**ABSTRACT**

This document aims to explain the Check Point approach to securing access to Internet. It provides architectural references for what, why and how organizations should consider when securing access to Internet in modern and effective way.

**Contents**

Abstract ................................................................................................................................................................................................. 2  
Business drivers for secure web access .................................................................................................................................................. 2  
Understanding the cyber kill chain ..................................................................................................................................................... 3  
How to protect your business from today’s cyber threats .................................................................................................................. 4  
Check Point put to the test ................................................................................................................................................................. 5  
Check Point products and features .................................................................................................................................................. 7  
  Network protection ................................................................................................................................................................................ 7  
    Policy Enforcement ............................................................................................................................................................................. 8  
    Threat Prevention ................................................................................................................................................................................ 8  
    Data Protection .................................................................................................................................................................................. 8  
    Additional Features ............................................................................................................................................................................. 8  
    Endpoint Protection .......................................................................................................................................................................... 9  
How to integrate new solutions into existing systems ..................................................................................................................... 10  
Best practices for configuration ...................................................................................................................................................... 12  
Use cases ........................................................................................................................................................................................... 19  
Threat scenario .................................................................................................................................................................................. 21  
Conclusion ......................................................................................................................................................................................... 22

**BUSINESS DRIVERS FOR SECURE WEB ACCESS**

Today, the Internet has become an instrumental part of business operation. Being connected is essential to running a modern-day company. The evolution of web-applications has increased the complexity of our interactions with the internet; with this comes an increased security risk. Some of these include:

- **Malware threats**: Popular applications can be manipulated and weaponized against the users to propagate malware.

- **Exploits**: File-sharing programs, forums etc. are exploited by bad actors and used to propagate malware and pivot into networks.

- **Bandwidth hogging**: Applications that use a lot of bandwidth, such as streaming media, can limit the bandwidth that is available for alternate applications, which may be more crucial for business operation.
Loss of Productivity: Employees are known to spend time on social networking sites, and other applications, which can seriously decrease business productivity. As employers are not aware of the extent of the misuse of company time, they are unable to effectively track how their business is affected by such practices.

An effective web access solution should fulfill the following requirements:

- **High Security**: Protect against known and unknown threats including sophisticated multi-vector cyber-attacks. Prevent infection and mitigate post-infection risk if necessary.
- **Easy Administration**: Simple and intuitive management consoles, unified policies, single point of logging and monitoring.
- **User Interaction**: Educate employees on proper Internet usage, and highlight inappropriate use and Internet dangers thought user feedback.
- **Low TCO**: Consolidated and automated security infrastructure will result in savings on both capital expenditure and operating expenses.

**UNDERSTANDING THE CYBER KILL CHAIN**

Unfortunately, there is no way to protect the entire network with a single product. In order to build an appropriate defense and choose a proper set of solutions, it is important to understand the “Cyber kill chain”, as coined by the Lockheed Martin Corporation. The kill chain model proposes that although attacks may occur in phases, each can be disrupted through strategically established controls.

Lockheed Martin illustrate a how a cyber threat impacts a network through a cyber-attack model, whereby the attack progresses through several stages; beginning with the initial infiltration and culminating in total data capture. The progression of the attack can be viewed as follows:

- **Reconnaissance**: The intruder selects a target, researches it, and attempts to identify vulnerabilities in their network.
- **Weaponization**: A remote access malware weapon is created, such as a virus or worm, tailored to capitalize on one or more vulnerabilities.
- **Delivery**: The weapon is transmitted to the target (e.g. via e-mail attachments, websites or USB drives).
- **Exploitation**: The weapon’s program code is triggered and takes action on the target network to exploit its vulnerability.
- **Installation**: The malware weapon installs an access point (e.g. "backdoor") to be used by the intruder for persistent access to the target network.
- **Command and Control**: The intruder now has "hands on the keyboard" access, as a result of the communication and access provided by the malware weapon.
- **Actions on Objective**: The intruder is now free to successfully take action and achieve their intended goals; such as data exfiltration, data destruction, or encryption for ransom.
The cyber kill chain along with our knowledge of user behaviour has lead organisations to adopt a multi-point approach to protecting from internet-based threats and specifically threats presented to user. The following paper outlines some common best-practice architecture that aims to reduce the attack surface for user-egress traffic and limit the blast-radius of attacks should they be able to infect users.

Security professionals world-wide are aware of the threats posed by users and the intent; the following best-practice is the first line in protecting organisation where these dangers exist.

**HOW TO PROTECT YOUR BUSINESS FROM TODAY’S CYBER THREATS**

In the current cyber environment, where multiple attack vectors are far too common, it is not enough to only rely on the security gateway.

Defensive courses of action must be taken against the cyber kill chain:

- **Detect**: Determine whether an intruder has gained interest in the company network.
- **Deny**: Prevent information disclosure and unauthorized access.
- **Disrupt**: Stop or change outbound traffic (to the intruder).
- **Degrade**: Counter-attack unauthorized command and control.
- **Deceive**: Interfere with a command and control attack.
- **Contain**: Initiate network segmentation changes.

It is necessary to build a fully consolidated cyber security architecture that will provide protection against the latest and most advanced cyber-attacks at every stage, as well as future cyber threats across all networks, endpoint, cloud and mobile.

Check Point offers ultimate security architecture; designed to resolve the complexities of growing connectivity and inefficient security, and allow enterprises to integrate aligned security architecture into their current security strategy, rather than rely on point solutions.

This architecture is able to protect threats coming through networks, endpoint, cloud and mobile.
Check Point’s solution is simple, yet powerful and includes various technologies capable of stopping an attack at every stage of the kill chain. It also intends to combine protection at the network level and at the endpoint itself.

This holistic product is vital for forward thinking businesses, as Endpoint Security provides an extra layer of protection guarding beyond threats, which can be stopped at the perimeter using powerful security gateways, especially since the internet is not the only attack vector.

**CHECK POINT PUT TO THE TEST**

NSS Labs, Inc. released results for its 2019 Breach Prevention Systems (BPS) Group Test and recognized Check Point Next Generation Threat Prevention Appliance with Endpoint Security, as NSS Labs Recommended.

The NSS Labs BPS report significantly incorporates multiple solutions that enable a vendor to provide a breach prevention posture to its customers. Involving multiple solutions provides synergy between various security components that, when combined, effectively block attacks throughout the cyber kill chain. In Check Point’s case, the solution involved a myriad of technologies such as SandBlast Network, SandBlast Agent, threat extraction, anti-bot and more.
In the introduction to its analysis of the BPS Security Value Map, NSS Labs wrote: “The Breach Prevention Systems (BPS) Security Value Map (SVM) is based upon data collected over thousands of hours of testing during NSS’ most recent tests including our Next Generation Firewall (NGFW), Next Generation Intrusion Prevention Systems (NGIPS), Breach Prevention Systems (BPS), and Advanced Endpoint Protection (AEP) Group Tests”.

These results mark Check Point’s third NSS Labs Recommended, in 2019, and the 20th NSS Labs Recommended rating since the company began testing with NSS in 2010.

Download the report and Security Value Map to learn more about the NSS Labs test and how Check Point performed:

- Clear #1 ranking in breach prevention posture
- #1 in NGFW + AEP combined
- Demonstrated significant added value when using network and endpoint protections together (Infinity)
- 100% block rate
- 100% malware PREVENTION, email and web
- 100% exploit resistance
- 100% catch rate in post infection
- 98.4% Overall Security Effectiveness
- 0% False positives

View Check Point’s other awards and recognitions: https://www.checkpoint.com/about-us/awards-and-recognition/
CHECK POINT PRODUCTS AND FEATURES

Network protection

Comprehensive threat protection is available in two simple packages for Check Point appliances:

- **Next Generation Threat Prevention (NGTP):** Includes multi-layered protection from known, signature-based threats including Antivirus, Anti-Bot, IPS, App Control, URL Filtering and Identity Awareness.
- **Next Generation Threat Prevention & SandBlast™ (NGTX):** Extends NGTP multi-layered protection with zero-day attacks protection using SandBlast Threat Emulation / SandBlast Threat Extraction.
- **Threat Emulation and Treat Extraction:** Protects against unknown zero-day attacks by detecting and blocking evasion-resistant malware, while rapidly delivering safe content to users. Delivered as a SandBlast appliance or as a cloud service.

Real-time security intelligence delivered from ThreatCloud:

- Leverage the industry's first collaborative network to fight cybercrime.
- Identify over 280 million addresses analyzed for bot discovery, over 12 million malware signatures and 1 million malicious websites.
- Dynamically update attack information from a worldwide network of sensors and the industry's best malware feeds.
- Combine information on remote operator hideouts, botnet communication patterns and attack behavior to accurately identify bot outbreaks.
- Receive up-to-the-minute bot intelligence from the ThreatCloud knowledgebase, including zero-day bot attacks discovered by Check Point Threat Emulation.

Protection from malicious downloads and applications:

- Identify websites delivering malware.
- Prevent malicious files from being downloaded.
- Acceleration technologies ensure high threat prevention performance.
– Enable specific applications while blocking risky or insecure applications.

**Policy Enforcement**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Limits network access to only permitted services and allowed network segments</td>
</tr>
<tr>
<td>Identity Awareness</td>
<td>Limits access to users with the proper credentials i.e. only to those who have authorized access</td>
</tr>
<tr>
<td>Application Control</td>
<td>Limits access to approved applications and enable and educate users on safe use of the Internet</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Limits access to approved sites and enable safe use of the Internet</td>
</tr>
</tbody>
</table>

**Threat Prevention**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS</td>
<td>Enables virtual-patching of network services and applications that may be vulnerable to exploits</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Prevents known malware</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>Detects and block bot behaviors and communications with known Command and Control servers</td>
</tr>
<tr>
<td>Anti-Spam</td>
<td>Detects and block known email sources of spam</td>
</tr>
<tr>
<td>Sandboxing</td>
<td>Inspects files for malicious content and behaviors</td>
</tr>
<tr>
<td>Threat Extraction</td>
<td>Delivers safe content to users while files are analyzed in the background</td>
</tr>
</tbody>
</table>

**Data Protection**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Awareness</td>
<td>Restricts the Data Types that users can upload or download</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>Protects personal healthcare information (PHI), personally identifiable information (PII), financial data and others</td>
</tr>
</tbody>
</table>

**Additional Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Decryption</td>
<td>Performs analysis inside the encrypted traffic</td>
</tr>
<tr>
<td>User Check</td>
<td>Interacts with users in case of incidents, educate users on safe use of the Internet</td>
</tr>
<tr>
<td>Proxy</td>
<td>Supports legacy connection methods</td>
</tr>
</tbody>
</table>
## Endpoint Protection

### Endpoint Security Client + SandBlast Agent protections installed on the endpoints

<table>
<thead>
<tr>
<th>Protection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall and Compliance</td>
<td>Limits network access to only allowed services and allowed network segment building Zones</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>Detects and blocks bot behaviors and communications with known Command and Control servers</td>
</tr>
<tr>
<td>Antimalware</td>
<td>Detects and remediates all forms of malicious behavior including zero-day malware</td>
</tr>
<tr>
<td>Safe Browsing</td>
<td>Prevents access to malicious websites</td>
</tr>
<tr>
<td>Anti-Ransomware</td>
<td>Prevents cyber-extortion attacks and automatically reverses any damage done to files from the attack</td>
</tr>
<tr>
<td>Anti-Phishing</td>
<td>Detects and blocks malicious URLs sent to the device</td>
</tr>
<tr>
<td>Forensics</td>
<td>Monitors and records all endpoint events: files affected, processes launched, registry changes, network activity</td>
</tr>
<tr>
<td>Media Encryption</td>
<td>Enforces encryption of removable storage media</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>Secures all information on endpoint hard drives including user data and Operating System files</td>
</tr>
</tbody>
</table>

A combination of the Security Gateway and Endpoint protections ensures that a business is secure at every stage of the cyber kill chain and lets them maximize protection through unified management, monitoring and reporting.
HOW TO INTEGRATE NEW SOLUTIONS INTO EXISTING SYSTEMS

Check Point customers can easily enable additional features on their current Internet gateway.

<table>
<thead>
<tr>
<th>Network Security (14)</th>
<th>Management (0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control:</td>
<td></td>
</tr>
<tr>
<td>☑ Firewall</td>
<td></td>
</tr>
<tr>
<td>☑ IPSec VPN</td>
<td></td>
</tr>
<tr>
<td>☑ Policy Server</td>
<td></td>
</tr>
<tr>
<td>☑ Mobile Access</td>
<td></td>
</tr>
<tr>
<td>☑ Application Control</td>
<td></td>
</tr>
<tr>
<td>☑ URL Filtering</td>
<td></td>
</tr>
<tr>
<td>☑ Identity Awareness</td>
<td></td>
</tr>
<tr>
<td>☑ Content Awareness</td>
<td></td>
</tr>
</tbody>
</table>

SandBlast:  
☑ Threat Emulation  
☑ Threat Extraction  
Threat Prevention:  
☑ IPS  
☑ Anti-Bot  
☑ Anti-Virus  

Advanced Networking & Clustering:  
○ Dynamic Routing  
○ SecureXL  
☐ QoS  
☐ Monitoring  
Other:  
☑ Data Loss Prevention  
☐ Anti-Spam & Email Security

Gateway security features

Access policy fragment

List of applications and social network widgets are available at [AppWiki (https://appwiki.checkpoint.com/)]:

---

1 Most features include a 30 days trial period. Please note that this may affect network performance and user accessibility.
The application database is sizable (8000+ apps) and is grouped by multiple characteristics simplifying rule base creation. It also includes 250000+ social network widgets.

Typically, it is recommended to prohibit applications with critical risk for all users.

Administrators can block the Anonymizer category, which contains 200+ entries and automatically grows as the Check Point research team adds new anonymizers. This guarantees that users will be unable to bypass corporate policies, without extra effort from the administrator.

Furthermore, with a single rule administrators can block everything related to games, such as web sites, network games, social networks widgets and more. Categories are being updated automatically, so administrators need not be concerned when new games become available.
Check Point offers a consolidated security solution across both network and endpoint. This includes a unified Management Server for managing both the Network environment (gateways) and the endpoint environment (desktops / laptops / servers) from a single location.

Benefits:
- A single Management Server and a single SmartConsole assures easier administration and decreases time to deployment.
- The single Security Events Management platform provides near real time security monitoring across all layers. Having the relevant attack diagnostics and visibility enables organizations to respond quickly and remediate their systems in case of a security breach.
- Reduces hardware and licenses costs, as well as operational IT maintenance costs.

**BEST PRACTICES FOR CONFIGURATION**

1. **Activate security blades on the Internet gateway in the SmartConsole**
   
   Use Access control (Application Control, URL Filtering, Identity Awareness, Content Awareness) as well as Threat Prevention and Sandblast (IPS, Anti-Bot, Anti-Virus, Threat Emulation Threat Extraction).

2. **Build Network Security policy**
   - Block abuse/high risk applications.
– Block the download of executables (i.e. from untrusted sites).

– Inform users about block reason using the Blocked Message (User Check).

– Control user uploads to avoid confidential information leakage.

– Create rules according to user roles (groups).

– Educate users on proper Internet usage.

– In addition to outgoing web access, create other network access rules including Internet/DMZ, LAN and Data Center – all in the same console.
3. Build a Threat Prevention policy
   - Create rules for different scopes (the data center may require extra protections).
   - Configure security profiles.
   - Configure Threat Emulation and Threat Extraction.

4. Activate Outgoing SSL Inspection to control encrypted traffic
– Choose relevant gateways.

– Create exceptions if needed (for example, ‘do not inspect financial services to comply with legislation/privacy requirements’).

5. Configure Endpoint Security

– Access rules including NAC integration with 3rd party solutions.

– Threat Prevention blades.
### Add additional components if needed.

- **Full Disk Encryption**
  - Default Full Disk Encryption settings for the entire organization
  - **Entire Organization**
    - Do not encrypt local hard disks - Encrypt only minimum volumes required
    - Authenticate user before OS loads (Pre-boot)
    - Automatically learn and authenticate logged in users
    - Disable lock screen authentication (OneCheck)

- **Media Encryption & Port Protection**
  - Default Media Encryption settings for the entire organization
  - **Entire Organization**
    - Allow reading any data from storage devices
    - Encrypt business-related data written to storage devices
    - Allow connecting essential devices (keyboard, mouse and network adapters)
    - Advanced
      - Allow offline access to encrypted storage devices (upon creation)
      - Require storage devices to be scanned and authorized, allow self-...
7. Deploy Endpoint Security clients

8. Monitor and fine-tune policies
**USE CASES**

**Common Internet access cases**

1. **Direct connection**
   - Default route through the Internet perimeter gateway
   - Suitable for endpoints and servers even if their applications do not support proxy
   - All security features including Threat Emulation and Threat Extraction

2. **Additional NGFW/NGTP/NGTX Internet gateway**
   - Direct connection (as #1)
   - All security features
   - Security policy is centrally managed (the same or slightly differ from the HQ)
   - Sandboxing (TE/TEX) is implemented via Sandblast in HQ

3. **Through HQ via VPN**
   - Remote Office gateway uses the Internet only to establish Site-to-Site VPN to the HQ
   - All traffic including the Internet is routed through the VPN to the HQ
– Outgoing Web Access policy is enforced by the HQ gateway
– All security features

4 HQ Security Gateway as a proxy
– Browsers of Remote Office users are configured to use the HQ security gateway as a proxy
– The same policies and security features are enforced as for ‘direct connection’ (point 1)

5 3rd party proxy
– Legacy 3rd party proxy can be used for the transition period
– Application Control, URL Filtering and Identity Awareness Security Gateways can use X-Forward-For HTTP header, which is added by the proxy server, to see identities of users behind the 3rd party proxy IP address and apply individual policies to users.
THREAT SCENARIO

Consider the following triple attack: Emotet + Trikbot + Ryuk.

The first stage of the attack starts with a weaponized Microsoft Office document attached to a phishing email. This file contains a malicious, macro-based code. Once the user opens the document, the malicious file will run cmd and execute a PowerShell command. The PowerShell command attempts to download the Emotet payload.

When the Emotet payload executes, it looks to continue its malicious activity by further infecting and gathering information on the affected machine. It initiates the download and execution of the Trickbot Trojan by communicating with and downloading from a pre-configured and remote malicious host.

TrickBot is a modular Trojan. Once the machine is infected with TrickBot, it begins to steal sensitive information. Meanwhile, the attackers check to see if the target machine is part of an industry they are looking to target. If it is, they download the Ryuk ransomware payload and use the admin credentials, stolen using TrickBot, to perform lateral movement, and reach the assets they intend to infect.

The ransomware dropper Ryuk.exe checks the system architecture and drops its main payload accordingly. The dropper also stops multiple services and processes related to antimalware products by using the netstop and taskkill commands. The main Ryuk payload injects itself into multiple processes and achieves persistence using the registry.

To ensure the victim is forced to pay to decrypt the valuable files, Ryuk changes the configuration of and deletes the Virtual Shadow Copy. Ryuk then encrypts files on the disk, changes the extension to .RYK, and drops a ransom note RyukReadMe.txt created with notepad.exe in every processed folder.

Looking to the MITRE ATT&CK Enterprise matrix, which provide a list of methods and techniques used by hackers, it can be seen that Check Point can detect and prevent such an attack at almost every stage:
MITRE ATT&CK matrix: Technics used by Emotet + Trikbot

Besides stopping the attack, it is also possible to generate a comprehensive report at the endpoint.

Ryuk malicious activity in the MITRE ATT&CK Matrix format.

CONCLUSION

There are many options to secure Internet web access: from very simple solutions to utilizing extremely complicated and expensive technology. The multi-vendor approach requires multiple solutions, such as gateways to protect the Perimeter, proxy/web isolation for outgoing Internet access, multiple endpoint protections and more. Simply deploying a sole protection across these varied environs is challenging, i.e. it is difficult to keep policies consistent when using proxy and for direct connections.

Moreover, multi-vendor solutions typically require more effort to be put into place because the administrator will have to coordinate the integration of disparate (and potentially incompatible) systems. Procurement efforts are also higher as negotiations of multiple contracts will need to take place, and not every contract will be the same length.
and/or will be renewed at the same time. The management and monitoring of consoles, product upgrades, staff training and more, will require significant time and labor input, as well as a high monetary investment.

<table>
<thead>
<tr>
<th></th>
<th>Network</th>
<th>Endpoint</th>
<th>Operations</th>
</tr>
</thead>
</table>
| Multi-vendor| Perimeter firewall Proxy / web isolation     | Antivirus + antimalware | 3 management servers  
|             |                                              |          | 3 consoles  
|             |                                              |          | Inconsistent policies  
|             |                                              |          | Multiple service contracts |
| Check Point | Firewall NGTX²                               | Endpoint Security³ | 1 management server  
|             |                                              |          | Unified consoles and policies  
|             |                                              |          | Single point of support |

Check Point delivers an effective security architecture by uniquely combining three key elements:

- One security platform: leverages unified threat intelligence and open interfaces.
- Preemptive threat prevention: blocks the most sophisticated attacks before they happen.
- Consolidated system of single management, modular policy management and integrated threat visibility.

With 64 different security engines, Check Point protects against known and unknown threats across all networks, endpoints, cloud, mobile, and IoT. In addition, Check Point SandBlast Zero-Day Protection provides advanced protection against zero-day malware with technologies such as threat emulation (sandboxing), threat extraction (safe content delivery), anti-phishing, endpoint forensics, and anti-ransomware.

![Engines for Known Threats](image1)

![Engines for Unknown Threats](image2)

See if your business is vulnerable to newly deployed attacks: [Instant Security Assessment](#)

² Includes multi-layered protection from known threats AND zero-day attacks using SandBlast Threat Emulation, SandBlast Threat Extraction, Antivirus, Anti-bot, IPS, App Control, URL Filtering and Identity Awareness

³ Endpoint Threat Emulation and Extraction, Zero-Phishing, Anti-Ransomware, Endpoint Anti-Bot, Anti-Exploit, Behavioral Guard, Endpoint Anti-Virus, Forensic collection and automated reports; Endpoint Firewall, Application Control, Port Protection, Endpoint Compliance, Remote Access VPN; Full Disk Encryption (FDE), Media Encryption (ME)
Or request a free Security Check Up.