Hewlett Packard
Enterprise

Business white paper

Securing cloud environments with HPE DCN: Policy-based security automation and micro-segmentation overview

Table of contents

Abstract

Cloud architectures rely on Software-Defined Networking to deliver on-demand services and overcome many networking and security challenges imposed by cloud requirements. HPE Distributed Cloud Networking (DCN) delivers policy-based automation for network and security infrastructures to accelerate cloud deployments and provide on-demand service delivery.

This white paper provides an in-depth overview of the policy-based security features in HPE DCN, and examples of the primary use cases, such as micro-segmentation and secure multi-tenancy.

Cloud security challenges

As organizations rapidly build out their cloud environments, security concerns and requirements are frequently cited as the most challenging obstacle to overcome. In addition, to achieve many of the benefits of cloud architectures, organizations must make fundamental changes in virtualization and networking, which in turn necessitate new approaches to security in the modern datacenter. Cloud requirements that affect network and security policies include:

- **Secure multi-tenancy:** Cloud architectures assume there are multiple tenants sharing the same datacenter infrastructure, but it cannot be assumed these tenants are always trusted. Additional layers of security within the cloud are required to ensure security between tenants and applications if they are sharing the same server and network. This has led to a proliferation of security devices and policy enforcement points that increase the complexity of new application deployments.
- **On-demand service delivery:** Clouds are designed with the promise of on-demand service delivery and nearly instantaneous user-driven spin-up of applications in the private datacenter or public cloud. With each tenant and application potentially having specific security requirements, managing and deploying security policies can hinder the ability to deploy new services in a timely fashion.
- **Application-specific policies:** Traditional approaches to network security have been very network-centric, that is, dependent on network attributes and the network topology. In multi-tenant cloud environments, each tenant or application is likely to have its own security policies and requirements. A single security appliance may have to support different policies on different traffic flows, a challenge that few legacy security devices were designed to address.
- **Location independence:** To take advantage of cloud benefits and server virtualization, in general, application workloads must be location-independent, able to run on any server, in any rack, in any site, and potentially in both the private cloud and a public cloud location. Traditional security solutions have relied on security devices being in a fixed network location, potentially in-line with traffic flow between source and destination. Or they imposed a network topology that restricted where applications could be placed, requiring that they be either isolated or connected to other services. This type of security is completely incompatible with cloud architecture: a new virtualized security approach is required.
- **Elastic scale-out:** Similar to the need for location-independence, the cloud allows for elastic scale-out of new capacity in various locations. This may require the immediate, on-demand scale out and provisioning of additional security services. This type of scalability cannot be supported with traditional approaches and physical security appliances.
- **Untrusted cloud providers:** In addition to tenants not trusting each other in a cloud environment, many organizations have been unable to trust their most sensitive applications to public cloud providers. This lack of trust hinders their ability to take advantage of solutions that could potentially be more cost-effective. A security approach that protected sensitive data and traffic from compromise by the hosting facility is required.

Limitations and evolution of traditional datacenter (non-SDN) security approaches
Traditional (non-Software-Defined Networking (SDN)) datacenter security approaches have been unable to adapt to cloud requirements and have needed to evolve in much the same way that traditional networking has evolved to virtual networking and SDN.

- **Perimeter-centric evolving to zero-trust models:** Traditional datacenter security focuses on the perimeter of the datacenter, ensuring that malicious traffic cannot enter from the outside. All traffic inside the datacenter is assumed to be trusted. This limited approach does not address multi-tenancy or the proliferation of east-west traffic (between servers in the datacenter) in highly virtualized environments. Cloud networks have had to evolve to zero-trust models, where, by default, applications and workloads trust no other workload (connectivity is dropped) unless explicitly authorized.

- **Physical security appliances becoming virtualized:** Cloud architectures rely more on virtual security appliances rather than physical appliances to address virtual applications and virtual networking. They need to support workloads at any location and to be able to add security services on demand. Software-only security nodes can be added and scaled on-demand to address cloud requirements.

- **Automated service insertion and service chaining:** Frequently the most tedious and error-prone step in deploying new virtual applications is connecting the security nodes or appliances into the virtual application network. The process of adding firewall and application delivery controllers to the application network with the right policy configurations is referred to as “service insertion” or “service chaining” (when more than one service is connected between application tiers). The ability for an SDN platform to automate service chaining of security devices is a key feature in enabling cloud deployments and accelerating the rollout of multi-tier applications on-demand.

- **Security policies mapped to applications, not the network:** With the advent of cloud networking and multi-tenancy, security policies have evolved to be much more application-centric (for example, specific to application requirements, such as type of application, who the tenant is, which tier of the application is being protected) than network-centric (for example, network addresses and VLAN attributes). This emphasis on application-centric security policies has led to new features in security devices themselves, as well as the underlying SDN platforms that provision them into the application networks.

Introducing the HPE Distributed Cloud Networking

HPE Distributed Cloud Networking (DCN) is an SDN overlay networking solution that delivers policy-based automation of both network and security operations (provisioning, management and monitoring). SDN policies are managed in the Virtualized Services Directory (VSD), while the Virtualized Services Controller (VSC) automates changes to the cloud network and supporting devices, both physical and virtual. (See Figure 1.) Together the VSD and VSC comprise what is typically thought of as an SDN controller.

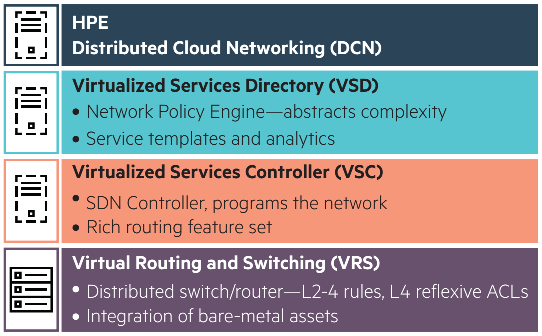
HPE
Distributed Cloud Networking (DCN)
Virtualized Services Directory (VSD)
• Network Policy Engine—abstracts complexity
• Service templates and analytics
Virtualized Services Controller (VSC)
• SDN Controller, programs the network
• Rich routing feature set
Virtual Routing and Switching (VRS)
• Distributed switch/router—L2-4 rules, L4 reflexive ACLs
• Integration of bare-metal assets

Figure 1. HPE DCN is an SDN cloud networking platform that includes the SDN controller and virtual networking infrastructure.

The Virtual Routing and Switching (VRS) component of the HPE DCN architecture forms the virtual network and provides VXLAN overlay encapsulation to virtual workloads. VRS is typically a hypervisor-resident virtual switch that provides full Layer 2 and Layer 3 networking capabilities, including enforcement of network security policies through traditional switching capabilities such as access control lists (ACLs).

Micro-segmentation

HPE DCN delivers and manages logical overlay application networks on shared datacenter infrastructures, managing connectivity between both physical and virtual workloads. By including virtual and physical security devices in these application networks, HPE DCN is able to enforce a zero-trust model, where security policies are potentially enforced between every tenant, application network and individual workload. This ability to provide fine-grained security policies to the individual workload level is called "micro-segmentation." (See Figure 2.) Micro-segmentation and a zero-trust model can halt the lateral spread of malware within a datacenter in contrast to traditional perimeter security approaches.

Security policies can be enforced directly within the VRS component of HPE DCN, which includes a Layer 4 distributed firewall. Alternatively, more advanced security policies can be enforced with best-of-breed security solutions from a rapidly growing ecosystem of security partners that includes Palo Alto Networks, vArmour and Guardicore.

In this SDN-based design, security policies are application- and workload-specific, and not dependent on the placement of the workload. The hypervisor-resident virtual switch can enforce ACL policies specific to each virtual machine (VM), while policies are managed and distributed from the centralized SDN controller. As VMs migrate between racks or between datacenters, the appropriate policies are always enforced in the new location. Physical security appliances can be included in the traffic flow to/from any application through automated service chaining.

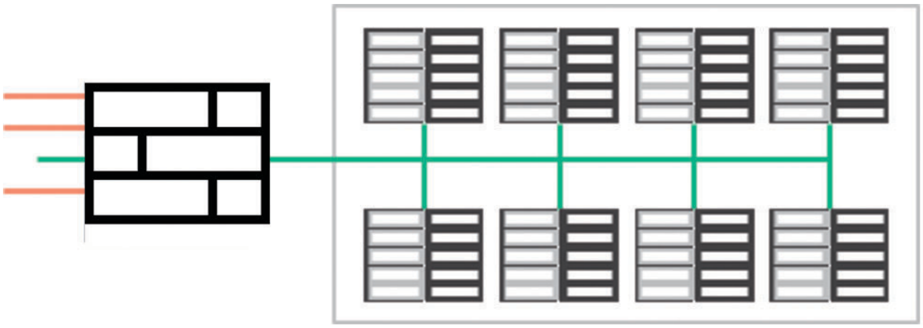

Figure 2. Traditional datacenter security policies focused on perimeter firewalls, but had few controls within the datacenter for east-west traffic.

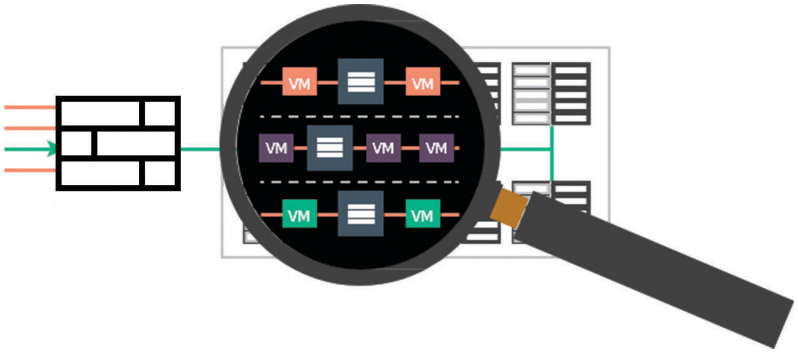

Figure 3. Looking closer, micro-segmentation provides security controls between individual workloads, as well as between applications, tenants and virtual networks. This level of granularity and sophistication can only be implemented within a large cloud environment with the help of SDN policy-based automation.

HPE DCN automatically creates and deploys reflexive Layer 4 ACLs to enable responses back through the firewall. This approach simplifies policy management and reduces the number of explicit rules. To implement reflexive ACLs, the network keeps track of valid network flows or connections and allows packets that match a known or active connection to travel back to the host. This also enables the organization to establish different security requirements to initiate a connection and maintain one.

ACL policies are not limited to traditional network-specific addresses such as source IP address, destination IP address, or port number. Policies can be constructed in the HPE SDN policy model based on mapping to the tenant, the application, application-type, and so on. This provides greater flexibility to security architects and aligns security rules with business-level requirements.

Through a rapidly growing ecosystem of best-of-breed security partnerships and certification program, customers can include a wide range of security solutions in the HPE SDN policy model with automated service insertion. The ecosystem includes leading vendors of next-generation firewalls, application delivery controllers, and intrusion prevention systems.

Micro-segmentation use cases

A primary use case for micro-segmentation is between application tiers in a multi-tier application network, such as between the application tier and the database tier in a web-based service. Each application tier can have its own access rules and security policies, and multiple instances of the same application network can be assigned to the same policy group to easily inherit the right security policy automatically.

Micro-segmentation can also ensure secure access to shared services, such as a backup service. Each endpoint can be connected to a common server or service, while individual endpoints, perhaps represented by different tenants, cannot access each other.

When malware affects one virtual host, micro-segmentation can be used to quickly restrict connectivity to other parts of the trusted network, by reassigning the affected workload to a quarantine group. Rather than needing to physically remove the compromised application, reassigning it to a new policy group for quarantine would allow blanket policies to restrict access to only remediation services automatically.

One particular multi-tenant use case is secure Virtual Desktop Infrastructure (VDI) environments. Individual desktop environments sharing the same server and hypervisor can be easily isolated, while restricting access to specific individual desktop owners.

Table 1: Micro-segmentation use cases with allowed and blocked traffic policies

	Multi-tier applications	Shared Services	Quarantine Workloads	Desktop Virtualization
Allow	Between application tiers	Access to shared service	Remediation service to infected app	From owner to individual desktop
Deny	All other non-whitelist traffic	Access between endpoints	Traffic from infected endpoints	Between VDI desktops

HPE security policy model

The capabilities of any SDN platform to implement and enforce security policies are determined by what can be represented in the SDN policy model, or the policy management language of the SDN platform. The HPE DCN policy model mirrors the organizational and application-based relationships that determine IT security policies.

In the HPE policy model, security policies are grouped by application and workload types, or by trust zones. For example, all workloads of a particular application, like a developer tool, can be placed in a named policy group and inherit a common baseline of security restrictions. Or policies could be assigned to workloads based on a named security attribute or requirement, such as a PCI-compliance zone, or a quarantine zone for malware-infected applications as described earlier. These application policy zones can be grouped into larger groups by tenant or organization, or specific virtual networks. (See Figure 4.)

The individual application and zone security policies are template-based, meaning that existing policies can be easily modified and re-used as new applications and requirements are generated. Security policies can be updated centrally in a domain template and updates are propagated across all applicable endpoints, as well as across all applications and subnets that inherit from that template.

For example, organizations can block a specific port used by newly found malware by simply updating the policy centrally in the template. Any virtual network or application domain that is based on the template will inherit the new security policy automatically. Global compliance and security updates can also be rolled out easily and individual application workloads ensured of consistent configurations.

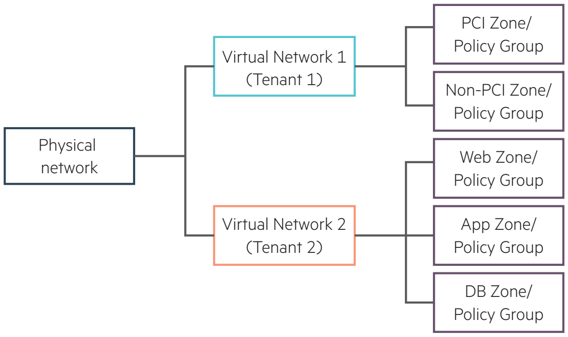

Figure 4. The HPE security policy model includes zone or group definitions that inherit policies from templates or higher level groups, and can be organized by tenants, applications and logical networks, for example.

Unlike traditional firewalls, the HPE security model is not limited to networking attributes when determining access privileges or allowing network traffic to pass. Business-level security policies can be built based on the application type, tenant name, logical zone, and so on. This provides greater flexibility and better representation of actual security policy requirements.

HPE partner ecosystem integrates best of breed security solutions

SDN has always been about open systems and interoperability. Initially this was focused on networking, but over time has extended to the integration and control of a wide range of security solutions and platforms as well. While HPE DCN manages and distributes many of the network security policies across the cloud infrastructure, it makes sense that enforcement of some of the security policies be handled by best-of-breed security solutions in categories such as firewalls, intrusion preventions systems, security analytics, access control, and more. (See Figure 5.)

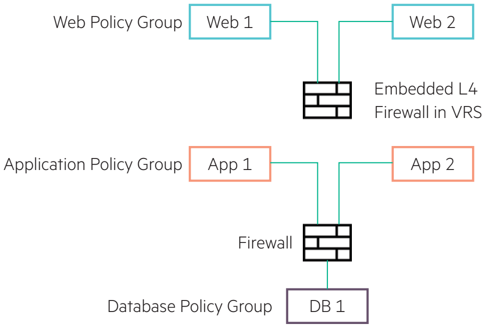

Figure 5. HPE DCN enforces security policies between application tiers in a virtual network with firewall features in the VRS, or by service chaining third-party security devices such as a next-generation firewall or intrusion prevention system (either physical or virtual).

HPE has developed a Solution Certification program that ensures the interoperability of third-party appliances and virtual solutions with the HPE DCN. By validating that the solutions work alongside those of its partners, HPE provides peace of mind for customers as they move their business applications to the cloud.

HPE DCN: A hardened and secure platform

In addition to the security policy enforcement capabilities in the HPE DCN policy model and with third-party security solutions, the Platform itself is hardened and secure, and resistant to compromise and hacker attacks. It underwent a detailed security audit by a third-party security firm to ensure the platform and the communications between components are secured. The audit included a detailed architecture and design review, as well as a code review, including analysis of overflows, key management features and cryptographic design. Penetration testing was conducted to identify security vulnerabilities and determine possible impacts of a successful attack.

Communications within the HPE DCN system are end-to-end encrypted and based on certificate-based authentication between components to eliminate man-in-the-middle attacks and access to sensitive information. Administrative privileges within the system are enforced with role-based access control in conjunction with a Lightweight Directory Access Protocol server. All administrative access and security policy changes are logged to detect any unauthorized events.

Summary

HPE DCN extends the benefits of SDN from networking to security policy management and orchestration. With cloud requirements including secure multi-tenancy, and fine-grained, application-specific security policies, automation of security devices and policies is the only way to achieve cloud-level scale and on-demand deployments. HPE DCN provides this SDN automation of the security infrastructure across network devices, its own virtual networks, and a broad ecosystem of security solutions.

This automation of security and networking policies greatly reduces IT overhead, and provides a verifiable path to compliance across large multi-tenant environments. The micro-segmentation capabilities deliver application-specific security policies to each tenant and workload, while preventing the spread of lateral attacks and malware. The automated approach to security remediation, including automated quarantine through HPE DCN group policies, provides faster incident response in the event of attack or data breach.

Sign up for updates

Hewlett Packard Enterprise

a00008822ENW, June 2017