CYBER TALK

NEXT GENERATION FIREWALL BUYER'S GUIDE

TABLE OF CONTENTS

The Cyber Security Landscape Is Shifting 3

Firewall Defined 4

The State of the Art: The "Next Generation Firewall"
Becomes the "Enterprise Firewall" 6

Enterprise Firewall Mandatory Requirements 6
- Security Management 6
- Threat Prevention 7
- Application Inspection and Control 7
- Identity-Based Inspection and Control 7
- Hybrid Cloud Support 8
- Scalable Performance with Services 8
- Encrypted Traffic Inspection 8

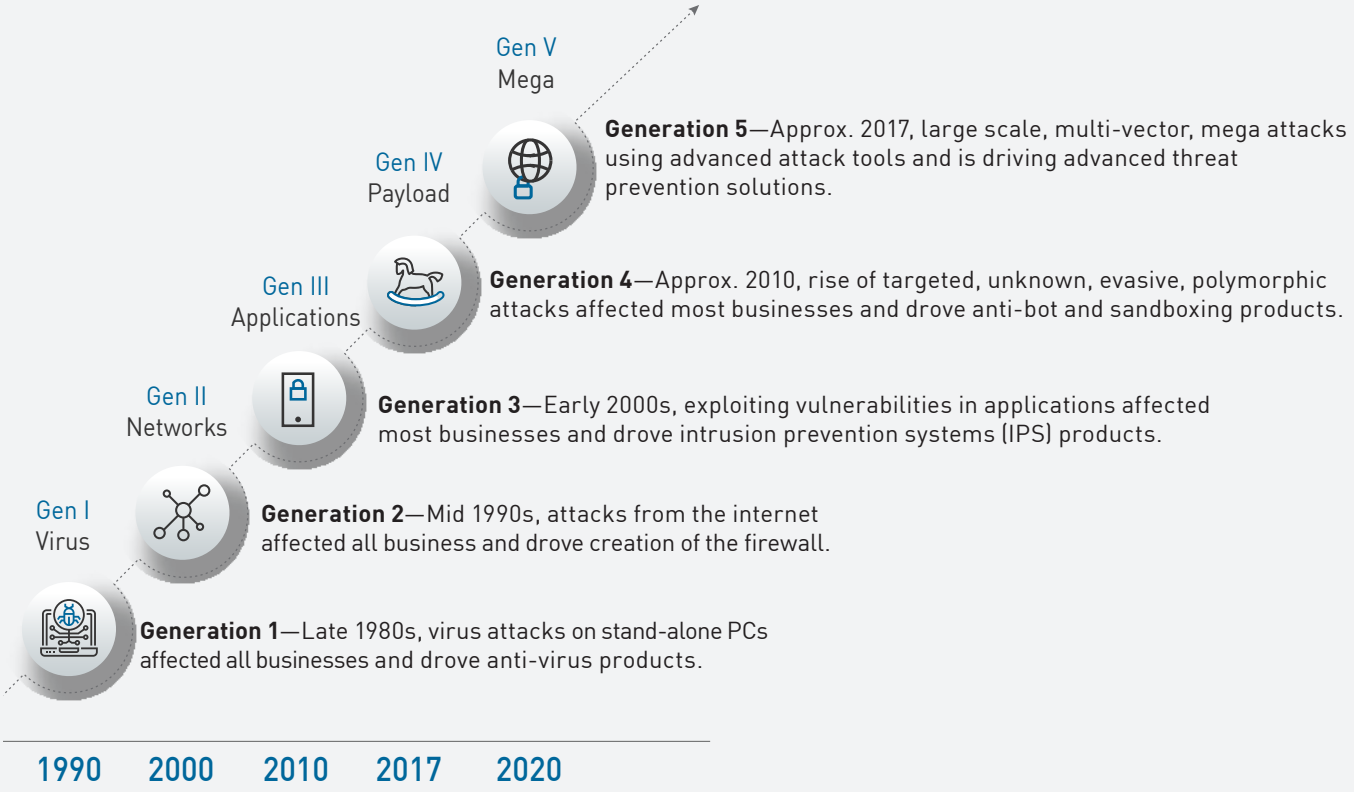
A Holistic View to Enterprise Firewalls 9

CEnterprise Firewalls:
From Next-Gen to a Security Architecture 10

Summary and Next Steps 14

The Cyber Security Landscape Is Shifting

Internet traffic volumes are doubling every 3 years. Corporate networks are growing about 25% every year.[1] At the same time, security attacks are becoming more sophisticated and have entered the 5th generation of cyber attacks. The 5th generation includes the emergence of nation state sponsored attacks and malware as a service (MaaS). Check out the graphic below to understand the different generations of cyber attacks.[2]



In 2018, we saw multiple ransomware attacks like WannaCry impact healthcare and expand the threat attack surface to IoT medical devices. In 2019, the World Economic Forum listed Cyber attacks among the top 5 threats to global economic development.

The frequency and costs of data breaches also continue to climb. The global average total cost of a data breach is $3.92 million. The highest country average is the United States at $8.19 million. The highest industry average is healthcare with a cost of $6.45 million. The time to identify and contain a breach isalmost a year at 279 days.[3] How will Next Generation Firewalls cope with 5th generation cyber attacks and traffic growth at hyper-scale?

Firewall Defined

A Firewall is a network security device that monitors incoming and outgoing network traffic. A Firewall enforces an organization's security policy by filtering network traffic. At its most basic a Firewall is essentially the boundary or barrier between two networks to identify threats in incoming traffic and blocks specific traffic, once flagged by a defined set of security rules, while allowing non-threatening traffic through.

Firewalls have existed since the late 80's and started as "packet filters," which were networks set up to examine packets transferred between computers. They've come a long way since then, but the basic principle behind why they're so important remains: It allows an organization to enforce security policies at the network level, protecting all the devices behind the firewall without having to implement these policies on every device.

TYPES OF FIREWALLS

- **Packet Filtering:** Data is blocked or permitted based on a small amount information (e.g. network address) in the header of each packet.
- **Proxy Service:** Network security system that protects while filtering messages at the application layer.
- **Stateful Inspection:** Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall:** Deep packet inspection Firewall with application-level inspection.

WHAT DO THEY DO?

A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls are able to react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

WHY DO YOU NEED THEM?

Every network needs malware defense, and advanced malware defense involves many layers of safeguards, including continuous network scans. There are many types of malware that a Firewall can protect against, including:

Virus: A virus is a malicious, downloadable file that attacks by changing other computer programs with its own code. Once it spreads those files are infected and can spread from one computer to another, and/or corrupt or destroy network data.

Worms: A worm is a standalone malware that can propagate and work independently of other files, where a virus needs a host program to spread. They can slow down computer networks by eating up bandwidth as well as the slow the efficiency of your computer to process data.

Trojan: A trojan is a backdoor program that creates an entryway for malicious users to access the computer system by using what looks like a real program, but quickly turns out to be harmful. A trojan virus can delete files, activate other malware hidden on your computer network, such as a virus and steal valuable data.

Spyware: Much like its name, spyware is a computer virus that gathers information about a person or organization without their express knowledge and may send the information gathered to a third party without the consumer's consent.

Adware: Can redirect your search requests to advertising websites and collect marketing data about you in the process so that customized advertisements will be displayed based on your search and buying history.

Ransomware: This is a type of trojan cyberware that is designed to gain money from the person or organization's computer on which it is installed by encrypting data so that it is unusable, blocking access to the user's system.

It also should be noted that Firewalls are ubiquitous in regulatory compliance regimens. They are usually mandated to protect in-scope systems from the Internet and from other parts of the organization's environment. They are configured with security policies that deny all traffic except that required for production applications, and can also apply threat prevention controls required to be in compliance.

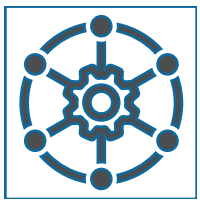
The State of the Art: The "Next Generation Firewall" Becomes the "Enterprise Firewall"

Enterprises have standardized on next generation firewalls (NGFW) because of their broad support for multiple critical security functions and application awareness. In fact, Gartner has started using the term Enterprise Firewall to describe the rapid expansion in functionality beyond NGFW.[4] Enterprise firewalls are a critical element of any security architecture, but trying to choose which one to buy is not a simple task. While firewall technology used to be fairly straightforward, these days enterprise firewalls are true security gateways which support a wide variety of functions and capabilities.

This Next Generation Firewall Guide will define the mandatory capabilities of the next-generation enterprise firewall . You can use the capabilities defined in this document to select your next Enterprise Firewall solution. Given the term "Next Generation Firewall" (NGFW) is still used by a majority of the industry we will use both "Next-Generation" and "Enterprise" firewall terms interchangeably in this document.

Enterprise Firewall Mandatory Capabilities

Cyber security experts believe that in order to defend against a rapidly expanding threat landscape, an Enterprise Firewall must support seven critical capabilities:



MANAGEMENT

Effective enterprise firewall architectures are impossible without superior management. The features on a firewall are useless if they can't be used efficiently, so the quest for a next-gen firewall starts with the management platform. Security management is not simply a matter of configuration; the complete security operational paradigm must be considered:

- Number one is ease of use, where the UI reduces the man-hours required to complete an operation. In other words, choose the best tool for the job.
- Consistent policy implementation across the security infrastructure (including but certainly not limited to the firewalls)
- Threat detection and incident response life-cycle management

- Scale (devices under management, number of administrators, and number of roles/teams involved in operations)
- Change management, workflow and segregation of duties
- Automation and orchestration: With third-party IT and Security solutions, and with data center virtualization, cloud and DevOps automation;
- Compliance and audit control validation and reporting

THREAT PREVENTION

The most significant capability added to enterprise firewalls has been the integration of robust threat prevention. Initially the focus was on integrating IPS to consolidate hardware, but modern firewalls must go far beyond that: sandboxing, anti-phishing, anti-virus and anti-bot are all possible threat prevention techniques. Many vendors use cloud-based analytics and threat intelligence in conjunction with their firewalls. These cloud platforms push threat prevention updates down to the firewalls, and receive malware indicator updates so they can be shared with others. In addition, today's enterprise firewall must integrate with third party NAC and analytics systems that dynamically push IoCs to the firewall, creating a more secure and resilient ecosystem.

APPLICATION INSPECTION AND CONTROL

As applications have become more sophisticated, firewalls have had to evolve in order to identify them, as otherwise it's impossible to write a reliable policy rule based on application. Therefore it's key to pick a firewall that has application support that is broad (as many apps as possible), deep (sub-functions within applications), intelligent (able to find the app even if evasion technology is used) and dynamic (frequent updates as applications proliferate or change).

IDENTITY-BASED INSPECTION AND CONTROL

Firewall rules based on simple IP addresses are becoming less and less relevant given the move to dynamic addressing, cloud architectures, and group-based policies. An enterprise firewall must support policies based on users or (more importantly) groups of users. The most common situation is a group-based policy that leverages the organization's primary identity store, typically Active Directory group membership. Policies such as these are tremendously beneficial as they automate typical processes (user moves/add/changes), and decrease configuration changes required on the firewall. selecting a vendor.

HYBRID CLOUD SUPPORT

It is axiomatic that cloud-based IT has joined on-premises infrastructure as viable enterprise architectures. Therefore, enterprise firewalls must extend securing strategic workloads. Obviously this means that the offering must include hardware and software based options, but that is insufficient for true enterprise support. The vendor must also embrace the automation and orchestration management models in use, scalable performance based on dynamic workloads, and consumption models that allow cost-effective deployment.

SCALABLE PERFORMANCE WITH ADVANCED SECURITY FUNCTIONS

The wide variety of services supported by next-gen firewalls require significant quantities of compute and memory resources, which can create performance bottlenecks and affect application availability and user experience. There are multiple approaches to dealing with this consideration, all of which have their advantages and drawbacks. However the key requirements are being able to easily scale performance as requirements increase, and that hardware limitations don't prevent you from deploying the latest threat prevention technologies and algorithms, or result in very different performance considerations in virtual or cloud versus hardware deployments.

ENCRYPTED TRAFFIC INSPECTION

A recent Google study showed that over 80% of the web traffic generated by the end-user Chrome browser activity was encrypted.[5] Unfortunately at the same time, malware creators have learned to leverage Certification Authority (CA) automation initiatives like encryption to create phishing sites trusted by browsers. As encrypted traffic and threats proliferate, firewalls must be capable of inspecting such traffic both to apply control policy and for threat prevention. It also must be sophisticated enough to support complex policies such as selective decryption so that certain traffic (e.g. employee's on-line banking) can be excluded from decryption to avoid regulatory or liability pitfalls.

[1] Cisco Global Cloud Index, Forecast and Methodology, 2016-2021

[2] Check Point Software Technologies, LTD

[3] 2019 Cost of a Data Breach Report, Ponemon Institute

[4] Gartner Enterprise and Network Firewall MQ, 2018, 2019

[5] Google Transparency Report on HTTPS encryption on the web; transparencyreport.google.com

A Holistic View to Enterprise Firewalls

Our cyber security experts take a holistic approach to security architecture. Each component leverages real-time threat intelligence to provide a unified view of the threat landscape, so cyber attacks can be discovered and mitigated quickly. This approach is in stark contrast to the isolated security point solutions on the market today. The evolution of firewall capabilities and applications hasn't changed this unified approach. We believe that firewall gateways fit into a broader security narrative, one in which firewalls are:

Network-Based Supporting Both On-Premise and Across Clouds

A network-based solution that provides threat prevention and segmentation on-premises and across hybrid clouds

Centralized Management

Centralized management of unified policy that supports application-based controls that are user, content and data aware

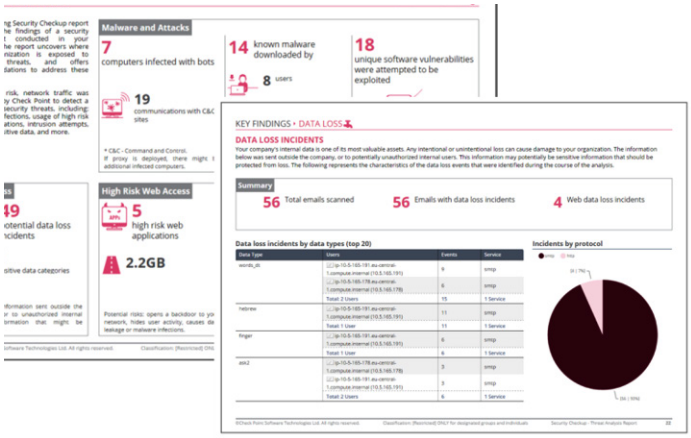
Automation

Fully automated rules and shared intelligence

Security Events and Compliance

Full visibility into security events and continuous compliance posture assessment

Virtually all organizations are struggling to operationalize security, in large part because they acquire point solutions and try to integrate them (unsuccessfully) into an inevitably complex security architecture. Therefore, we believe that organizations selecting a next-gen or enterprise firewall need to think in the context of operations at scale, instead of looking at product-specific feature lists or price/performance claims.

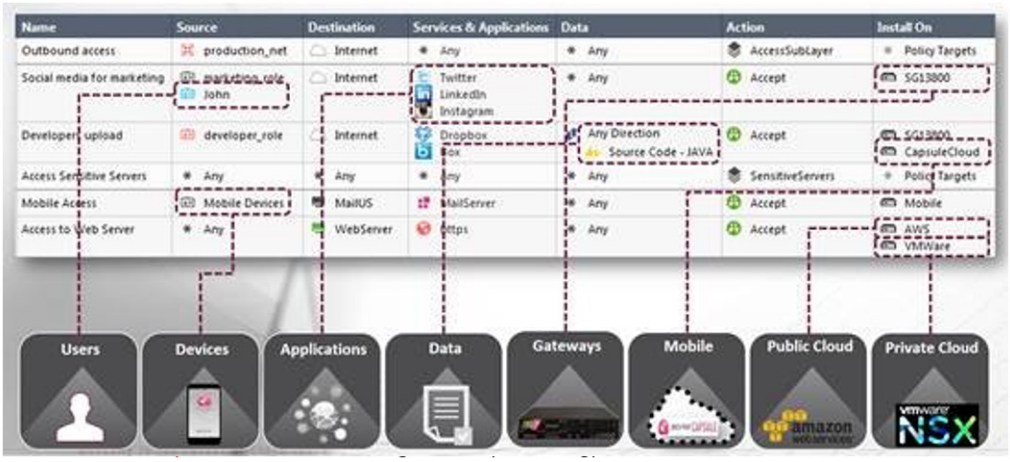


Firewalls: From Next-Gen to a Security Architecture

MANAGEMENT

Security management has always played a fundamental role in our architectures, and drives operationally viable policy management, incident response, and compliance. At the highest level, management architectures should support:

- A single policy construct across all enforcement points in the Infinity architecture
- Combined threat prevention and segmentation policies in a unified policy table across appliances, virtual and cloud
- Compliance control validation, with template support for common compliance regulations
- Consolidated event management and export via SmartEvent
- Group-based delegation of administration authority, with full workflow support
- Orchestration integration for virtual and cloud environments, including automated services insertion
- Open APIs for ecosystem integrations

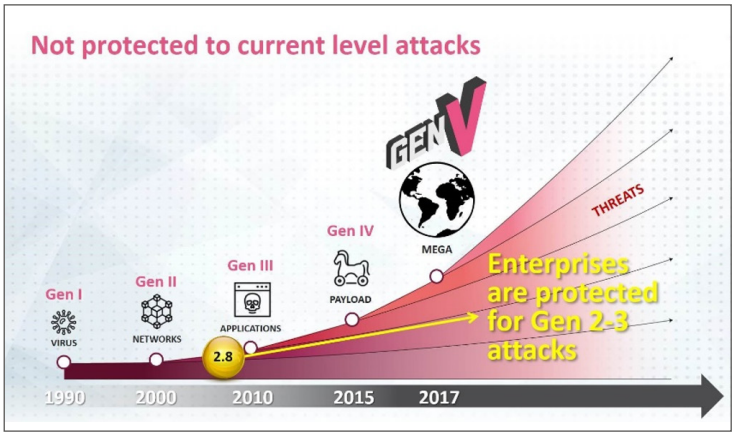


Unified Access Policy: Write once, deploy anywhere with full identity and application awareness.

Check Point Software's management has been developed based on the real-world lessons learned over 25 years of customer experience operating our firewalls and security gateways. As a result, we are able to deliver up to a 50% reduction in human investment for ongoing operations. An exhaustive description of our management capability is clearly beyond the scope of this document, however in the final analysis it's the management that makes the difference between success and failure when it comes to operationally viable network-based security.

THREAT PREVENTION

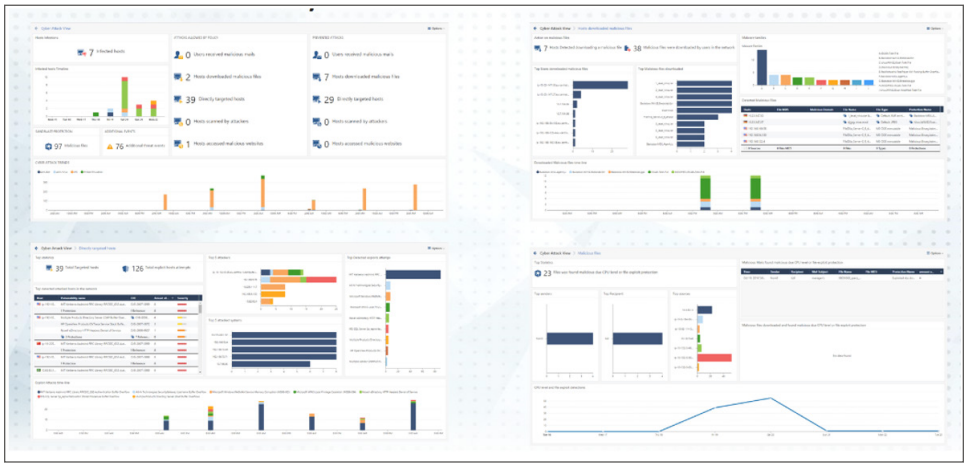
A key Check Point differentiator when compared to other firewalls is the integration of best-in-class threat prevention across the architecture. While others concede attackers will get in and are pivoting to detection and response, our focus remains on stopping attacks before they succeed. This includes tackling the latest large-scale, multi-vector GenV attacks, in addition to more conventional attacks that are still widely used.



Many enterprises still rely on outdated prevention technology.

This focus is demonstrated in capabilities that include:

- **ThreatCloud** is a Cloud-based platform that shares and delivers real-time dynamic security intelligence to the Infinity architecture, including our firewalls, security gateways, mobile and endpoints
- **New ThreatCloud AI engines** that detect malware well beyond AV and static analysis, while reducing false positives ten-fold
- **SandBlast Threat Emulation** sandboxing which blocks even zero-day attacks before they can begin their evasion techniques
- **SandBlast Threat Extraction** which delivers safe and clean files to users thus protecting them from infection. Includes web threat extraction and document sanitation for web downloads
- **Anti-phishing** which detects phishing attacks and blocks them before users can get infected
- **Anti-Ransomware** which detects and blocks ransomware attacks, and restores any files initially encrypted



Cyber Attack Dashboard: See overall threat trends with full drill down to identify and respond to high-risk attacks immediately.

APPLICATION INSPECTION AND CONTROL

Check Point's Application Control capability supports security policies to identify, allow, block or limit usage of thousands of applications, including Web and social networking, regardless of port, protocol or evasive technique used to traverse the network. It currently understands over 8,100 Web 2.0 applications with more being added continuously. Advanced user interaction features allow security administrators to alert employees in real-time about application access limitations, and query them as to whether application use is for business or personal use. This enables IT administrators to gain a better understanding of Web usage patterns, adapt policies and regulate personal usage without interrupting the flow of business.

IDENTITY-BASED INSPECTION AND CONTROL

Check Point pioneered the development of user and group based policies. Our firewalls and management integrates with Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers and with 3rd parties via a Web API. And because the management console supports these polices across our portfolio, you can limit the integration with the identity store to this one interface, and still get broad security coverage based on a single set of identity-policies. This support extends to security monitoring via the SmartEvent console. The combination of identity and application awareness is mandatory for building scalable security policies that protect the business without compromising user experience.

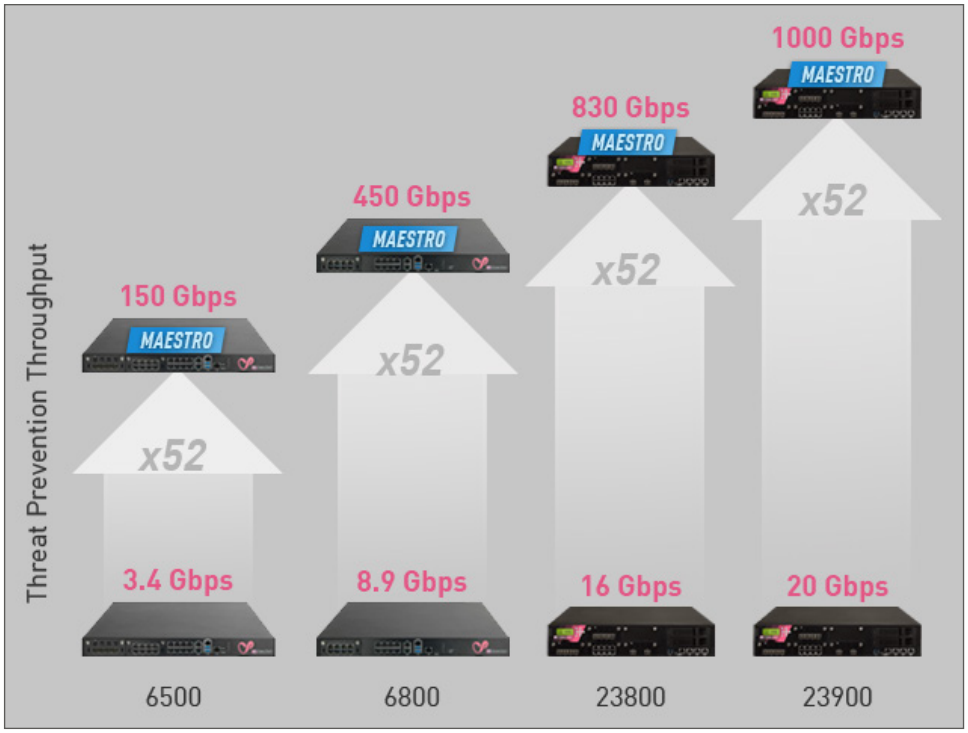
HYBRID CLOUD SUPPORT

Check Point firewalls support both virtual and cloud deployments, in addition to a complete portfolio of appliances that span remote office to data center requirements. Virtual systems support allows a single software security gateway to be segmented into multiple zones with independent resources and management. In addition to traditional vSphere, we support both NSX and Cisco ACI software-defined networking environments. For IaaS public cloud, all major vendors are supported including AWS, Azure, GCP, Oracle and Alibaba Clouds. Integration with cloud automation provides instantiation of both virtual gateways and template-based security policies without manual intervention. This enables new workloads to be secured as they are deployed, without implementation delays caused by manual security configuration.

SCALABLE PERFORMANCE WITH ADVANCED SECURITY FUNCTIONS

Check Point's portfolio offers powerful scaling options for both hardware and software-based firewalls. The Maestro Hyperscale solution brings the scale, agility and elasticity of the cloud on premise with efficient N+1 hardware clustering based on Check Point HyperSync technology. Up to 52 gateways/firewalls can be clustered to deliver up to 1,000 Gbps of throughput, while still being managed as a single entity. Start with what you need today, knowing that you can easily scale when needed without risky and complex upgrades or network re-designs.

For cloud deployments, Check Point offers CloudGuard, available in both Pay-as-you-go (PAYG) and Bring-your-own-license (BYOL) pricing models. CloudGuard supports the same services as our physical firewalls, with transparent policy management across on-premises, virtual, and cloud gateways.



Maestro Hyperscale brings agility and non-disruptive scale to the data center for business of all sizes.

ENCRYPTED TRAFFIC INSPECTION

Check Point enterprise firewall software includes SSL/TLS decryption and inspection, so that security policies can be applied to encrypted traffic. The software leverages crypto hardware acceleration built into Intel processors. Furthermore, our SecureXL technology supports crypto acceleration using Check Point hardware models available on many of the security gateways. This acceleration is critical in situations requiring high-scale inspection and policy enforcement upon HTTPS encrypted traffic. Finally enterprise firewalls must securely categorize HTTPS traffic using the Server Name Indication (SNI) extension, inspect all of the latest cipher suites and curves such as TLS 1.2 and have plans for securing TLS 1.3 traffic.

Summary and Next Steps

It should be clear from this Buyer's Guide that "next-generation firewalls" are much more than enforcement points for network traffic policies. These enterprise-class devices are really security gateways, which include Layer 7 application intelligence and multi-dimensional threat prevention. When selecting an enterprise firewall vendor, ask the follow questions while reviewing the mandatory capabilities:

- How should I weigh the importance of each capability, based on what is most important to me?
- Can I eliminate other tools and devices if I deploy enterprise firewalls broadly, lowering both capital investment and staff costs?
- What is going to be my approach to scaling performance, given the inevitable increase in traffic and sophistication required to combat the ever-evolving threat landscape?
- What IT and Security infrastructure will I need to integrate with the firewalls and their supporting components?
- Most importantly: Have I thought through the complete operational model I will use to provision, monitor, and upgrade these devices, consistent with my staff size and capabilities?

Like any technology, next-gen firewalls are only part of the solution: people, policies and procedures are essential to building and operating an effective security architecture. By combining all of these, organizations take a big step towards protecting their sensitive assets, meeting compliance requirements, and driving digital transformation.

For more information:

- https://www.checkpoint.com/products/
- https://www.checkpoint.com/products/security-gateway-appliances/
- https://www.checkpoint.com/products/next-generation-firewall/
- https://www.checkpoint.com/products/maestro-hyperscale-network-security/
- https://www.checkpoint.com/solutions/data-center-firewall/
- https://www.checkpoint.com/solutions/enterprise-firewall/
- https://www.checkpoint.com/solutions/small-medium-business/

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com