CHECK POINT™

CloudGuard

CloudGuard Network Security for Microsoft Azure

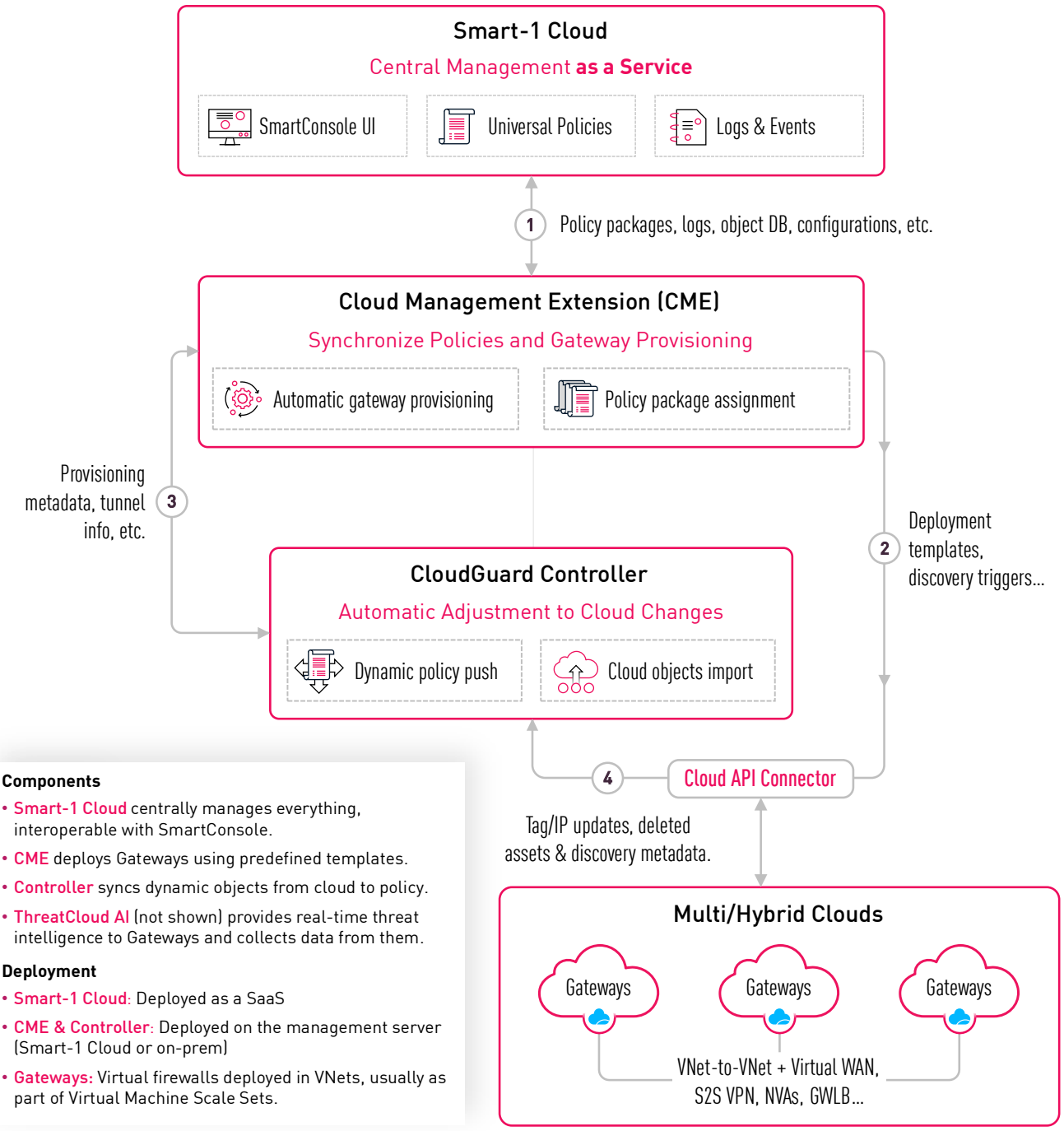
Architecture, Performance, Features, and Capabilities.

About This Document

This document contains a comprehensive technical breakdown of Check Point CloudGuard Network Security's key features, capabilities, performance, deployment models, security functions, automation and scaling mechanisms, content security, monitoring, and advanced networking features, designed to help organizations secure dynamic, cloud-native environments on Microsoft Azure with maximum flexibility and visibility.

Contents

CloudGuard Components and Architecture



Components

- Smart-1 Cloud centrally manages everything, interoperable with SmartConsole.
- CME deploys Gateways using predefined templates.
- Controller syncs dynamic objects from cloud to policy.
- ThreatCloud AI (not shown) provides real-time threat intelligence to Gateways and collects data from them.

Deployment

- Smart-1 Cloud: Deployed as a SaaS
- CME & Controller: Deployed on the management server (Smart-1 Cloud or on-prem)
- Gateways: Virtual firewalls deployed in VNets, usually as part of Virtual Machine Scale Sets.

Performance

CloudGuard Network Security R81.20 – Azure v5 Machines

Capability Tested	2 vCPU	4 vCPU	8 vCPU
Firewall only (Gbps)	7.8	11 .0	11 .0
Firewall with Intrusion Prevention (Gbps)	4.1	7.6	11 .0
Firewall with Intrusion Prevention and App Control (Gbps)	2.7	5.8	11 .0
Full Threat Prevention Suite (Gbps)	1.0	2.2	4.4
Firewall with Site-to-Site VPN (Gbps)	2.5	5.0	10.0
Remote access VPN - Concurrent users* (with firewall & IPS)	500	1,000	1,700
Remote access VPN - Concurrent users* (with complete threat prevention**)	400	750	1,500

Notes:

- **Throughput was measured** using Check Point Enterprise testing conditions.
- **Firewall with site-to-site VPN** was tested using the iPerf tool with UDP traffic and 1300-byte packet size under controlled conditions.
- **Accuracy range:** ±5%.

* At the time of testing, concurrency was limited by Azure to 512K. For the latest limitations, please refer to Azure Virtual Machine Network Throughput and Bandwidth.

** **Complete threat prevention** includes access control, threat prevention (known and zero-day), IPsec VPN, Intrusion Prevention, App Control, Content Awareness, URL Filtering, Anti-Bot, and Anti-Virus.

Deployment

- **Auto Scaling Support in Microsoft Azure:** Supports deployment in Azure VMSS, allowing CloudGuard gateways to scale automatically based on demand, ensuring high availability and cost-efficient elasticity.

- **Lifecycle-Aware Automation via Cloud Management Extension (CME):** CME automatically handles onboarding and decommissioning of gateways during VMSS scale-out and scale-in events. It provisions security configuration, installs a restrictive drop policy, executes post-provisioning scripts or hotfixes, and finalizes with complete policy installation.
- **Token-Based Gateway Registration:** Secure Internal Communication (SIC) is established using a one-time token injected into gateway templates, enabling secure, zero-touch onboarding.
- **Template-Driven Provisioning:** Templates define each gateway's configuration, including version, software blades, IPv6 support, NAT behavior, logging settings, initial policy, and custom scripts, ensuring standardized deployments across environments.
- **Automatic Hotfix and Jumbo Installation:** Gateways can be bootstrapped with pre-approved hotfixes or jumbo packages during deployment, with optional retry logic to ensure compliance.
- **Support for Azure Gateway Load Balancer and Virtual WAN:** Enables seamless insertion of CloudGuard firewalls into Azure traffic flows via GWLB or as Network Virtual Appliances (NVAs) within Azure Virtual WAN architectures.
- **Zero-Touch Hardware Onboarding:** Physical or virtual gateways can be automatically discovered by Smart-1 Cloud when connected to the network and registered using a portal-issued token, requiring no manual configuration.

Management, Visibility, and Monitoring

- **Unified Cloud-Based Management:** Smart-1 Cloud delivers object and policy central management uniformly applying to all gateways, logging, and configurations for CloudGuard deployments in Azure environments.
- **Cloud-Aware Logging and Troubleshooting:** CME logs include detailed metadata such as operation results, timestamps, data center names, and durations. Logs can be filtered by blade and exported for compliance and forensics.
- **SIEM Integration and Log Export:** Gateways can forward logs to up to three external destinations, supporting Syslog, CEF, LEEF, JSON, and Splunk formats, with support for secure TLS transmission.
- **Real-Time Topology Awareness:** The CloudGuard Controller maintains constant visibility into Azure-native objects and automatically updates changes to gateways, reducing the need for manual sync operations.
- **Identity Sharing Across Auto Scaling Gateways:** Auto-scaling gateways can receive user identity data from designated PDPs, ensuring consistent user-based policy enforcement without redundant integrations.
- **Per-Controller Performance Tuning:** Administrators can adjust scanner interval, API timeouts, and other CME settings to accommodate large Azure environments and mitigate API rate-limiting concerns.

Security

- **Flexible Blade Enablement:** Templates can activate Network Security, Threat Prevention, HTTPS Inspection, Identity Awareness, and other blades as part of the provisioning flow.
- **Autonomous Threat Prevention for Azure Virtual WAN:** CloudGuard NVAs deployed in Azure Virtual WAN can be provisioned with built-in autonomous threat prevention capabilities using the CME API.
- **VPN and Identity Support:** Full support for site-to-site VPN, NAT, and identity-aware policy enforcement powered by deep integration with Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers, and more, for consistent policy for local and remote users on Windows, macOS, Linux, Android, and Apple iOS platforms.
- **Drop-All First-Time Policy for Secure Bootstrapping:** During provisioning, gateways can apply a restrictive policy to block unintended traffic (particularly useful when inserted via GWLBs).
- **Cloud-Native Identity Awareness:** Gateways can enforce user-based policies by consuming identity data from external PDPs, allowing identity enforcement in dynamic, distributed environments.
- **Automatic NAT and Access Rule Creation for App Gateway Scenarios:** When connected behind Azure Application Gateway, CME can automatically generate NAT and Access rules based on listener tags, eliminating manual configuration efforts, with additional application control features based on 8,000+ pre-defined application *signatures* (i.e., not limited to Domain/FQDN filtering).
- **Dynamic Object-Based Policy Enforcement:** Gateways consume real-time updates from Azure, including subnets, tags, Application Security Groups (ASGs), and Private Endpoints, for use in access policies without hardcoded IPs.
- **Cross-Cloud Policy Abstractions:** Dynamic Data Center Query Objects enable creation of policy rules that combine Azure assets with objects from other cloud environments, using logical operators.

Cloud Integration & Automation

- **Native Azure Integration:** CME and CloudGuard Controller integrate directly with Azure APIs to discover and synchronize objects such as VNets, subnets, NSGs, ASGs, tags, and Private Endpoints, meaning native cloud elements turn into dynamic policy objects.
- **Multiple Onboarding Methods:** Azure environments can be connected using Service Principal credentials or managed identity, allowing secure and flexible integration.
- **Automation with APIs, CLI, and Terraform:** The full provisioning lifecycle can be controlled via RESTful APIs, the autoprov_cfg CLI utility, or through CloudGuard VNet Gateway Module Terraform, offering powerful automation options for DevOps and platform teams.
- **Asynchronous API Support with Request Tracking:** CME APIs provide async operation handling with request IDs for tracking provisioning status of templates, policies, ingress rules, and hotfix installations.

- **Template-Level Defaults and Inheritance:** Global defaults can be defined and applied automatically to all new gateway templates, streamlining policy enforcement and consistency.
- **Multi-Tenant and Multi-Subscription Governance:** Supports mapping Azure subscriptions and environments to separate management domains, enabling secure and scalable control of complex Azure estates.

Network Features

- **Built-In IPv6 Support:** IPv6 can be enabled during onboarding via template attributes, allowing dual-stack deployments across Azure environments.
- **Advanced VPN Support:** Includes support for IPSec site-to-site VPN and remote access scenarios. Configuration flexibility includes manual topology setup, external interface tagging, and NAT rule management.
- **NAT Configuration at Template Level:** Templates allow pre-configuration of NAT settings, supporting consistent deployment of hide-NAT and other rules aligned with Azure requirements.
- **Traffic Insertion via Azure** GWLB**:** Allows CloudGuard gateways to inspect East-West or North-South traffic transparently by sitting inline with Azure's native GWLB.
- **Secure Internal Communication:** All communication between gateways and Smart-1 Cloud is secured using Check Point's SIC protocol, automatically established during deployment.
- **Ingress Management for Azure Virtual WAN:** CME APIs allow full provisioning of Azure NVAs in Virtual WAN, including creation of NSG rules and Load Balancer configuration for secure and scalable ingress traffic control.
- **Policy-Aware Bootstrapping:** To ensure reliable Azure health probe responses and secure traffic handling, a restrictive default policy is applied during gateway bootstrap and automatically replaced upon full provisioning.

Read more about CloudGuard Network Security for public clouds.

Marketplace links: Firewall & Threat Prevention and CloudGuard for Azure Virtual WAN.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com

Microsoft Partner
Microsoft