the sixth flag

Concept Overview and Operational Guide

Version 1.2

June 2015

Contents

Overview

The Sixth Flag is a Desktop-as-a-Service offering provided by The Sixth Flag, Inc. The desktop service is browser-based, HTML-rendered and Cloud orchestrated. The objective of The Sixth Flag is to offer customers a Desktop-as-a-Service that is simple, secure, and easy to manage while being light on the wallet. All design principles center on achieving those four goals.

Background

The Sixth Flag DaaS was initially developed in response to the rise in Advanced Persistent Threats (APTs) successfully exploiting end user desktops. In particular, the founders observed a disturbing trend in which non-technical remote users are singled out for exploitation. From an attacker's perspective, targeting this demographic makes sense for the following reasons:

- The user often operates disconnected from the organizational network and is less likely to be current with patches, malware signatures and security updates.

- The user is often operating several time zones from organizational IT team, including administrators and help desk personnel. As such they rarely rely or communicate with them regarding issues or incidents. Furthermore, incidents recorded in an organizational IDS / IPS may become buried by events even within a few hours.

- Many remote users are involved with business development and client facing services. They are incentivized through timely and accurate responsiveness. Assiduous commitment to following corporate security policies will often adversely impact such responsiveness.

Security Concepts and Functions

Supported Authentication

TSF supports two types of authentication; Internal and SAML 2.0. Internal authentication uses The Sixth Flag's highly secure authentication service.

Ephemeral Desktop

A key security feature is the destruction of the virtual desktop after each session. While all user data and settings persist on a separate volume, the system partition is destroyed after each session. This serves to mitigate the long-term effects of any malware or other advanced persistent threats that may find their way on to the virtual desktop. It also ensures consistent configuration management of the desktop over time and allows for centralized patch management.

Encrypted Data Store

All user data is stored on a separate encrypted volume that is only available to the end user and system administrators. Should it be necessary to reassign a user's data to another user, it is as simple as removing a user's access to the data volume and assigning it to the new user.

Amnesic Credentialing

The Sixth Flag strips all persistent credentials during the login process and replaces them with randomly generated credentials. Should the user's desktop session become compromised by malware that successfully attacks the credential store, the credentials compromised are of no value. This addresses a significant attack vector used against traditional desktops.

cleanroom.tsf™

cleanroom.tsf™ is a highly secure configuration which allows users to conduct traditional desktop computing and collaboration in what is essentially a sealed environment. Users can optionally upload files to their virtual desktops, but cannot download, print or copy content out of the virtual desktop. Internet access is disabled.

dewdrop.tsf™ Watermarking technology

The Sixth Flag has developed a patent-pending watermarking technology, **dewdrop.tsf™**, that discourages the unauthorized disclosure of sensitive data through screen captures or screen photography. Administrators can enforce the watermarking feature on a per user group basis.

When a watermark enforced user logs in to their TSF Desktop, a dot-encoded pattern is overlaid on top of their desktop session. The watermark references session-identifying information, including user identity, time of session, and other useful metadata. The watermark is translucent, allowing the user to see and work with the underlying content.

Should a screen capture or photograph of a watermark protected desktop surface, the administrator needs to merely log in to the watermarking administrative console and use the watermark lookup tool. A match will provide the administrator all information regarding the relevant desktop user, date, and time.

User Management

Users

A user is a person associated with a set of credentials. A user is typically assigned to one or more sets of desktop profiles, though a user can be assigned no desktop profile, which is traditionally done for the purpose of granting administrative access. (See Profiles).

Profiles

A desktop profile is the configuration, data and settings for a TSF virtual desktop associated with a user. A user can have multiple profiles, but can only access one profile at a time. This is analogous to a user having several physical desktops, each with different settings and installed software. Each desktop serves a different purpose, supporting various user roles.

Each profile is independent of other profiles that the user may have. There is no shared storage or configuration. This assures that there is no leakage of data between profiles, inadvertent or otherwise.

Groups

Groups represent a set of profiles that share the following properties:

- TSF Permissions including the ability to upload and download files, copy and paste files to/from the virtual desktop, print documents, and access the Internet.
- Desktop Image.
- Storage per profile.

Image Management

Images are templates of desktop configurations that are presented to user profiles. An image is essentially a snapshot of a Windows™ "C drive." Images are associated with groups so each group can have its own image.

During initial account setup, an organization is provided set up “Gold Master” images that are maintained and updated by The Sixth Flag. It is recommended that the first step an organization takes is to make a copy of the Gold Master and use that image as their base image. This allows an organization to take control of its update schedule.

Creating and updating images

Creating an image. This is done by selecting a “parent” image to copy and giving the new image a name.

Updating the image. This is done by selecting the image and selecting “Edit Content.” An image build instance is launched that allows the administrator to modify the image, such as applying patches and updates, installing or removing software, and changing configurations. Once the changes are complete, the administrator logs out and chooses “Commit Changes.” This updates the image. Once the image update is complete, the next time a user logs in, they will be presented the updated desktop.

Reference Architectures

The Sixth Flag offers two core reference architectures: Shared and Dedicated. A third reference architecture, Premise-Based, is not being addressed in this paper. Organizations interested in a Premise-Based solution should contact The Sixth Flag for details.

Shared Environment

The shared environment is appropriate for organizations that are smaller or have less complex requirements. Administrators can manage Users, Profiles, Groups and Images. User and organizational data is segregated from that of other organizations. The shared environment has two restrictions that distinguish it from the dedicated environment. They are:

- Custom authentication is not supported.
- Custom egress routing, including site-to-site VPN connectivity, is not supported.

See Figure 1.

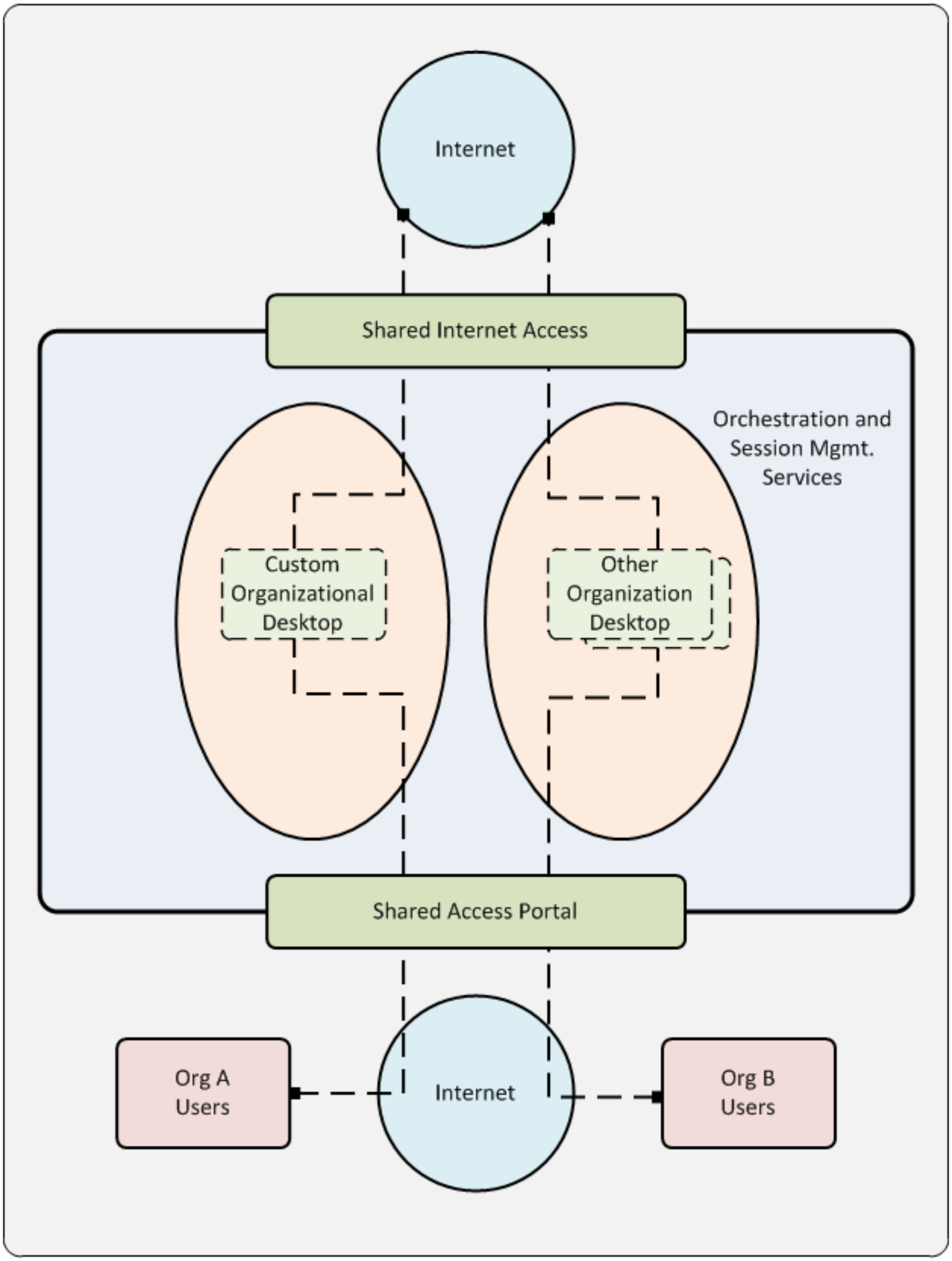
Internet
Shared Internet Access
Orchestration and Session Mgmt. Services
Custom Organizational Desktop
Other Organization Desktop
Shared Access Portal
Org A Users
Internet
Org B Users

Figure 1 – Shared Environment

Dedicated Environment

For organizations with more complex requirements, particularly the need for custom authentication or network level connectivity to their internal network, The Sixth Flag offers a dedicated environment. The dedicated environment offers all the functions and features of the shared environment with two additional capabilities:

- Custom authentication. In addition to offering authentication services hosted by The Sixth Flag, custom authentication using SAML is available. This allows organizations to use their internal authentication services, such as Active Directory.

- Custom Egress Routing. The dedicated environment allows organizations to set custom egress routing, including routing some or all traffic through a VPN, perform policy-based inspection of egress traffic, blocking traffic by IP or DNS and more. This allows organizations to grant TSF users access to internal organizational resources such as file servers and applications such as database, line-of-business and collaboration platforms.

See Figure 2.

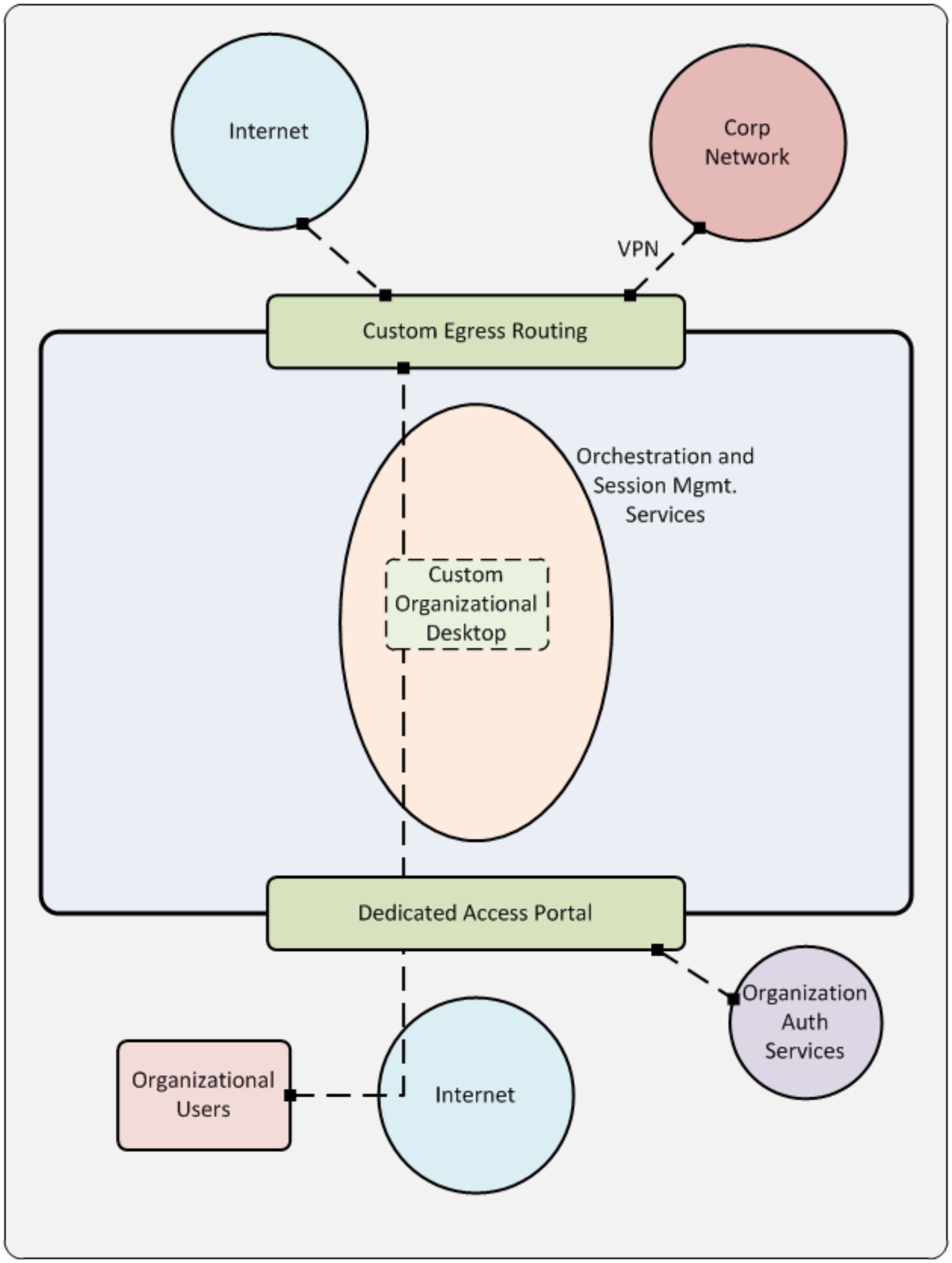
Internet
Corp Network
VPN
Custom Egress Routing
Orchestration and Session Mgmt. Services
Custom Organizational Desktop
Dedicated Access Portal
Organization Auth Services
Organizational Users
Internet

Figure 2 – Dedicated Environment

Supported Clients

Current Web Browsers

The Sixth Flag virtual desktop is tested and supported on major current browsers, including Firefox, Chrome, Safari and Internet Explorer. Platforms including Windows, OS X, Linux as well as major tablets are supported.*

**HTML5, Canvas and JavaScript are required.*

Thin Client

The Sixth Flag has developed a special configuration for use with managed browser based thin clients including Google Chrome devices. This offers a full thin client experience that is both cost-effective and offers system administrators the ability to manage user hardware.

Internet Connectivity Requirements

As a purely hosted service, The Sixth Flag offers no offline capability. In order to enjoy the most positive experience, the following requirements are set regarding Internet connectivity:

- Reliable Internet connectivity. Regular outages will reduce the user experience significantly.

- Bandwidth. The Sixth Flag uses bandwidth conservatively. Even the most modest broadband connection is more than adequate to provide a productive desktop session.

- Latency. The Sixth Flag offers its service on five continents, minimizing the impact of latency and resulting in a highly satisfactory real time experience. Because of the bidirectional traffic required, satellite Internet connectivity is not recommended.