AlienVault Unified Security Management™ [5.1]

Solutions Center Design Guide

Barry O'Meara

Lead Pre Sales Engineer
Global Pre Sales Engineering EMEA

Contents

Introduction

This document describes the detailed design of the EMEA solutions center used for Sales Engineering demonstrations and use case scenario walk throughs with potential prospects.

This document is intended for use by the sales engineering team EMEA to present and showcase the Alien Vault USM product capabilities and features.

This Solutions Center is not intended to be used for support purposes and is maintained and managed by Sales Engineering team for controlled cutomer presentations.

1. Architecture Overview

The Solutions Center design is divided into two segments.

- VMWare Environment
- Alien Vault USM MSSP Solution Architecture

1.1. VMWare vSphere Architecture

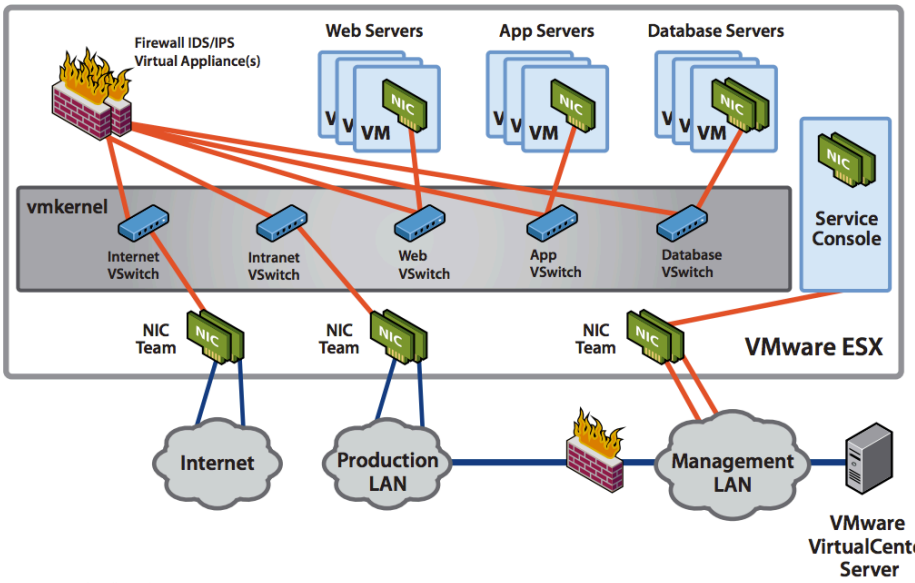
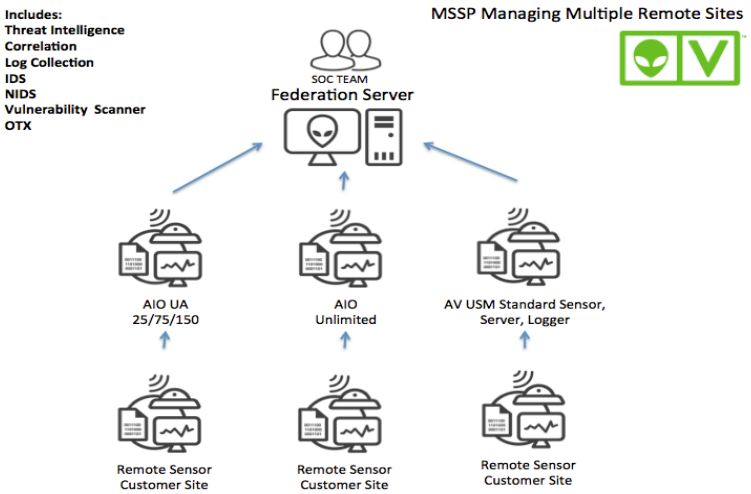


Figure 5 — Fully collapsed DMZ

1.2. Alien Vault USM Architecture



2. Detailed Design

The detailed design for the Sales Engineering Lab is divided into two sections the first section details the build of the VMWare ESXi Environment that will host the Alien Vault USM Appliance and the second section details the design of the Alien Vault USM Appliance and all of the relevant componenets.

2.1. VMWare vSphere Detailed Design

2.1.1.1. Physical Host Design

Attribute	Specification
HOSTNAME	**AVCRKSCESX01**
HA	**DISABLED**
DRS	**DISABLED**

2.1.1.2. Hardware Specifications.

Hardware Specification	
Form Factor	**1U**
Length x Width x Height (In)	**26.6 x 17.2 x 1.7**
Weight (lb)	**42**
Power Supply	**2 x 700 / 750W**
Network Interfaces	**6 x 1GbE**
CPU	**2 x Intel Xeon E5620 2.4GHz 8 Cores**
Storage Capacity (TB) Compressed 4/ Uncompressed	**9.0 /1.8**
Disk Array Configuration	**RAID 10**
Memory GB	**24**
Redundant Power Supply	**Yes**
IPMI Interface	**Yes**
Max Heat Dissipation (BTU/hr)	**439.55**

2.1.1.3. VMware vCenter Server Design

VMware recommends deploying vCenter Server using a virtual machine as opposed to a standalone physical server. That enables the customer to leverage the benefits available when running in a virtual machine, such as vSphere High Availability (vSphere HA), which will protect the vCenter Server virtual machine in the event of hardware failure.The specifications and configuration for the vCenter Server virtual machine are detailed in the following table and are based on the recommendations provided in the “vCenter Server Requirements” section of the ESXi and vCenter installation documentation. vCenter Server sizing has grown by 20 percent over the first year. VMware also recommends separating VMware vCenter™ Update Manager from vCenter Server for flexibility duringmaintenance.

2.1.1.4. VMWare vCenter Server Virtual Appliance Specifications

As an alternative to installing vCenter Server on a Windows machine, you can download the VMware vCenter Server Appliance. The vCenter Server Appliance is a preconfigured Linux-based virtual machine optimized for running vCenter Server and associated services.

Attribute	Specification
vCPU's	**2**
Disk	**70GB**
Memory	**8GB**

2.1.1.5. VMware vCenter Update Manager Design

Update Manager will be implemented as a component part of this solution for monitoring and managing the patch levels of the ESXi hosts.VMware recommends installing Update Manager in a separate virtual machine to enable future expansion to leverage benefits that vSphere 5.0 provides, such as vSphere HA. The specifications and configuration for the Update Manager virtual machine are detailed in the following table and are based on recommendations provided in the Update Manager installation documentation.

Attribute	
Vendor Version	**Microsoft SQL 2008 64-bit SP2**
Authentication	**SQL account**
vCenter Statistics Level	**1**

Attribute	
Estimated Database Size – vCenter	10.4GB
Estimated Database Size – Update Manager	150MB initial + 60–70MB per month
Estimated Disk Utilization – Update Manager	1,050MB initial + 500MB per month

2.1.1.6. vCenter Update Manager Database

This section details the VMWare vSphere Update Manager specifications used in the Solutions Center design.

Attribute	
Vendor Version	Microsoft SQL 2008 64-bit SP2
Authentication	SQL account
vCenter Statistics Level	1
Estimated Database Size – vCenter	10.4GB
Estimated Database Size – Update Manager	150MB initial + 60–70MB per month
Estimated Disk Utilization – Update Manager	1,050MB initial + 500MB per month

2.1.1.7. VMware vSphere Datacenter Design

This section details the VMWare Virtual Datacenter Design specifications used in the Solutions Center design.

Attribute	
NAME	AVCRKSCDC01
HA	DISABLED
DRS	DISABLED

2.1.1.8. Cluster Design

Attribute	
Name	**AVCRKSCCL01**
HA	**DISABLED**
DRS	**DISABLED**

2.1.1.9. VMware vSphere High Availability

At the time of writing this design document there is currently only 1 ESXi Host this restricts theenablement of High Availability.

2.1.1.10. Design Considerations

At the time of writing this design document there is currently only 1 ESXi Host this restricts theenablement of High Availability.

2.1.1.11. Resource Pools

At the time of writing this design document there is currently only 1 ESXi Host this restricts theenablement of High Availability.

2.1.1.12. Network Design

The network layer encompasses all network communications between virtual machines, vSphere management layer and the physical network. Key infrastructure qualities often associated with networking include availability,security and performance.The network design is broken into two key sections the physical network designand thevirtual network design.

2.1.1.12.1. Physical Network Design

The current physical environment consists of a pair of Cisco 3750E 48-port switches in a stacked configuration per rack. A top-of-rack approach has been taken to limit the use of copper between racks and within the datacenter. The current switch infrastructure has sufficient ports available to enable the implementation of the virtual infrastructure. Each top-of-rack Cisco 3750E pair of switches is connected to the core switch layer, which consists of a pair of Cisco 6500 switches and is managed by the central IT department.

2.1.1.12.2. Virtual Network Design

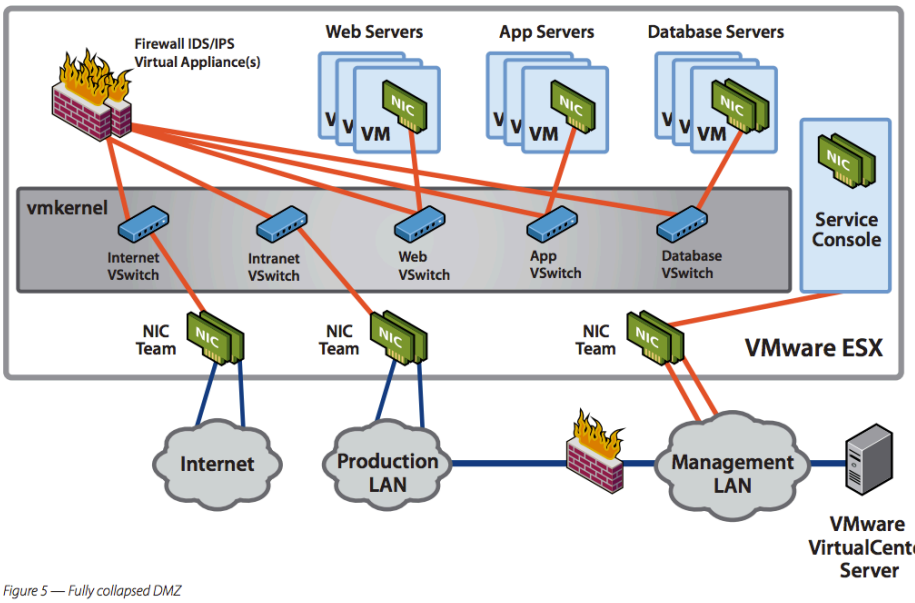


Figure 5 — Fully collapsed DMZ

2.1.1.12.3. Network Design Considerations

The proposed virtual network design is a fully collapsed DMZ. Taking full advantage of VMware technology, this approach, virtualizes the entire DMZ — including all network and security devices. Sometimes described as a “DMZ in a box,”.

2.1.1.12.4. IP Addressing Scheme

Attribute		
NAME	**IP ADDRESS**	**VLAN**
Service Console		
VMKernel		

2.1.1.12.5. vSwitch, Port Group, and VLAN's

For the purposes of the Sales Engineering LAB we will be connecting each USM to a shared management IP address and to a dedicated Portgroup and VLAN per tenant for production traffic.

Production vSwitch

Attribute			
VLAN	**101**	**102**	**103**
Port Goup	**TenantA**	**TenantB**	**TenantC**
vSwitch	**Production**	**Production**	**Production**

Management vSwitch

Attribute			
VLAN	**100**	**100**	**100**
Port Goup	**TenantA**	**TenantB**	**TenantC**
vSwitch	**Management**	**Management**	**Management**

2.1.1.13. Virtual Machine Design

The following Virtual Machines will bedeployed for each tenant allowing the Sales Engineering team to demonstrate in detail events by application and device type.

Attribute		
Role	**Operating System**	**Volume**
Domain Controller	**Windows Server 2012**	**RAID GROUP 2**
Web Server	**LINUX**	**RAID GROUP 2**
Database Server	**SQL Server**	**RAID GROUP 2**

2.1.1.14. Storage Design

At the time of writing this document only local storage is available for use. The re-prurposed servers local storage will be re-configured into 2 RAID Groups. The first RAID group is for the installation of ESXi and the remaining allocated storage is to used for Virtual Machine Storage.

Attribute		
NAME	**VOLUME SIZE**	**VOLUME GROUP**
AVCRKSCVMFS01	**100GB**	**RAID GROUP 1**
AVCRKSCVMFS02	**900GB**	**RAID GROUP 2**

2.2. Alien Vault USM Detailed Design

The Solutions Center Alien Vault USM deployment will be based on the MSSP federated architecture model. This model is currently the focus for the Sales Engineering team and represents the complex distributed charaterictics that many of our clients needs and demands Today whether they are registering as an MSSP and wish to see federated alarms or perhaps it is an end user who will be deploying USM the MSSP Federated Solution architecture allows us to showcase the full potential of Alien Vault USM.

2.2.1.1. Federated Architecture Design

- The Federation server will be deployed and connected to the “Management vSwitch”
- Tenant AIO USM’s will be deployed and connected to the “Production vSwitch” and the Management vSwitch” alarms will feed upstream via the management network to the Federation Server
- Virtualised Tenant Firewalls will be deployed and connected for each tenants VLAN on each Tenants “Production vSwitch” events from the firewalls will be fed to the tenant USM’s