UNISYS

Unisys Stealth Solution Suite

Regional Isolation: An Information Embassy

Regional Site Challenges

As companies look to multiple geographies for new business opportunities, IT challenges can quickly become a nightmare. Confidentiality requirements or geopolitical challenges that may compromise IP and data integrity necessitate that systems at geographically dispersed centers be kept separate from the corporate data center. However, some regional access to the corporate data center is required. And some 'super-users' may require access to a subset of systems at any location. Consider an information embassy designed to protect data and resources within its boundaries and to control and secure access to and from the embassy.

An Information Embassy with Stealth

Unisys Stealth Solution™ ("Unisys Stealth") helps secure sensitive data, servers and applications within a specific regional site, as well as assets in the corporate data center, to accomplish these objectives:

- Isolate regional site assets from local threats
- Further segregate regional site assets from each other
- Allow selective regional site access to the corporate data center

Unisys Stealth allows enterprises to shield data assets within a designated region while controlling access to corporate assets from users in that region. Creating an information embassy with Unisys Stealth enables an organization to establish a secure regional site in various geographic locations.

Securing the regional site with Unisys Stealth helps protect the information assets developed in that region from local threats. Using Unisys Stealth to connect the regional site to the corporate data center limits visibility and access of corporate servers, data, and applications to only those with explicit permission.

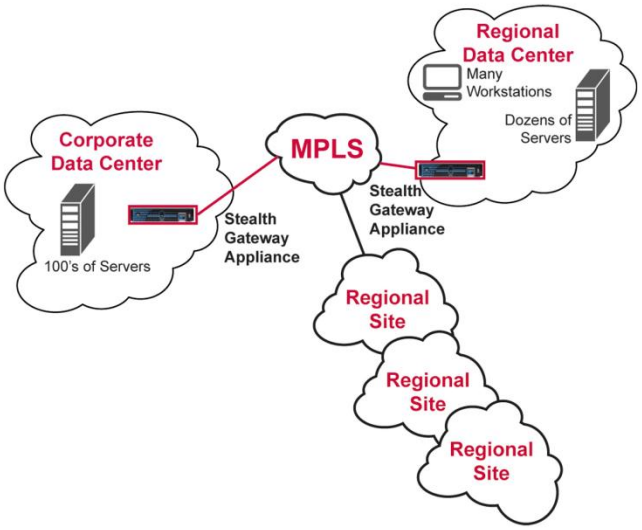
Stealth Provides a Better Strategy

To secure and isolate regional sites, companies usually construct separate physical networks for each region, though this is not foolproof since the vulnerable connection points provide a target for attacks. Not only is configuring and maintaining separate physical networks an expensive and complex endeavor; it hampers support administrators who need access to all systems and networks. In an age when access to information is critical to success, separate topologies inhibit synergy, creating a liability when data must be shared between isolated regions.

In territories where controlling geopolitical entities exist, regional sites using typical VPN-based solutions over a public network cannot prevent scrutiny of data communication from said entities. Also, these solutions are often poorly integrated with the corporate data center's identity management system, and hence prone to vulnerabilities that defeat the purpose of regional isolation.

Unisys Stealth takes a better-than-both-worlds approach to this problem. Unisys Stealth creates a communications tunnel cloaked from everyone except those who are pre-identified as part of the "secure community" referred to as a Community of Interest (COI).

COI members are cryptographically isolated from anyone not in the same COI. This isolates the COI members like they are alone on the network, and members have zero visibility to anyone or any servers or applications not in the same COI; you can't hack what you can't see.



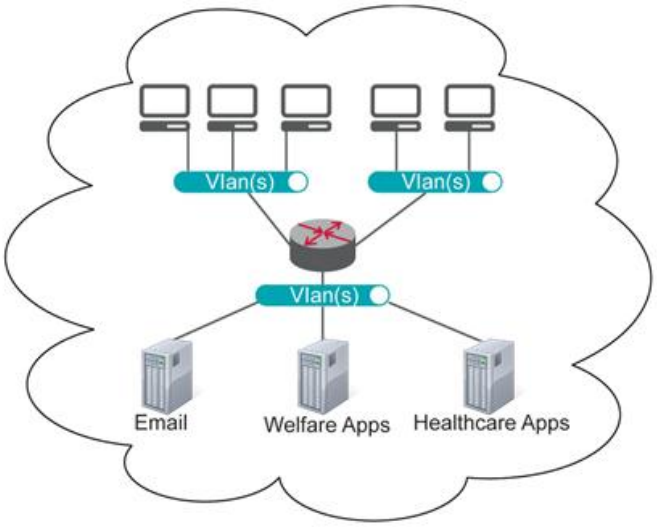
What this means is that Unisys Stealth can be deployed in lieu of, or in conjunction with, existing network topologies to isolate different regional sites. Separate COIs for each regional site ensure that users and resources at each regional site are hidden from other regional sites, as though invisible.

Unisys Stealth allows users to belong to more than one COI, a feature that can be exploited, allowing super-users or administrators to have controlled access to multiple regional sites.

Security in the Information Embassy

Within the information embassy, Unisys Stealth is designed to protect access to selected applications, hosting servers and virtual instances more efficiently and securely than other network configurations.

In a traditional tiered network, security is accomplished by physical segmentation. This requires additional network equipment and is subject to the risks of VLANs and firewalls.

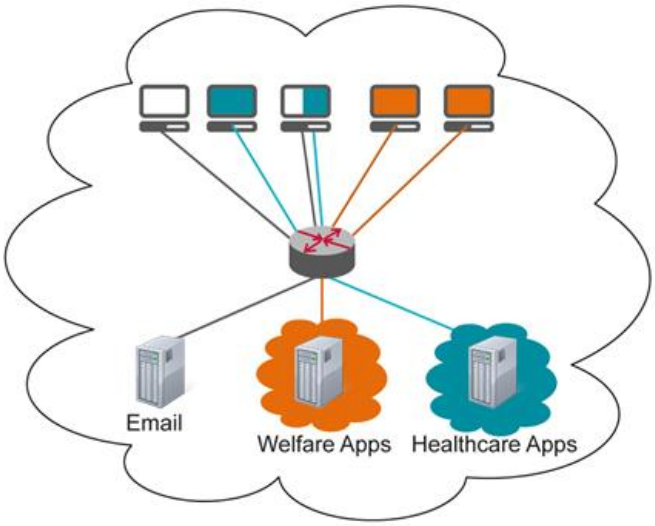


In contrast, Unisys Stealth enables security by using COIs, allowing the network to be simplified while isolating visibility and access to different servers and applications.

If the Welfare Applications in this example are strategic programs, only the users who dynamically receive the matching COI key information based on their user credentials will be able to see and access the servers housing those applications.

If an end-point tries to connect to Welfare Apps and does not have the correct COI key configuration, which means that the end-point is not a recognized member of the COI, Stealth "fails closed" and no communication path is established.

Unisys Stealth can be deployed on top of the existing infrastructure for ease of integration. At the endpoints, Unisys Stealth can be configured to communicate via



Stealth-secure channels and non-Stealth paths concurrently.

Security in the Corporate Data Center

Despite the advanced protection provided by Unisys Stealth, managing Unisys Stealth is very simple. COIs are defined by the enterprise's Identity Management system, such as Microsoft Active Directory. Unisys Stealth leverages the identity management system to authenticate the user and create the specific keys to maintain access control of COI members based on their user credentials.

What's truly unique about the Unisys Stealth architecture is that data from multiple COIs, multiple domains, and multiple workgroups can traverse the same network securely isolated from other data and users. Individuals in different departments, different organizations, on different projects can work on the same network yet be isolated from each other. This sharply reduces the risk of insider and outsider attacks. At the same time, it reduces the complexity of managing many variables across multiple networks.

Unisys Security

At Unisys, we design and develop mission-critical solutions that secure resources and infrastructure for governments and businesses. Our approach integrates resource and infrastructure security, creating the most effective and efficient security environment possible and freeing our client to focus on best serving its citizens and customers. Unisys security solutions can be found worldwide in 600+ airports, 1,500 government agencies, 100+ banks, among others.

For more information visit www.unisys.com/stealth

Printed in the United States of America August 2012