# QuickSpecs

HP Virtual Controller + Virtual Firewall for VMware vSphere 1-processor Software License

*Overview*

## Models

| | |
|---|---|
| HP Virtual Controller + Virtual Firewall for VMware vSphere 1-processor Software License | JC560A |

## Key features

- Single solution for physical & virtual data center
- Purpose-built for virtualization security
- Real-time visibility of entire virtual data center
- VMware certified, VMsafe compatible
- Security policies follow VMs

## Introduction

The HP TippingPoint Virtual Controller + Virtual Firewall (vController+vFW) extends our leading IPS Platform for data center security from the physical to the virtual data center enforcing security policies in VMs and mobile VMs. The vController+vFW and Virtual Management Center are purpose built software solutions designed to enable and enforce full data center firewall segmentation and IPS inspection between trust zones for physical hosts, virtual machines (VMs) and even mobile VMs. vController+vFW+vFW intercepts all packets within the hypervisor and based upon user defined policies permits traffic, blocks traffic, or tunnels packets to a HP TippingPoint N-Platform IPS for inspection.

## Features and Benefits

### Technical features

- **Consolidated data center security and management**: The HP TippingPoint Secure Virtualization Framework is designed to provide IT personnel a single, yet flexible solution for extending the HP TippingPoint IPS Platform with its best of breed threat protection into the virtualized data center. The solution includes 2 components: (1) Virtual Controller + Virtual Firewall (vController+vFW), and (2) Virtual Management Center (vMC) – both vMC server and client are included with vController+vFW.
- **Purpose-built data center security solution**: The HP TippingPoint vController+vFW and vMC are purpose built software solutions designed to enable and enforce full data center firewall segmentation and IPS inspection between trust zones for physical hosts, virtual machines (VMs) and even mobile VMs. vController+FW intercepts all packets within the hypervisor and based upon user defined policies tunnels packets to a HP TippingPoint N-Platform IPS for inspection.
- **Extend IPS Platform into the virtual data center**: vController+vFW extends HP TippingPoint's industry-leading IPS Platform and Digital Vaccine Labs (DVLabs) security research capabilities into the virtual data center. vController+vFW enables enterprises to apply IPS security policies to all traffic from physical hosts and virtual machines. This enables IT administrators to extend their existing security processes, methodologies, tools and knowledge to secure their virtual infrastructure.
- **Leverage previous HP TippingPoint IPS Platform investments**: With the vController+vFW solution, customers gain the peace of mind of continuing to use already proven IPS Platform technology. Further, units that have been purchased for physical data center protection and segmentation can easily be utilized with the vController+vFW to also protect their virtual data center infrastructure. This makes virtual data center protection much simpler and cost-effective for IT administrators.
- **Protect the entire data center attack surface**: The vController+vFW as a component of the HP TippingPoint Secure Virtualization Framework can be used to protect the entire data center attack surface. This includes protection of or inspection of network infrastructure; host servers; virtualization tools including the hypervisor; operating systems; enterprise applications and Web applications; virtual desktop infrastructure (VDI); and VM traffic, mobile VM traffic, and VM to VM traffic.
- **Maintain security separation of duties**: One of the difficulties imposed on IT by virtualization deployments is the inherent challenge in maintaining necessary separation of duties between networking, security and other IT responsibilities. The

*Overview*

vController+vFW security solution is completely managed by vMC which is integrated with the HP TippingPoint Security Management System (SMS), making it easy to keep security management functions contained and available only to IT security personnel.

- Proactive security policy enforcement: Automated policy enforcement across physical and virtual data center infrastructure virtually eliminates the need to respond to myriad alerts, or to clean up after cyber attacks have compromised network resources. IT security costs are reduced by eliminating ad-hoc patching and alert response, while simultaneously increasing IT productivity and profitability through elimination of emergency patching and protection of critical applications.
- Single set of security policies: Extending the HP TippingPoint IPS Platform solution with vController+vFW in to the virtual data center means IT security personnel can maintain and enforce security across the entire data center including physical hosts, VMs and mobile VMs with a single set of security policies. The integration of SMS and vMC gives IT personnel a single console for data center security policy management.
- Dynamic security policy enforcement: vMC is used to automatically discover every VM in the data center and deploy vController+vFW on each virtualized physical host. This ensures appropriate security policies are dynamically applied to and enforced by vController+vFW and the IPS Platform for all deployed / discovered VMs.
- Security policies follow VMs: Virtualization of data center infrastructure creates new challenges for security personnel due to the ease with which VMs can move from host to host and even data center to data center. However, vController+vFW and vMC give IT the tools to easily maintain visibility into the location and state of every VM and to ensure that the appropriate security policies are applied regardless of the VM state (on, off, or in motion).
- Virtual patching: DVLabs delivers IPS filters to guard entire vulnerabilities, not just known exploits. These filters block all the various exploits for a given software vulnerability, creating in essence a "Virtual Patch". In the virtual data center, this virtual patching capability covers possible patch management issues created due to VM roll-backs and or server/VM shut-downs. vController+vFW and the IPS Platform protect the data center against these possible patch management issues.
- Create simple vController+vFW policies: The Virtual Management Center (vMC) makes creation of vController+vFW policies simple. Within vMC IT personnel create simple routing policies based on defined services, trust zones, traffic direction and associated action sets. These policies then get deployed to all vController+vFWs on every virtualized physical host ensuring all VM traffic can be appropriately segmented and/or inspected on a physical or virtual IPS Platform.
- Easily create a list of services: vMC makes it easy to create a list of services to be monitored within vController+vFW policies. Examples of services include DNS, DHCP, NFS, and HTTP. These services then become one of the key building blocks for vController+vFW policies.
- Easily create a list of trust zones: vMC makes it easy to create a list of data center trust zones. These zones allow IT to keep data centers segmented for security purposes. Trust zones are typically groups of similar machines and VMs such as lines of business (e.g. HR, finance), or different physical data centers (e.g. Dallas DC, London DC), or even different VM administrators or IT departments. These trust zones then become one of the key building blocks for vController+vFW policies.
- Create default VM policies: Virtualization makes the creation and replication of VM environments extremely easy. In fact, this is one of the key benefits of virtualization and HP TippingPoint's vControlle r+vFW solution is designed to support this benefit by giving IT personnel the ability to create default vController+vFW policies that are applied to all newly created or untrusted VMs or zones ensuring that security policies are applied to the entire data center as appropriate.
- Cloned VMs inherit parent policies: The replication of VM environments can be extremely easy and for this reason HP TippingPoint's vController+vFW solution is designed such that all cloned VMs can automatically inherit the policies associated with the parent VM once again ensuring that security policies are applied to the entire data center as appropriate.
- VMware certified: Both vController+vFW and vMC are certified by VMware ensuring proper interoperability and integration. Both products are certified on VMware vSphere 4 update 1 (ESX4 and ESXi4).
- VMware vCenter integration: the HP TippingPoint vMC is integrated with VMware's vCenter management console for virtual data center discovery and visibility
- VMware hypervisor integration via VMsafe API: The HP TippingPoint vController+vFW is integrated with the VMware hypervisor through the VMsafe API. VMsafe is an API developed by VMware that allows technology partners such as HP to develop tightly integrated security functionality at the hypervisor level.
- Auto-discovery of VMs: once installed, the vMC through integration with VMware's vCenter provides for auto-discovery of all VMs in the virtualized data center, making it easy for IT security personnel to ensure the full scope of virtualization in the data center is contained; this capability allows security personnel to maintain visibility into and awareness of the virtualized data center environment, and to dynamically maintain enforcement of proper security policies for all VMs
- Auto-Deployment of vController+vFW: The vMC makes it extremely easy for IT security personnel to automatically deploy

*Overview*

vController+vFW to all virtualized physical hosts after VM discovery giving security teams the confidence that the entire physical and virtual data center is protected by the appropriate security levels and that all data center trust zones are appropriately segmented.

- Visibility to control VM sprawl: vMC gives IT security personnel complete visibility of the virtualized data center helping them control and secure the sprawl of VMs. Virtualization makes it easy to create, copy and roll-back VMs creating an environment where VMs can propagate without proper oversight and security controls. The vMC / vController+vFW solution gives IT security personnel the tools to properly control and secure these heretofore uncontrolled environments.
- Follow PCI-DSS requirements: Payment Card Industry Data Security Standard (PCI-DSS) does not specifically outline requirements for virtualized infrastructure, but the underlying security tenets still apply. Hence, the HP TippingPoint vController+vFW solution is designed to enforce security policies for Cardholder Data Environments (CDE) in both physical and virtualized environments. This is critical where VMs containing cardholder data reside on the same host as VMs containing other applications
- Prepare for future PCI-DSS virtualization requirements: The next version of PCI-DSS is likely to include requirements or at least security guidance for CDE in virtualized data centers. So use the HP TippingPoint vController+vFW solution to get ahead of the PCI-DSS curve accelerating and simplifying future PCI-DSS audits.

*Technical Specifications*

| | | |
|---|---|---|
| HP Virtual Controller + Virtual Firewall for VMware vSphere 1-processor Software License (JC560A) | Minimum system hardware | 640 MB RAM memory<br>1 GB storage |
| | Supported platforms | VMware ESX/ESXi 4.0 |
| | Notes | vController solution requirements:<br>• HP TippingPoint IPS running TOS v3.1.1 or later<br>• Network devices that support VLANs<br>vMC requirements:<br>• Operation within a virtual machine<br>• Network communication with the VMware vCenter servers and with the ESX/ESXi hosts<br>• Minimum system requirements—single CPU, 2 GB of RAM, 2 GB of disk space<br>• Client minimum system requirements—Windows® XP or later, single CPU, 1 GB of RAM, 200 MB of disk space |
| | Services | Refer to the HP website at www.hp.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local HP sales office. |

To learn more, visit visit www.hp.com/networking

© Copyright 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.