UNISYS

Stealth(cloud) XDC for Microsoft Azure

Overview

Unisys Stealth(cloud)™ Extended Datacenter (XDC) for Microsoft Azure is an advanced security solution that helps you protect your digital and physical assets deployed inside the enterprise as well as in the Azure cloud.

Stealth(cloud) XDC for Microsoft Azure enables your organization to create virtual machines on demand in Microsoft Azure cloud and provision them with award-winning Stealth security technology. The result is an agile environment that provides the flexibility and security your enterprise requires.

Stealth(cloud) XDC for Microsoft Azure starts with a Stealth deployment in your datacenter. Stealth uses encryption to cloak both servers and virtual machines from unauthorized users and protect communication between Stealth-enabled endpoints. Stealth-protected endpoints are invisible to hackers and unauthorized users – pings and probes from unknown users are simply ignored. Stealth also enables you to micro-segment your datacenter, establishing access control on a need-to-know basis. A Stealth protected endpoint communicates only with pre-authorized groups of users and devices from pre-defined Communities of Interest (COIs). Stealth COI members share encryption keys, enabling them to communicate among each other, while remaining inaccessible to non-COI members. COI membership is based on user identity, and COIs are defined by mapping groups in the enterprise identity system (Active Directory or LDAP).

Stealth(cloud) XDC for Microsoft Azure expands your Stealth deployment in the datacenter to the Microsoft Azure cloud. It enables you to provision Azure VMs on demand in the Microsoft Azure cloud and provision these Azure VMs with Stealth. It provides end-to-end encryption of data from a workstation, server or VM in your datacenter all the way to the destination VM in the Azure Virtual Network – as well as between VMs in the Azure Virtual Network. Stealth-protected Azure VMs remain invisible to unauthorized users but at the same time can participate in the COIs and micro-segmentation established in your datacenter.

Components of Stealth(cloud) Extended Datacenter for Microsoft Azure

Components of a Stealth(cloud) XDC for Microsoft Azure environment include the following:

1. Stealth software version 3.x
2. Stealth(cloud) appliance
3. Microsoft Azure endpoint VMs

The Stealth software and Stealth(cloud) appliance are installed in the datacenter while VMs on Azure can be launched from your datacenter into an Azure Virtual Network.

1) Stealth Software Version 3.x Components

Management Server

The Stealth Management Server is installed in the datacenter and runs the Enterprise Manager software. This is the central component of Stealth deployment, which provides a web interface and is responsible for registering endpoint devices, authorizing the COI memberships of users, license management, and supporting the Stealth logging functions. The Enterprise Manager enables you to configure Stealth solution and create endpoint packages that can be deployed to your endpoints. Access to the Enterprise Manager portal (EM portal) is restricted to users with specific administrative privileges.

The Stealth Management Server runs on a dedicated server or VM with a multi-core processor and at least 6 GB RAM, running Windows Server 2012 R2 or Windows Server 2008 R2 x64.

Standalone Authorization Server (Optional)

In a production environment, it is a best practice to configure at least one standalone Authorization Server for redundancy, high availability, and additional security. A standalone Authorization Server provides a subset of the functionality of the Management Server, specifically authorization of endpoints, licensing and logging. You can use your Management Server to authorize your standalone Authorization Servers and use your standalone Authorization Servers to authorize your endpoints, which can help to separate the management and authorization functions and add security to your environment.

Hardware requirements for the standalone Authorization Server are similar to that of the Management Server.

Endpoints

Endpoints can either be end-user workstations, servers or any device that runs Stealth Endpoint software. The endpoints can either run in the datacenter or on Microsoft Azure as Windows or Linux VMs.

A Stealth software agent is installed on each endpoint that needs to be secured using Stealth. The endpoint software is responsible for communicating with the Management Server or Authorization Server to authorize users into their respective COIs, claim licenses and log Stealth-related events.

Endpoints VMs in the Datacenter

For endpoints launched in the datacenter, Stealth endpoint packages are created on the management server and then deployed in client or server mode.

Stealth Endpoint Software	
Server operating systems (Each server endpoint consumes a Stealth server license)	Windows Server 2008 R2, 2012 and 2012 R2 (IPv4 and IPv6), Ubuntu Linux 12.04 and 14.04 (IPv4 and IPv6) AIX v6.1 and v7.1 (IPv4) SUSE Linux Enterprise Server 11 (IPv4 and IPv6)
Client operating systems (Each client endpoint consumes a Stealth client license)	Windows 7, 8 and 8.1 (IPv4 and IPv6)

2) Stealth(cloud) Appliance

Organizations who have deployed Stealth within their enterprise can extend their Stealth environment into their Microsoft Azure Virtual Network. This involves the provisioning of Stealth(cloud) templates which reference Stealth-enabled Azure virtual machines. These templates are in turn associated with Stealth(cloud) appliance blueprints. You commission VMs from blueprints, which select the appropriate template from which to launch a VM and provision that VM with configuration information sufficient to allow it to communicate with the Enterprise Manager in the datacenter.

The Stealth(cloud) appliance helps provision Stealth-enabled virtual machines in the datacenter and Microsoft Azure cloud. The appliance provides a browser-based, customizable self-service console with underlying automation for requesting and controlling provisioning services.

Stealth(cloud) Appliance	
Stealth(cloud) XDC Management Server	A Unisys ES3000 Model 3560R G3 Enterprise Server with: • Two 64-bit Intel Xeon processors E5-2600 series (Ivy Bridge) • 64 GB memory • Two 600-GB hard disks in a RAID 1 configuration • Six 1-gigabit Ethernet ports • Optical drive bay with DVD +/- RW drive • Windows Server 2008 R2 embedded licenses
Stealth(cloud) XDC Management Server Software	Stealth(cloud) XDC software comes preloaded with vSphere 5.5 and VM appliances that run on the Stealth(cloud) appliance
Database	Microsoft SQL Server 2008 R2 for embedded systems
Support Warranty	ES3000 3560R G3 3yr NBD Warranty
Number of VMs supported on Microsoft Azure	3000

In order to extend your datacenter into Microsoft Azure, a site-to-site VPN must be established between your enterprise and your Virtual Network(s). This VPN, which is likely to be an IPsec tunnel, although MPLS or other fully-encapsulating VPN techniques could be used, extends the enterprise IP topology and address space into the Virtual Network.

The Stealth(cloud) appliance allows configuration and deployment of multi-tier applications with Web, App and DB server VMS using Microsoft Azure resources. The application which basically is a portal provides the following capabilities:

- Create a Stealth-secured Microsoft Azure VM from a selected blueprint
- Perform commission, decommission, start, and stop operations on Microsoft Azure VMs
- Associate a Microsoft Azure VM with a project or internal cost center
- Select the lease period for a Microsoft Azure VM
- Monitor status of a Microsoft Azure VM

3) Microsoft Azure Endpoints VMs

Stealth-secured Azure VMs are assigned membership to Communities of Interest (COIs) and can communicate only with other endpoints in the same COI, either in the datacenter or in the Azure Virtual Network. These VMs can then reference to various resources within the resource providers (for instance, Storage accounts, NIC etc.).

Stealth Endpoint Azure VMs	
Delivery Method	Azure Virtual Machines provisioned by the Stealth(cloud) appliance
Operating systems supported	Windows Server 2012 R2, Windows Server 2008 R2 SP1, Ubuntu Server 14.04 SUSE Linux Enterprise Server 11 SP4

Authorization of Endpoints

Once the logon credentials of the endpoint have been authenticated, the Stealth endpoint agent communicates to an Authorization Server (either the Management Server or a standalone Authorization Server). The Authorization Server queries the identity management system (Active Directory or LDAP) to determine the user's security groups and COIs. The endpoint is then assigned the appropriate Stealth protection policies, which the endpoint agent uses to match Stealth COIs, and to filter Stealth and clear-text traffic. As a result, only endpoints (either in the datacenter or on Microsoft Azure) that share a COI membership can communicate with each other.

Extending Micro-segmentation from Your Datacenter to Azure Virtual Network

Stealth deployment in the datacenter can be extended to the Microsoft Azure cloud using Stealth(cloud) XDC for Microsoft Azure. This enables endpoints in your datacenter and VMs in the Azure Virtual Network that share COI membership to communicate with each other, while remaining cloaked from other systems in the datacenter or Azure Virtual Network that do not belong to the same COI.

The Stealth Enterprise Manager application displays a Stealth network dashboard, which provides an overview of your configuration.

Communication between datacenter and Azure VMs that share membership of a COI is encrypted using OS-native Internet Protocol security (IPsec) with 256-bit encryption. The IPsec Internet Key Exchange (IKE) protocol is preceded by the Unisys-developed Security Community of Interest Protocol (SCIP), which controls the IKE and IPsec parameters used to setup, rekey, and transport data through encrypted tunnels. SCIP/IPsec is completely transparent to applications running on the Stealth-enabled datacenter and Azure VMs.

The use of SCIP/IPsec ensures that a Stealth-protected endpoint does not respond to pings or probes from endpoints with which it does not share a COI, effectively cloaking it from any communication from non-authorized endpoints. The use of identity-based COIs rather than IP addresses to define access policies significantly lowers complexity and cost of managing access control among the workloads in the Virtual Network and datacenter.

These capabilities enable extension of micro-segmentation to the Azure Virtual Network. Stealth(cloud) can also help your enterprise meet compliance standards such as PCI DSS, HIPAA and SOX, in addition to reducing the cyber-attack surface area of application environments running within your datacenter and Virtual Network.

For more details, please refer www.unisys.com/stealth

For more information visit www.unisys.com

Printed in the United States of America 03/16 16-0118