Skyhigh Secure Topologies

Table of contents

1. [Topology 1](https://success.myshn.net/Skyhigh_for_Sanctioned_IT/MVISION_Cloud_for_Salesforce/zzSkyhigh_Salesforce_On-Premise_Deployment/Skyhigh_Secure_Topologies#Topology_1)
2. [Topology 2](https://success.myshn.net/Skyhigh_for_Sanctioned_IT/MVISION_Cloud_for_Salesforce/zzSkyhigh_Salesforce_On-Premise_Deployment/Skyhigh_Secure_Topologies#Topology_2)
3. [Load Balancers](https://success.myshn.net/Skyhigh_for_Sanctioned_IT/MVISION_Cloud_for_Salesforce/zzSkyhigh_Salesforce_On-Premise_Deployment/Skyhigh_Secure_Topologies#Load_Balancers)
4. [Platform Security Features](https://success.myshn.net/Skyhigh_for_Sanctioned_IT/MVISION_Cloud_for_Salesforce/zzSkyhigh_Salesforce_On-Premise_Deployment/Skyhigh_Secure_Topologies#Platform_Security_Features)

The modular and stateless architecture provides the flexibility to configure MVISION Cloud to work in different network topologies. As long as the connectivity between MVISION Cloud and the Dictionary Server is preserved, and as long as this topology allows interception of the web traffic and routing, MVISION Cloud will function properly. This flexibility provides customers with the ability to deploy MVISION Cloud in multiple network architecture configurations, either on-premises or as a hosted service in the cloud.

In the typical on-premise deployment, servers reside in a trusted zone and are configured to intercept traffic that arrives from trusted users/clients. The trusted zone includes users that access MVISION Cloud from within the organization network, remote users that use VPN to connect the organization users, Salesforce callouts that are sent from Salesforce into workstations that reside in the organization network, and emails that are generated within the Salesforce platform.

Topology 1

In the first toplogy scenario, all servers (Proxies, Key Server, Dictionary) are in a trusted zone. Web access (HTTP/HTTPS/SMTP) to MVISION Cloud is allowed only from within the trusted zone or trusted origin (i.e. Salesforce). This requirement can be enforced on the IP level.

Example 1: Inbound (WAN to LAN)

Block any access from outside to MVISION Cloud except the following:

* Responses to requests that originated from MVISION Cloud (HTTP/HTTPS).
* Web-services callout (HTTP/HTTPS from Salesforce’s static IPs range to the proxies and only if the MVISION Cloud implementation includes integration with web-services).
* SMTP traffic (from Salesforce’s static IPs range to the Proxies and only if the MVISION Cloud implementation includes integration with emails).

Exampe 2: Outbound (LAN to WAN)

Allow all access from MVISION Cloud to the WAN (HTTP/HTTPS/SMTP)

* Remote/mobile users use VPN
* DNS configuration – can use either local or global DNS settings.

Note: There are additional ports that need to be opened to enable proper operation of MVISION Cloud (mostly for internal communication of the MVISION Cloud servers or for integration with external servers like the Token Dictionary or NFS server). For more details go to the network requirement section.

Topology 2

Sometime Salesforce/MVISION Cloud  implementation requires a topology that allows MVISION Cloud to handle traffic originates from unknown origins, for example mobile/remote users (the organization users that don’t use VPN), or customers/partners of the organization that need to have access to the customer org (like partners that need to access/post sensitive data on a customer portal).

In this case our recommendation is to use the architecture that is presented below and place MVISION Cloud servers in the DMZ.

Other Considerations include:

* MVISION Cloud Public IP. Required only if need to intercept emails and/or Salesforce’s web-services callout. Use port-forwarding or similar mechanism to route HTTP/HTTPS/SMTP traffic from the MVISION Cloud CASB external IP address to the Proxy server’s internal IP addresses.
* DNS configuration. Can use either local or global DNS settings. Domains that are associated with Salesforce’s web-services callout and the MVISION Cloud MX record must be registered publicly.
* Email. Emails sent from Salesforce into the organization are trusted and organizations can use the FW setting approach (Topology 1) to guarantee that the incoming email messages come from Salesforce.

Sometimes your Salesforce implementation requires that MVISION Cloud accept email traffic that arrives from unknown sources (e.g. Email-To-Case). In this case customers would usually prefer to route the email to the organization’s email gateway for vulnerability scanning and then route it to MVISION Cloud.

Emails sent from Salesforce using MVISION Cloud's MX domain need to be routed to the organization mail gateway. That means MVISION Cloud's MX record should point to the Email Gateway IP, and the organization’s mail gateway should be configured to route the MVISION Cloud emails to the MVISION Cloud proxies.

Load Balancers

Suitable for any topology, optional load balancers can be configured to maintain high availability. The load balancer should reside between the proxies for incoming requests from end users, email, or web services callouts.

Platform Security Features

Another level of security can be achieved by enabling the following platform security features:

* TLS /Security for emails. Secure the email communication between Salesforce and MVISION Cloud.
* Secure callout. Uses a two-way SSL authentication between Salesforce callouts and your web services.
* File system. NFS (SAN/NAS).
* Token Dictionary.