

Security on the Skytap Platform

Implementing comprehensive security controls in the cloud

Created By: John Bradshaw, Principal Architect - EMEA

April, 2020

Revision Number 0.1

# Table of Contents

[Table of Contents 2](#_Toc37014217)

[Precis 4](#_Toc37014218)

[Overview 5](#_Toc37014219)

[Best Practices 7](#_Toc37014220)

[Security as a Service 7](#_Toc37014221)

[Legend 7](#_Toc37014222)

[Secure by Design 8](#_Toc37014223)

[Platform 9](#_Toc37014224)

[Security Policies 9](#_Toc37014225)

[Notifications 9](#_Toc37014226)

[Authentication, Authorisation and Accounting 9](#_Toc37014227)

[Users, Groups, Projects and Departments 9](#_Toc37014228)

[Users 10](#_Toc37014229)

[User Permissions 10](#_Toc37014230)

[Extended User Permissions 10](#_Toc37014231)

[Groups 11](#_Toc37014232)

[Projects 11](#_Toc37014233)

[Project Permissions 11](#_Toc37014234)

[Project Example 12](#_Toc37014235)

[Departments 13](#_Toc37014236)

[Single Sign-On 13](#_Toc37014237)

[Labels 13](#_Toc37014238)

[Auditing 14](#_Toc37014239)

[Management 15](#_Toc37014240)

[Antivirus 16](#_Toc37014241)

[Supported Implementations 16](#_Toc37014242)

[Patching 16](#_Toc37014243)

[Supported Implementations 16](#_Toc37014244)

[Authentication, Authorisation, Accounting 16](#_Toc37014245)

[Supported Implementations 16](#_Toc37014246)

[Backup 16](#_Toc37014247)

[Supported Implementations 17](#_Toc37014248)

[Secrets Management 17](#_Toc37014249)

[Supported Implementations 17](#_Toc37014250)

[Log Management 17](#_Toc37014251)

[Supported Implementations 17](#_Toc37014252)

[Example Architecture 18](#_Toc37014253)

[Edge Networking 19](#_Toc37014254)

[Outbound Proxy 19](#_Toc37014255)

[Supported Implementations 20](#_Toc37014256)

[Inbound Proxy 20](#_Toc37014257)

[Supported Implementations 20](#_Toc37014258)

[VPN / Private Connection 20](#_Toc37014259)

[Site-to-Site VPN 20](#_Toc37014260)

[Private Network Connection (PNC) 21](#_Toc37014261)

[Firewall 22](#_Toc37014262)

[Supported Implementations 22](#_Toc37014263)

[Intrusion Detection System / Intrusion Prevention System 22](#_Toc37014264)

[Supported Implementations 22](#_Toc37014265)

[Architecture 23](#_Toc37014266)

[Virtual Machines 24](#_Toc37014267)

[VM Templates 24](#_Toc37014268)

[Authentication, Authorisation and Accounting 24](#_Toc37014269)

[Supported Implementations 25](#_Toc37014270)

[Patching 25](#_Toc37014271)

[Supported Implementations 25](#_Toc37014272)

[Antivirus 25](#_Toc37014273)

[Supported Implementations 25](#_Toc37014274)

[HIDS/HIPS 25](#_Toc37014275)

[Supported Implementations 25](#_Toc37014276)

[Firewall 25](#_Toc37014277)

[Supported Implementations 26](#_Toc37014278)

[Example Architecture 26](#_Toc37014279)

[Internal Networking 27](#_Toc37014280)

[Implementation Guides 28](#_Toc37014281)

[References 29](#_Toc37014282)

# 

# Precis

To be removed from final document

Project LANDMINE was set up to address several security incidents customers have experienced over the last 12 months.

1. Customers expect Skytap to have a position on good design
   1. This is Skytap’s platform, we should know how to best use it
   2. We should have known good designs that customers can use
2. Customers expect Skytap to have technology recommendations
   1. With our experience, we should have known good applications/services
3. Customers expect Skytap to tell them if they’ve made a bad decision
   1. Poor design choices by customers create the impression that Skytap is an incomplete or insecure platform
   2. Customers hold Skytap accountable

To be removed from final document



# Overview

Secure operations in a cloud environment require a multidisciplinary and multi-layered approach; this document outlines the steps necessary to achieve a robust implementation on the Skytap platform. The report breaks down into Best Practices, Implementation Guides and Implementation Assets.

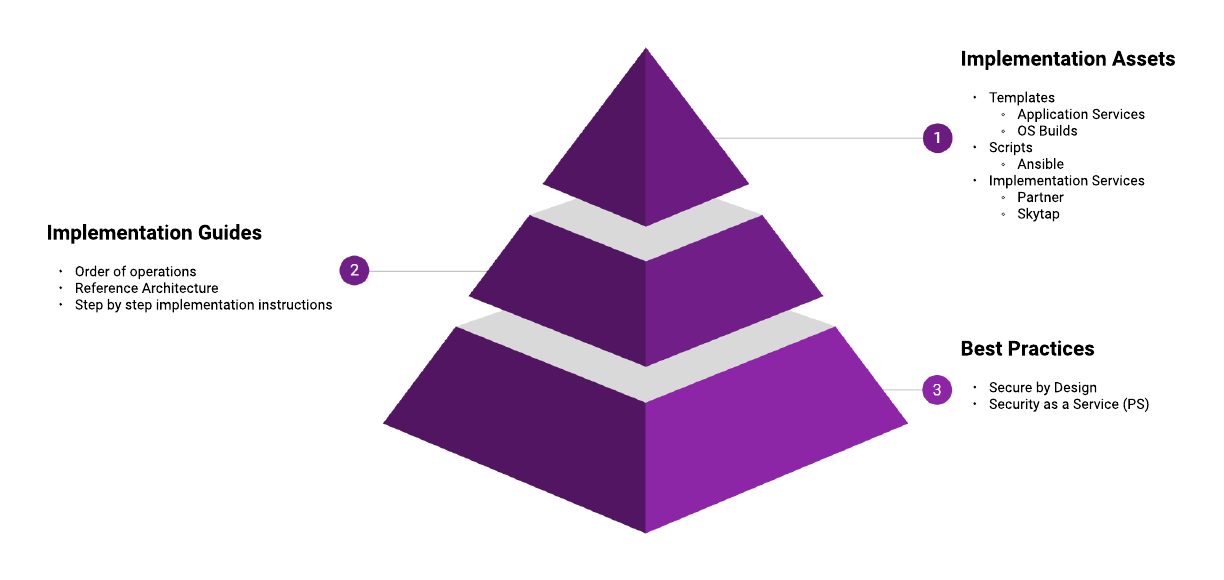
[](https://www.lucidchart.com/documents/edit/237d79f0-1b99-4e17-8b79-efc233429397/6?callback=close&name=docs&callback_type=back&v=5947&s=612)

Figure - Control Map

Each layer in this model builds on the capabilities delivered in the layer below; you cannot know how to secure a virtual machine without understanding how they can be secured and why they need to be.

Accompanying this document is a **Skytap - Security Controls Workbook** that should be referred to as you develop your High-Level Designs and Low-Level Designs, it outlines each area discussed herein with specific controls that should be applied. It also contains an example of a Risks and Mitigations register that should be considered as part of any cloud project.

The approach to the cloud must be integrated within your organisation’s Target Operating Model; this allows for the appropriate security controls to be accounted for, architected and implemented.

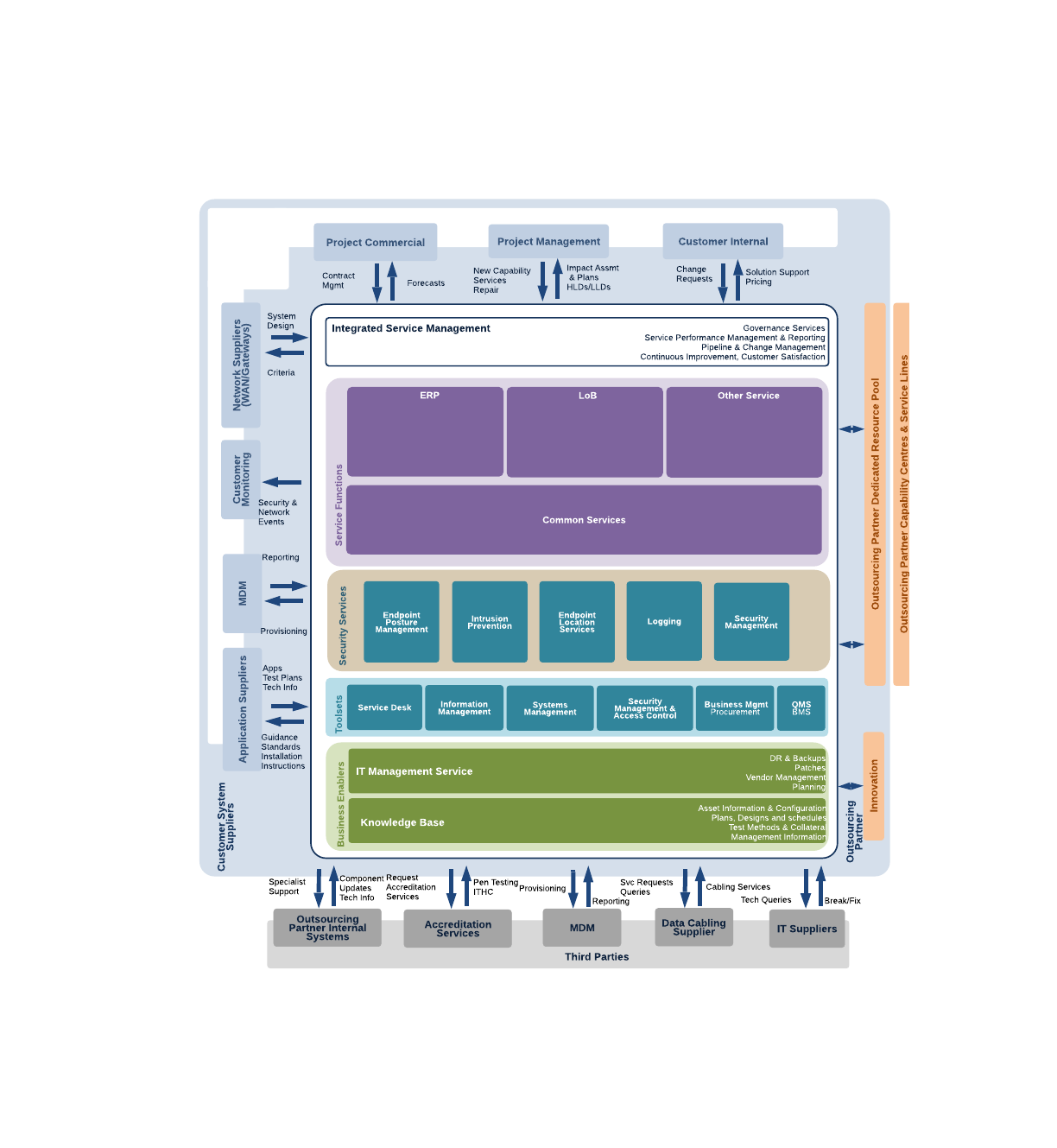
[](https://www.lucidchart.com/documents/edit/f5794a4f-e45d-4a70-9e12-9f0abf4579bb/0?callback=close&name=docs&callback_type=back&v=1701&s=612)

Figure - Example Target Operating Model (TOM)

Most organisations will have multiple cloud vendors, supported by systems integrators or outsourced management functions. Your various clouds need to be managed holistically but controls applied specifically, for example, all logging across your organisation should be consolidated into a single Security Incident Event Monitoring (SIEM) system, but the approach to management and remediation will be custom to each workload and each platform.

# Best Practices

## Security as a Service

Given the breadth of security controls available across multiple cloud vendors, the changing threat landscape and the need to support modern and legacy workloads in the enterprise space it can be difficult for organisations to provide those services internally.

Skytap works with a variety of Security as a Sevice vendors who can manage your cloud workloads and who have expert knowledge in securing clouds, and in particular Skytap.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Vendor | Capabilities | | | | | | | | | | |
| A | B | C | D | E | F | G | H | I | J | K |
| Meridian IT | ✔️ |  |  |  |  |  |  |  |  |  |  |
| IBM |  |  |  |  |  |  |  |  |  |  | ✔️ |

### Legend

|  |  |
| --- | --- |
| Key | Capability[[1]](#footnote-2) |
| A | Business continuity and disaster recovery (BCDR or BC/DR) |
| B | Continuous monitoring |
| C | Data loss prevention (DLP) |
| D | Email security |
| E | Encryption |
| F | Identity and access management (IAM) |
| G | Network security |
| H | Security assessment |
| I | Security information and event management (SIEM) |
| J | Vulnerability scanning |
| K | Web security |

## 

## Secure by Design

Within Skytap, there are four key areas to build a control framework around the Platform, Management, Internal Networking, Edge Networking and Virtual Machines.

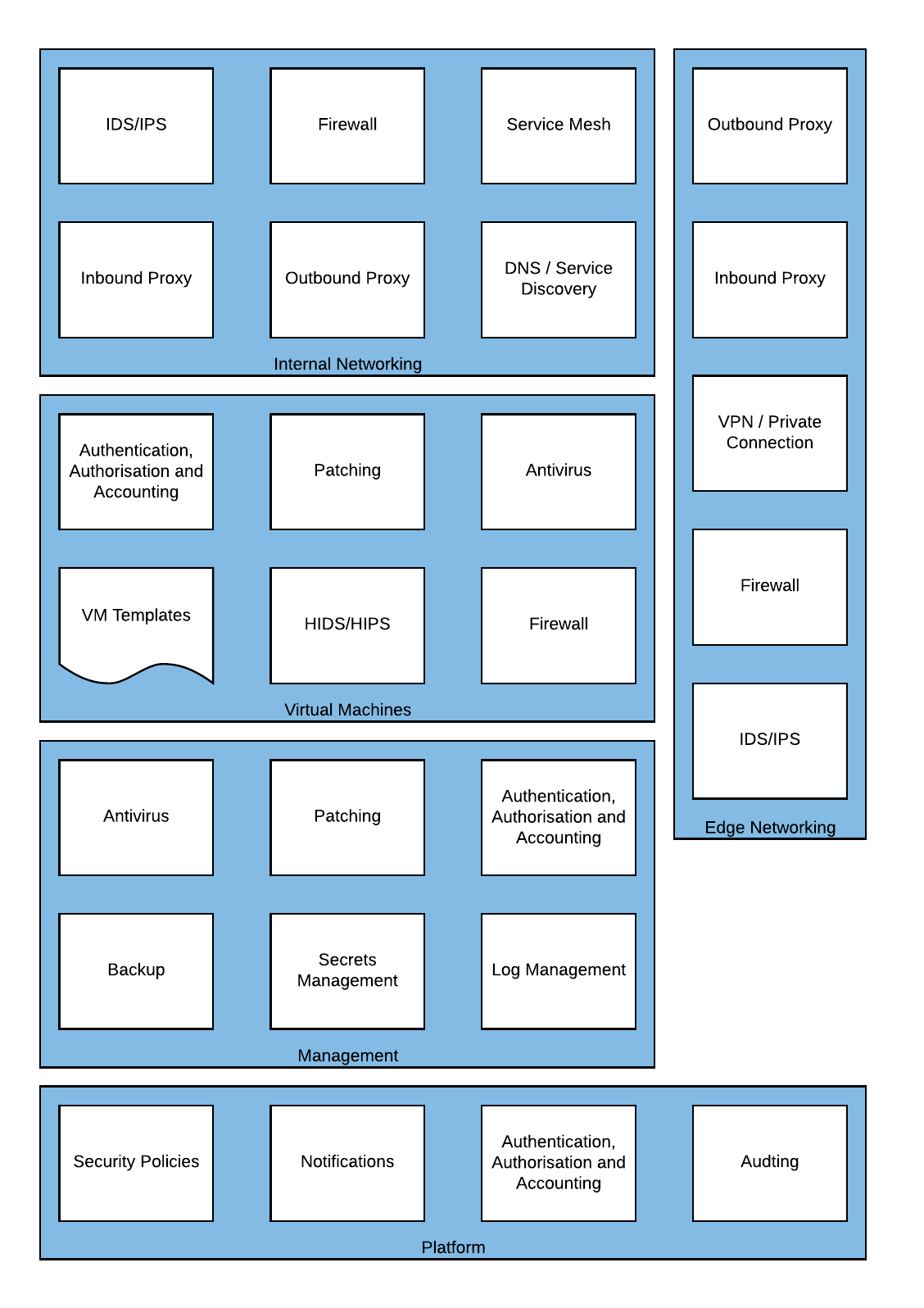
[](https://www.lucidchart.com/documents/edit/237d79f0-1b99-4e17-8b79-efc233429397/7?callback=close&name=docs&callback_type=back&v=5947&s=564)

Figure - Cloud Security Capabilities

### Platform

The Skytap platform provides controls for Security Policies; Notifications; Authentication, Authorisation and Accounting; and Auditing.

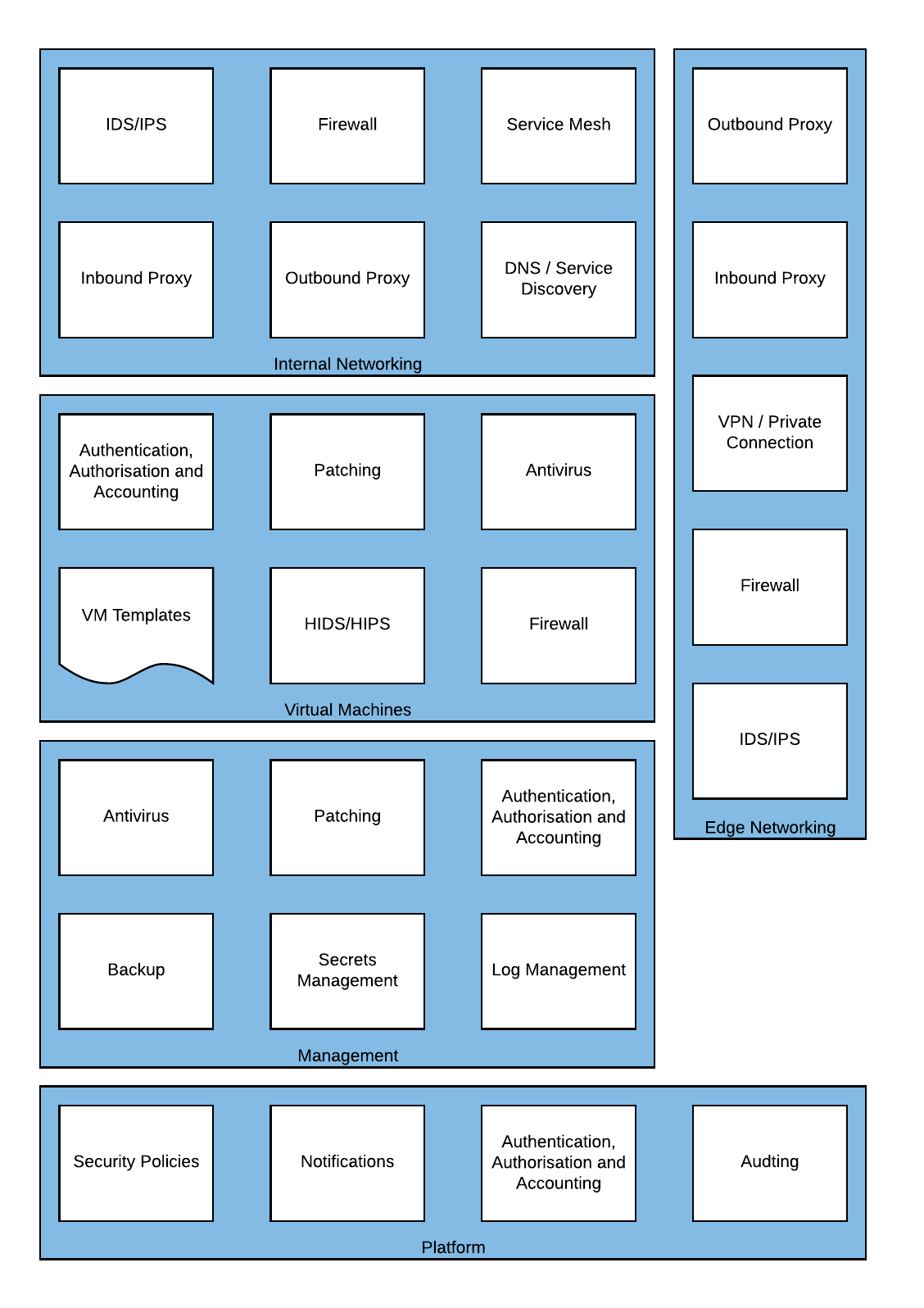
[](https://www.lucidchart.com/documents/edit/237d79f0-1b99-4e17-8b79-efc233429397/7?callback=close&name=docs&callback_type=back&v=5947&s=564)

Figure - Platform Required Capabilities

#### Security Policies

The security policies control access to the platform for authenticated users, this can restrict connectivity to approved IP addresses (such as those on the corporate network), password complexity rules (for those not using SSO) and session timeouts (prompting for reauthentication).

#### Notifications

Notifications can be used to alert administrators and/or users of capacity or consumption events that may need to be addressed.

#### Authentication, Authorisation and Accounting

##### Users, Groups, Projects and Departments

The Users, Groups, Projects and Departments are used to control Cost and/or Access to services; they should be configured to align with your organisation’s best business processes and operational best practice.

|  |  |  |
| --- | --- | --- |
|  | Cost Control | Access Control |
| Users | ✔️ | ✔️ |
| Groups |  | ✔️ |
| Projects |  | ✔️ |
| Departments | ✔️ |  |

A User is a named individual or service account that can authenticate to the platform. Once authenticated, it can then assume either a Restricted User, Standard User, User Manager or Administrator platform role.

Groups are a collection of user accounts with the same access level, for example, a team of developers on a Project.

Projects are a collection of resources: environments, templates and assets. Groups or Users can be added to the project with different permissions.

Departments are used to consolidate consumption allowances and reporting, and Departments can be created with hard limits on the resources they can consume. A user may be a member of a single Department.

###### Users

The restricted role is best for users who need tightly controlled access to a limited number of resources. The standard role is not recommended unless Skytap is operating in an isolated fashion, i.e. not connected to other clouds or the corporate network. The user manager role is best for users who need to manage and organize users and groups but who don’t need full administrator capabilities. The administrator role is best for trusted users in your organization who need to manage users, resources, and account-wide settings.

It is recommended to set most users to Restricted and grant additional access through project membership, outlined below.

User Permissions

| Restricted | Standard | User Manager | Administrator | Can do this |
| --- | --- | --- | --- | --- |
| ✔️ | ✔️ | ✔️ | ✔️ | Access shared project resources |
| \* | ✔️ | ✔️ | ✔️ | Create and own projects |
| † | ✔️ | ✔️ | ✔️ | Create environments, templates, and assets |
|  |  | ✔️ | ✔️ | Create and edit users and groups |
|  |  | ✔️ | ✔️ | Delete groups |
|  | ‡ | ‡ | ✔️ | Create and view reports |
|  |  |  | ✔️ | Create and edit departments |
|  |  |  | ✔️ | Delete users |
|  |  |  | ✔️ | Create and edit account-wide settings (password policies, access policies, usage limits, etc.) |
|  |  |  | ✔️ | Edit and delete environments, templates, and assets owned by all users in the account. |

\* A restricted user can’t create a project, but another user can make a restricted user a project owner.

† Restricted users have limited permission to create environments.

‡ An administrator must grant reporting privileges for a user to create and view reports.

Skytap has additional permissions that can be enabled or disabled for each user. Some of these permissions are displayed only when specific features are enabled in the platform.

The table below shows the additional permissions that are **optional (O)** for each type of user.

* Most permissions are **mandatory (M)** for administrators and can’t be disabled.
* Restricted users can’t have most permissions enabled.

Extended User Permissions

| Restricted | Standard | User Manager | Administrator | Permission |
| --- | --- | --- | --- | --- |
| O | O | O | M | This user is able to access [public templates](https://help.skytap.com/Public_Templates.html) and [public assets](https://help.skytap.com/Using_Public_Assets.html). |
|  | O | O | M | This user is able to [import VMs](https://help.skytap.com/importing-vms-overview.html) into Skytap. |
|  | O | O | M | This user is able to [export VMs](https://help.skytap.com/Exports.html) from Skytap. |
|  | O | O | M | This user is able to [generate reports](https://help.skytap.com/Reports.html) from Skytap.  Reporting can be enabled for the entire account or just the user's department. |
|  | O | O | O | This user is able to set [promiscuous mode](https://help.skytap.com/Enabling_Promiscuous_Mode.html) on VM network adapters for Skytap. This permission is displayed when your customer account is enabled for promiscuous mode. |

###### Groups

Groups help you manage access to project resources for a set of related users; a user can belong to multiple groups; the platform supports up to 100 groups; groups are managed by administrators and user managers.

###### Projects

Permissions are *additive*, so if a named user is granted Owner rights but is a member of a group with only Viewer permissions, they can use the Owner rights to perform actions on the project.

Projects support the concept of an Automatic Role; this role is granted to every new user on Skytap. This feature should be used sparingly to prevent excessive user permissions.

Project Permissions

| Owner | Manager | Editor | Participant | Viewer | Can do this |
| --- | --- | --- | --- | --- | --- |
| ✔️ | ✔️ | ✔️ | ✔️ | ✔️ | Access and use a running environment |
| ✔️ | ✔️ | ✔️ | ✔️ | ✔️ | Download assets |
| ✔️ | ✔️ | ✔️ | ✔️ |  | Control the power state of an environment |
| ✔️ | ✔️ | ✔️ | **‡** |  | Create an environment from a project template |
| ✔️ | ✔️ | ✔️ | **‡** |  | Copy environment |
| ✔️ | ✔️ | ✔️ |  |  | Copy template |
| ✔️ | ✔️ | ✔️ |  |  | Load an ISO |
| ✔️ | ✔️ | ✔️ |  |  | Save an environment as a template |
| ✔️ | ✔️ | ✔️ |  |  | Add, edit, and remove resources |
| ✔️ | ✔️ | ✔️ |  |  | Share resources with other projects (as Editor or Manager in both projects) |
| ✔️ | ✔️ | ✔️ |  |  | Permanently delete VMs |
| ✔️ | ✔️ |  |  |  | Add and remove project users |
| ✔️ |  |  |  |  | Delete the project |
| Administrator | | | | | Change project permissions |
| Permanently delete environments, templates, and assets that are in the project and owned by other users |

**‡**  The restricted user must be an editor or manager in at least one project to perform these actions as a participant. For example, if the user is a participant in project A and an editor in project B, the user can create an environment from a template in project A. The new environment is automatically added to project B (where the user has permission to add resources). Restricted users cannot own environments, templates, or assets outside of a project.

Project Example

**Scenario:** Let’s say you want to control and manage a set of company-wide golden templates in your customer account. You want a small set of users to maintain the templates (template creators), and you want all other users in the account to have permission to create environments from those templates (template users).

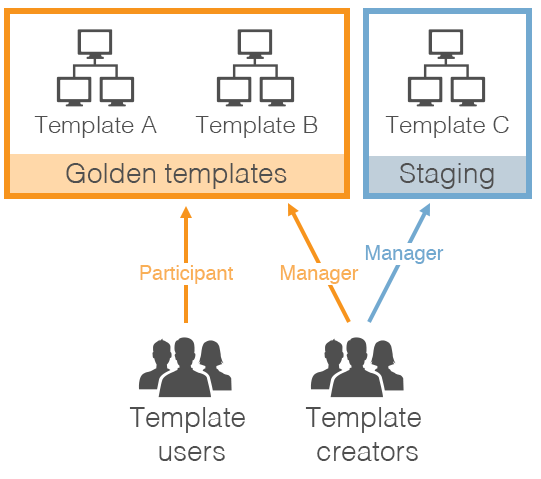


Figure - Example of Project Implementation

**Solution:** Create 2 projects:

* **Golden Templates** – Use this project to share golden templates with all users.
  + Add all finalised, approved templates to this project.
  + Add template creators to the project in the **Manager** role. **Managers** can:
    - Add templates to the project or remove templates from the project.
    - Add users to the project or remove users from the project.
  + Add all other Skytap users to the project in the **Participant** role. **Participants** can create environments from templates in the project.

Enable an **automatic role** on the project. With this setting, every new Skytap user is automatically added to this project as a **Participant**.

* **Staging** – Use this project to share in-progress environments and templates between template creators.
  + Add new, in-progress environments and templates to this project.
  + Add template creators to the project in the **Manager** role.
  + Do not add other Skytap users to this project. Because they don’t have project access, they cannot view or use environments and templates in this project.

###### Departments

Departments allow you to model company departments, business units, or project teams within the Skytap. With department monitoring and limits, you can:

* Create usage limits to cap the amount of storage, RAM hours, or concurrent RAM that department users can consume; this can guarantee that Skytap resources remain available to critical departments.
* Create usage reports to track and charge-back usage by each department.

Each user can belong to one department, and the platform supports up to 100 departments.

###### Single Sign-On

Skytap can be configured for SAML based Single Sign-On, thus making it compatible with Azure Directory Services, Corporate Active Directory and authentication services such as Ping Identity or Okta. By integrating with Single Sign-On organisations can enforce additional authentication controls such as endpoint integrity and verification, location-based authentication and conditional/just in time access.

##### Labels

Usage labels help administrators annotate environments, templates, and assets for more detailed usage reporting. After a label is added to a resource, the label appears in usage reports whenever that resource is used. The label data can be used for accounting chargebacks, cost allocation, and usage trending analysis.

Single Value label categories can be attached only once per environment, template, asset, or schedule. For example, a Single Value label of *Cost Centre* could be used for chargebacks or cost allocation purposes.

Multi-value label categories are suited for general reporting, for example, to group environments by applications in use.

#### Auditing

Auditing can be configured to send events to a Log Management tool or Security Incident Event Monitoring tool. These events are sent using Webhooks[[2]](#footnote-3), allowing for near real-time notifications to management tooling enabling security engineers to respond more rapidly than would otherwise be available.

Additionally, usage events can also be sent via Webhook to this tooling or a separate service; this can be used to monitor capacity and spend to prevent cloud sprawl or an economic denial of service.

### 

### Management

The Management layer sometimes referred to as Shared Services, contains the components necessary to secure and enforce compliance on the workloads running on Skytap.

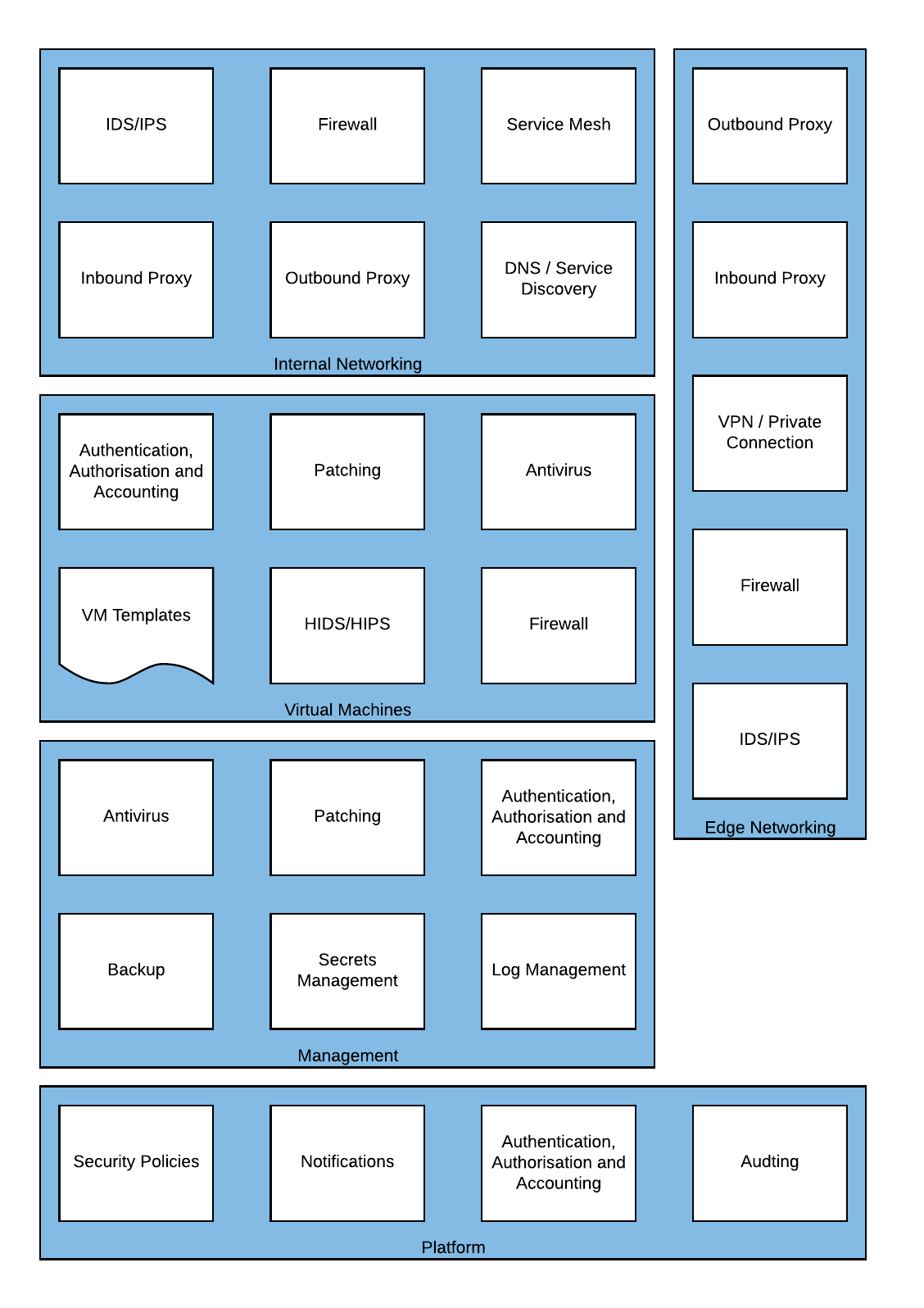
[](https://www.lucidchart.com/documents/edit/237d79f0-1b99-4e17-8b79-efc233429397/7?callback=close&name=docs&callback_type=back&v=5947&s=389)

Figure - Management Required Capabilities

The Skytap cloud service runs IBM Power, with operating systems such as AIX, IBM i, Linux and x86 workloads, with operating systems such as Linux and Windows. Although Operating Systems that run on Power are less numerous than x86, threat actors still target these platforms given they are more likely to hold valuable data. Also, should these workloads be connected back to corporate assets in other clouds or on-premises they then represent a vector for malware to propagate to other systems and services.

A Patching strategy should encompass all workloads in Skytap, including Development, Test and Production. Application Vendors and Operating System Vendors are continually releasing security hotfixes, and functionality improvements and these should be applied judiciously to Virtual Machines and LPARs running in the Skytap Cloud.

Authentication, Authorisation and Accounting should support all workloads operating in Skytap; a centralised repository of credential information reduces the operational burden of managing multiple directories on a per Environment basis but also improves security by consolidating the logging and administration of users and service accounts.

A Backup strategy should encompass the native capabilities of the Skytap platform, such as Templates which create a point in time clone of an entire workload from network configuration to data. However, Templates are not designed to replace regular backups and are not intended to help recover a single row in a database that was deleted by mistake, for example. Templates can save copies of running x86 Virtual Machines but can only copy shutdown LPARs on the Power platform.

Secrets Management is used to protect sensitive application data, certificates, keys or credentials. It provides a secure enclave to perform sensitive cryptographic functions such as transaction signing or user/service authentication. For example, an application server may make a call to the Secrets Manager for credentials to access the database server. These keys are then held in RAM, or valid only for a short period, therefore if the VM is compromised the security of the database server is not.

Log Management should be used to consolidate security and application logs from Virtual Machines or LPARs running in Skytap. Centralised logging can assist operations or development teams in understanding application performance, an incident resolution. Many workloads in the cloud, and in particular Skytap, are short-lived this makes discovering and mitigating threats from bad actors particularly challenging because by the time an incident has been discovered the suspect Virtual Machine or LPAR may well have been destroyed. Centralised logging allows for the more comprehensive discovery of threats as well as their mitigation

#### Antivirus

A cloud-aware antivirus solution is critical for the secure deployment of any hosted workload.

Policies should be set centrally and pushed out to workloads running on the platform, these policies should be cognisant of the nature of the workload, for example, is it transient or long-running, is it a database server or application middleware. An organisational security policy should require the use of Antivirus on all Virtual Machines or LPARs.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### Patching

W

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### Authentication, Authorisation, Accounting

W

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
| Active Directory | Microsoft |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### Backup

W

Incremental backups

Complete backups

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
|  | Veeam |  |  |  |  |  |
|  | Storix |  |  | ✔️ |  |  |
| ICC | IBM |  |  |  | ✔️ |  |

#### Secrets Management

W

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
| [Vault](https://www.vaultproject.io/) | HashiCorp | ✔️ | ✔️ | ✔️ | ✔️ | ✔️ |
|  |  |  |  |  |  |  |

#### Log Management

W

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### 

#### Example Architecture

These components translate into an architecture that approximates the following:

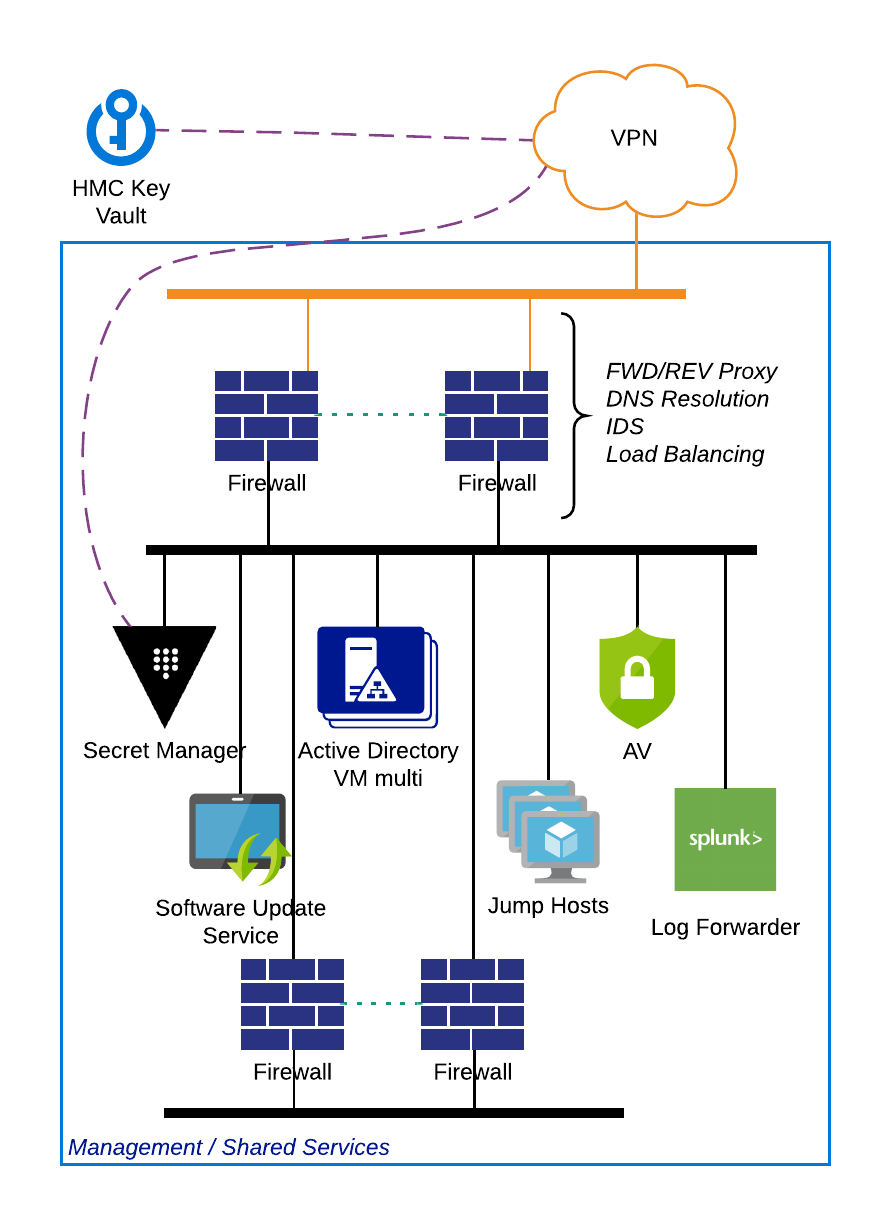
[](https://www.lucidchart.com/documents/edit/237d79f0-1b99-4e17-8b79-efc233429397/2?callback=close&name=docs&callback_type=back&v=5947&s=445)

Figure - Example Management Architecture implemented in Skytap

These services are controlled and managed by corporate administrators accessing via the VPN/Private Connection. The services are then made available to workloads within Skytap through the use of an Inter Configuration Network Routing ([ICNR](https://help.skytap.com/Networking_Between_Environments.html#ICNRoverview)), this is a low touch automated mechanism to connect logically distinct environments. Transit through an ICNRs is not possible; therefore, multiple environments of a different security profile can be connected via a Shared environment, but traffic cannot flow.

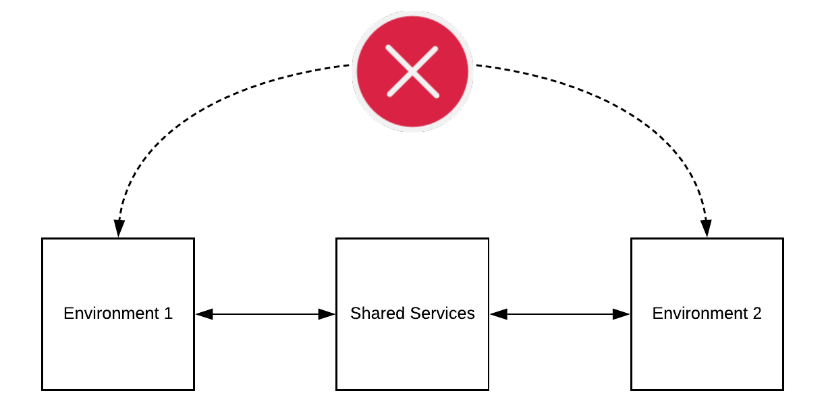
[](https://www.lucidchart.com/documents/edit/237d79f0-1b99-4e17-8b79-efc233429397/8?callback=close&name=docs&callback_type=back&v=5947&s=612)

Figure - Transit ICNR Traffic is Automatically Denied

### Edge Networking

The Edge Networking capability provides access to resources outside of the immediate environment in Skytap, and as such, represents a significant area of exposure. Workloads running in the cloud have legitimate needs to access services or resources either on the Internet or behind the corporate network. To do this safely and efficiently consolidating this ingress and egress into a centralised service can help to enforce good practice and reduce risk.

The Outbound Proxy and Inbound Proxy filter what Virtual Machines can connect to and what in turn can connect to them. For example, an Outbound Proxy may be configured to allow an Application Server to request data from a public API; whereas, an Inbound Proxy (sometimes called a protocol break) terminates external client connections to protect the internal servers from direct internet exposure. The Inbound Proxy can then perform validation on the request from the client, such as determining if the client is a known bad actor or if the request is appropriately formed.

The VPN or Private Connection provides secure and restricted connectivity to on-premises or third-party cloud access in a controlled manner. For example, only the Production environment may be allowed to communicate over the Private Connection to the database running on-premises; however, the Development/Test environments can be connected to by the Engineering team via VPN.

Firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are typically consolidated onto a single device, but they do provide distinctly different functionality. A Firewall can restrict connectivity between devices based on source or destination information sent with the traffic. In contrast, an IDS/IPS attempts to understand the context of the traffic passing through and responds accordingly. The IDS/IPS is designed to detect unauthorised intrusions on your network by matching traffic flows to known signatures

When providing Internet or VPN access, this stack is typically implemented, as below. With the reverse being true for outbound traffic.

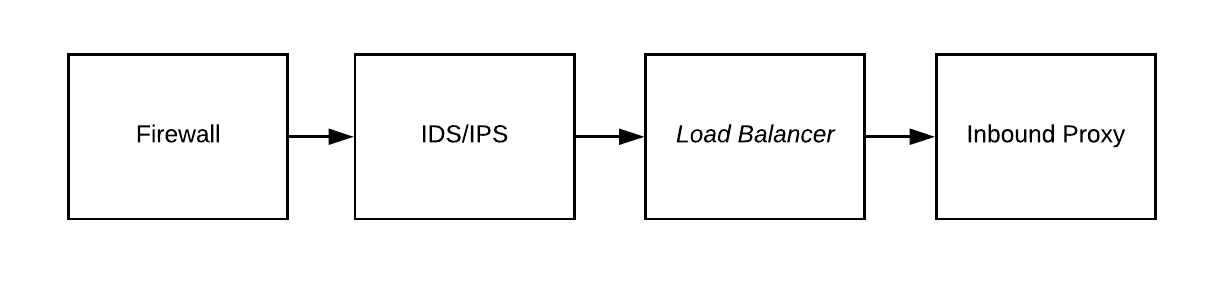
[](https://www.lucidchart.com/documents/edit/237d79f0-1b99-4e17-8b79-efc233429397/10?callback=close&name=docs&callback_type=back&v=6458&s=612)

Figure - Typical Traffic Flow[[3]](#footnote-4)

#### Outbound Proxy

An Outbound Proxy should be configured to restrict access to websites, Internet-connected services and on-premises services to only what is required for typical operation. For example, connection to an application or operating systems update service is appropriate.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### Inbound Proxy

The Inbound Proxy sometimes referred to as Reverse Proxy, sits between the client and the webserver or application server hosted in Skytap. A reverse proxy accepts a request from a client, forwards it to a server that can fulfil it, and returns the server’s response to the client.

The proxy enhances security by shielding the backend servers from the outside network, and this prevents malicious clients from accessing them directly to exploit any known vulnerabilities. It can also protect these backend servers by rejecting traffic from blacklisted IPs or rating limiting the number of connections from clients, reducing the risk of a distributed denial-of-service (DDoS) attack.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
| [NGINX](https://www.nginx.com/) | F5 | ✔️ | ✔️ | ✔️ | ✔️ | ✔️ |
| [Squid](http://www.squid-cache.org/) | Squid | ✔️ | ✔️ | ✔️ | ✔️ | ✔️ |
| [pfSense](https://www.netgate.com/solutions/pfsense/) | Netgate | ✔️ | ✔️ | ✔️ | ✔️ | ✔️ |

#### VPN / Private Connection

Skytap supports Site-to-Site VPN as well as Private Network Connections (PNCs) using [Azure ExpressRoute](https://azure.microsoft.com/en-gb/services/expressroute/) and [Equinix Cloud Exchange](https://www.equinix.com/solutions/cloud-infrastructure/public-cloud/connectivity/).

##### Site-to-Site VPN

The Skytap [Site-to-Site VPN](https://help.skytap.com/vpn-configuration-parameters.html#VPNconfigurationoptions) supports an IPSec VPN using IKEv1 or IKEv2 using Pre-Shared Keys (PSK), AES 256 bit and Perfect Forward Secrecy (PFS).

The Skytap Site-to-Site VPN secures traffic that traverses the public Internet, but not private connectivity. Multiple VPNs can be created for high availability and to connect multiple corporate data centres to the Skytap cloud.

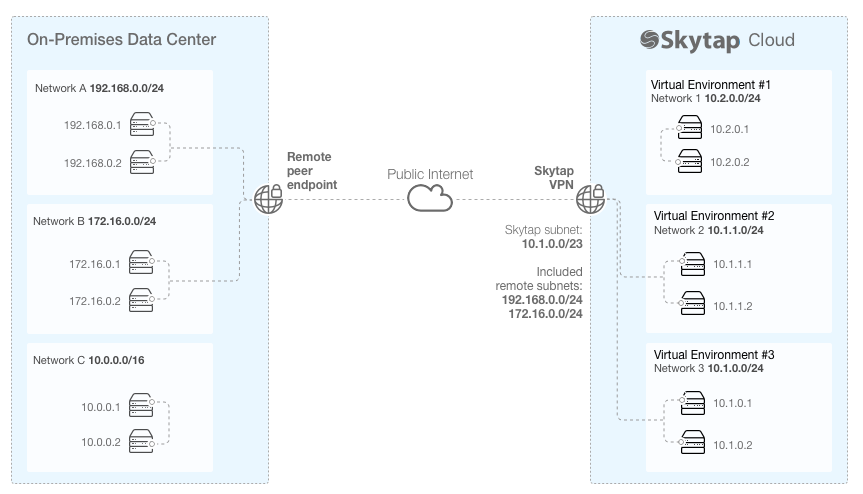


Figure - Example VPN Connection Scheme

##### Private Network Connection (PNC)

An Azure ExpressRoute or Equinix Cloud Hub connection are referred to as Private Network Connections (PNCs) in Skytap.

In the example below, the PNC connects the on-premises data centre with the Skytap cloud environments. It should be noted that while this connection is private, using Multiprotocol Label Switching (MPLS), which logically isolates traffic, it is not however encrypted.

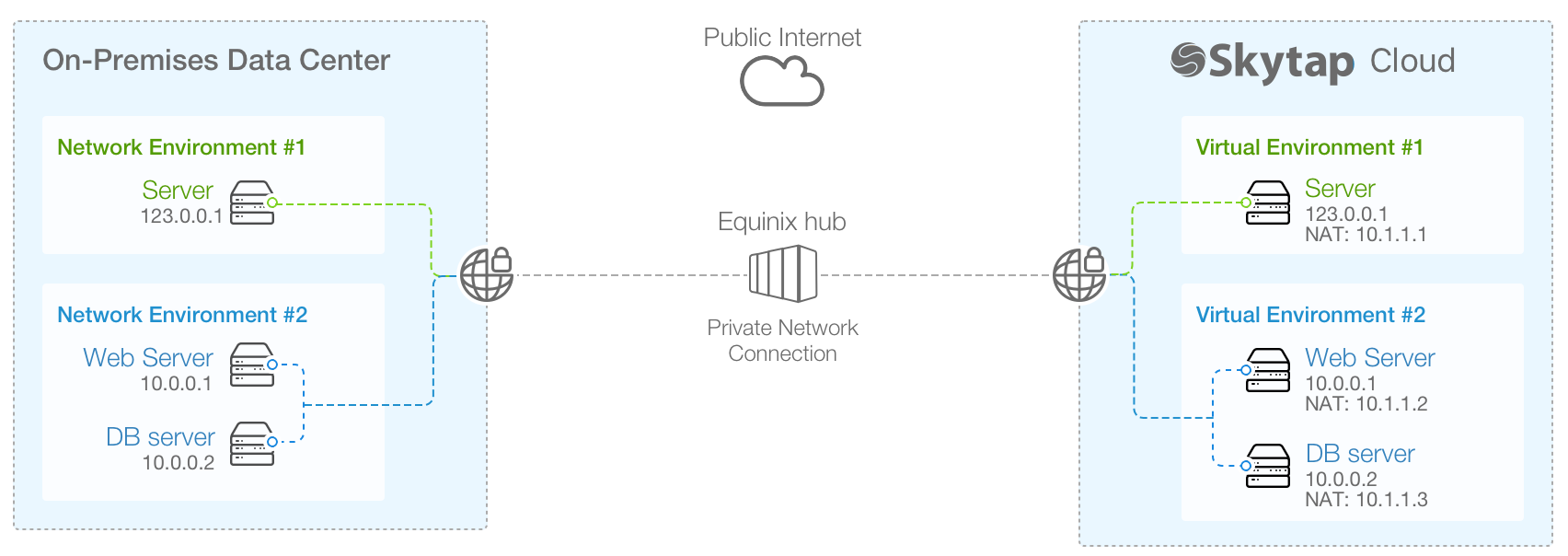


Figure - Example Private Connection Scheme

When a PNC is used traffic between Skytap and the On-premises datacentre or other cloud providers should be encrypted at the edge of the environment using a Firewall to create the site-to-site connection or by using point to point encryption from a service mesh network. Service Mesh networking is covered in the **Internal Networking** section of this document.

#### Firewall

A Firewall should be implemented to protect the edge of the Skytap platform, both to defend the workloads running in Skytap but also any onward connection to the corporate datacentre or other clouds.

Internet to Environments filtering should take place to only permit acceptable connections, for example, HTTPS connection to the Inbound Proxy but discard all other forms of traffic attempting to connect to Environments directly.

Environments to Internet filtering should restrict egress of traffic except via the Outbound Proxy; the proxy decides as to what external sites and services are acceptable.

VPN/PNC to Environments, blanket access to Environments even from private connections such as VPNs is inadvisable. Outside of machine to machine connectivity to support application operations, such as Database calls or Directory Lookups, user access should be brokered via a Jump/Bastion host held in the Management environment.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
| [pfSense](https://www.netgate.com/solutions/pfsense/) | Netgate | ✔️ | ✔️ | ✔️ | ✔️ | ✔️ |
|  |  |  |  |  |  |  |

#### Intrusion Detection System / Intrusion Prevention System

Typically Intrusion Detection Systems or Intrusion Prevention Systems are consolidated on the firewall but shown here as a discrete capability for completeness. The IDS/IPS performs a vital monitoring function to alert administrators and security personnel of unauthorised attempts to access the network. Intrusion is of particular concern with internet-facing applications.

In Skytap an IDS/IPS must be placed in line with the traffic as port mirroring is not supported, hence the preference to include it as part of the Firewall capability.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
| [pfSense](https://www.netgate.com/solutions/pfsense/) | Netgate | ✔️ | ✔️ | ✔️ | ✔️ | ✔️ |
|  |  |  |  |  |  |  |

#### Architecture

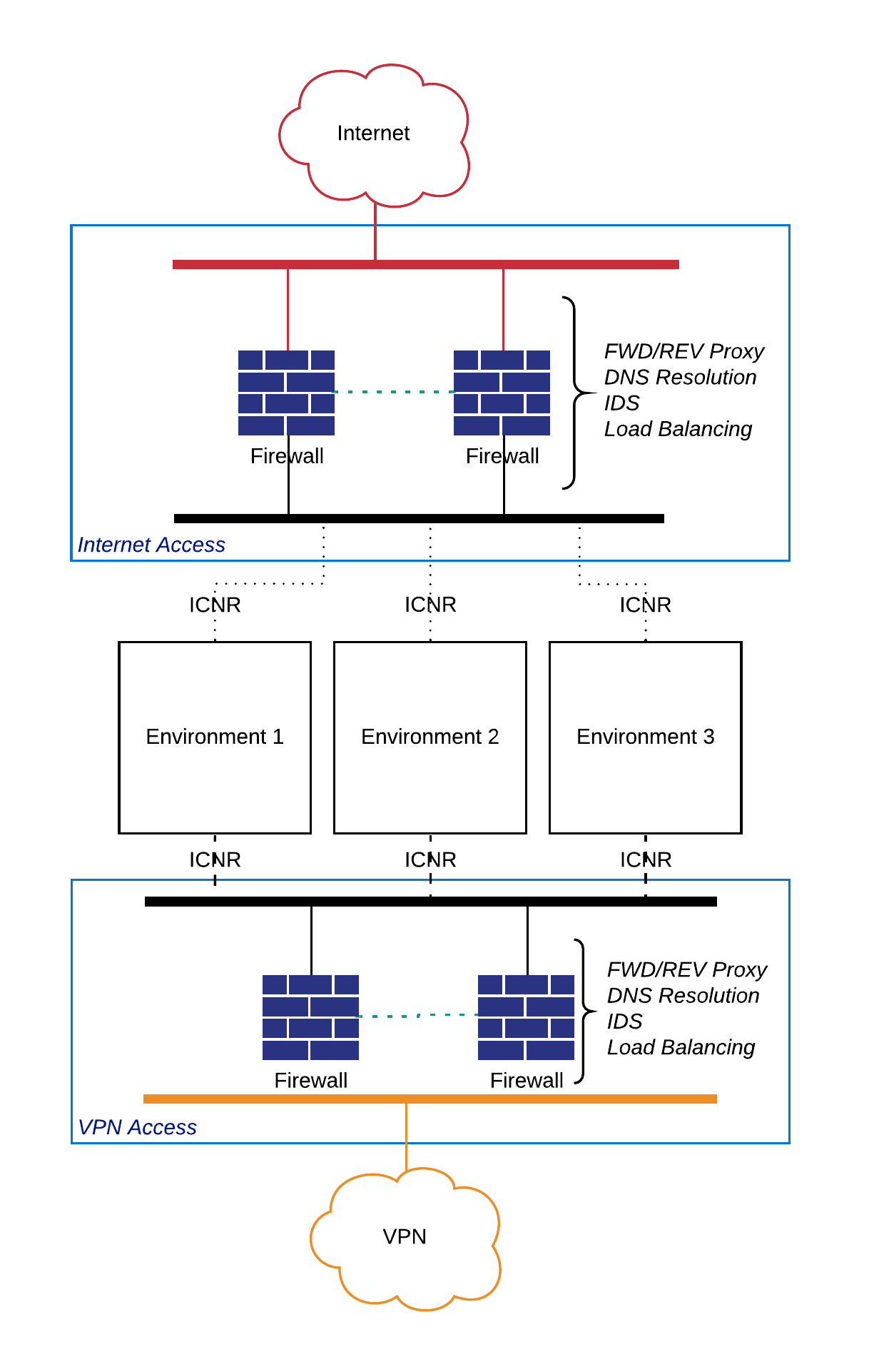
[](https://www.lucidchart.com/documents/edit/237d79f0-1b99-4e17-8b79-efc233429397/9?callback=close&name=docs&callback_type=back&v=6359&s=612)

Figure - Example Internet and VPN Connection Scheme

### Virtual Machines

The Virtual Machines capability encompasses VM Templates; Authentication, Authorisation and Accounting; Patching; Antivirus; HIDS/HIPS; and Firewall. This area relates to the Environments running in Skytap and any templates associated with them.

A screenshot of a cell phone

Description automatically generated

Figure – Virtual Machine Required Capabilities

#### VM Templates

In Skytap the Virtual Machine template contains a point in time and idempotent copy of an entire Environment. An Environment or Template includes any connectivity it may have, such as Internet access or VPN connections, the state of any x86 or Power Virtual Machines (LPARs) including their memory state (if x86), disks, MAC addresses and other configuration items.

Pre-configured templates should be made available to users of the Skytap platform that conform to organisational security policies. These templates should have pre-installed anti-virus and Host-Based Intrusion Detection Systems/Host-Based Intrusion Prevention Systems; installed licenses; up to date patching for security vulnerabilities of operating systems and applications; and an enabled Firewall.

From these base templates or Golden Images, users on the Skytap platform can build or operate their workloads from a known good configuration. The use of Golden Images prevents accidental misconfiguration or unauthorised use of operating systems which may not align with organisational standards or software licensing exposure.

These base templates can be made available to users via Projects, as described earlier in this document.

#### Authentication, Authorisation and Accounting

Access to Virtual Machines and LPARs in Skytap Environments should be centralised, and the use of a directory service enables that. A local directory server, in the Environment, can be made available to Virtual Machines and LPARs or authentication traffic can be passed to the Shared Services environment.

Password-based authentication should be avoided in most cases, with public/private key being preferred. Certificate authentication for users is atypical in Windows deployments but is supportable and considerably more secure.

Lightweight Directory Access Protocol (LPAP) is a supported authentication technology on Linux, IBM i and AIX.

Terminal access should be protected with certificates, SSH can be configured to use signed certificates validated by the Secrets Manager and should be used to reduce key reuse and automated repudiation of compromised keys or users no longer with authority to connect. With IBM i the TN5250 ‘Green-Screen’ service should be secured using SSL/TLS certificates, some guidance is documented [here](https://www.ibm.com/support/pages/configuring-ssl-telnet-and-host-servers-server-authentication-first-time), as the Green-Screen is a telnet based session which has no encryption and is supsceptible to interception and exploitation.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
| Active Directory | Microsoft | ✔️ | ✔️ | ✔️ | ✔️ |  |
|  |  |  |  |  |  |  |

#### Patching

The regular updating of operating systems and applications with security patches prevents vulnerabilities being exposed and exploited by bad actors. A patching service should be configured to regularly apply new security patches, these patches should also be integrated into any master/gold templates in use on the Skytap platform.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
| Ansible | Red Hat | ✔️ | ✔️ | ✔️ |  | ✔️ |
| Windows Update | Microsoft | ✔️ |  |  |  |  |
|  |  |  |  |  |  |  |

#### Antivirus

All Virtual Machines and LPARs should have Antivirus protecting them, they should be configured to update regularly (hourly), scan frequently and report any events centrally.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

#### HIDS/HIPS

A Host-Based Intrusion Detection System or Host-Based Intrusion Prevention System can help to secure against unauthorised access.

Typically these applications detect malicious login traffic, changes to privileged files or the installation of software outside the approved process. Logs generated from these systems should be centralised, with the potential to invoke automated defences such as quarantine.

In some production systems, any direct login to a Virtual Machine or LPAR is considered an attack and would cause the VM to self-destruct.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
| Fail2Ban |  |  | ✔️ |  |  | ✔️ |
|  |  |  |  |  |  |  |

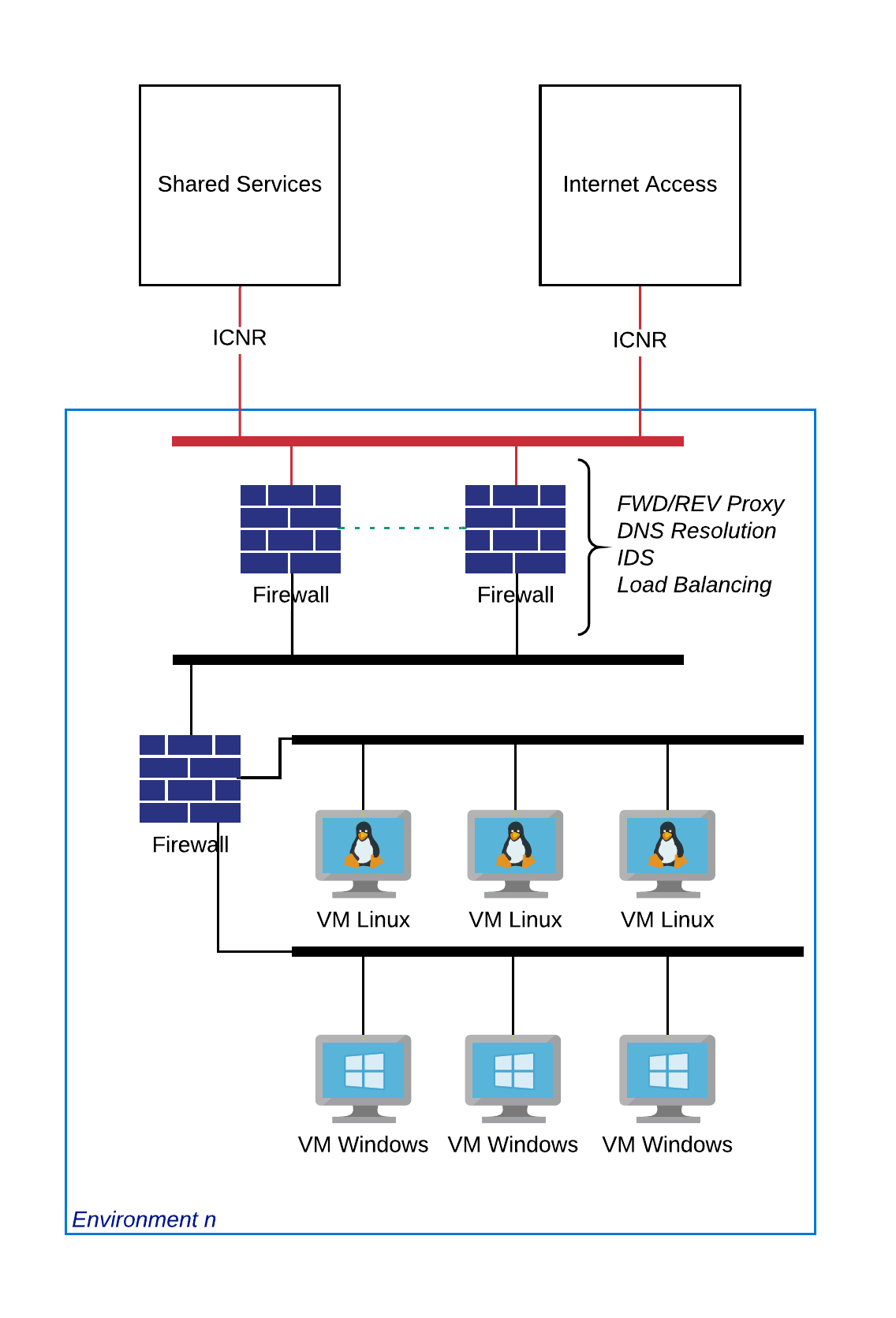
#### Firewall

Skytap enables cross-network communication by default, and in additional to local network firewall protection Virtual Machine protection should be enabled to restrict open ports only to those that are approved. For example, a database server should only allow database traffic from know application servers; any other attempts to connect to a database management port should be ignored and reported.

##### Supported Implementations

| Application | Vendor | x86 | | Power | | |
| --- | --- | --- | --- | --- | --- | --- |
| Windows | Linux | AIX | IBM i | Linux |
| Windows Firewall | Microsoft | ✔️ |  |  |  |  |
| iptables | N/A |  | ✔️ |  |  | ✔️ |
| ipfilters | IBM |  |  | ✔️ |  |  |

#### Example Architecture



### Internal Networking

d

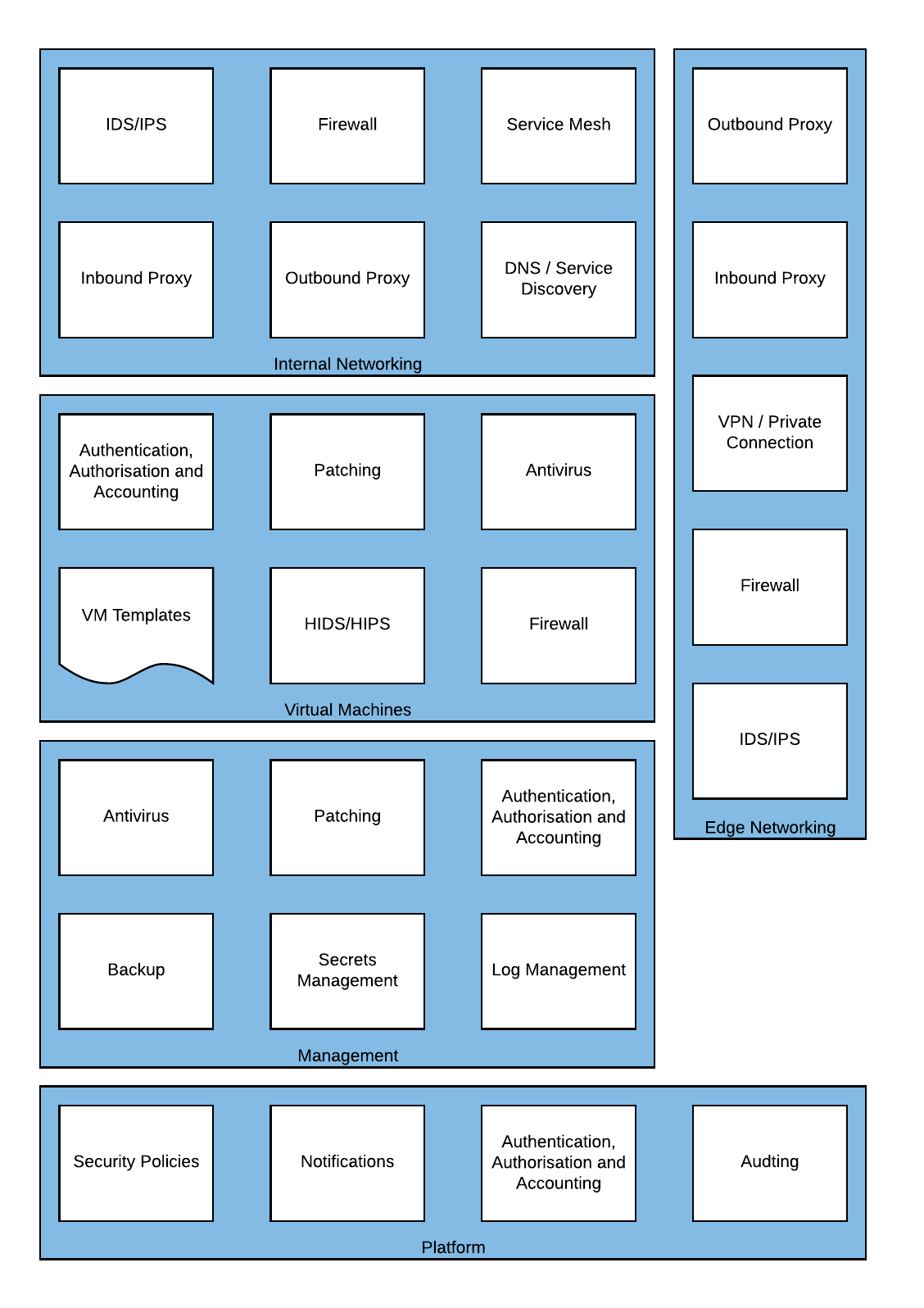
[](https://www.lucidchart.com/documents/edit/237d79f0-1b99-4e17-8b79-efc233429397/7?callback=close&name=docs&callback_type=back&v=5947&s=389)

Figure – Internal Networking Required Capabilities

# Implementation Guides

# References

Wikipedia. (2020, April 4). *Webhook*. Retrieved 4 5, 2020, from Wikipedia: The Free Encyclopedia: http://en.wikipedia.org/wiki/Webhook

1. *Cloud Security Alliance.* [*"Defined Categories of Security as a Service"*](https://downloads.cloudsecurityalliance.org/assets/research/security-as-a-service/csa-categories-securities-prep.pdf) *(PDF). Cloud Security Alliance. Retrieved 5 June 2017.* [↑](#footnote-ref-2)
2. A webhook in web development is a method of augmenting or altering the behavior of a web page, or web application, with custom callbacks. These callbacks may be maintained, modified, and managed by third-party users and developers who may not necessarily be affiliated with the originating website or application. (Wikipedia, 2020) [↑](#footnote-ref-3)
3. A Load Balancer is shown for reference but is not within the scope of this document. [↑](#footnote-ref-4)