?
The first two public IP addresses allocated to each cloud network cannot be removed. Any additional public IP address blocks requested by clients can be removed.

Security best practices

Administrator account management
Restrict knowledge of the primary administrator account
The most powerful user account for any MCP client is the primary administrator account. Access to this account should be restricted and it should not be used for daily MCP management operations. Dimension Data recommends the use of a long passphrase and that the password used for this account is not used for any other system or service. As a best practice it is recommended that the primary administrator account should also not be used for any routine MCP operations, as it cannot be traced back to an individual administrator.

Allocate sub-administrator roles
For all normal MCP CloudControl operations, sub-administrator accounts should be used, with their access rights restricted to the networks and servers within their account. As with the primary administrator, each sub-administrator account should not use a password which is used anywhere else.

For the greatest network security, sub-administrators should not be granted the ‘Network’ Role unless they require the ability to create and modify networks (including ACL rules).

Audit log management
Dimension Data recommends that administrator audit logs are reconciled with expected activities on a regular basis. The CloudControl API interface allows for collection of administrator audit logs, allowing logs to be automatically downloaded and imported into a log analysis tool. Dimension Data recommends the use of Security Event and Incident Management technology which has behavioural learning capabilities for intelligent log analysis and generation of alerts when high risk or unexpected actions are undertaken.

Virtual server security
Whilst Dimension Data provides server images in a secure format, some settings should be further hardened to match client security requirements. For example, direct root access is enabled (and required during server builds) for SSH access on Linux servers. Post deployment of servers, clients should apply additional security settings relevant to their information security management framework and related standards.

Network security controls

Default network security posture
When a network is created, it is automatically allocated a private IP address range and a small block of public IP addresses. Outbound access to the Internet is immediately possible due to source NAT being configured automatically. Inbound ACL rules exist by default to allow access to ports 80 and 443 on any IP address within the cloud network. Inbound access from the public Internet is not enabled until a static NAT rule is created to map one of the public IP addresses to the private IP address of a server. If multiple cloud network layer-2 VLANs are setup, care should be taken to modify ACL rules accordingly to explicitly restrict access to IP addresses or ports that should not be accessed (e.g. application and data tier servers not in a DMZ).

ACLs
All communication into and out of every cloud network is governed by the ACLs applied to that network. Each network has an Inbound and outbound ACL which controls the ability for other networks to initiate connectivity to the network, or allow hosts within the network to reach other networks, or the Internet.

For each cloud network, there are invisible ACLs in place which allow the client’s remote access VPN to reach all cloud networks created under the primary account.