Reflection Network
Product Description

Version 02 Author: Dewar McCambridge
August 04, 2022

Approved for distribution by TekMonks.
All the following aspects of the Reflection Network product are proprietary and developed in-house by TekMonks.

TABLE OF CONTENTS

Introduction

This report is intended for architects, cybersecurity analysts and partners wanting to obtain a complete understanding of TekMonks Reflection Network, regardless of the question type (i.e. financial, customer or technical). **It is assumed that the reader is familiar with the basic concepts of the Reflection Network and has knowledge of fundamental network protocols, such as TCP/IP, which underpin the modern network and the internet.**

The data contained in this report was measured in a controlled environment and results obtained in other environments may vary.

Components

Internal Server, Application, Device – This is the server/application or device which is sealed inside the corporate network and is being reflected out to the Mirror Server via the Reflector component.

Reflector – This is the component which reflects the required internal server, application or device to the Mirror Server.

Mirror Server – This is the end point architecture which is serving the users. A Portal is sometimes added to this architecture based on requirements. For example, a Portal where users log into and pass Smart Firewall authentication, gaining access to the Mirror.

Smart Firewall – This is a security component of the Mirror which only allows access to specific authenticated users.

The components together make up what TekMonks call a Reflection Network which is suitable for:

- Securing applications and assets which must be exposed to the internet.
- Applications used by business partners. – Utilized for agents, agencies, resellers etc. Examples include mobile B2B applications, like Agency Portals or Reseller Portals, that require secure access.
- Ensuring limited traffic. The reflection network ensures that all client traffic is limited through the Mirror Server and no client can actually establish their own connection to the original servers.
- Replacing current VPN/Proxy configuration. The Mirror Server itself contains no data and access privileges to the original server; meaning, even if a breach occurs, no data can be taken from the mirror itself and a connection back to the original server can not be established. If a breach on a Proxy Server or VPN gateway takes place, a connection back to the original server can be then formed.

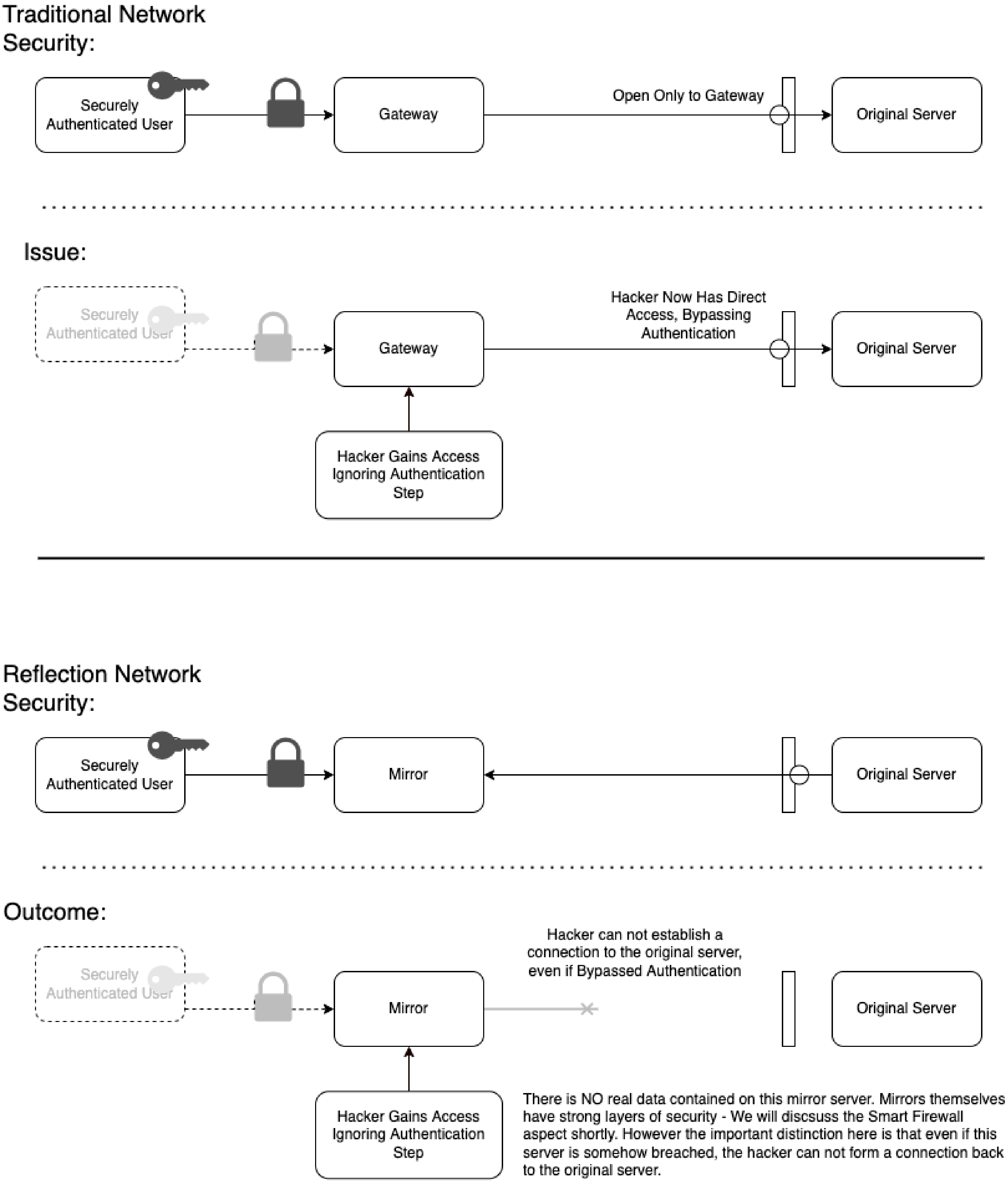
Benefits Compared - Traditional VPN / Proxy Gateways

In this section, it is assumed that the reader is familiar with the basic concepts of traditional corporate network segmentation and protection tools in terms of Firewalls, VPNs and Proxy Gateways. A comparison of this traditional network architecture to a Reflection Network will be made along with showcasing the advantages provided by Reflection.

- Unlike VPN and Proxy Gateways, apps on the users' device do not have access to the companys' network. This reduces risks related to personal apps, exploits, and malware on the users' personal devices and networks which are not managed by IT.
- Whether the user has malware, trojan horses, vulnerable apps or is targeted by hackers, the companys' network assets remain safe as there is no direct network tunnel between the user and the companys' network.
- Deploying the traditional model is similar to opening all of the company networks ports to any application on the remote users device. This would require a full-blown network security audit and hardening. When considering hardening includes dividing the network into subnetworks to reinforcing passwords, closing unnecessary ports and other pertinent steps, it is easy to see that the security preparations for deploying VPNs is a considerable project in and of itself. Utilizing Reflection means these steps are not required as only the accessible apps & web apps are published requiring zero open ports or network changes.
- There are fine grained role-based controls. For example, if using Reflection, a HR user may only be provided access to HR web applications. With Traditional VPNs/Proxies everything is available to remote users and there is no role-based access control. You can also think of this as a secured office building. Traditional VPN/Proxies are like having the front door be the only security access to the whole company, there is nothing stopping people from walking where they please once authenticated. Reflection is like adding a door to each floor (floors representing each individual system) with multi-level security systems in place so even though one can pass that first entry door, they cannot go to any system in the network as they all have their own doors with multiple security measures.
- Reflection technology saves significant bandwidth and can support much more users than VPNs by ensuring the only bandwidth used is the corporate traffic between the user's laptop and the corporate network. The rest of the personal traffic goes over the regular internet.

Furthermore, the critical difference between the architectures can be summarized in Figure 1.

Figure 1:


Traditional Network Security:
Securely Authenticated User
Gateway
Open Only to Gateway
Original Server
Issue:
Securely Authenticated User
Gateway
Hacker Now Has Direct Access, Bypassing Authentication
Original Server
Hacker Gains Access Ignoring Authentication Step
Reflection Network Security:
Securely Authenticated User
Mirror
Original Server
Outcome:
Securely Authenticated User
Mirror
Hacker can not establish a connection to the original server, even if Bypassed Authentication
Original Server
Hacker Gains Access Ignoring Authentication Step

There is NO real data contained on this mirror server. Mirrors themselves have strong layers of security - We will discsuss the Smart Firewall aspect shortly. However the important distinction here is that even if this server is somehow breached, the hacker can not form a connection back to the original server.

Smart Firewall Benefits

The Distinction:

There are additional benefits including access segregation with the Smart Firewall on the Mirror Servers. Each internal application, desktop or server that is being reflected out to the Mirror, is then allocated to its own distinct access port on said Mirror and is then closed by the Smart Firewall component. These ports are subsequently only opened for authenticated users who have authorization to access those specific apps.

For example, TekMonks reflects an Engineer related server to port A, and an HR related web application to port B. When an Engineer then authenticates correctly, Smart Firewall will only open port A, related to the Engineer's role, removing the ability to attempt a lateral movement and blocking any attempt to access the HR application.

Additional Benefits (include but may not be limited to):

- Smart Firewall preemptively bans attacks on IPs using the largest IP database (DB) from curated blacklists.
- Integration with NIST – NVD (US Govt, National Vulnerability Database) and Exploit-DB for Anti-Malware, Anti-Spam and Anti-Virus protection.
- Malware-App detection for Mobile Apps – integration with Google App Store and Malpedia DBs.
- URL and Script Blocks to prevent external hosted script attacks, e.g. XSS, even if the Reflected web App itself has vulnerabilities.
- Preventing various injection attacks via query parameter parsing at Layer 7 – SQL, XML, XSS injections.
- Ability to convert any application into an MFA compliant application.
- Heuristic rules for Layer 7 outbound data protection against leaks.
- Deep logging and audits via the SOC module, multi-level logs from User to Admin to Audit.

Client Journey - Deployment Options

When it comes to deploying a Reflection Network, the deployment process can differ depending on the client requirements. There are granular choices on deployment location such as Mirror and Portal servers being on prem, on cloud, inside/outside of the client DMZ or even hosted in the TekMonks cloud. However, in all cases, the Reflector component must be installed inside the internal network.

Related to the Reflector component itself, there are two distinct choices a customer can make for deployment. For the following scenario, TekMonks is under the assumption that the Mirror and Portal servers are deployed in the TekMonks cloud.

Reflector Deployment Options

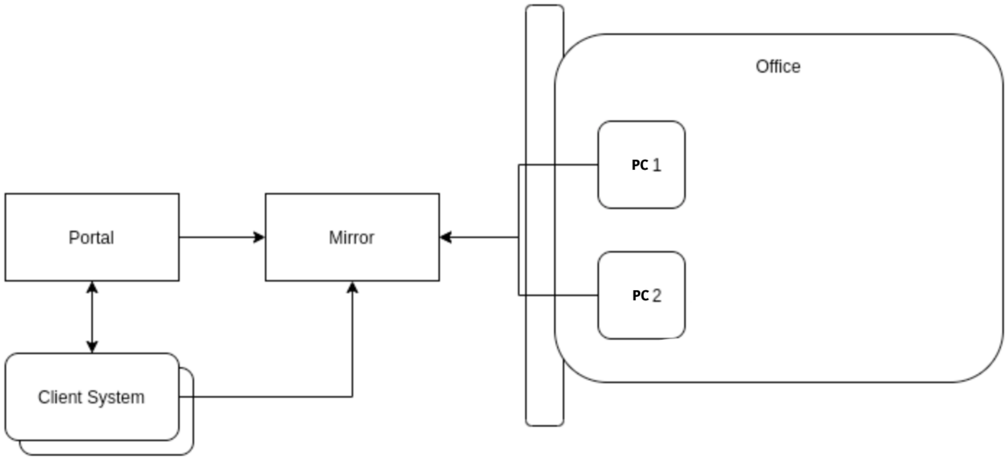
1. Using installers for each office desktop.
2. Deploying a Reflector Virtual Machine (VM) / Hardware within the network.

Option #1: Installers

When clients choose this method, an installer executable file, provided by TekMonks, will need to be run on all the clients office Desktops that they wish to connect to securely.

Below is a simple diagram (figure 6) of a Reflection Network architecture using installers. In this instance, both PCs have used the installer to install a personal Reflector component that then connects to the Mirror individually under a distinct port number. This method is used when only accessing desktops remotely. Ie. not other internal applications.

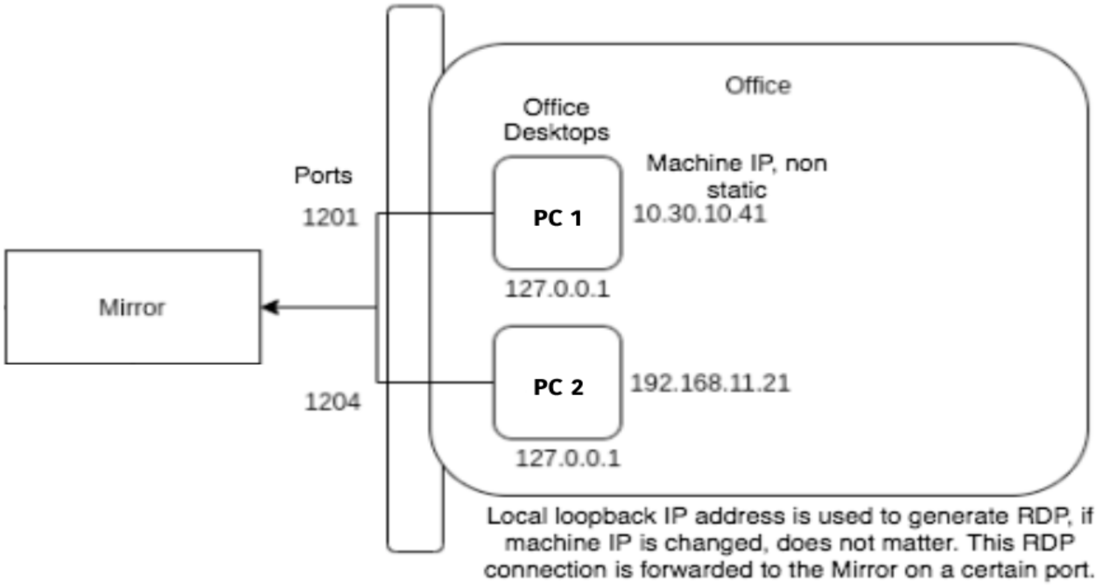
Figure 6:



When running the installer, each machine utilizing that installer is mapped to a mirror port which is then mapped to an app for a certain user to access on their Portal. After the installation, a Reflector has been successfully set up on the specific office desktop itself, and will then formulate a connection to the Mirror Server.

If the IP of the office desktop changes, via DHCP or some other method (i.e. changing from wireless to ethernet to ensure stability) the installer that's running will restart the service itself and the connection is refreshed. The office desktop will then connect to the mirror again. Most importantly, the previous port number it connected to on the Mirror originally also remains the same.

Figure 7:



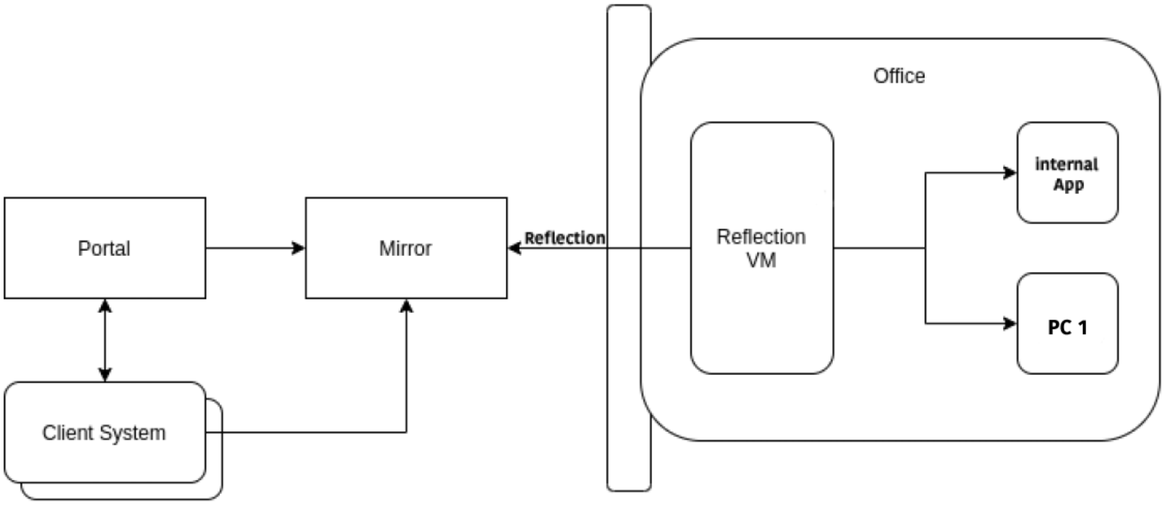
Local loopback IP address is used to generate RDP, if machine IP is changed, does not matter. This RDP connection is forwarded to the Mirror on a certain port.

During the time the users run the installer, a popup also appears that allows the user to then create their authentication account to use as login credentials on the Portal. If the user chooses "No" for creating an account during the installer phase, they are given a service account number which, in turn, is a unique ID meaning they can add it as an additional application to their currently existing authentication account on the Portal instead. Successful installation of desktop installers maps the machine's rdp to a mirror port even if the account is not created using them.

Option #2: Reflection VM

Instead of the Reflector component running on the machine itself and creating connections to the mirror per machine, this approach deploys a Reflection VM (containing multiple Reflectors) in the same perimeter of the network as the desired services/systems to be remotely accessed. The VM is a large-scale Reflector that is responsible for forwarding all the desired connections to the mirror. Each internal component that is reflected out is still mapped to an individual mirror port.

Figure 8:



This architecture is required when the desired access is not only Office Computers.

In the above diagram (figure 8), note that one system is a Windows Desktop for RDP and the other is an Internal App / Service. This architecture covers a variety of internal access requirements. For example, a NAV server or a Legacy Application. In short, anything you wish to connect to securely, that is not an Office desktop, will require this architecture.

To send these connections to the Mirror Server, access must first be gained via the use of this Reflection VM which is why it needs to be installed within the same network segment as the applications desired to be accessed are. The Reflection VM contains a list of ports that the Mirror can provide authenticated access on, so these connections are then forwarded by the VM to the mirror. The IP addresses are stored inside the Reflection VM as a reference. This means if the original system IP addresses are changed, the Reflection VM needs to be updated.

Customers Journey

The customers journey for setting up this architecture is as follows:

1. Receive VM files and set up manually.
2. Install the VM in the desired location | Join a call with a representative from TekMonks and get walked through the installation.
3. Notify TekMonks when completed.
4. TekMonks will then access the VM remotely and make all configurations.

As for installing the VM, the options of installation are:

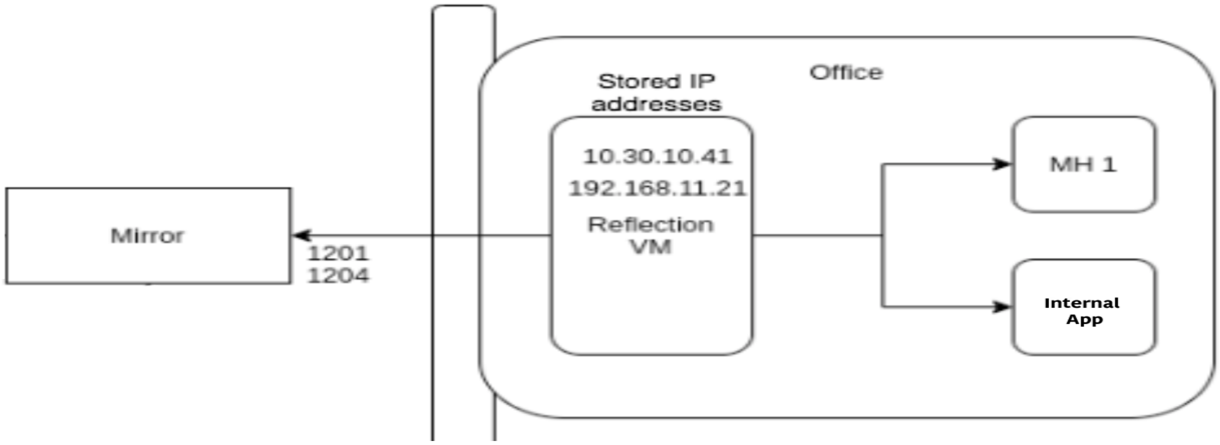
1) VM OVA* or Hyper-V file provided by TekMonks.

2) A DEV Reflector provided by TekMonks which can run on an existing Windows computer.

**An OVA file is a virtual appliance used by virtualization applications such as VMware Workstation and Oracle VM Virtualbox. It is a package that contains files used to describe a virtual machine, which includes an .OVF descriptor file, optional manifest (.MF), certificate files, and other related files.*

Additionally, TekMonks supports a plug and play model where the client is sent a physical hardware box with the Reflector (Reflection VM) already installed. Once confirmation that both power and ethernet on the box have been plugged in, TekMonks then administers this setup remotely - Skipping steps 1 - 3. The end result after configuration, whether it be VM or Hardware, is depicted in figure 9 below.

Figure 9:



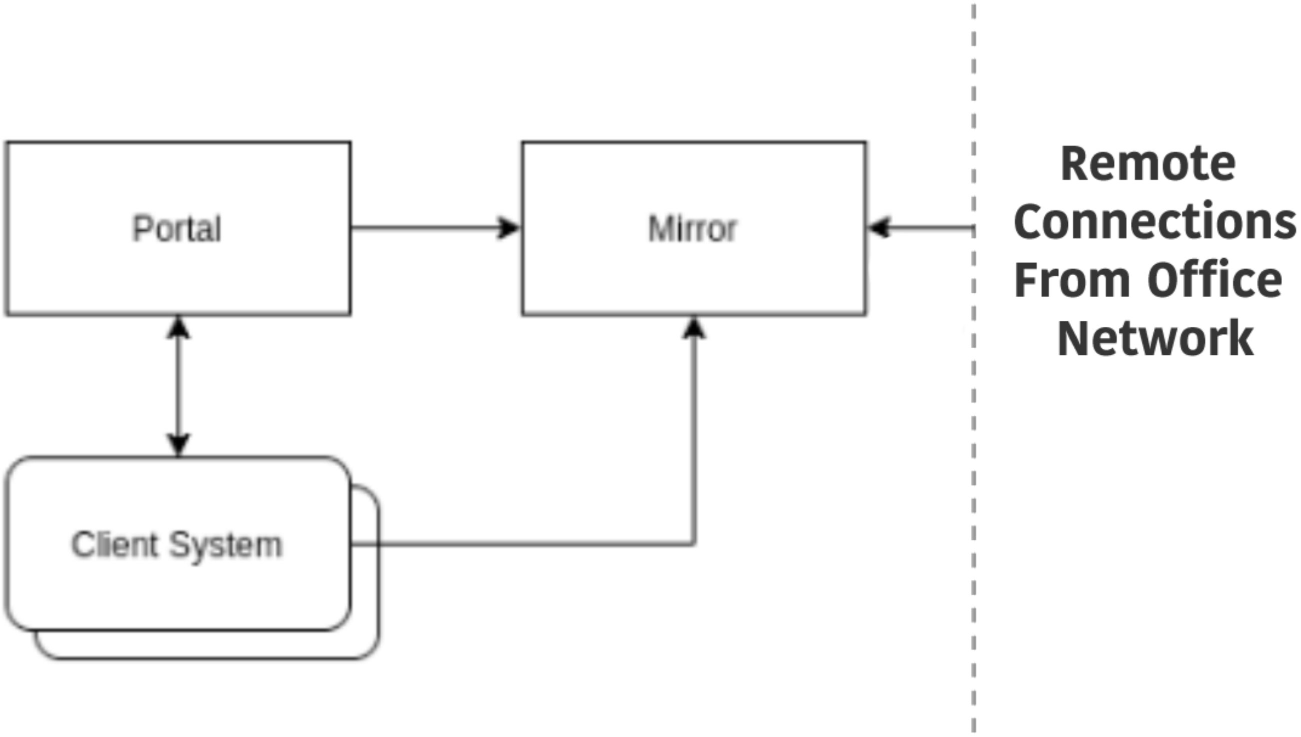
Shared Architecture

1. Portal
2. Mirror

Now that the differences between each architecture have been discussed, the shared architecture between the two options will be highlighted. This can be summarized in figure 10.

As stated earlier, customers also have a choice to use TekMonks hosted Mirror and Portal, or have their own deployed Mirror and Portal. There are also some instances where clients have not requested a Portal server and instead are authenticated via a program on their client system that then instructs the mirror to open a connection for that particular user.

Figure 10:



Summary

Setup using installers:

- DHCP and Static IP both supported.
- Support clipboard and file transfer restrictions.
- Only available for Windows Servers and Office Desktops.

Setup using Reflection VM:

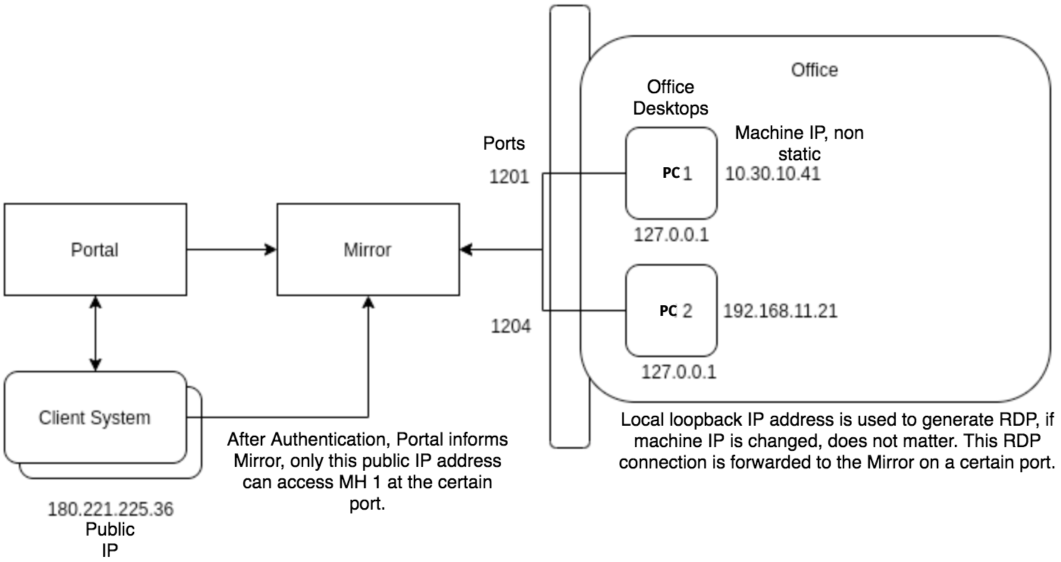
- Can be used to connect to other applications in the internal network, not just office computers.
- Requires machines with static IP
- Supports sending a wake on lan message to remotely turn on Windows PCs.
- Does not support DHCP changes for the machine addresses.

What they have in common:

- Each device/application that is reflected, is mapped to a mirror port which is then mapped to an app to be accessed via the Portal.
- Users can be assigned apps based on access control.

Figure 11:

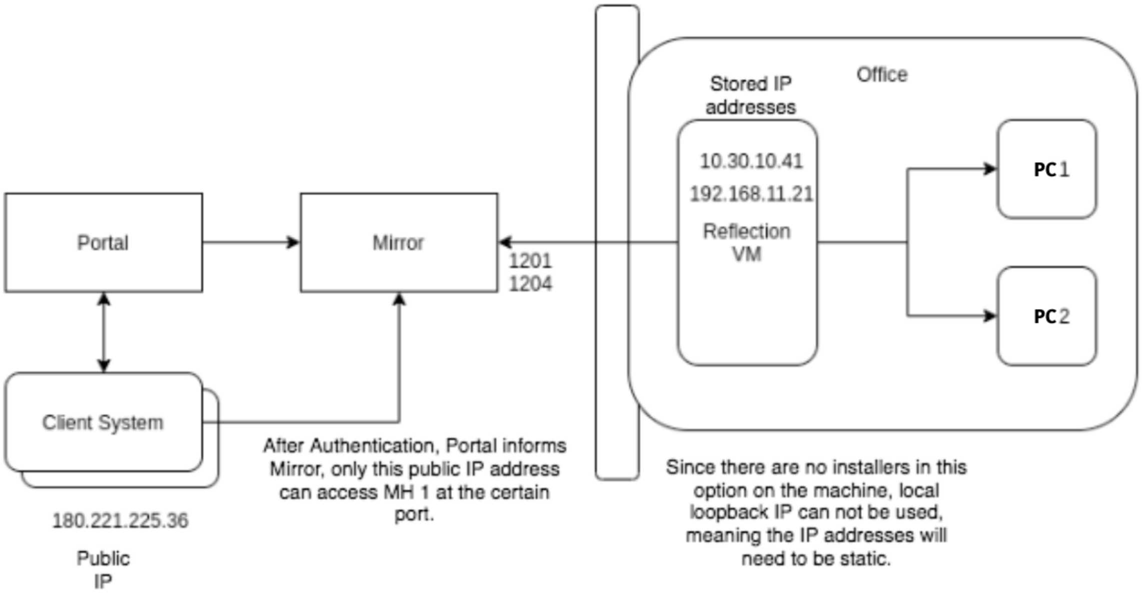
Installer



After Authentication, Portal informs Mirror, only this public IP address can access MH 1 at the certain port.

Local loopback IP address is used to generate RDP, if machine IP is changed, does not matter. This RDP connection is forwarded to the Mirror on a certain port.

Reflection VM



After Authentication, Portal informs Mirror, only this public IP address can access MH 1 at the certain port.

Since there are no installers in this option on the machine, local loopback IP can not be used, meaning the IP addresses will need to be static.

Case Two, Insurance Company.*

**We cannot disclose the name of this business due to NDA but will refer to it as "Insurance Company."*

***Adoption Year**: 2020*

***Adoption Duration As of 2022:** 2 years*

***Challenge**:* Various applications set in the Insurance Company had critical functions with associated data utilized by users for daily tasks.

Virtual Private Network (VPN) was used for remote connectivity and communications from outside the office. Having limited security options, they were vulnerable to threats upon access of office resources. Explicit support for custom solutions was also lacking for remote access, particularly for AS400-like applications.

***Solution**:* Terminated the need for VPN and implemented Reflection Network instead with built-in smart-firewall in mirrors. Associated vulnerabilities were then bypassed for extra emphasis on security. Reflection Network allows users to block any incoming connection to their internal office network that makes them completely secured while serving the mirrored services. Hence, only those registered users are allowed for remote access to office resources via a Portal that connects to mirrored connections.

Figure 13:

<NDA Required to View Diagram>

Case(s) Two: Japanese Companies - Working from Home*

**Currently in the process of asking each company for consent to provide their name in our use cases.*

***Adoption Year**: 2020*

***Adoption Duration As of 2022:** 2 years*

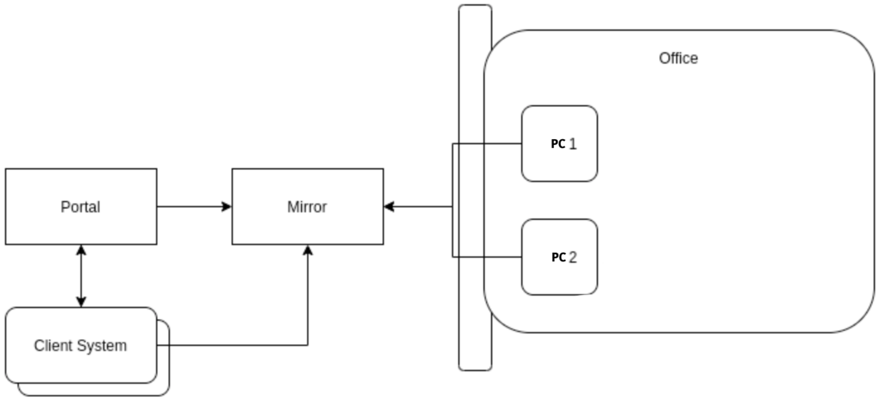
***Challenge**:* Teleworking is increasingly popular for a variety of reasons, including work life balance. The basic widespread availability of internet access and mobile computing devices makes it a viable option for all types of organizations. To hit on a current issue everyone is facing globally, the COVID-19 pandemic is causing a great number of individuals to work from home. Organizations are struggling to find a way to allow easy, secure and reliable access to their organizations systems while still keeping their employees' safety in mind.

***Solution**:* TekMonks created an architecture where both Mirror and Portal are hosted on TekMonks cloud, and various Japanese companies have set up a complete work from home solution effectively and efficiently, as all they were required to do is run an installer provided. There are the various benefits the architecture of Reflection Network that have been expressed throughout this document and, of course, the security mentioned in the document applies here, but additional benefits and reasons for adoption, in relation to adapting to the pandemic, are as follows:

1) No change to their corporate network.
2) Extremely fast and simple setup procedure.
3) Other work from home options had limitations, i.e. no MacOS support for home - or tablet, or even smartphone - TekMonks supported all these devices to be used when working from home.
4) No cap on amount of office desktops a user can add to their account (some clients use multiple different desktops, and even share computers among each other) - Other products in market have certain limitations such as 1 device per user, or having to buy licenses in bulk - TekMonks provided a ‘license as required’ model.

Figure 14:

In these use cases, all customers are accessing their internal office desktops via a TekMonks hosted mirror and Portal. Their only requirement is to run an



installer on their office PCs for account creation and Reflection set up.

Financial Benefits

The very nature of preventing a cyberattack is an immeasurable financial benefit to a corporation. As stated in the previous user case section, TekMonks will be using Leading Global e-Commerce Business as the primary example of the estimated financial benefits gained from their journey with TekMonks. However, as Leading Global e-Commerce Business, and most companies do not disclose this information, estimations with what known facts TekMonks have will be made. Following that, a more generic overview of Reflection Networks financial benefits.

Regarding The Leading Global e-Commerce Benefits:

Our client corporations calculate their financial risk themselves and do not share with anyone. However, TekMonks can generate a rough estimation as follows:

Stated in the previous section, before the Leading Global e-Commerce Business approached TekMonks, they were facing at least 1 cyberattack each month. When using information on impactful hacking statistics of 2020, “The average cost of a data breach is $3.860,000 USD”[1]. This figure is excluding very large data breaches, and very small ones, as to not skew the data.

This numerical value was deduced from various stages of response to an attack. When a breach occurs, heavy costs are incurred due to the corporation requiring to pour resources into processes such as:

1) Investigation, audit, assessment services and general crisis management.
2) Notifying all key third parties and stakeholders with emails, letters, general notice and engagement with outside experts.
3) Attempting to prevent or minimize the loss of business with various activities - this can be a side effect from the attack, such as business disruption, due to systems being down. The cost of losing customers and additionally having to regain new customers is also critical, among avoiding reputation loss and bad faith.
4) Post response after the attack, having to spend fees on legalities and recuperating losses. Adding in new support and new patches to systems - training help desk staff and so on.

With this outlook, TekMonks can make a rough estimation of financial benefits to the Leading Global e-Commerce Business. In our five years with the client, they have never been subjected to an attack or breach. As previously stated, they were facing at least 1 cyberattack each month, for 6 months prior to contacting TekMonks.

[1] IBM, “Cost of a Data Breach Report,” 5.

This means before adopting the Reflection Network (even if TekMonks underestimate the cost of an attack to $2,000,000 USD) they were facing up to $12,000,000 USD in damages in their prior 6 months of joining. If TekMonks use this figure as a year cost basis, it is $24,000,000 USD. Seeing as this Leading Global e-Commerce Business has been with us for 5 years, that would be a grand total of $120 million USD of potential damages caused due to cyberattacks.

This was then reduced to zero when implementing Reflection.

Now, of course this number is not going to fit into every single company. As a company's losses, if they are hacked, depends on various factors such as size, severity and response. For a large company, losses can be hundreds of millions of dollars and for a small company it will be less. There are also a lot of costs spent from the company's own agency - i.e. if they decide to hire external help / pay legal fees etc., which will also lead to different costs, as it is dependent on the resolution path they take.

Other Financial Benefits

Related to other financial benefits that Reflection Network brings - nonspecific to a response to an attack, TekMonks can overview as follows:

- All security measures like AMP, CDN, WAF, Firewall, DDoS mitigation are built into the mirror already at no extra cost. Reflection will save you money by removing the need to buy additional security software.

- Easily meet PCI compliance as client data is on a fully isolated server.

- Easily meet security audit goals as confidential data is on a fully isolated server and all communication is AES 256 encrypted with military grade encryption.

- GDPR and similar compliance - Store data on local servers inside the foreign country, yet be able to act on the data for business use cases globally.

- Improved bandwidth performance (in cases, up to 50%) over VPN. This is crucial for companies who serve a large volume of clients or perform critical business remotely, as faster speed means less delay and an overall improvement in job performance.

Conclusion

TekMonks Reflection Network not only will provide you with peace of mind that your data is secure, but provides great benefits as well. It reduces stress on your employees while increasing potential for productivity, reduces your overall cost and risk while increasing your safety and security, and ensures you are able to allocate your funding to what is important to your company while keeping your assets and data safe.

TekMonks' goal is to provide streamlined organizational software solutions that reduce cost and inspire productivity to meet your business goals. We achieve this by remaining intensely focused on our work and client satisfaction without other distractions or side goals. We look forward to working with your company in the future. Please let us know if you have any questions or concerns.