ESG Lab Validation

Advanced Cloud Security with Check Point CloudGuard IaaS

Protecting Assets in Public, Private, and Hybrid Clouds with Check Point CloudGuard IaaS

By Tony Palmer, Senior ESG Validation Analyst; and Alex Arcilla, ESG Validation Analyst

March 2018

This ESG Lab Report was commissioned by Check Point Software Technologies and is distributed under license from ESG.

Contents

ESG Validation Reports

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

Executive Summary

ESG Lab evaluated Check Point CloudGuard IaaS to validate that it provides adaptive security in cloud environments via agile and automated deployment methods, while enabling unified management and control across different cloud platforms, specifically those leveraging VMWare NSX, VMWare ESXi, Amazon Web Services (AWS), and Microsoft Azure.

We verified that the CloudGuard IaaS solution offers three key benefits:

Any Cloud, Any Service—ESG Lab verified that the CloudGuard gateway can work with multiple cloud service providers (CSPs) and software-defined data center (SDDC) solution providers. We examined an environment where CloudGuard gateways were deployed in VMware NSX, AWS, and Azure. We saw how Check Point establishes trust relationships with CSP/SDDC solution providers, enabling consistent security policies, management, and enforcement across cloud platforms, reducing the inherent complexity of managing security in multi-cloud environments.

Agile and Automated Deployment—ESG Lab verified that Check Point has automated the deployment and configuration of CloudGuard gateways. Check Point has leveraged existing workflows within AWS and Azure to allow users to deploy CloudGuard gateways via templates. Leveraging AWS and Azure workflows also allows the user to leverage other features offered by both CSPs, such as automatic scaling and failover, to enable both resiliency and scalability of the CloudGuard gateway.

Unified Visibility and Control—ESG Lab verified that the Check Point management architecture enables the user to view security events across a heterogeneous, hybrid cloud environment, correlating events to applications and policies. The timeline view allows for additional tracking and traceability while individual logs can be examined and filtered by specific categories for targeted investigation.

If your organization has deployed or is planning to deploy any application or service into the cloud, you would do well to take a close look at Check Point CloudGuard. In ESG testing, Check Point provided automated, agile security— well suited to dynamic multi-cloud and hybrid environments—with a single, unified management platform to manage multiple, disparate cloud platforms as a single cohesive system.

Background

When it comes to cloud security, ESG research uncovered many challenges that organizations stated that they face as they continue to adopt the cloud into their overall IT infrastructure. Prominent challenges include securing controls to new workloads (34%), assessing the overall security status of cloud infrastructure (34%), and cross-cloud monitoring (34%), and protection (31%).[1] In ESG's annual IT spending intentions survey, 81% of organizations state that they plan to use two or more public cloud infrastructure providers (infrastructure-as-a-service (IaaS) and/or Platform-as-a-service (PaaS).[2] Having said that, any organization that relies on public and/or private cloud environments to do business faces new challenges when it comes to securing traffic that runs within and between different cloud platforms.

With traditional on-premises networks, securing the network perimeter was extremely important, but once organizations began to leverage public and private clouds as part of their IT infrastructure, the challenge shifted. As workloads and applications are moved to hybrid clouds, virtualization maximizes the utilization of the underlying physical resources while enabling business agility and resiliency. However, the nature of virtualization introduces a new security risk—traffic that moves between virtual machines (VMs) within the public or private cloud. The security precautions taken within the cloud are primarily designed to protect the entire cloud infrastructure rather than the traffic that flows between VMs. Cloud

[1] Source: ESG Research Report, *The State of Cloud Security in the Enterprise*, October 2016.
[2] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

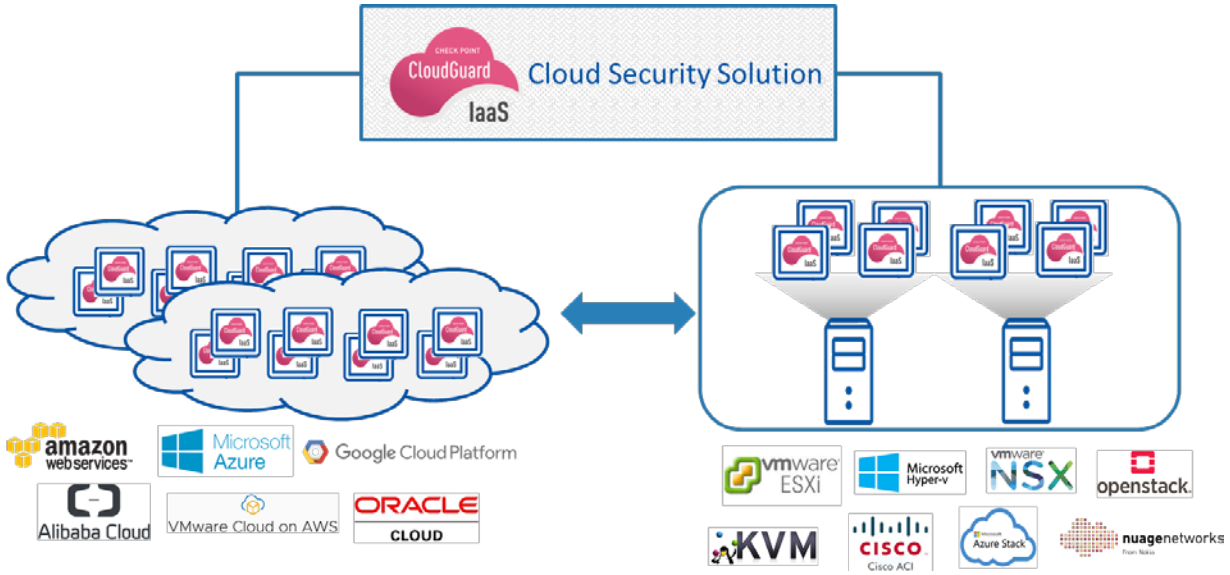
solution providers are not responsible for securing individual customer traffic streams. This responsibility lies with the organization that uses cloud resources. This concept is known as the shared responsibility model.

Organizations that leverage the cloud for their IT operations must secure workload and application traffic at the VM level. This requires looking at both inter-cloud security, as the perimeter of an organization's cloud environment can change at any time when VMs are moved, as well as intra-cloud security, especially when attacks can propagate between VMs.

The Solution: Check Point CloudGuard IaaS

CloudGuard IaaS is designed to extend to virtual environments all the same advanced security functions and capabilities found in Check Point solutions that protect physical infrastructures. Specifically, CloudGuard enables IT to protect cloud environments against all variants of attacks from viruses, bots, OS and application attacks, as well as previously unknown and zero-day attacks. CloudGuard enables organizations to deploy security policies consistently across virtualized workloads and applications in public, private, and hybrid multi-cloud environments. Policies remain consistent as these workloads move within and across cloud environments and virtualized data centers, eliminating the need to repeatedly configure and apply security policies.

Figure 1. Check Point CloudGuard IaaS for Public and Private Cloud Security



Source: Enterprise Strategy Group

As seen in Figure 1, Check Point has integrated CloudGuard into the solutions provided both by public CSPs and SDDC solution providers. The company has integrated CloudGuard into existing workflows to minimize the amount of manual overhead needed to implement security policies, preestablishing the trust relationships between CloudGuard and CSPs/SDDC solution providers.

The solution consists of the CloudGuard gateway and the Check Point management architecture. For virtualized data centers that leverage VMware NSX, IT automatically deploys a CloudGuard gateway on every ESX host via the NSX Controller. VMware NSX users employ the CloudGuard Controller to apply security policies consistently and adjust them dynamically as workloads and associated traffic move within the data center, such as IP address changes. Traffic between workloads within the data center are secured, minimizing the chances that any threats spread to adjacent ESX hosts.

With AWS and Microsoft Azure, IT can automatically deploy CloudGuard gateways by provisioning them via the user interface (the AWS Marketplace or the Security Menu in Azure) or via scripts/templates (i.e., Ansible, PowerShell, or

Python). Check Point has also designed CloudGuard to leverage the CSPs' automatic scaling capabilities such that the number of CloudGuard gateways can increase or decrease depending on the amount of traffic to be secured.

CloudGuard's integration with ESXi, NSX, AWS, and Microsoft Azure is engineered to address many challenges that IT faces in securing virtualized workloads and applications. IT can provision CloudGuard gateways across multiple VMs with little manual intervention. Since CloudGuard gateway security policies are assigned at the VM level, IT can move VMs between ESX hosts, between VPCs/VNets, and between an organization's data center and public or private cloud resources without having to reconfigure security policies. East-west traffic within and between cloud resources remains secure, minimizing the chances that threats will propagate.

SmartConsole enables management and visibility across entire IT infrastructures, including all public, private, and hybrid cloud instances. While SmartConsole leverages a graphical user interface (GUI), IT can choose also to access management capabilities through Check Point APIs or the portable SmartConsole. The SmartConsole allows IT to view all deployed CloudGuard gateways across multiple public and private cloud resources. The unified view enables IT to monitor and manage CloudGuard gateways across multiple cloud platforms and configure security policies across multiple cloud platforms as well as physical security gateways, ensuring consistent policy deployment.

ESG Lab Validation

ESG Lab performed hands-on evaluation and testing of the CloudGuard Cloud Security Solution at Check Point Software Technologies headquarters located in San Carlos, California. Testing was designed to demonstrate how organizations would use CloudGuard across different public and private cloud solutions and how they would implement CloudGuard in an agile and automated manner, with unified visibility and control across all CloudGuard gateways in an organization's cloud environment.

The test environment was designed to simulate an organization's private cloud. An ESXi server hosted test VMs representing web, application, and database servers, along with VMware NSX Manager and CloudGuard for NSX. The environment also consisted of both an AWS VPC and a Microsoft Azure VNet. All resources were interconnected via an on-premises Ethernet switch and a physical perimeter security gateway. We used a laptop to connect to the lab environment via a wireless gateway. Another isolated environment consisted of ESXi servers with virtual PCs and servers as well as a CloudGuard ESXi Virtual Edition gateway.

Any Cloud, Any Service—Adaptive Security

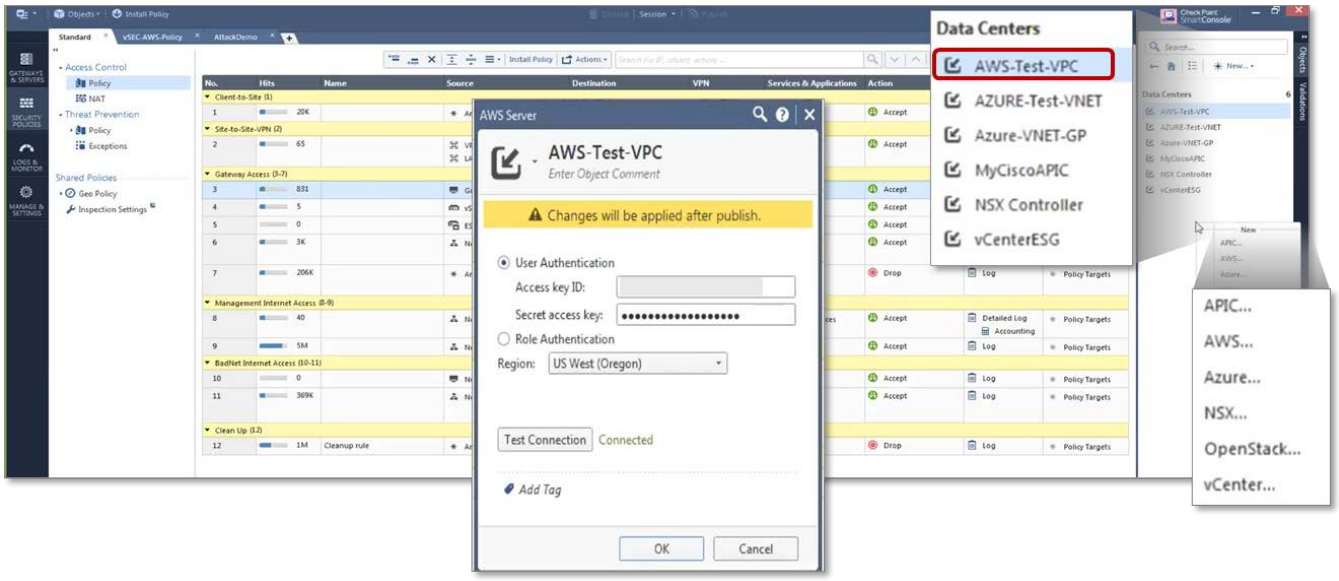
Organizations that leverage multiple public cloud resources and/or SDDC solutions must ensure that security is consistent across their cloud environments. This consistency can help IT ensure that they can assign the same security policies to specific workloads regardless of the cloud platform on which they reside.

To help IT address this challenge, Check Point has integrated its CloudGuard IaaS Cloud Security Solution with multiple public cloud and SDDC workflows that allow IT to provision the CloudGuard gateway while setting up a new public or private cloud.

ESG Lab Testing

ESG Lab began by examining the *GATEWAYS & SERVERS* tab of SmartConsole. This view allows an administrator to view the CloudGuard gateways that are deployed in an organization's environment (cloud and physical). On the right-hand side of the screen, we saw the CloudGuard gateway options that were preconfigured with security policies and rules. For this testing session, CloudGuard gateways were automatically deployed in data centers created with AWS, Azure, VMware NSX, VMware ESXi, and simulated Cisco ACI, as shown in Figure 2.

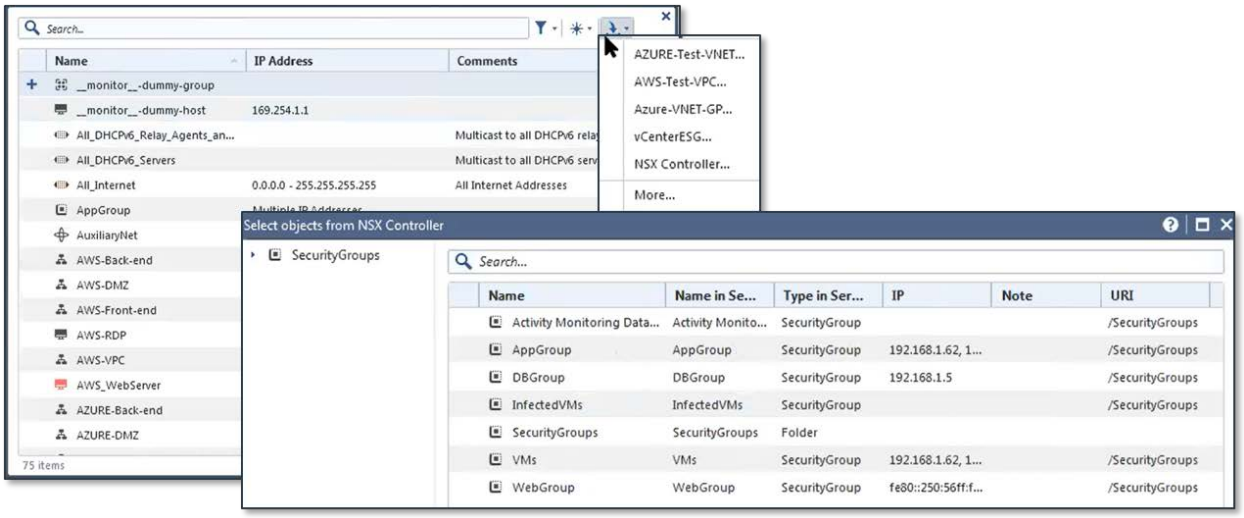
Figure 2. SmartConsole View of Insertion of CloudGuard Gateways into Multiple Cloud Platforms



When we clicked on *AWS-Test-VPC*, we saw the pop-up window indicating the authentication details for setting up this specific cloud environment, called a Data Center by Check Point. A similar window appeared when we clicked on the *AZURE-Test-VNET* option, confirming the trust relationships established with both AWS and Azure.

ESG Lab then observed how establishing this trust relationship can help to import policy objects easily from CSP/SDDC providers and deploy those into existing physical and virtual Check Point gateways (see Figure 3). We opened a window that displayed all objects across both the physical and virtual data centers visible in the SmartConsole. We then chose "NSX Controller" to display its security policy groups. From here, IT can select specific policies and apply them to gateways either deployed within the NSX environment or across other public or private cloud platforms without the need to configure each gateway individually, decreasing the time that an organization's IT infrastructure is potentially vulnerable.

Figure 3. Applying Security Policies Dynamically Across Cloud Environments



Why This Matters

As organizations continue to migrate their on-premises IT infrastructure to the cloud, security becomes more challenging. At any given time, the VMs can move anywhere within the environment, making it difficult for IT to secure traffic moving between VMs. Breaches on VMs can potentially spread to other VMs without detection by perimeter defenses. Also, as organizations employ a combination of multiple cloud resources provided by both CSPs and SDDC solution providers, traffic can potentially pass between public and private clouds without consistent governance.

Check Point is addressing these issues by integrating CloudGuard with multiple public and private cloud platforms. A user of the CloudGuard IaaS solution can deploy and configure firewall and advanced security capabilities onto CloudGuard gateways across multiple cloud platforms with trusted relationships and integration with a cloud platform's workflows and automation.

ESG Lab validated an environment where CloudGuard gateways were deployed in VMware NSX, AWS, and Azure. We saw how Check Point establishes trust relationships with CSP/SDDC solution providers enabling consistent security policies, management, and enforcement across cloud platforms, reducing the inherent complexity of managing security in multi-cloud environments.

Agile and Automated Deployment of CloudGuard IaaS

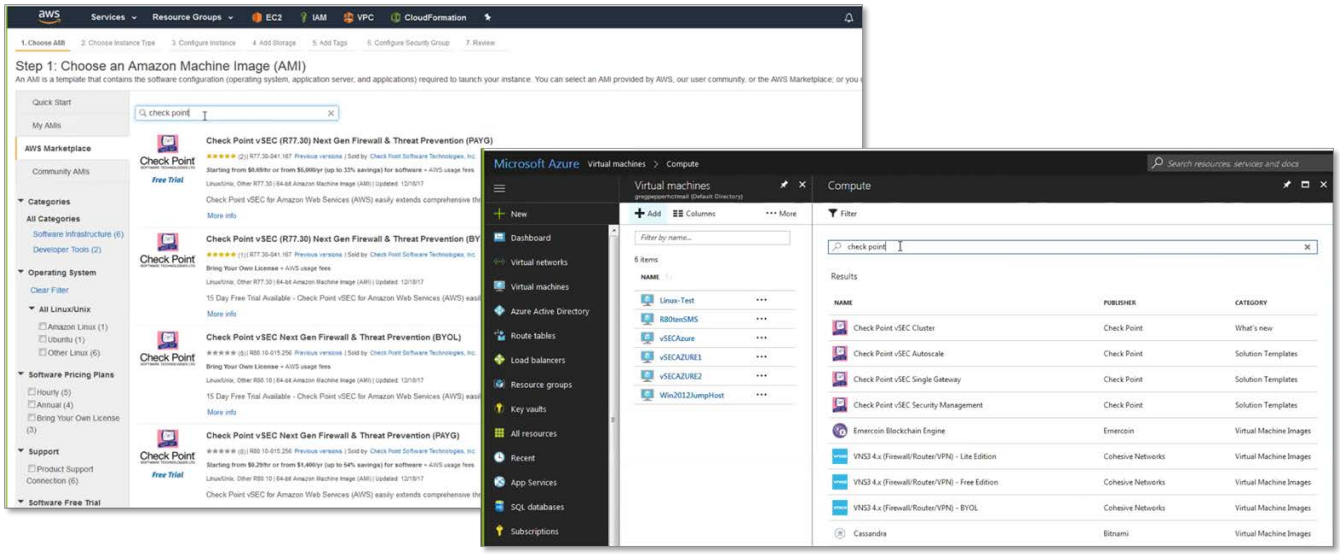
The dynamic and elastic cloud environments of today are very different from the static networks organizations have managed in the past. Infrastructure can grow or shrink on demand, resources can go dormant and wake up spontaneously, or move from place to place—all by design—and security must not be a bottleneck to realizing these fundamental cloud attributes.

Check Point has designed the CloudGuard gateway to address these challenges by enabling IT to deploy it in an agile and automated way, minimizing user intervention and automatically aligning an organization's entire security ecosystem against ongoing and potential threats—seamlessly across multiple clouds.

ESG Lab Testing

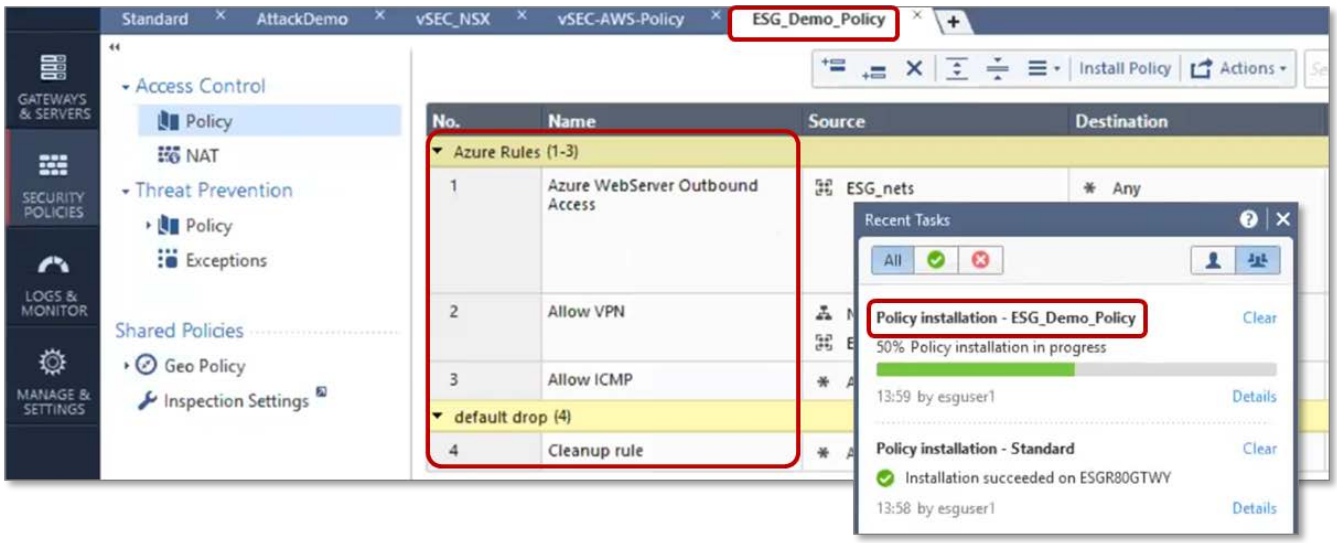
ESG Lab began by examining how IT can deploy a CloudGuard gateway instance via both the AWS and Azure cloud platforms. Figure 4 shows the webpages from both AWS and Azure that display available Check Point CloudGuard gateway options after typing "check point" in the search box. For both AWS and Azure, a user can launch one option and proceed through the subsequent menus based on templates provided through both platforms. We noted that templates existed for deployment of a single gateway, high availability clusters, and AWS Auto Scaling groups/Azure VM Scale Sets. Alternatively, the user can launch a CloudGuard gateway via templates provided by either Check Point or write custom templates leveraging APIs from Check Point's API library.

Figure 4. Check Point Templates Provided by AWS and Azure



To show how Check Point has achieved CloudGuard gateway configuration and automated deployment, we ran an Ansible template on Azure to deploy a CloudGuard gateway. This template contained five sub-templates breaking down the steps for inserting a CloudGuard gateway, including policy configuration and gateway deployment into a VNet. As we ran the code, it instructed Azure to create a resource group called *ESG-demo-rg*. A resource group is a collection of resources that are treated as an individual instance in Azure. This group represents a complete CloudGuard gateway that contains policies defined in the template, along with network connections and storage required to operate in an Azure VNet.

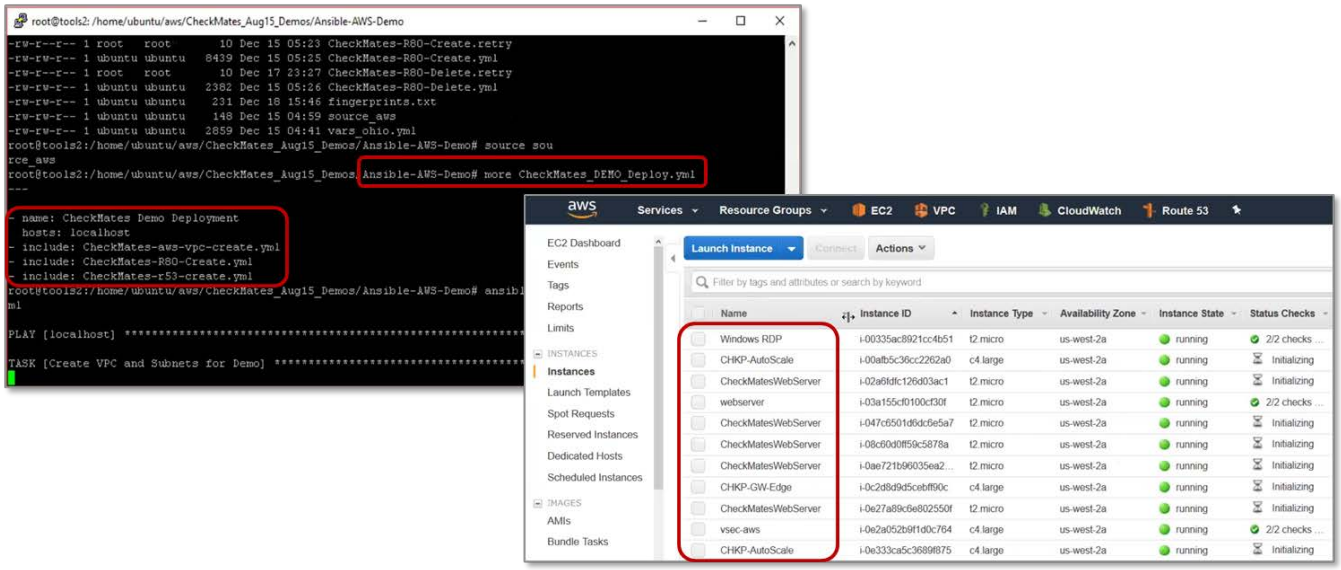
Figure 5. Deployment of CloudGuard gateway in Azure via Template



As the templates ran the code, ESG Lab observed that the code also deployed the access control security policies as indicated in the circled list in Figure 5, called *ESG_Demo_Policy*, onto the newly created CloudGuard gateway.

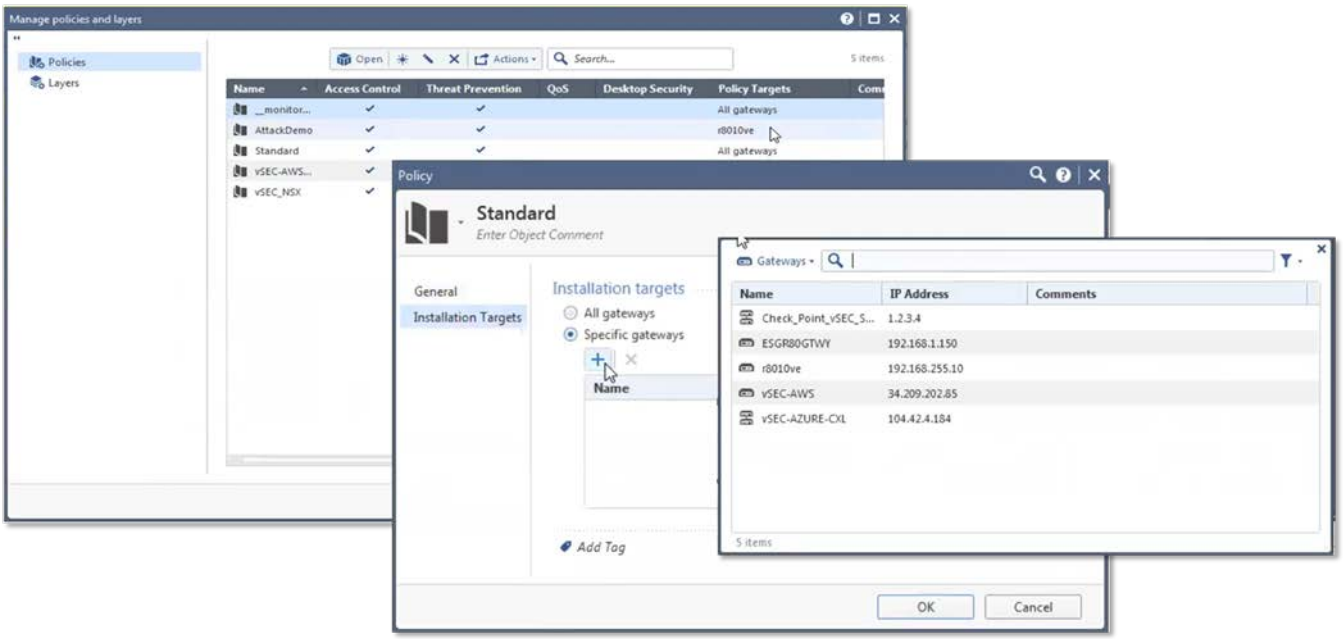
The deployment and configuration of a CloudGuard gateway in AWS via Ansible templates was very similar to deployment in Azure. Figure 6 shows the summary of steps completed by the template named CheckMates_DEMO_DEPLOY.yml. It should also be noted that the template enabled this CloudGuard instance to automatically scale, leveraging AWS's native Auto Scaling features, without the need for the user to add more gateways.

Figure 6. Deployment of CloudGuard Gateway in AWS via 3rd Party Automation Tools



Finally, we observed how Check Point allows the user to apply security policies across CloudGuard gateways deployed in multiple platforms to ensure consistency, regardless of where the policy was initially applied. Using the *Manage Policies and Layers* view in the SmartConsole, we chose the option for viewing all deployed security policies. All policies contained rules for dealing with both access control and threat prevention, as shown in Figure 7. The window also listed the policy targets, which are the CloudGuard and physical gateways that applied these specific policies within a given environment. After double-clicking on the *Standard* policy, we then clicked on Specific *Gateways* under *Installation Targets*. The user can specify those CloudGuard instances that enact the standard policy.

Figure 7. Applying Security Policies to Desired CloudGuard Gateways



Why This Matters

Deploying security policies in an organization's IT infrastructure becomes complex and time consuming when integrating multiple cloud resources. No longer is traffic confined within a set security perimeter given the cloud's elastic nature. The ability to secure traffic within and between public and private clouds quickly, easily, and consistently, regardless of the underlying cloud platform, would help IT to ensure consistent security policies across an organization.

By leveraging existing workflows and templates, Check Point allows a user to deploy and configure CloudGuard gateways into a cloud environment quickly and easily. The approach provides consistency of security policies across a heterogeneous environment. The Check Point management architecture allows the user to apply policies deployed in one cloud platform to be configured onto CloudGuard gateways deployed on other cloud platforms.

ESG Lab verified that Check Point has leveraged existing workflows within AWS and Azure to allow users to deploy CloudGuard gateways via templates. Leveraging AWS and Azure workflows allows the user to leverage other features offered by both CSPs, such as automatic scaling and failover, to enable both resiliency and scalability. We also observed how a user can easily import and apply policies regardless of CloudGuard instance and the underlying cloud platform, minimizing the need to configure the same policy across an organization's cloud resources.

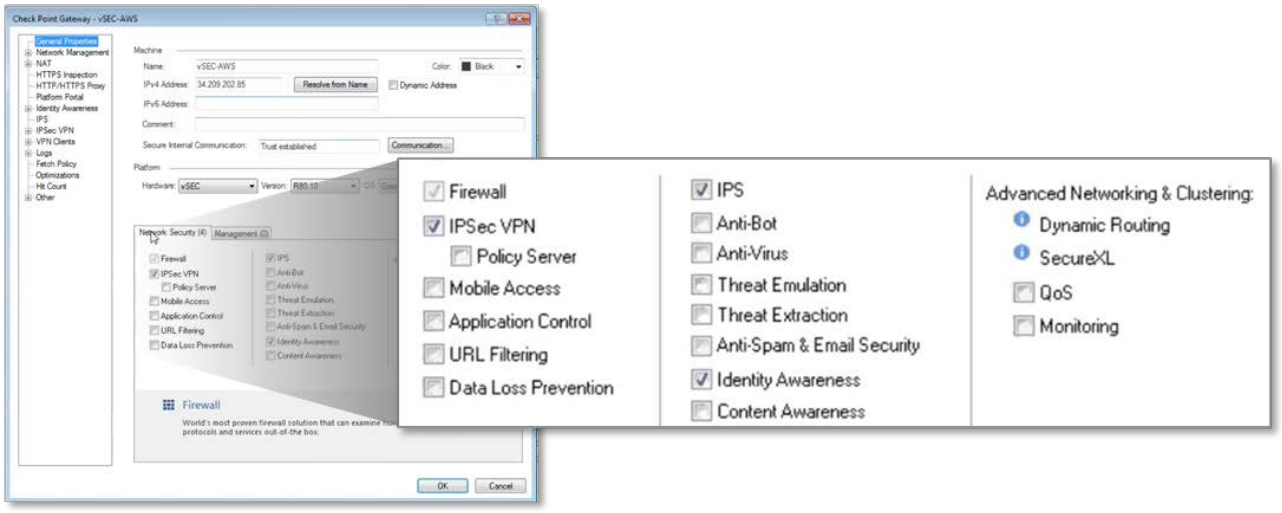
Unified Visibility and Control

When dealing with a multi-cloud environment with different workflows and management systems, IT faces the task of maintaining policy consistency, protection, and visibility across disparate cloud platforms. To minimize both time and error, the Check Point management architecture provides visibility into all CloudGuard instances deployed across the cloud platforms referenced in Figure 1 in one unified view. The Check Point management architecture provides for native API integrations, SIEM integrations, enhanced logging, event correlation, and reporting.

ESG Lab Testing

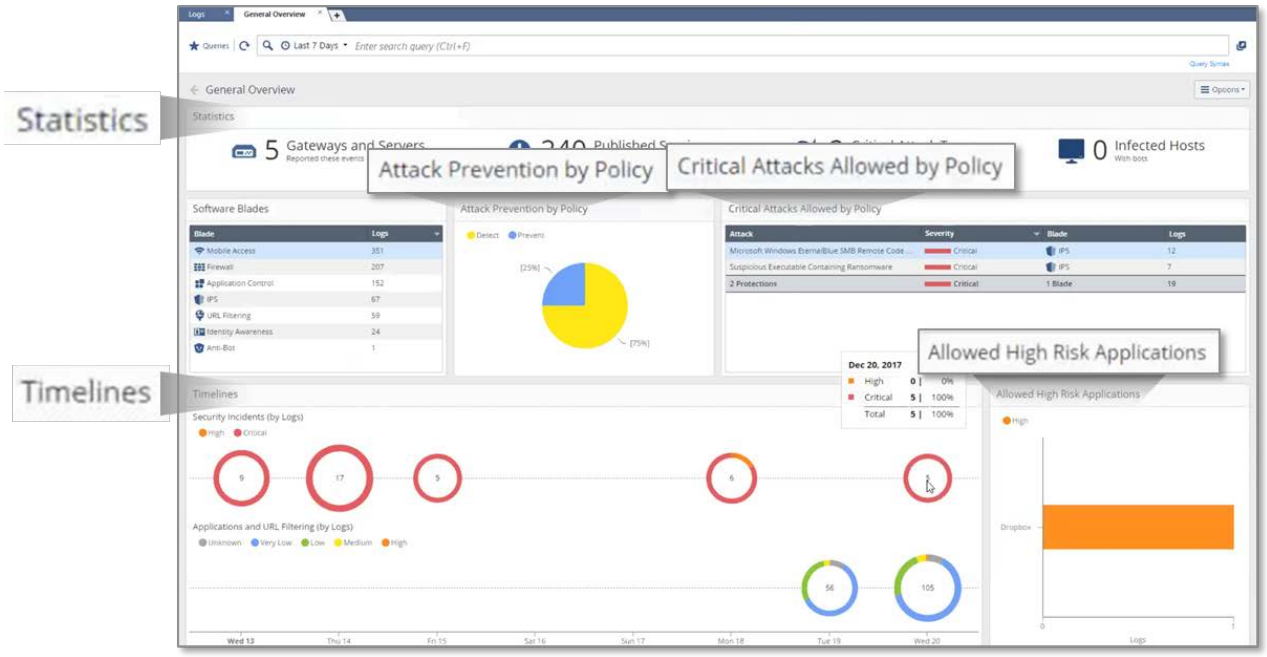
ESG Lab first viewed the security policy on the AWS CloudGuard gateway. We double-clicked on the ***AWS*** gateway in the ***Gateways&Servers*** tab (shown in Figure 8). A user can apply additional security protections to the CloudGuard gateway aside from the default ***IPSec VPN***, ***IPS***, and ***Identity Awareness*** protections already applied via the Ansible template. Depending on the location of the CloudGuard gateway in the cloud environment, the user can apply additional features as well as policies at any time.

Figure 8. Activating Advanced Security for Cloud Services



We then examined visibility from a security event perspective. We clicked on the *Logs and Monitor* option on the SmartConsole screen to arrive at the view shown in Figure 9. On the *General Overview* tab, we viewed a summary of all events that occurred over all Check Point security components within the test environment. The view includes summary statistics, allowed and prevented attacks by policy, and event timelines over a chosen timeframe, which can aid the user in assessing overall security and detect specific issues to monitor to prevent breaches.

Figure 9. General Overview of Security Events Across All CloudGuard Gateways



ESG Lab also viewed incidents across all components from a log perspective, offering the user a more detailed view of events. When we clicked on the *Logs* tab, we found that we could view logs over a given timeline or choose to filter the log view based on specific categories. Clicking on an individual log revealed details such as *Log Info* (e.g., origin and timestamp), Protection Details (e.g., attack name and severity level), and *Traffic* (e.g., source and destination). Finally, we saw that the user can take appropriate action to modify the rules associated with this log type to prevent a breach. The user can also view relevant logs via a rule definition.

Why This Matters

Effectively managing security in a multi-cloud environment means having to coordinate security policies across heterogeneous environments, each with its own management framework and security paradigm. This presents a serious challenge to IT.

Check Point CloudGuard ingests information from all CloudGuard and physical gateways, regardless of the cloud platform or geography on which they reside, and summarizes that information to provide a holistic view into an organization's security policies. The Check Point management architecture enables a user to examine the effectiveness of deployed policies in securing an organization from threats, breaches, and attacks.

ESG Lab viewed security events and policies across a heterogeneous, hybrid cloud environment, correlating events to applications and policies. The timeline view enables additional tracking and traceability while individual logs can be examined and filtered by specific categories for targeted investigation. This enables organizations to secure, monitor, and manage their heterogeneous multi-cloud environment as one holistic organism.

The Bigger Truth

Organizations are increasingly moving more of their on-premises IT infrastructure to the cloud, whether public, private, or hybrid. ESG research revealed that 81% of organizations that use infrastructure-as-a-service (IaaS) will use two or more cloud service providers.[3] Prominent challenges that organizations stated that they face as they continue to adopt the cloud into their IT infrastructure include securing controls to new workloads (34%), assessing the overall security status of cloud infrastructure (34%), and cross-cloud monitoring (34%), and protection (31%).[4]

In this modern IT environment, where organizations leverage multiple public and private clouds to provide an agile IT infrastructure, managing security policies consistently focusing on workloads and applications becomes critical. However, the nature of cloud and virtualization introduces a new security risk—traffic that moves between VMs and instances within and between the public or private cloud. CSPs' native security infrastructures are designed to protect the entire cloud infrastructure. They are not designed to secure traffic that flows between instances. This means that breaches and attacks can easily propagate between VMs and instances.

Organizations that leverage the cloud for their IT operations must secure workload and application traffic at the VM level. This requires looking at both inter-cloud security, as the perimeter of an organization's cloud environment can change at any time when VMs are moved, as well as intra-cloud security, especially when attacks can propagate between VMs.

ESG Lab verified that Check Point CloudGuard IaaS works with multiple CSPs and SDDC solution providers with integrated deployment; consistent, cross-platform policy creation and enforcement; and unified management and visibility into all deployed security resources.

If your organization has deployed or is planning to deploy any application or service into the cloud, you would do well to take a close look at Check Point CloudGuard. In ESG testing, Check Point provided automated, agile security—well suited to dynamic multi-cloud and hybrid environments—with a single, unified management platform to manage multiple, disparate cloud platforms as a single cohesive system.

[3] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

[4] Source: ESG Research Report, *The State of Cloud Security in the Enterprise*, October 2016.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.