VPN Cloud

Mako's SD-WAN Technology

January 2022 v7.3

Introduction

Mako VPN Cloud is a secure, scalable, and flexible encrypted wide area networking solution from Mako Networks. It is designed to link remote or distributed Mako-connected locations to one or more physical or virtual data centers, head offices, and to each other.

Mako VPN Cloud is a patented SD-WAN (software-defined wide area network) that does not tie organizations to a single carrier or ISP.

Mako VPN Cloud offers the ability to form secure and robust VPNs with user-definable resiliency including circuit, hardware and geographic redundancy. A zero-packet-loss option ensures critical data is never lost or delayed in transit so long as at least one WAN circuit is available.

A Mako VPN Cloud consists of one or more Mako Security Gateways, grouped into a “cloud” architecture, allowing all Mako devices within the group to maintain secure connectivity to a centralized network(s) and/or each other via flexible and redundant routing.

A VPN Cloud comprises any type of Mako security device, including physical and virtual VPN concentrators.

A typical Mako VPN Cloud is made up of one or more Mako rack mounted VPN concentrators (7000 and 8000-series) in one or more data centers and/or Mako’s virtualized VPN concentrators running in Google, AWS or Azure cloud infrastructures. Mako security devices at remote sites are then connected to this network of concentrators, creating redundancy at every level to complete a Mako VPN Cloud solution.

A Mako VPN Cloud can span multiple data centers, providing geographic redundancy. Each Mako device connects to its own internet circuit(s) to provide circuit redundancy.

Unlike legacy technologies, such as MPLS, a Mako VPN Cloud has no single point of failure. No network traffic traverses The Mako Central Management System, a cloud based application, through which Mako VPN Clouds are configured and monitored.

Current Challenges

Modern networks incorporate multiple wide area networking technologies, often utilising more than one access medium with different pricing models based on connectivity, speed and access reliability.

Network security, availability and cost are key business drivers in any business network. Modern businesses now require and expect reliable and secure distributed networks at the core of their business operations.

Mako VPN Cloud technology delivers a solution that is flexible enough to meet these needs by supporting a wide range of networking requirements, using a wide variety of readily available broadband networking technologies, without compromising enterprise security or incurring significant engineering overheads.

High Availability

A business connects its small-site/distributed Mako Security Gateways to any combination of wired and/or cellular broadband. The combination of a Mako VPN Cloud and Mako's small-site/distributed site devices allows connectivity over multiple internet connections, delivering cheaper, faster and more resilient connectivity than any other method available today, including legacy MPLS or private satellite networks.

Mako technology provides redundancy at both the small-site/distributed site locations and data center/head office ends of the connection, delivering the best possible combination of price, speed, security and reliability.

Small–Site Multi-WAN Failover

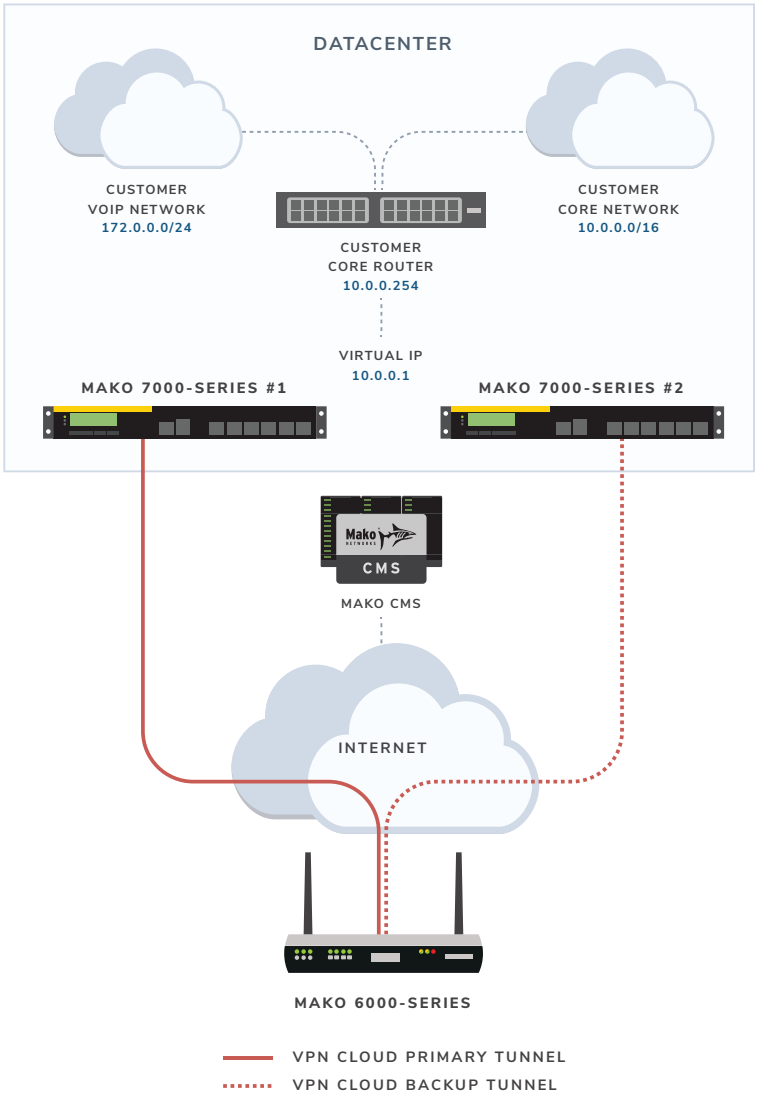
Mako technology is designed to operate securely over any Internet connection: cable, DSL, Ethernet, fiber, and cellular. For example, 6000-series small-site Security Gateways can support up to 4 WANs and seamlessly use whatever internet connections they have available to access and form their part of the VPN Cloud. These multiple connection types can be configured in a variety of combinations from always-on and load balanced to a ranked failover setup in which only one connection is used at a time. Mako's VPN Cloud keeps critical business systems online during unexpected network outages. It also avoids the need to deploy more expensive backup links such as leased lines and MPLS.

Datacenter Multi-Mako Failover

Organizations often provide mission critical services at one or more data centers, which in turn require a high degree of network availability and connectivity. Mako VPN Cloud can be deployed on multiple Mako devices (typically 7000-series, 8000-series or virtual Makos) using any of the architectures below:

- ***Mako-Mako Failover***

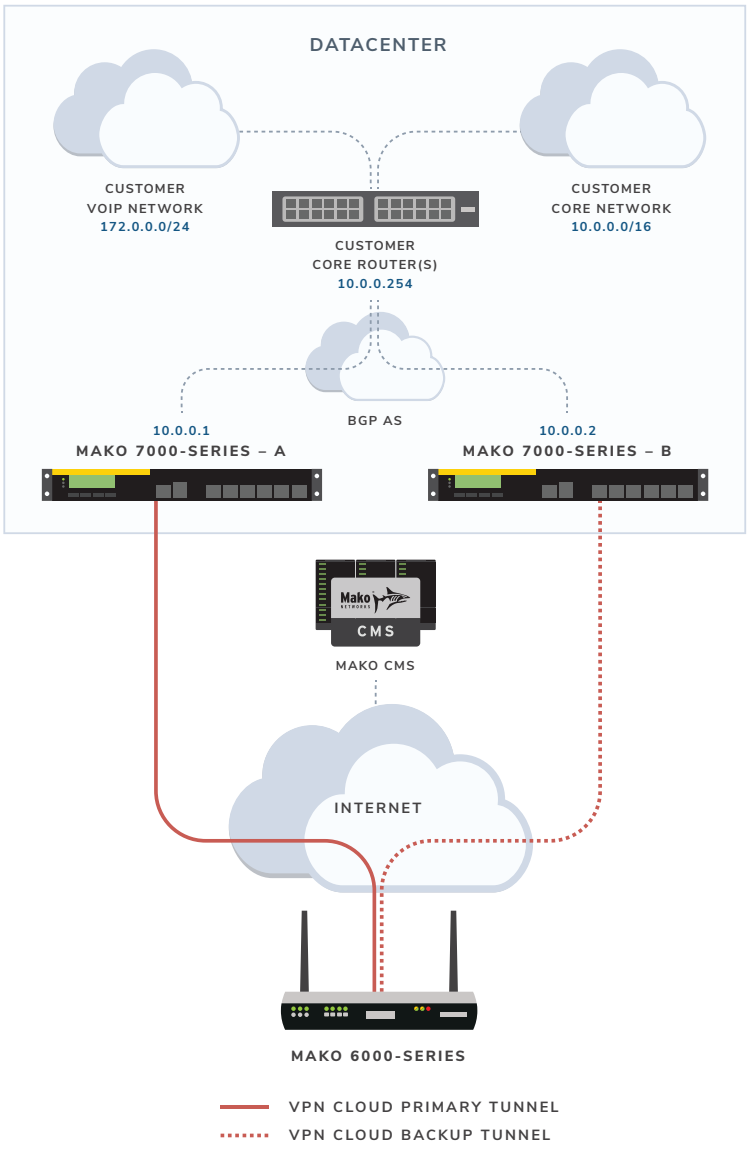
Using two Mako VPN Concentrators of the same type to form an HA pair, the pair shares a virtual IP address on a common LAN. The primary concentrator owns the IP address at any point in time, and VPN connections route their traffic through this primary concentrator. If the primary concentrator fails due to an ISP outage, power outage, or physical issue, the secondary concentrator will seamlessly take over ownership of the virtual IP address, and all VPN connections will route their traffic through it instead.



Mako-Mako Failover is not limited to data centre deployment, it can also be deployed (typically at edge locations or HQs) using any two Mako devices of the same type (e.g. 2 x Mako 6000-series Security Gateways).

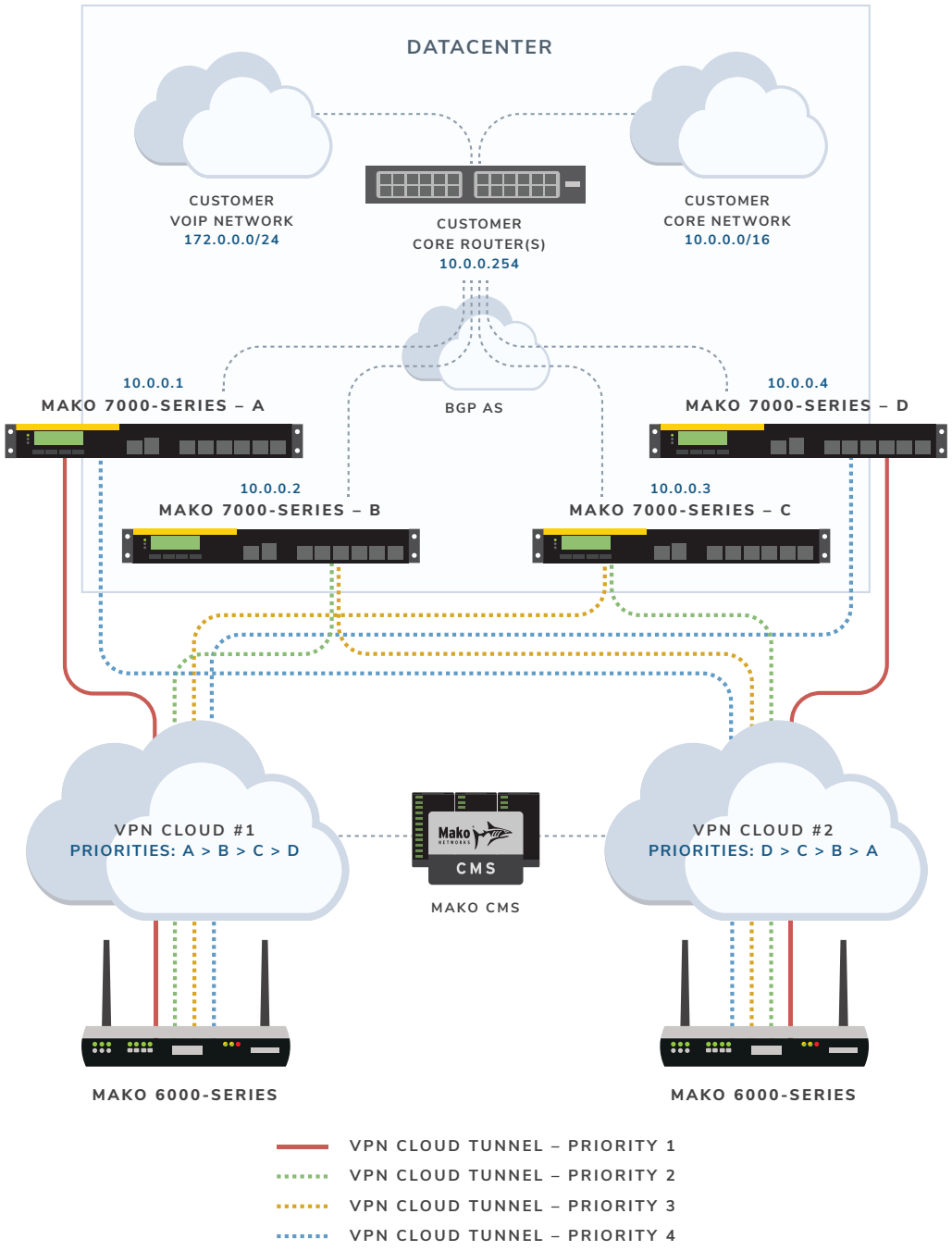
- ***BGP Remote Route Injection***

Using two or more Mako VPN Concentrators of any hardware combination, BGP is run on each of the concentrators to inject the routing information of all participating Mako VPN Cloud devices back into the organization's core network. This approach avoids the need for a shared virtual IP, and allows more flexibility when allocating load across the various concentrators.



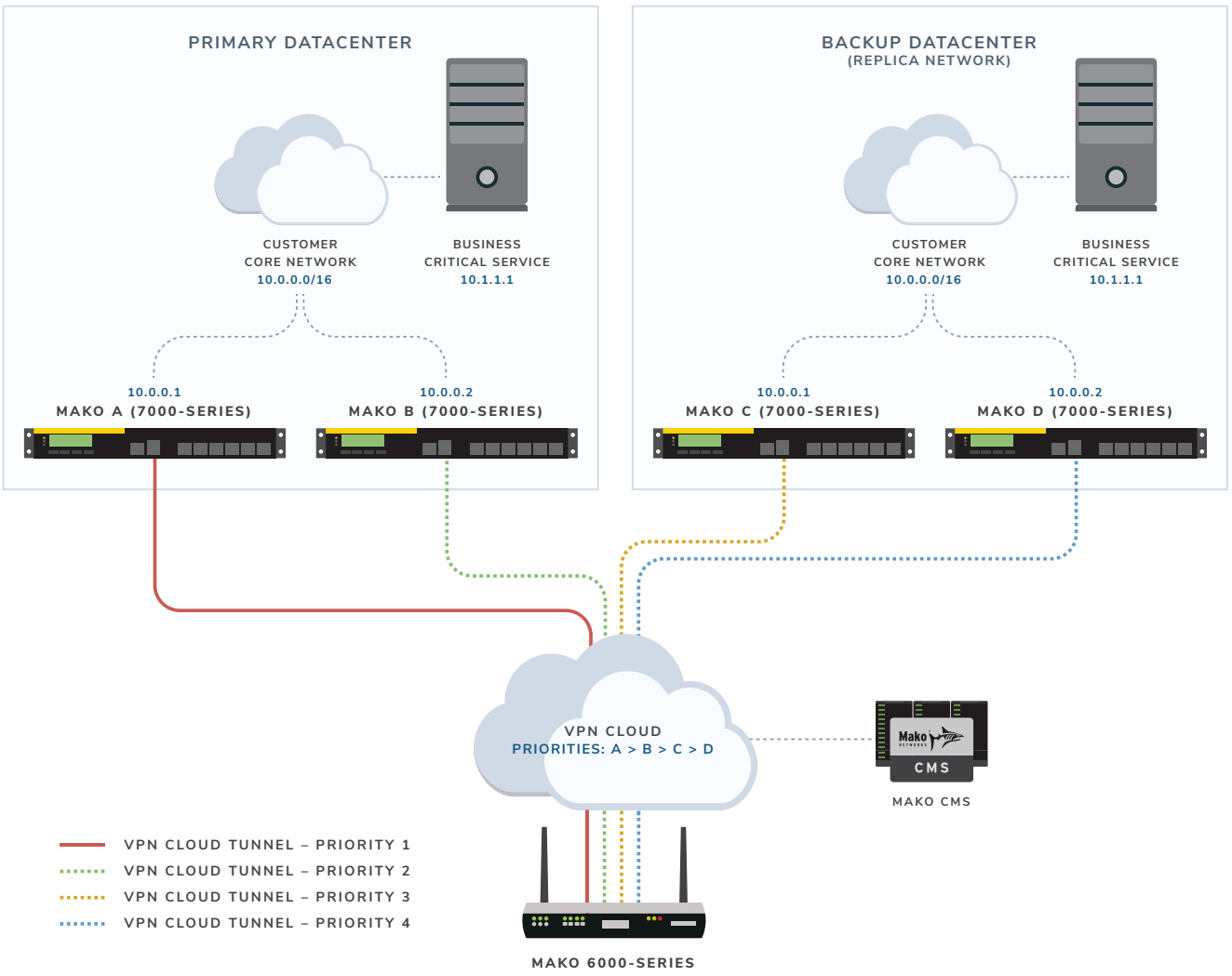
For example, each Mako VPN Concentrator can terminate connections from multiple VPN Clouds, with each Cloud treating that specific concentrator with a different priority.

Users can create two Clouds. The first prioritizes traffic to connect to concentrator A first, then to concentrator B then C then D. Users can then create a second Cloud that prioritises traffic in the reverse order: first connect to concentrator D, then C then B then A. Users would then assign half their sites to use the first Cloud and the other half to use the second, thus creating a highly redundant VPN Cloud solution.

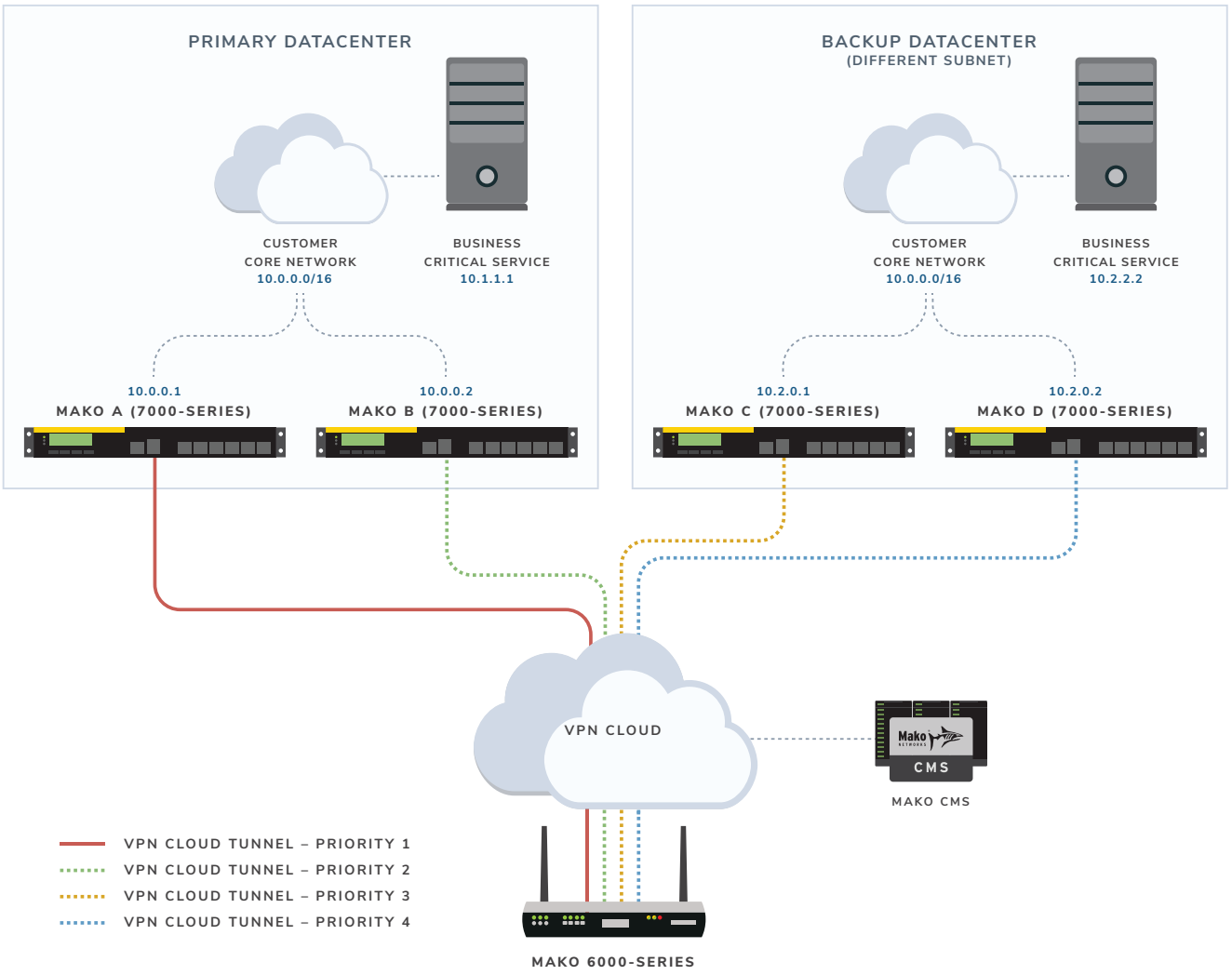


- ***Geographic Redundancy***

Mako VPN Cloud supports geographic redundancy through two or more data centers. Each data center can be configured with identical replica networks of different priorities and the Mako VPN Cloud will seamlessly send traffic to the best one currently available based on Mako's proprietary routing algorithm.



Alternatively, each data center can have unique addressing, with end-user applications configured to use the fallback addresses.



- ***BGP-based Geographic Redundancy***

If the data centers are interconnected by a network such as MPLS, then BGP can be used to dynamically import routes from both data centers. BGP runs between the user routers and the Mako VPN Concentrators.

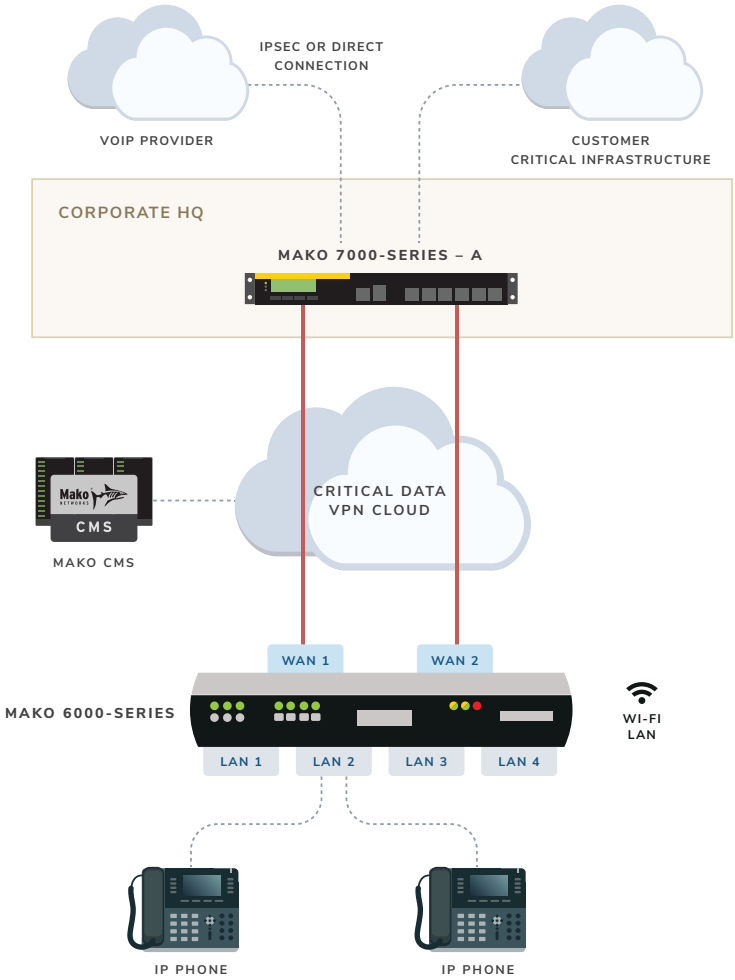
- ***Zero packet loss***

Mako VPN Cloud has a zero-packet loss capability called VPN Cloud Critical Data, where it uses two or more WANs on a Mako device to ensure every packet is delivered across the VPN even if one of the WANs has a failure. This capability differs from other vendors in that not a single packet is lost when one

of the WANs becomes inoperative, experiences high packet loss or latency, or has other issues between it and the VPN Cloud concentrator.

VoIP and other real-time, latency or packet-loss-sensitive applications benefit the most from this feature.

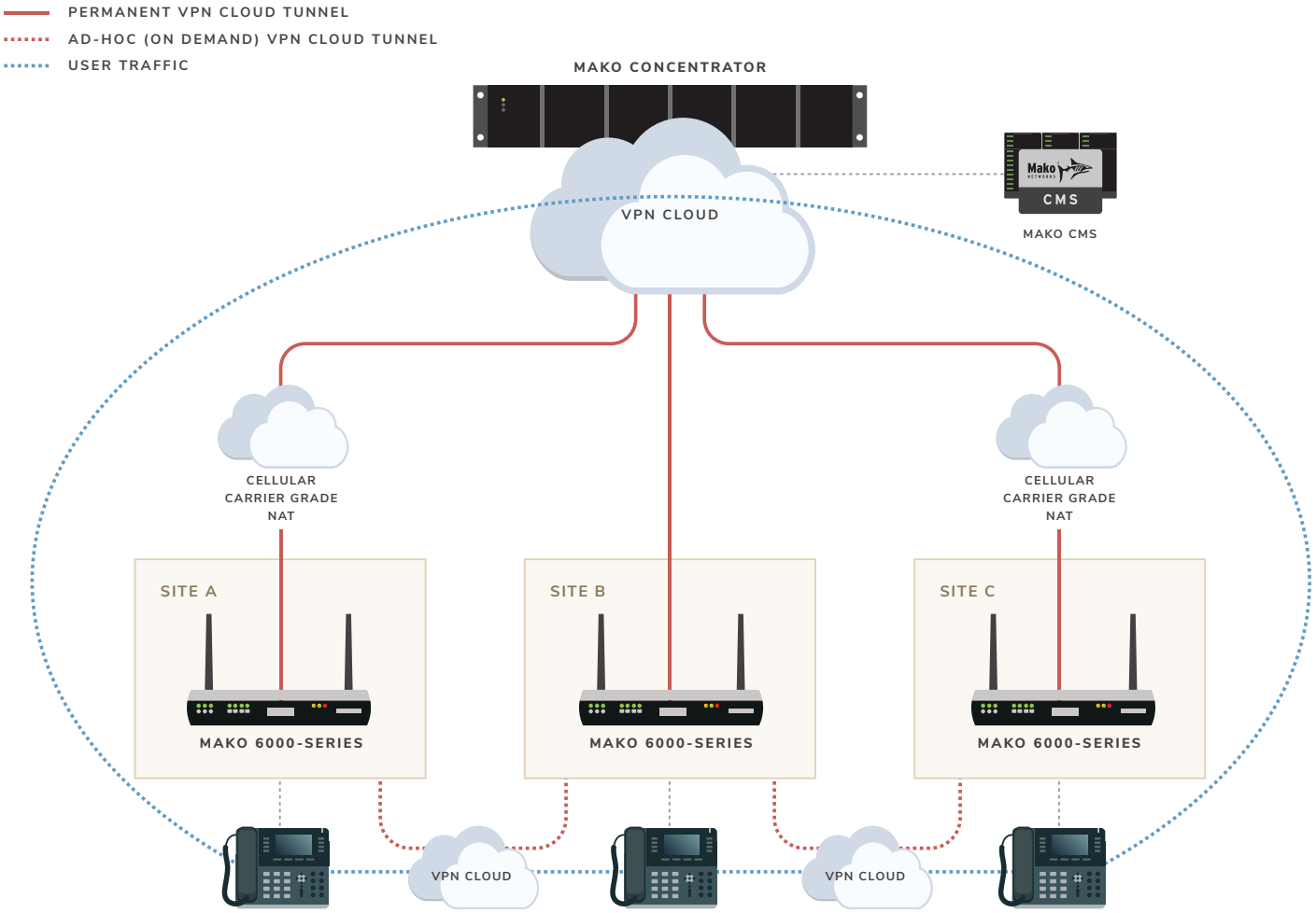
When this feature is enabled, all priority packets are treated as critical data and sent across both WANs, and seamlessly reassembled on the VPN concentrator. The fastest packet is always picked, which also minimizes latency and jitter. DSCP can be used to indicate packet priority, or the Mako can prioritise based on firewall rules. Using this feature reduces the maximum VPN bandwidth by up to 50%, less if not all traffic is critical data.



Routing and SD-WAN

Mako VPN Cloud inherently provides SD-WAN routing capabilities, with traffic dynamically routed across the best available WAN.

Use of optional, ad-hoc temporary connections allows two Mako devices to communicate directly with each other without having to send all VPN traffic via a concentrator. Instead, only the initial traffic is sent via the concentrator, after which the cloud automatically establishes a temporary direct connection between the two sites. If a direct connection is not possible (e.g. both sites are behind carrier grade NAT), then the concentrator will continue to route the traffic, ensuring it always reaches its destination.



Multiple Mako concentrators can be used across various locations to provide geographic resiliency for the mesh.

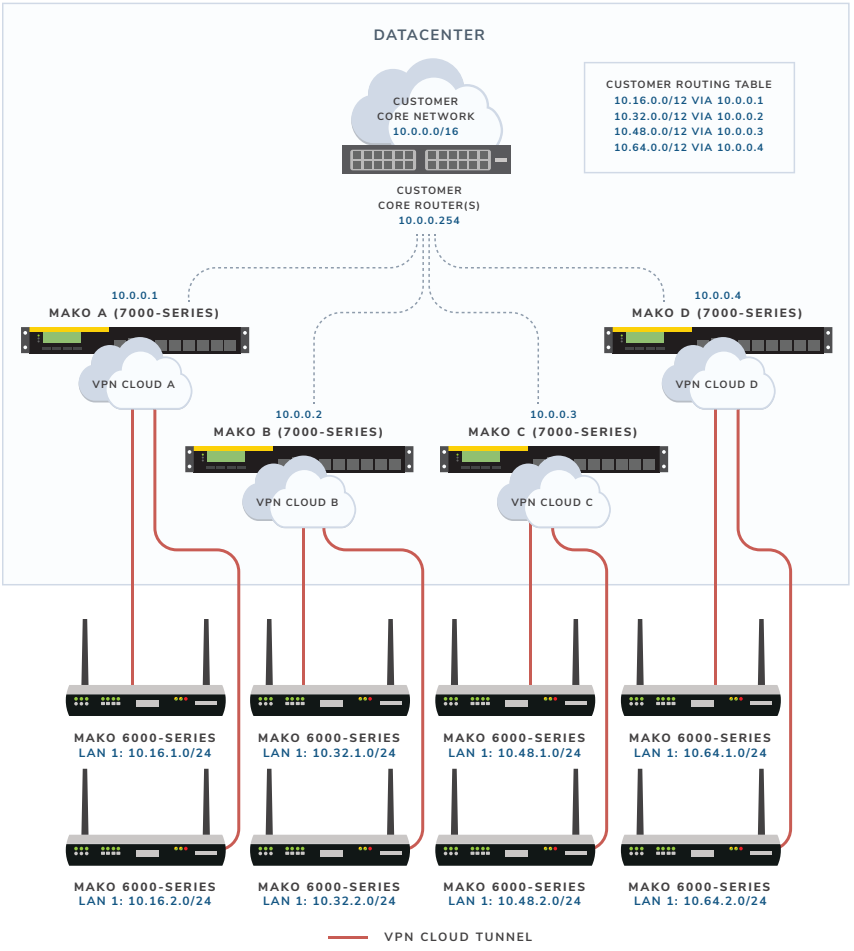
Scalability

Mako VPN Concentrators can be scaled to meet the bandwidth demands of host and remote sites by using multiple Mako concentrators to form the VPN Cloud. Each provides access to a portion of the sites. Return path routing from the data center back to the remote sites is handled either via static routing or BGP.

When using static routing, each Cloud's sites should fit within a specific supernet. For example, the networks could be allocated as follows:

VPN CLOUD	SUPERNET	CONCENTRATOR IP
Cloud A	10.16.0.0/12	10.0.0.1
Cloud B	10.32.0.0/12	10.0.0.2
Cloud C	10.48.0.0/12	10.0.0.3
Cloud D	10.64.0.0/12	10.0.0.4

Routers within the datacentre core would then route traffic back to the appropriate concentrator.



This step is not necessary when using BGP for return path route injection into the customer core network.

Monitoring

The Mako Central Management System (CMS) provides diagnostic tools to display an overview of the connection status of all Mako devices within the VPN Cloud, including VPN connection status and the duration of existing connections. Latency information is also available for each connection, making it simpler to identify sites with slow or poor WAN links.

Security

All access across the VPN Cloud is controlled by firewall rules. Most users simply apply straight-forward allow-in and allow-out policies. Advanced firewall rules are available for added security and control over the organization's network. Rules can be applied at both traffic egress and ingress. Mako Enterprise Templates can be used to ensure firewall rules are consistent across all locations.

All communications are securely encrypted using strong, industrial grade encryption (AES 128bit/256bit, or ChaCha20 256bit) required by the Payment Card Industry Data Security Standard (PCI DSS). Perfect Forward Secrecy (ECDHE) is used to protect private data against brute force offline attacks.

All endpoints, including both Security Gateways and Mako VPN Concentrators, are securely identified and authenticated using industrial grade certificates (ECDSA). Seamless certificate management and revocation is handled by the Mako CMS.

Each VPN Cloud has its own set of cryptographic keys, allowing multiple VPN Clouds to run on the same Mako securely and independently. Traffic cannot cross between VPN Clouds unless allowed by firewall rules.

Performance

Latency overhead of sending traffic through a Mako VPN Cloud is minimal, with an average increase of less than 3ms.

Throughput differs depending on the Mako device and exact encryption algorithm being used.

MAKO DEVICE	ENCRYPTION	THROUGHPUT	CONNECTIONS
4500	AES-GCM	20Mbit/s	20
	ChaCha20-Poly1305	40Mbit/s	20
4600	AES-GCM	20Mbit/s	20
	ChaCha20-Poly1305	40Mbit/s	20
6600	AES-GCM	80Mbit/s	50
	ChaCha20-Poly1305	120Mbit/s	50
7600	AES-GCM	300Mbit/s	5,000
	ChaCha20-Poly1305	500Mbit/s	5,000
8600	AES-GCM	300Mbit/s	8,000
	ChaCha20-Poly1305	500Mbit/s	8,000
Mako Virtual Concentrator	AES-GCM	150Mbit/s	5,000
	ChaCha20-Poly1305	150Mbit/s	5,000

While Mako VPN Cloud can route all LAN traffic securely to centralized Mako VPN Concentrators for centralized egress to the Internet, the optimal deployment uses local Internet breakout, dedicating VPN bandwidth for private/corporate communications only. Mako Enterprise Firewall Rules, Mako Guardian content filtering and Mako PCI or Enterprise Templates can all be used to enforce a consistent Internet access policy across all sites using local Internet breakout.

Mako VPN Cloud has an overhead of 84-bytes per packet, which equates to a 5.6% bandwidth overhead for a typical Internet connection with a 1500-byte MTU.

Configuration

Mako VPN Cloud automatically works with both dynamic and static Internet IP addresses, as well as in Network Address Translation (NAT) environments.

Mako VPN Concentrators using a static IP address will achieve the best failover performance, however a dynamic IP address can also be used without degrading security or management control. VPN concentrators can also be used behind a NAT device, provided the device can deliver the required port-forwarding to the Mako concentrator. Two Mako devices, in a configuration where both are behind NAT devices, can still securely send VPN traffic to each other using a Mako VPN Concentrator as an intermediary. Alternatively, the Mako Mesh Routing and Temporary Connections options can be activated to make a direct connection between the two NATed Mako devices, reducing traffic latency and VPN concentrator load.

Each LAN shared across the Mako VPN Cloud must use a unique subnet within the Cloud in order for traffic to be routed correctly. Source NAT (SNAT) can be used where multiple locations share the same LAN subnet. For example, with two locations both sharing LAN 1 with a subnet of 192.168.1.0/24, the user can allocate VPN Cloud SNATs of 10.0.1.0/24 and 10.0.2.0/24 respectively.

As well as LANs, Mako VPN Cloud can also share access to static routes, other Mako VPN Clouds, other IPsec connections, and imported BGP routes.

Example Scenarios

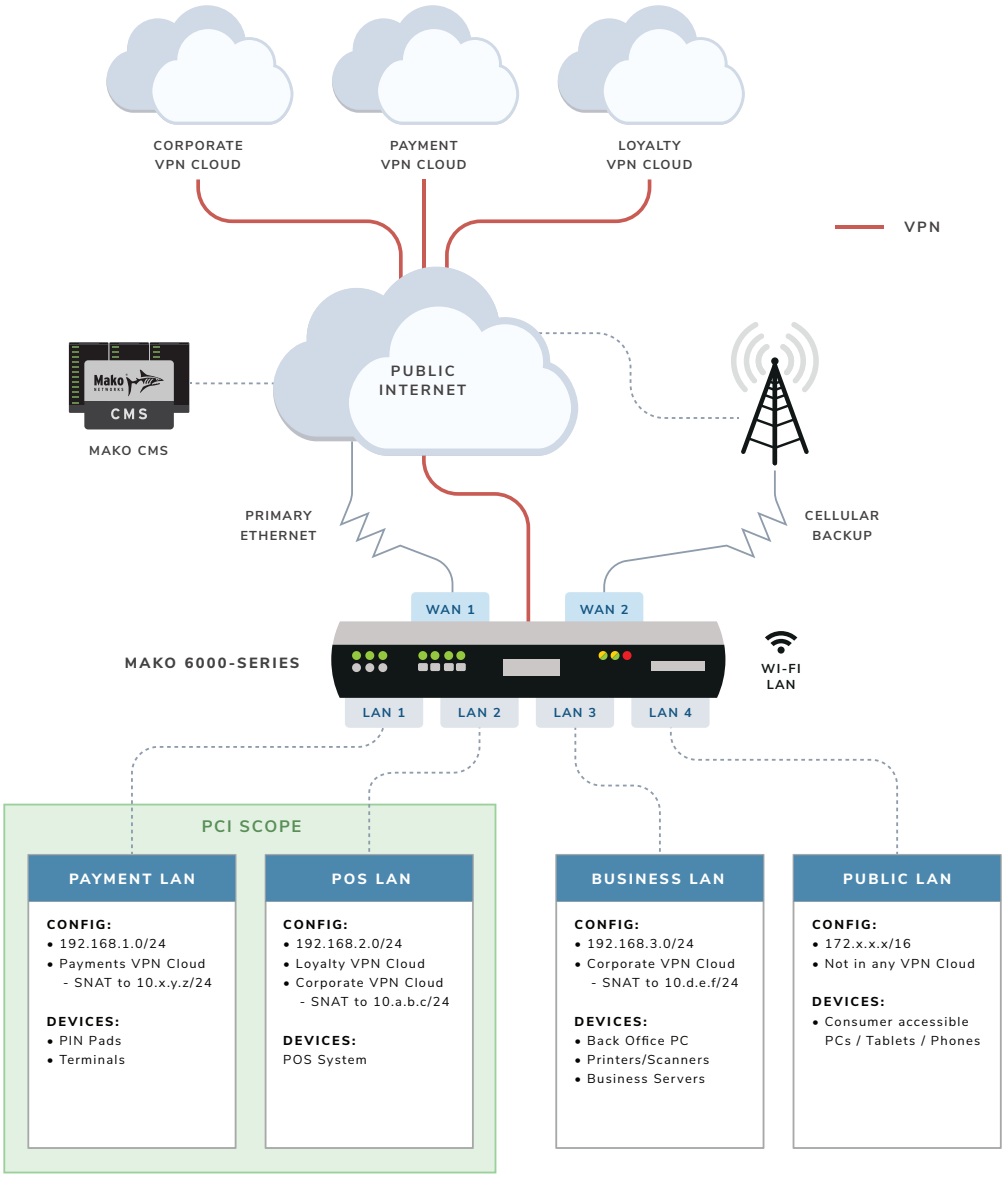
- ***Retail Merchant with payments over VPN Cloud***

In this example, a retail merchant with approximately 5,000 individual sites connected via a series of segmented VPN Clouds sends all payment transactions securely through a dedicated Payments Mako VPN Cloud to their central payment processor. An EPOS system separately tracks inventory changes and loyalty transactions through their Corporate Mako VPN Cloud and a third VPN Cloud set up with their loyalty partners.

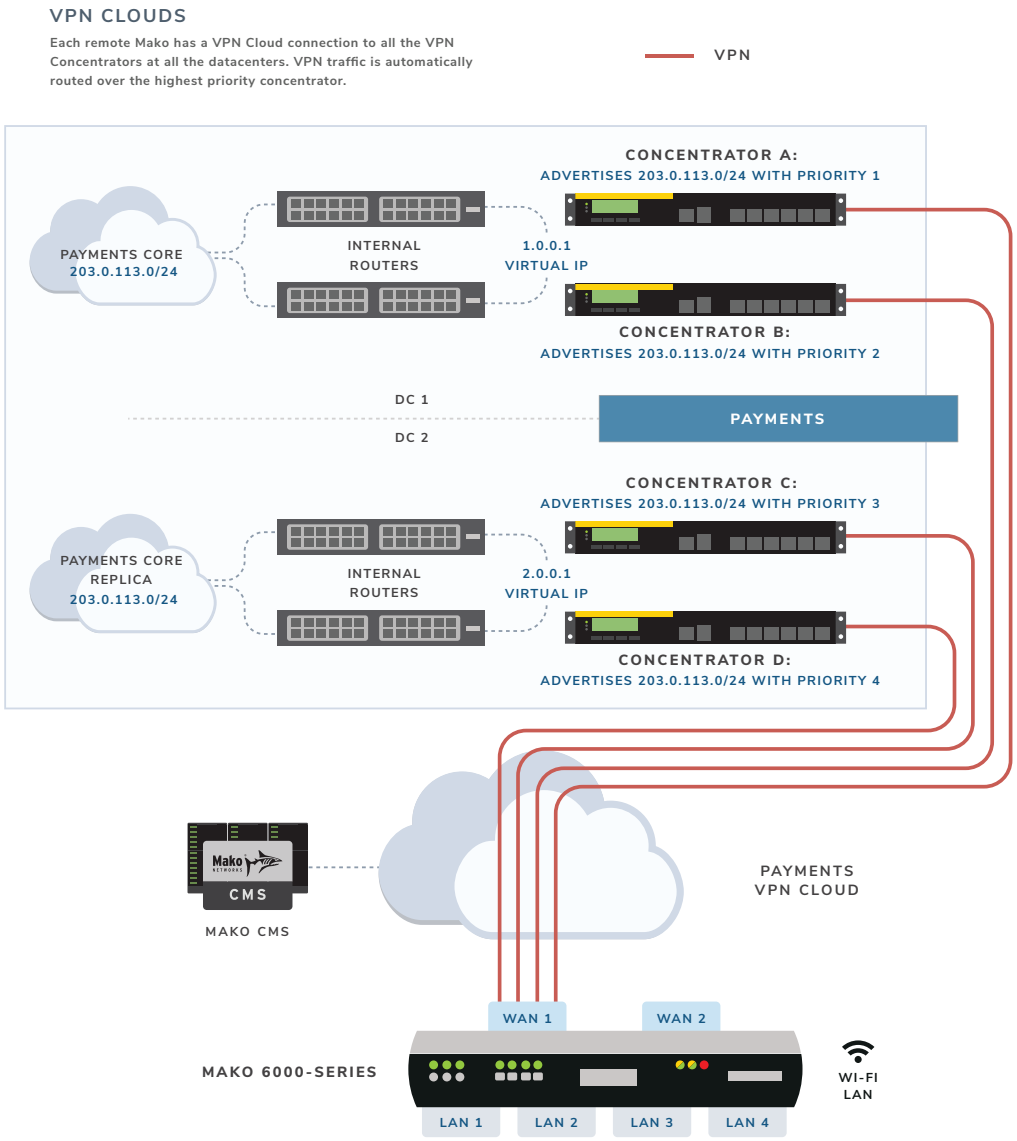
The customer has also set up two additional LANs internal to the stores, one for payments and one for other business traffic. The Payment LAN, which contains their POS equipment, is securely segmented from all other LANs, and firewall rules on the Payments Mako VPN Cloud don't allow any inward connections across the VPN. Similarly, the EPOS LAN is securely segmented from all other LANs, and the firewall rules on the Corporate and Loyalty Mako VPN Clouds don't allow any inward connections to the EPOS LAN. The Payment and EPOS LANs also have a source NAT (SNAT) applied, as the business always uses the same subnet address across all its stores for these LANs.

The Business LAN is for non-payment related activities such as CCTV, backups and email. It also has access to the Corporate Mako VPN Cloud, however the firewall rules in place on the Cloud allow for inward connections so the businesses support staff can remotely access their CCTV systems.

A cellular WAN is used in a failover configuration to ensure services are available during an outage of the Ethernet WAN but is limited to use only for the Payments network so cellular data costs are kept under control.


CORPORATE VPN CLOUD
PAYMENT VPN CLOUD
LOYALTY VPN CLOUD
VPN
PUBLIC INTERNET
CMS
MAKO CMS
PRIMARY ETHERNET
CELLULAR BACKUP
WAN 1
WAN 2
MAKO 6000-SERIES
WI-FI LAN
LAN 1
LAN 2
LAN 3
LAN 4
PCI SCOPE
PAYMENT LAN
CONFIG:
• 192.168.1.0/24
• Payments VPN Cloud
- SNAT to 10.x.y.z/24
DEVICES:
• PIN Pads
• Terminals
POS LAN
CONFIG:
• 192.168.2.0/24
• Loyalty VPN Cloud
• Corporate VPN Cloud
- SNAT to 10.a.b.c/24
DEVICES:
POS System
BUSINESS LAN
CONFIG:
• 192.168.3.0/24
• Corporate VPN Cloud
- SNAT to 10.d.e.f/24
DEVICES:
• Back Office PC
• Printers/Scanners
• Business Servers
PUBLIC LAN
CONFIG:
• 172.x.x.x/16
• Not in any VPN Cloud
DEVICES:
• Consumer accessible
PCs / Tablets / Phones

In this example, the Payments VPN Cloud data center end is shown split across multiple data centers and involves multiple Mako VPN Concentrators for high availability.



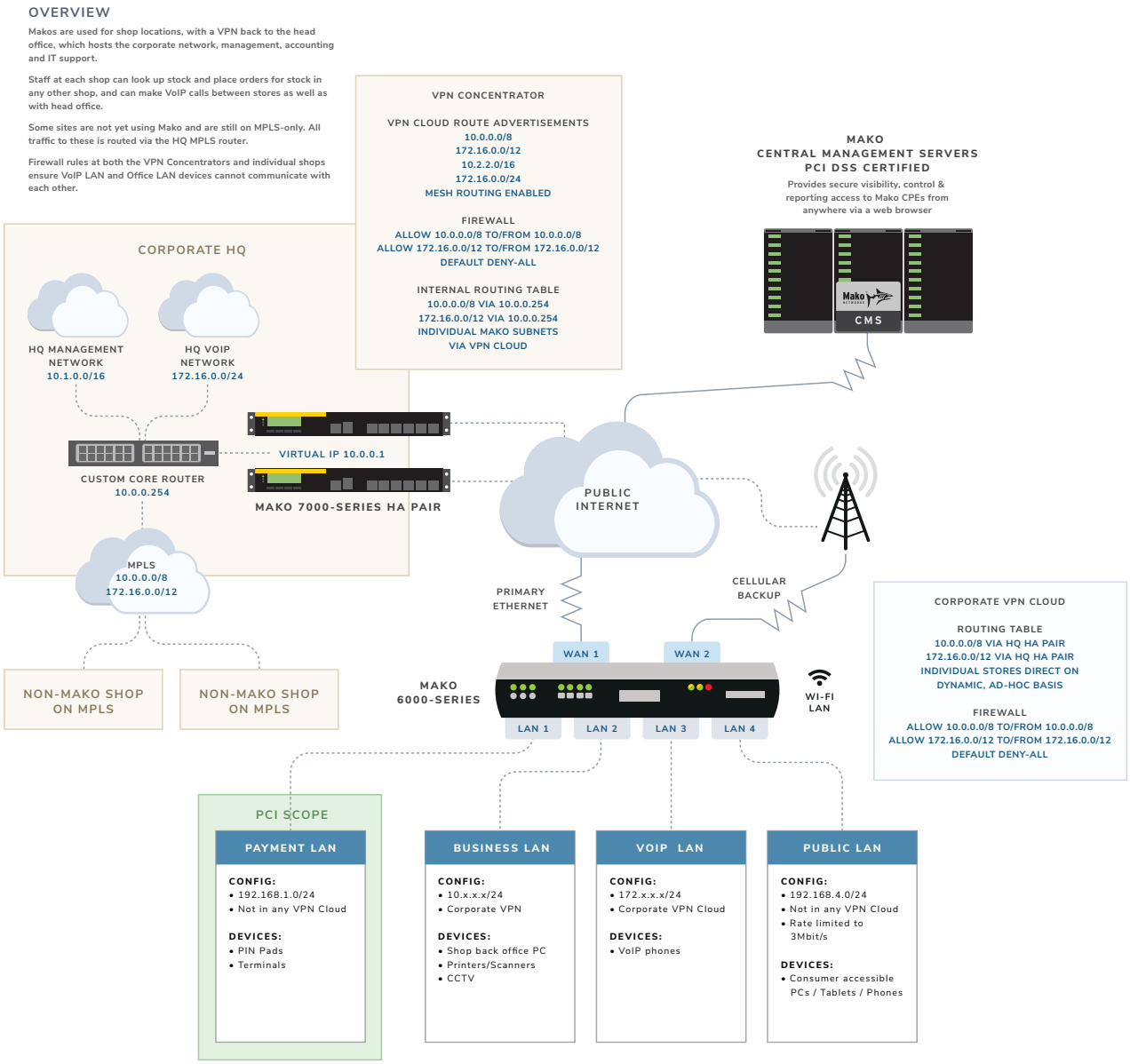
- ***Retail Merchant with payments over Internet***

Alternatively, in this example, payment transactions go directly over the local Internet connection to the organization's payment processor. A Mako PCI DSS Template is applied to the Payments LAN as a way to secure the environment and prevent any unauthorised traffic from entering or exiting the LAN.

Each store can use the Mako VPN Cloud to route VoIP traffic as well, allowing the included Mako quality of service (QoS) to manage the VoIP traffic running directly between the stores that are connected via the VPN Cloud.

Each store also has a Back Office LAN that includes an inventory management solution that other stores can query across the VPN Cloud. Initially, each store only has a Mako VPN Cloud connection to a Mako VPN Concentrator at their data center, however, the cloud's intelligent routing system will dynamically establish a temporary, secure tunnel direct between the two stores.

The direct link keeps latency to a minimum, which greatly benefits VoIP traffic. This also reduces the amount of traffic that flows through the Mako VPN Concentrator, allowing the concentrator save its processing power for traffic that needs to go through it.



VPN CLOUD

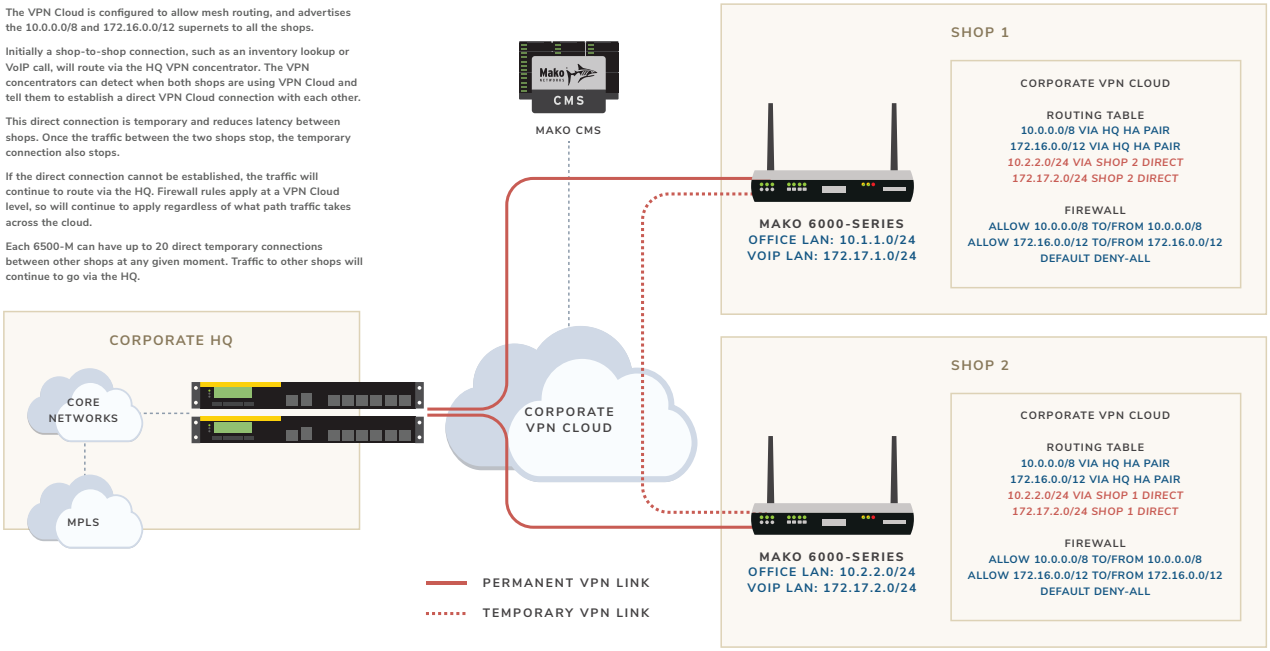
The VPN Cloud is configured to allow mesh routing, and advertises the 10.0.0.0/8 and 172.16.0.0/12 supernets to all the shops.

Initially a shop-to-shop connection, such as an inventory lookup or VoIP call, will route via the HQ VPN concentrator. The VPN concentrators can detect when both shops are using VPN Cloud and tell them to establish a direct VPN Cloud connection with each other.

This direct connection is temporary and reduces latency between shops. Once the traffic between the two shops stop, the temporary connection also stops.

If the direct connection cannot be established, the traffic will continue to route via the HQ. Firewall rules apply at a VPN Cloud level, so will continue to apply regardless of what path traffic takes across the cloud.

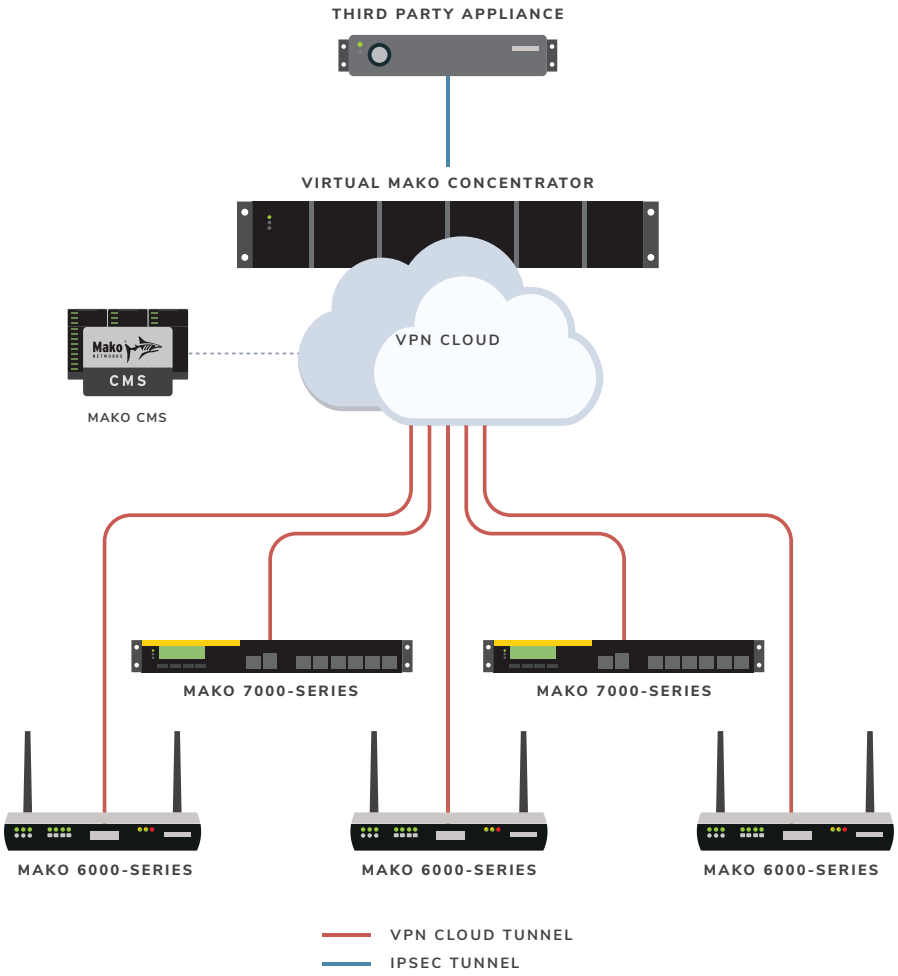
Each 6500-M can have up to 20 direct temporary connections between other shops at any given moment. Traffic to other shops will continue to go via the HQ.



Mako VPN Cloud and Virtual Makos

Third Parties can benefit from many of the features of Mako VPN Cloud without having to deploy their own VPN Concentrators and without having to terminate hundreds or thousands of VPNs on their internal network equipment. By using a Mako Networks-hosted Virtual VPN Concentrator, their customers' Mako devices can maintain Mako VPN Cloud connections to these Mako Virtual VPN Concentrators, and each concentrator will then have one or more IPsec tunnels into the third party's VPN appliances.

Mako users can also use their own Mako Virtual VPN Concentrators to link their sites together or to provide site-level access to one or more third parties without having to install and manage any physical equipment in a data center.

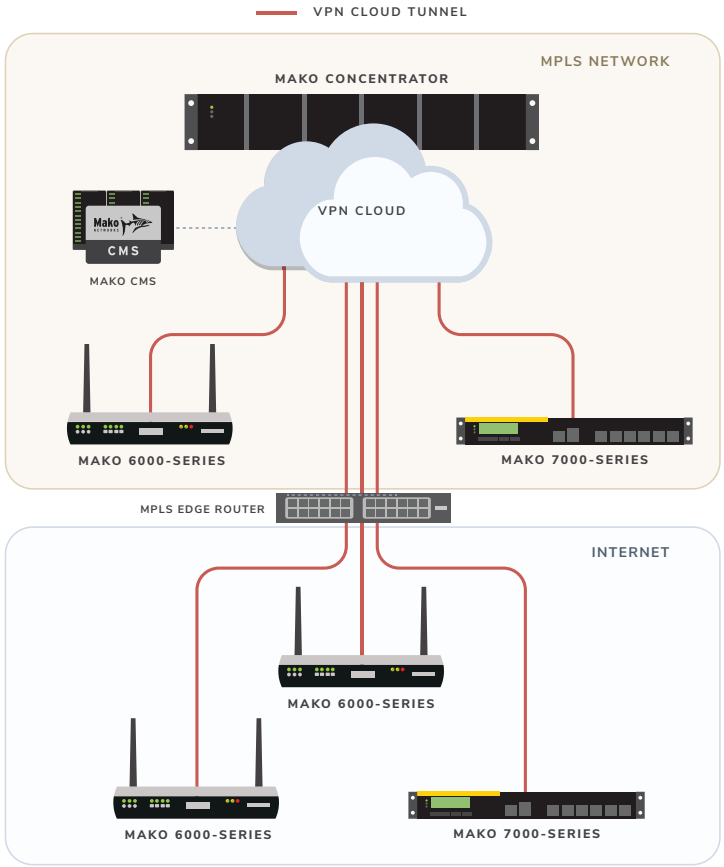


VPN Cloud and MPLS

Unlike MPLS and traditional private networks, each Mako-connected site can access the Internet directly from their local Internet connection, without the use of a centralized Internet breakout hosted at a data center. This reduces the throughput requirements of data center VPN concentrators, and provides a more responsive Internet experience for local users through reduced latency and greater bandwidth. Mako Enterprise Templates and Mako Guardian content filtering can be used to apply a consistent Internet firewall and web policy at all sites, removing one of the main drivers for a centralized Internet breakout at a data center.

Mako VPN Cloud co-exists with existing MPLS and other private networks by deploying one or more Mako VPN Concentrators within the MPLS environment, along with a breakout to the Internet for the VPN Cloud traffic. This can be achieved by assigning the Mako VPN Concentrator(s) a public, Internet routable IP address, or by assigning a private NAT IP to the concentrator and port forwarding traffic from a public, Internet routable IP address to it.

The MPLS infrastructure and Mako VPN Concentrators will have routing table entries for each other. Individual entries can be used for each site, however it's preferable if they can be grouped into supernets to simplify routing tables. For example, 10.0.0.0/9 could be for MPLS sites, and 10.128.0.0/9 could be for Internet Mako sites. BGP between the Mako VPN Concentrators and the MPLS routers is also an option.



Best Practices

- ***Firewall and Access Control***

We recommend placing egress and ingress Mako VPN Cloud firewall rules on the edge Mako Security Gateways. In particular, egress firewall rules ensure the VPN does not transmit traffic that will ultimately be denied at the final destination, reducing wasted VPN bandwidth.

To simplify management of Mako VPN Cloud firewall rules on large installations with many Mako Security Gateways, we recommend using Mako Enterprise Templates to automate and consolidate the firewall management process.

- ***Transit Traffic***

Installations with large amounts of transit traffic through the Mako VPN Concentrators, such as facilitating VoIP phone calls between locations, or file sharing between locations, typically results in a lot of traffic going through the Mako VPN Concentrator intermediary. This traffic, along with the increased latency associated with it, can be avoided by enabling Temporary Connections and Mesh Routing. The Mako VPN Concentrator will identify traffic flowing through it that would be better served by a direct VPN between the two locations, and automatically establish a temporary direct VPN. The VPN will last as long as there is traffic going between the two locations, and because it is automatically set up and torn down, there is no need for a user to manually manage such connections.

The Mako 6000-series Security Gateways can support up to 20 concurrent Mako VPN Cloud Temporary Connections in addition to their 50 normal permanent connections. Any site-to-site communications beyond the concurrent limit will continue to be routed via the VPN Concentrator transit and will automatically switch over to temporary direct connections when there is availability.

- ***High Availability***

We recommend the use of two Mako VPN Concentrator for high availability within a single datacentre. Each Mako VPN Concentrator should ideally be on a different power supply and Internet feed.

If using two concentrators is not possible, a degree of high availability of Internet access is still possible using a single device by converting one of the LAN ports to a second Ethernet WAN port.

- ***Scalability***

We recommend numbering LAN subnets such that it is easy in the future to introduce multiple Mako VPN Clouds and additional Mako VPN Concentrators to distribute the VPN load as your organization grows. Avoid allocating sequential subnets to each site and if possible spread the allocations evenly across a series of supernets. Refer to the main Scalability section for an example table of supernets. This makes it easier to utilise additional concentrators immediately across existing sites, rather than only for new sites or sites that can be renumbered.

VPN Technology Comparison

	MAKO VPN CLOUD	IPSEC	OPENVPN
Site to Site VPN	Yes	Yes	Yes
Remote user VPN	No	Yes	Yes
Encryption	AES-GCM 128/256bit ChaCha20-Poly1305 (256bit)	AES 128/256bit	AES 128/256bit
Authentication	Certificates	PSK, Certificates, Pluggable Auth	Certificates, User/Pass, Pluggable Auth
Forward Secrecy (PFS)	Mandatory	Optional	Optional
Configuration Complexity	Low	High	Medium
Scalable	Yes	Yes	Not easily
Throughput	***	*****	***
Hub-and-Spoke Routing	Yes	Yes	Yes
Mesh Routing	Yes	Requires vendor-specific overlay network and routing protocols e.g. Cisco DMVPN	No
Temporary Mesh Connections	Yes	Requires vendor-specific overlay network and routing protocols e.g. Cisco DMVPN	No
Network Layer	IP (L3)	IP (L3)	IP (L3) or Ethernet (L2)
Automated recovery on WAN failover	Yes	Requires vendor-specific overlay network and routing protocols e.g. Cisco DMVPN	Partial – connection will time out and reconnect
Zero packet loss option	Yes	No	No
Geographically Diverse Replica Networks	Yes	Requires vendor-specific overlay network and routing protocols	Yes
2-Factor Authentication	No	Yes, using extensions	Yes
SNAT LANs	Yes	Yes, vendor dependent	Yes, vendor dependent
NAT and CGNAT Internet	Yes	Yes. Limited vendor support, often compatibility issues	Yes
Cross-Vendor Support	No	Yes, except when using vendor-specific extensions or complicated setups.	Yes
Operational Status	Active	Active	Active

Cryptographic Profile

	ALGORITHMS	COMMENTS
Encryption	ChaCha20-Poly1305 (256bit, AEAD) AES-GCM (128/256bit, AEAD)	ChaCha20-Poly1305 recommended
Authentication	X.509 Certificates (ECDSA) CA Algorithm: P-521 (secp521r1) Device Algorithm: P-384 (secp384r1) Signature: ECDSA with SHA256	Certificate management/rotation lifecycle handled by the Mako CMS. Rotation periods are user configurable.
Forward Secrecy (PFS)	ECDHE using X25519, expanded via HKDF HMAC-SHA256.	

In Summary

Mako's VPN Cloud technology provides secure, scalable, highly redundant wide area networking and allows for transport across multiple carriers using virtually any Internet connection. The Mako VPN Cloud can also be modified in real time – Mako VPN Concentrators can be added or removed from a Cloud when needed. It offers distributed enterprises opportunities to improve network reliability, reduce costs and enhance security, while also creating high levels of visibility and control for internal network operators and management.

If you would like more information about our technology or its potential application within your organization, please contact us at sales@makonetworks.com.