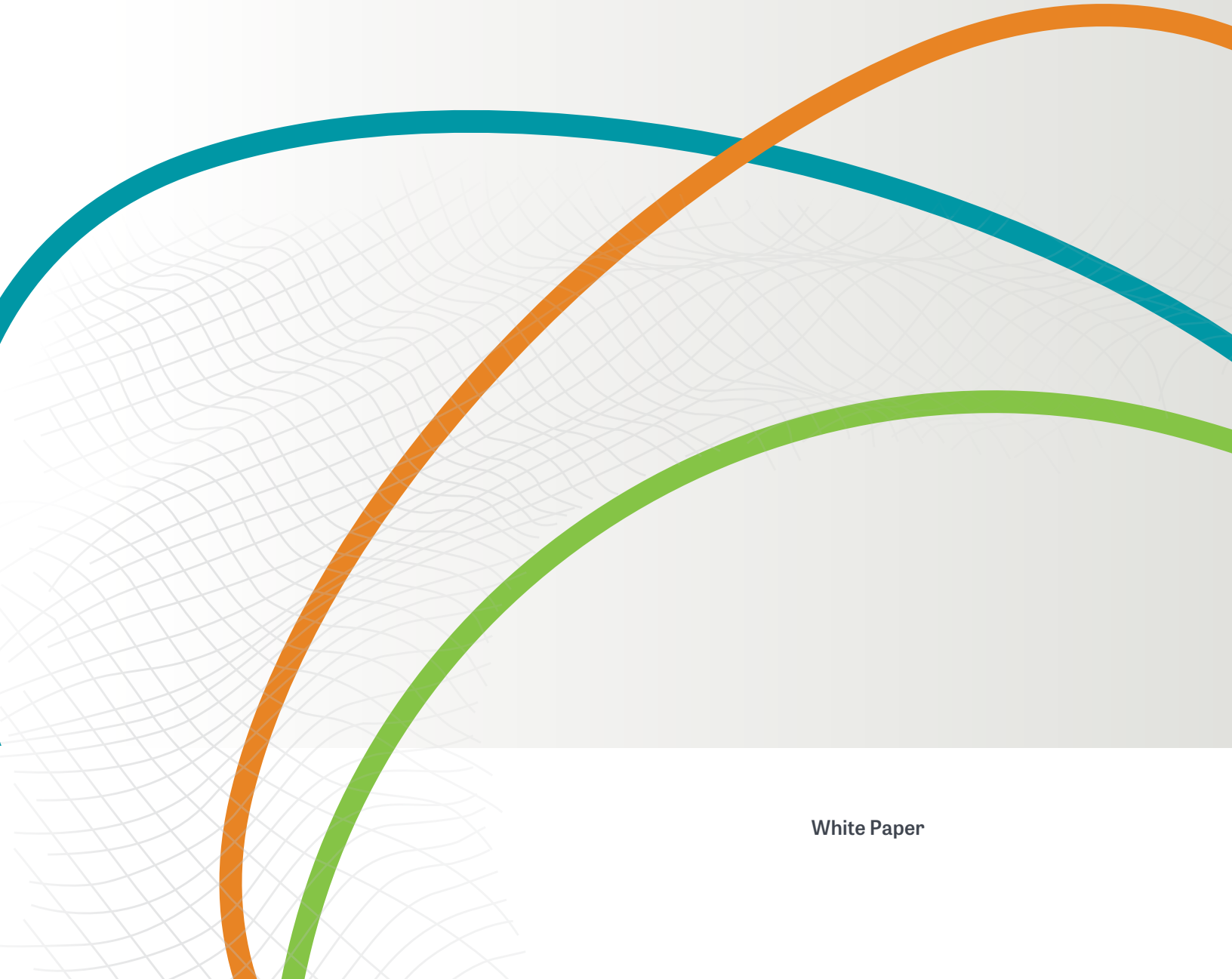
Multi-Tenant Security with vCMP

Learn how security and network architects and auditors secure multi-tenant environments with F5 Virtual Clustered Multiprocessing.



White Paper

Contents

Introduction

CIOs and architects are looking to maximize hardware and software ROI through virtualization technologies that enable them to squeeze every ounce of computing power from their existing data centers, as well as consolidate services and applications onto fewer platforms. While this need is most apparent in the world of application servers, other devices such as firewalls, routers, and Application Delivery Controllers (ADCs) could also benefit. F5's Virtual Clustered Multiprocessing (vCMP®) technology gives organizations a virtualization strategy for application delivery and isolating multi-tenant environments.

CSOs, on the other hand, want to know how secure the vCMP technology is. Managed service providers need to be able to completely assure their downstream customers that their network traffic cannot be seen or manipulated by other customers hosted on the same physical device.

vCMP combines the high-performance characteristics that CIOs require with the robust, high-security posture that CSOs demand.

Components of vCMP

Component	Description
CMP®	F5's Clustered Multiprocessing (CMP®) distributed architecture for scaling CPUs, cores, and blades
VIPRION®	The F5 scalable chassis to which modular blades and virtual BIG-IP® instances can be dynamically added without requiring reconfiguration or rebooting
Appliance	A non-modular hardware platform with a fixed number of ports and CPU cores on which vCMP instances can also be deployed
Guest OS	The operating system used by a virtual machine running on the chassis or appliance
Instance	A specific guest virtual machine (a host may run multiple instances)
Provider	The owner/operator of the vCMP implementation

Securing and Consolidating Application Delivery with vCMP

Virtualization and multi-tenant architectures are often implemented to address business and topological requirements, such as being able to consolidate services or acquire or merge existing networks. Organizations need to know that significant security mechanisms are built in to these architectures. Enterprises seeking the CapEx gains that virtualization offers

often run applications that have differing security requirements. For example, some e-commerce applications may have rigorous PCI DSS requirements, while healthcare applications may need to meet strict HIPAA standards.

In the case of service providers, their customers are often separate legal entities (they may even be competitors). These customers need assurance that their applications are isolated from each other even as their application traffic is delivered by the same virtualization platform.

F5 developed the vCMP technology with these factors in mind, while preserving the high availability, speed, and performance that are the hallmarks of all F5 products.

The provider (the owner/operator of the vCMP deployment) can offer this performance, scalability, and security to each of their downstream customers by creating discrete virtual BIG-IP® instances within vCMP. For performance, these virtual instances tap into the same application delivery acceleration hardware used by the hosting platform. To remain scalable for VIPRION® chassis, each guest instance spans multiple CPUs across multiple blades. As additional blades, and therefore CPUs, are added to the system, scalability increases linearly. Finally, to maximize security, vCMP uses a system of hardware- and software-based defense-in-depth security mechanisms to protect processes, secure access control, and isolate networks.

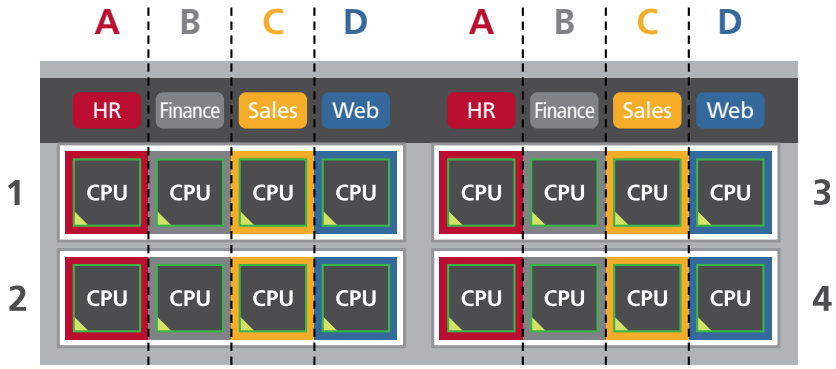


Figure 1: vCMP enables departments, customers, and partners to run their own F5 guest OSs.

Managed service providers have also found that the security of vCMP means their downstream customers can independently manage the isolated segments of their own services. For example, one downstream customer may run BIG-IP® Application Security Manager™ (ASM) or BIG-IP® Advanced Firewall Manager™ (AFM) from a vCMP guest instance to secure its application; another may be running BIG-IP® Access Policy Manager® (APM) to provide access control and authentication to its network services.

vCMP System Security

Security is built in to every aspect of vCMP. During vCMP design and development, the F5 product development and security teams examined and performed threat modeling on all of the attack surfaces—the most comprehensive security assessment in F5 history. Because of this, the vCMP system is included in the envelope of F5's Common Criteria's EAL4+ evaluation effort.

vCMP Hypervisor Security

An F5 Application Delivery Controller (ADC) is a strategic point of control within the network, and is a logical place to implement multi-tenancy and virtualization. F5's vCMP incorporates a purpose-built ADC hypervisor that features process isolation and discretionary access control. The vCMP hypervisor is specifically designed to work with F5's TMOS® operating system and the BIG-IP system to securely deliver applications. Because vCMP is purpose-built, it supports only F5-specific hardware and processes required by F5 software; F5 has complete control, making vCMP more efficient in design and operation than other hypervisors.

The vCMP hypervisor also isolates memory. It leverages the onboard hardware-level input/output memory management unit (IOMMU) to ensure that guests can't access memory from the hypervisor and from each other. In addition, the vCMP hypervisor does not read any memory that might have been written to by a guest OS except to process network traffic.

Appliance Mode

Appliance Mode is a security model designed specifically for federal and financial security requirements. It is enabled at license time and non-trivial to remove. Appliance Mode removes access to the underlying system shell, making script execution much more difficult. Access to the underlying system root account is also removed to force all users through the authentication system.

To review, three of the most prominent vCMP hypervisor security features are:

- Appliance Mode, which prevents script execution and root exploit.
- One-way memory access that protects the hypervisor from guests.
- Guest monitoring that allows only F5 guest software images.

These features secure the hypervisor against threats from hostile guests. The guests themselves have their own security subsystems.

vCMP Guest Security

From the inception of virtualization, a top concern has been isolating guests from each other. Security architects and auditors need assurance that one guest cannot manipulate another's data, or worse, break into it to steal assets. The F5 vCMP architecture has multiple countermeasures in place to prevent guest-to-guest malicious activity.

In the vCMP guest framework, only F5 product images such as BIG-IP® Local Traffic Manager™ (LTM), BIG-IP® Global Traffic Manager™ (GTM), and BIG-IP ASM may be deployed as guests, minimizing the threat surface. This policy is enforced at run time by the TMOS image installer and then at regular intervals by the vCMP hypervisor. Should a non-compliant software image be found running in a guest OS, its instance will be terminated.

Each vCMP guest is run as its own process on the TMOS host. The vCMP hypervisor manages guests and provides process isolation and memory isolation via the on-board IOMMU to restrict them from reading each other's process information, memory, or file systems.

Each guest offers a role-based access control (RBAC) system to control user access to keys, applications, security policies, audit logs, firewall rules, and more. This means that specific guests can be assigned to separate down-stream customers or business units whose credentials remain separate as well. When guests are deployed in this way, a compromised user account will remain isolated to a single, specific guest. Each vCMP guest OS instance gets its own provisioned disk space, and each CPU within the guest instance is allocated its own discrete memory, which is never swapped to disk, further increasing data isolation. Finally, each instance within vCMP runs on its own instance of the TMOS operating system, and each has the associated security benefits, including:

- Discretionary access control (DAC) via SELinux.
- Advanced access restrictions via F5's Appliance Mode.
- Encrypted interfaces via SSH and HTTPS.
- Separate RBAC system to control user access.

These security controls combine to enforce the isolation of each guest.

vCMP Network Security

Data Plane Network Security

vCMP uniquely benefits from an internal F5 hardware component that enforces network isolation outside of software. The TMOS-based hypervisor defines the VLAN assignments and works with the internal hardware switch fabric to control the traffic that reaches each guest. This prevents a guest OS from sniffing traffic or performing learning attacks and injections. Each blade in the VIPRION chassis has its own network interface that is separate from the management network, so a compromised guest cannot view or manipulate traffic destined for other guests via the data plane network.

vCMP network processing security

- Network traffic is isolated via a custom-built, guest-aware switch fabric.
- VLAN assignment is protected by the vCMP hypervisor.
- Data plane and management networks are physically separated.

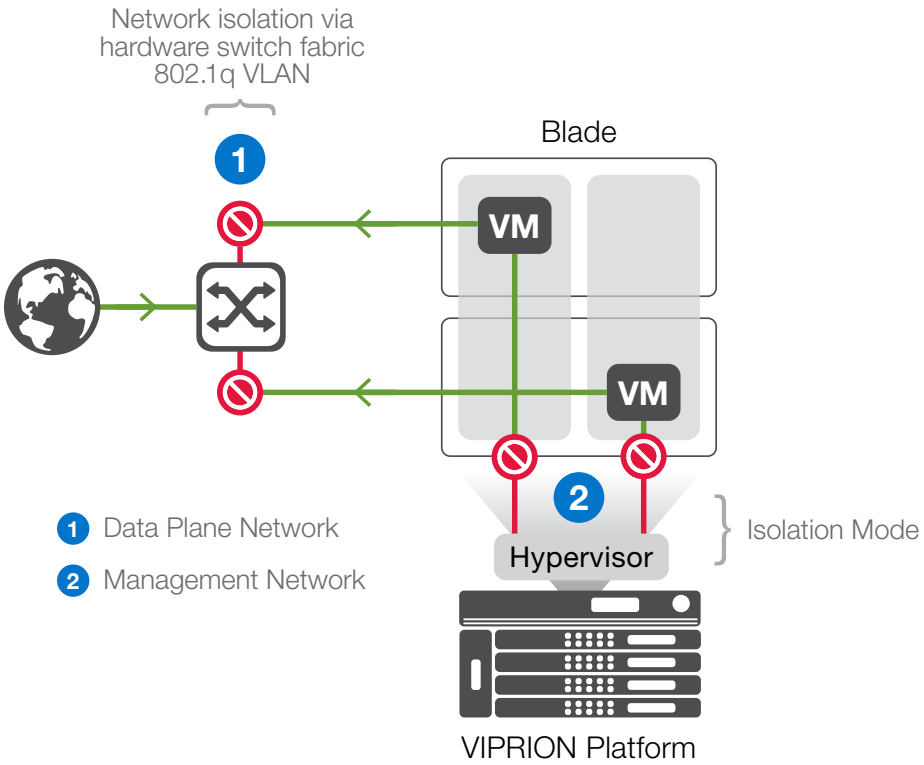


Figure 2: Network security with vCMP.

Management Network Security

The management network provides user interfaces and an iControl® portal to each guest instance (iControl is F5's REST- and SOAP-based control plane API). By giving each guest instance access to the management network, the provider can enable downstream customers to manage their own services. In a non-virtualized chassis, the management network ports are completely separated via a physical network. However, with vCMP, the network interfaces are virtualized via the vCMP virtual network bridge, enabling all guests to communicate both with each other and with the hypervisor.

For some organizations, particularly for those that have a private cloud and no downstream customers, it's important to enable guest OSs to communicate with each other across the management network. But for managed service providers and others who do host downstream customers in their own vCMP instances, it may be important to remove this access.

Isolation Mode

The provider can isolate each guest instance from the shared management network.

This is called Isolation Mode, and is configured at the vCMP hypervisor. With Isolation Mode enabled, the guest OS does not receive an interface on the virtual bridge. Isolation Mode can be configured on a per-guest basis.

Even in Isolation Mode, downstream customers can still manage their guest instances by configuring a Self IP address on the guest's data plane network. For those customers, this is the best of both worlds: access to their management interfaces but with network security enforced by the data plane's high-performance hardware switch fabric.

For example, when Isolation Mode is used, the guest OS cannot access the virtual management network bridge. Customers can create a Self IP address to allow protected access to the user interfaces through the data plane:

```
net self mgmt-dp {
    address 10.12.0.1/16
    allow-service {
        tcp:ssh
        tcp:https
    }
    vlan internal2
}
```

This solution benefits from the guest-aware hardware switching of the data plane network's VLAN-based security model (see Data Plane Network Security above).

Conclusion

As organizations adopt virtualization strategies for consolidation and operational efficiency, they will have to evaluate how those strategies mix with multi-tenancy requirements as well as how to maintain total security. F5's vCMP offers a unique, high-performance, true virtualization solution that meets the needs of both of security and multi-tenancy.

Security group	vCMP security features
Host container security	Process isolation means each guest OS gets its own memory.
	vCMP enforces that only F5 product images can be installed.
	The custom-built vCMP hypervisor is streamlined to reduce the threat surface.
Data plane network security	Network traffic is isolated via a custom-built, guest-aware switch fabric.
	VLAN assignment is protected by the vCMP hypervisor.
	Data plane and management networks are physically separated.
Guest security	The vCMP hypervisor does not read memory written to by any guest OS.
	Within each guest, discretionary access control is provided by SELinux.
	Appliance mode technology is available within each guest.
	Each guest is allowed only encrypted interfaces (SSH and HTTPS) for configuration and management.

F5 understands the significance of security in the virtualized environment. F5's extensive series of threat model assessments on vCMP technology resulted in a security model built on a defense-in-depth strategy and a proactive security posture. vCMP takes advantage of the unique, guest-aware switch fabric of the BIG-IP and VIPRION platforms to secure application delivery in a virtualized, multi-tenant environment.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

Solutions for an application world.