SecureIQlab®

Report

Next-Generation Firewall Command and Control Prevention Comparative Report

Test Period: February to March 2025

Last Revision: 11th April, 2025

Commissioned by: Palo Alto Networks

©SecureIQLab LLC, 2025. All rights reserved

1. Executive Summary

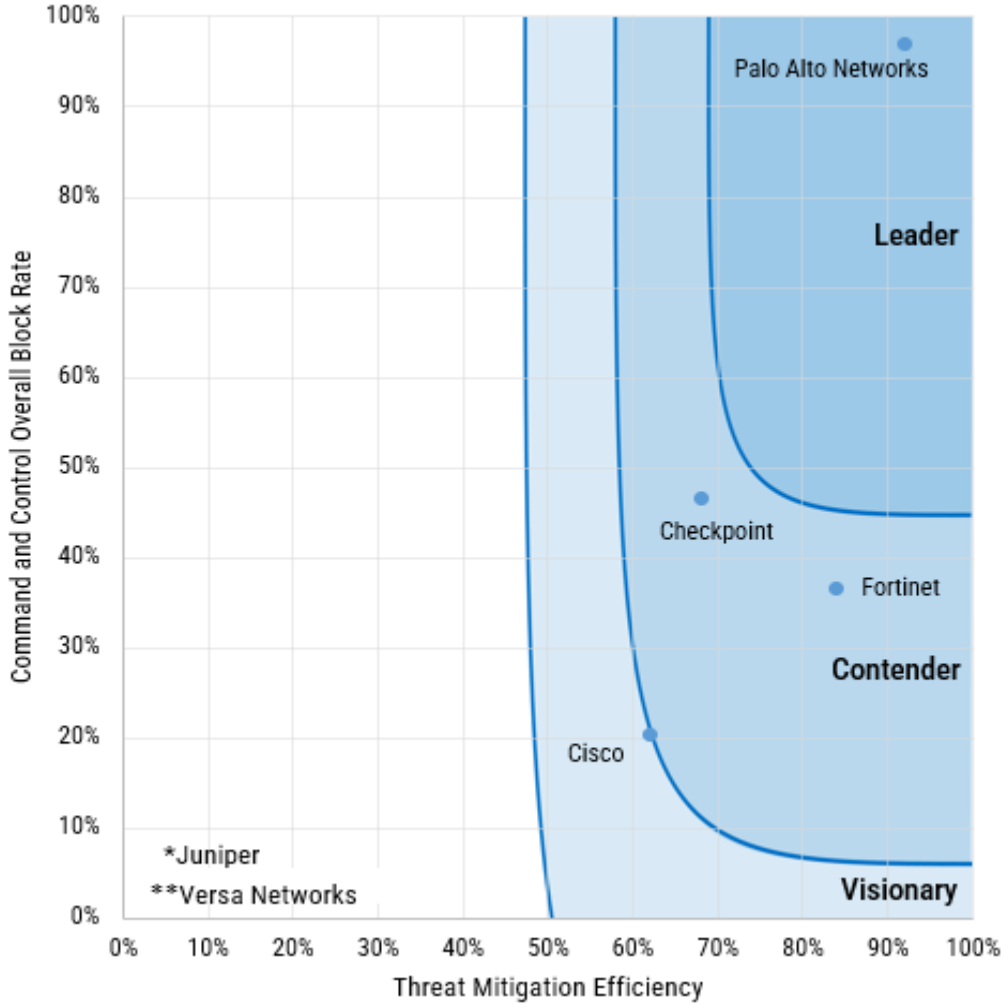

Figure 1. Overall Block Rate vs Threat Mitigation Efficiency

SecureIQLab tested the ability of next-generation firewalls to block the command-and-control capabilities using two different attack suites, Cobalt Strike and Empire, and validated their Threat Mitigation Efficiency. Six On-Prem firewalls were tested: The Checkpoint Quantum 6200P, Cisco Firepower 1140, FortiGate 600F, Palo Alto Networks PA-460, Juniper SRX340*and Versa Networks CSG2500**.

Note:

- *The Juniper SRX 340* test results were not published due to significant product issues encountered during testing, despite adhering to their best practice guide for setup, deployment, and configuration. These issues manifested as unexpected blocking behavior, widespread timeouts, and ultimately resulting in the product entering a non-functional state and preventing any meaningful evaluation.*
- *Versa Networks CSG2500** test results were not published due to licensing-related issues encountered during testing. Attempts to resolve these issues to ensure product quality and compliance before any testing result publication were not successful.*

The test measured the block rate of the firewalls against Cobalt Strike and Empire in seven attack scenarios. The overall command and control (C2) block rate are the average of the overall block rate for Cobalt Strike and Empire attack scenarios, and these are found in Table 1. The Threat Mitigation Efficiency, Table 1, was evaluated to measure the operational efficiency of the products under test to identify and respond to the Cobalt Strike and Empire campaigns delivered during testing. Figure 1 provides a comparative visual representation of the C2 Overall Block Rate and Threat Mitigation Efficiency.

SecureIQLab concludes that Palo Alto Networks provides superior command and control protection and ease of use.

* SecureIQLab was unable to complete the testing of Juniper SRX340 Firewall. Please see note above for details.
** SecureIQLab was unable to complete the testing of Versa Network CSG2500 Firewall. Please see note above for details

©SecureIQLab LLC, 2025. All rights reserved

Overall	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
C2 Overall Block Rate	46.59%	20.34%	36.56%	97.02%
Cobalt Strike Overall Block Rate	39.33%	11.31%	36.29%	94.04%
Empire Overall Block Rate	53.85%	29.37%	36.83%	100.00%
Threat Mitigation Efficiency	68.00%	62.00%	84.00%	92.00%

Table 1. Cobalt Strike Block Rate Results

2. Introduction

Command-and-control[1] (C2) attacks include implants that report back to the attacker's server and thereafter issue commands to a compromised machine. A compromised machine will carry out the commands issued by the attacker's server and may install additional software. This can be leveraged into complete control of the compromised machine and into pivoting to attack other hosts in the environment.

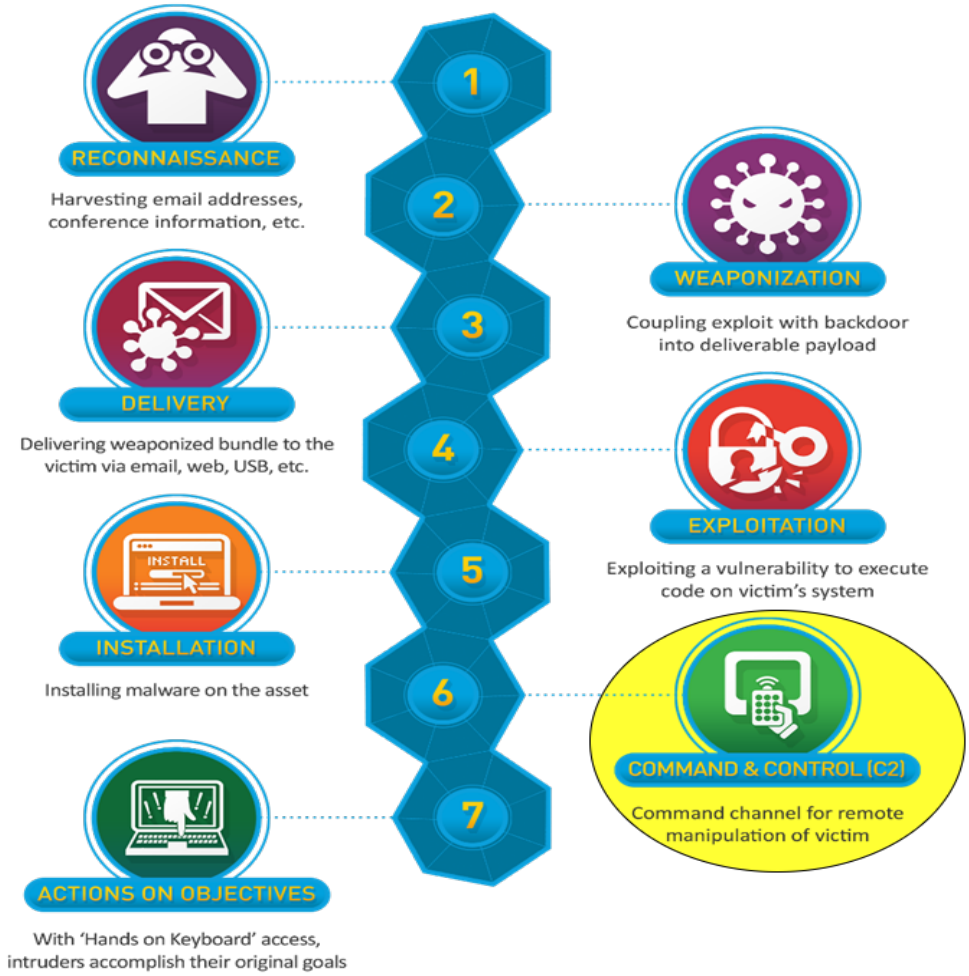

Figure 2. Position of Command and Control in the Lockheed Martin Cyber Kill Chain®

[1] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

©SecureIQLab LLC, 2025. All rights reserved

2.1. Cobalt Strike

Cobalt Strike is a commercial command-and-control attack suite now owned by Fortra (formerly HelpSystems). Their website states Raphael Mudge created the Cobalt Strike command-and-control framework in 2012 to assist red teams in testing enterprise defense postures against post-exploitation activity.

The Cobalt Strike GUI makes it very easy to use by even unsophisticated hackers. Access to this commercial tool has historically been highly restricted; however, cracked versions have recently become available. As a result, Cobalt Strike has become a favorite post-exploitation framework for threat actors[2] and become a force that security providers must reckon with.

Attacks using Cobalt Strike can change many settings. Together, a set of these settings is called a malleable C2 profile. These profiles are malleable because so many variables can be changed. In the wild, there has been a proliferation of publicly available malleable C2 profiles that can be used to evade detection by security products. Researchers have also created and shared tools to easily generate new randomized Cobalt Strike profiles.

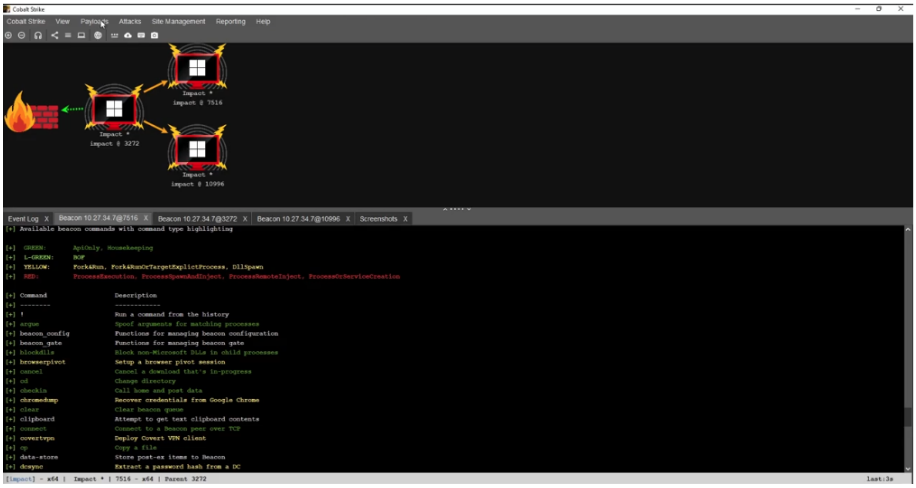

Figure 3. Official Screenshot of Cobalt Strike GUI from https://www.cobaltstrike.com/resources/videos/cobalt-strike-in-5-minutes

2.2. Empire

PowerShell Empire, an open-source post-exploitation framework initially developed by Will Schroeder and Justin Warner, Matt Nelson, and others[3], and later forked as Empire by BC Security, provides a flexible and modular command-and-control (C2) platform that leverages PowerShell for stealthy operations.

Unlike commercial tools like Cobalt Strike, PowerShell Empire has been publicly available on Github, making it accessible to both security professionals and malicious actors. Its ease of use and powerful capabilities have made it a popular choice among threat actors for post-exploitation activities.

Empire allows attackers to modify various configurations to adapt to different security environments. These customizable settings are similar to Cobalt Strike's malleable C2 profiles, enable adversaries to evade detection by security solutions.

[2] https://go.recordedfuture.com/hubfs/reports/cta-2025-0228.pdf
[3] https://cyble.com/blog/adversaries-actively-utilizing-powershell-empire

©SecureIQLab LLC, 2025. All rights reserved

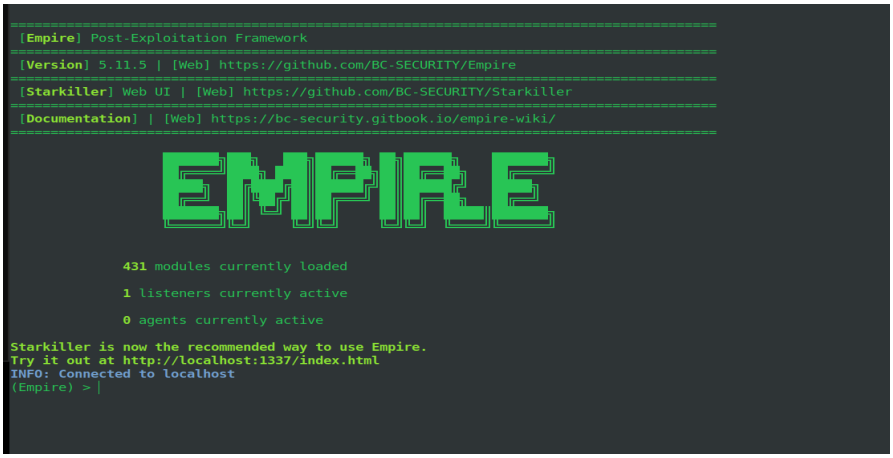

Figure 4. Screenshot of Empire

To provide protection against command-and-control network activity between a C2 "server" and "agents/implants", network security products typically utilize traditional IPS signatures to match against unique static strings and/or patterns in network streams specific to C2 framework communication. However, these signatures can be easily evaded with malleable profiles that can create endless combinations of arbitrary content that may have been used as "fingerprints" in the creation of static IPS signatures. To combat this, in addition to traditional IPS signatures, Palo Alto Networks utilizes its Advanced Threat Prevention service to detect and block these variations to command-and-control traffic in real-time.

Palo Alto Networks commissioned this test to measure the value of their Advanced Threat Prevention capability compared to other leading on-premises and cloud security solutions in protecting customers against popular C2 framework communication, particularly Cobalt Strike (v4.10) and Empire (v5.9.5). This report is intended to indicate protection not only empirical security efficacy numbers (i.e., "block rates") but also to evaluate the relative resiliency of the protection provided by each product when modifications are made to base malleable profiles to evade detection.

3. Test Environment

Cobalt Strike version 4.10 and Empire version 5.9.5 was used in this test, with Kali Linux as the platform. On the attack side, the Cobalt Strike team server and Empire were hosted on the public Internet.

Table 2 lists the on-prem products and firmware/software versions that were evaluated.

Vendors	Products	Version
Checkpoint	Quantum 6200P	SW Version R81.20 - HF 92
Cisco	Firepower 1140	software 7.6.0-113
Fortinet	FortiGate 600F	v7.6.2 build3462
Palo Alto	PA-460	v11.2.4-h2
Versa Networks	CSG2500	v22.1.4
Juniper	SRX340	24.4R1.9

Table 2. List of Vendors, Products, and Versions Evaluated

Prior to testing, all products' firmware was updated, and dynamic security content updates were configured/allowed to happen. Content that updated automatically, for example IPS signatures, continued to be updated during the test. Figure 5 provides a simplified diagram of the on-premises testing environment.

©SecureIQLab LLC, 2025. All rights reserved

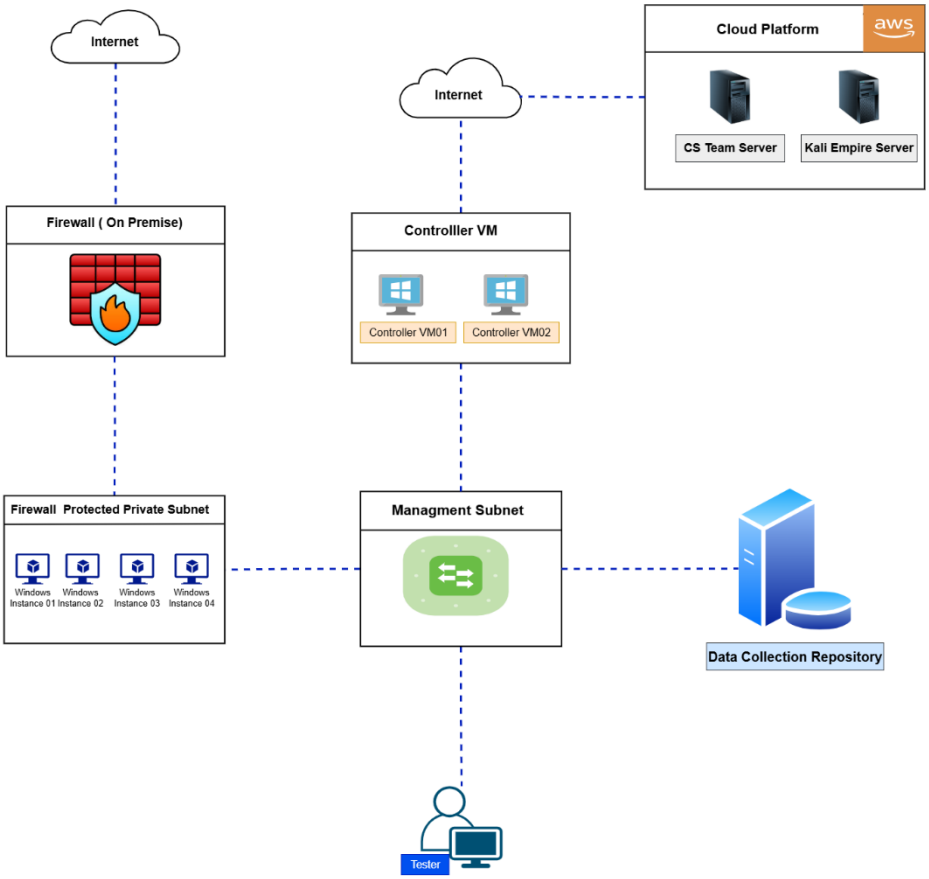

Figure 5. Command-and-Control On-Premises Testing Environment

High-security policies suitable for deployment in a typical enterprise environment were created for all available and applicable security functionality (e.g., DNS Security, Antivirus/Sandboxing, URL Filtering, Application Control, IPS/Vulnerability Protection, SSL/decryption). Because there were subtle differences in the product settings, URL Filtering, and Application Control policies were matched up as closely as possible across all products. These policies were specifically tailored to protect against command-and-control activity, and the configuration process was documented for each product.

Publicly available best-practice documentation and admin guides for each product were referred to confirm that all products were at least minimally configured to best-practice specifications for all security features/modules ("best-practice or better"). Because product performance is generally highly configuration-dependent, it is possible that results might have differed if different settings had been used for any of the products tested[4]. True positive testing was then performed to confirm the functionality of all configured security policies. This process ensured that each product's core capabilities effectively mitigated the targeted threats.

False positive testing was also performed as needed to conservatively tune the policies to what would be appropriate/acceptable for a typical enterprise; for example, the ability to browse to and render general popular websites as well as websites closely mirroring those used in various Cobalt Strike malleable profiles (for example, Amazon, Bing, CNN, MSNBC, Wikipedia) through the product as configured.

4. Test Procedure

The overall command-and-control test procedure included seven main categories of attack scenarios executed using the Cobalt Strike attack framework and Empire. Each of the seven categories examines a major aspect of the respective product's capabilities in a specific real-world scenario. HTTP over TCP port 80 was used for command-and-control communication unless otherwise noted. For each profile tested, an implant/beacon was generated and delivered to the "victims" for execution out-of-band prior to testing. In other words, only the capability of the product to intervene and protect against callback network activity was tested, not the ability to block the initial delivery of the beacon itself. Exploitation was assumed to have already taken place as the implants/agents were delivered out-

©SecureIQLab LLC, 2025. All rights reserved

of-band and then detonated, and the ability to provide subsequent protection against data exfiltration and malware delivery via an HTTP C2 channel with both Cobalt Strike and Empire was then assessed for each product.

The types of attacks we evaluated are:

1. **Basic Attack Scenario:** This test evaluated the product's basic protection against the most commonly available public attack profiles attempting data exfiltration and malware delivery via HTTP. Each scenario had a multitude of profiles that were evaluated as part of the Cobalt Strike attack framework and Empire.
2. **Random Attack Scenario:** This test was performed to evaluate the protection when the data transform language utilized in Cobalt Strike is leveraged to generate "randomized" attack scenarios using tools that are part of the Cobalt Strike arsenal of researchers and the public. This randomization increases the probability that the traditional threat defenses of the firewall might be rendered ineffective against data exfiltration and malware delivery.
3. **Custom Random Attack Scenario:** This testing was performed to assess the ability of each product to provide protection when publicly available tools are customized (e.g., replace default wordlists/dictionaries) and used to generate "randomized" profiles, further increasing the probability that traditional static signatures are rendered ineffective.
4. **Custom Attack Scenario:** This was the first of the confirmation tests, which used a smaller profile set. This test was performed using purposely chosen and modified attacks from the Basic and Random attack scenarios. Modifications were made to the different variables that are supported for customization. The variables were modified using data transform language.
5. **Nonstandard ports-based Attack Scenario:** The purpose of this testing was to confirm if the next-generation firewalls can continue to provide protection when attacks use HTTP over a nonstandard port.
6. **Modified Base Attack Scenario:** The purpose of this testing was to confirm whether the next-generation firewalls continue to provide the same level of protection when each of the base profile sets are modified as follows:
    - CHANGE GET to POST: HTTP "GET" verbs in profiles are changed to "POST"
    - CHANGE HOST HEADER: HTTP host headers in profiles are changed to use IP address rather than hostname
    - COMBINE 'CHANGE GET to POST' AND 'CHANGE HOST HEADER': HTTP "GET" verbs in profiles are changed to "POST" HTTP host headers in profiles are changed to use IP address rather than hostname
7. **Testing with additional Policy Scenario:** The purpose of this testing is to test multiple policies as required to adequately determine the efficacy of each product (e.g., a URLF policy that allows 'unrated/uncategorized' URLs and one that does not). All the above scenarios were tested with the policy that allows "unrated/uncategorized" URLs as well as the additional policy that blocks "unrated/uncategorized" URLs.

The tests did not have equal sample sizes. The Custom Attack Scenario and Nonstandard Ports-based Attack Scenario were verification exercises. Thus, they did not require many profiles. As a result, the vast majority of profiles were run in the Basic Attack Scenario, Random Attack Scenario, Modified Base Attack Scenario and Testing with additional Policies.

5. Scoring Criteria

Products under test earned blocking credit in four ways: First, by stopping the Cobalt Strike and Empire attack at the implant/agent communication stage, second, by blocking the attack at the exfiltration of 'whoami/all' command stage, third, by blocking the attack at the exfiltration of one or more screenshots stage, and fourth, blocking the malware dropped to victim via the established C2 channel.

Check-In: The communication stage is when the compromised machine checks in with the Cobalt Strike's Team Server and the Empire's Listener, and command-and-control is established. Blocking credit at the communication stage was earned by preventing the command-and-control link from establishing.
Reconnaissance: The exfiltration of Command Execution output ('whoami/all' command) stage is where an attacker gathers detailed information about the compromised system's user context and privileges.
Exfiltration: The exfiltration of 'screenshot' stage where an attacker attempts to capture sensitive information displayed on the victim's screen, such as credentials, emails, or restricted documents, without triggering file access logs. Blocking credit at this exfiltration stage was earned by blocking the output of one or more screenshots.
Delivery: The download stage is when the compromised machine sends out data or downloads malware, as directed in the communication stage. Blocking credit at the download stage was earned by preventing the download of malware.

©SecureIQLab LLC, 2025. All rights reserved

Scoring is weighted as follows: 5% for Check-in, 15% for Reconnaissance, 40% for Screenshot Exfiltration, and 40% for Malware Delivery. For instance, if a product achieves 80% overall block rate at the Check-in stage, its contribution to the overall score would be 0.05 × 80%= 4%. Similarly, if it blocks 90% at the Screenshot Exfiltration stage, the contribution to the overall score would be 0.4 × 90% = 36%.

6. Overall Block Rates for Cobalt Strike and Empire

Overall Block Rates for Cobalt Strike and Empire profiles is intended to give a general overview of the capability of products under test to withstand, absorb, and mitigate different variations of Cobalt Strike and Empire profiles generated via different tools and third party-maintained profiles. The higher the Overall Block Rates for Cobalt Strike and Empire profiles, the better. The Overall Block Rates for Cobalt Strike and Empire profiles are derived from the results from the 1680 Cobalt Strike profiles and 1208 Empire profiles evaluated respectively. The Overall Block Rate is computed by dividing the total number of attacks blocked by all the attacks launched for each framework.

$$Overall\ Block\ Rate = \left(\frac{blocked\ attacks}{total\ attacks} \right) \times 100\%$$

Equation 1. The Formula for Computation of Overall Block Rate for Cobalt Strike and for Empire

Cobalt Strike	Vendors and Products			
Command-and Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Overall Block Rate	39.33%	11.31%	36.29%	94.04%
Check-In	7.56%	4.82%	32.74%	84.52%
Reconnaissance	40.77%	6.67%	36.73%	94.94%
Exfiltration	42.80%	16.96%	38.21%	95.18%
Delivery	39.29%	8.21%	34.64%	93.75%

Table 3. Cobalt Strike Overall Block Rate Results by Block Stage

Empire	Vendors and Products			
Command-and Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Overall Block Rate	53.85%	29.37%	36.83%	100.00%
Check-In	3.81%	2.65%	4.39%	100.00%
Reconnaissance	66.56%	46.11%	54.22%	100.00%
Exfiltration	66.97%	47.27%	55.71%	100.00%
Delivery	42.22%	8.53%	15.48%	100.00%

Table 4. Empire Overall Block Rate Results by Block Stage

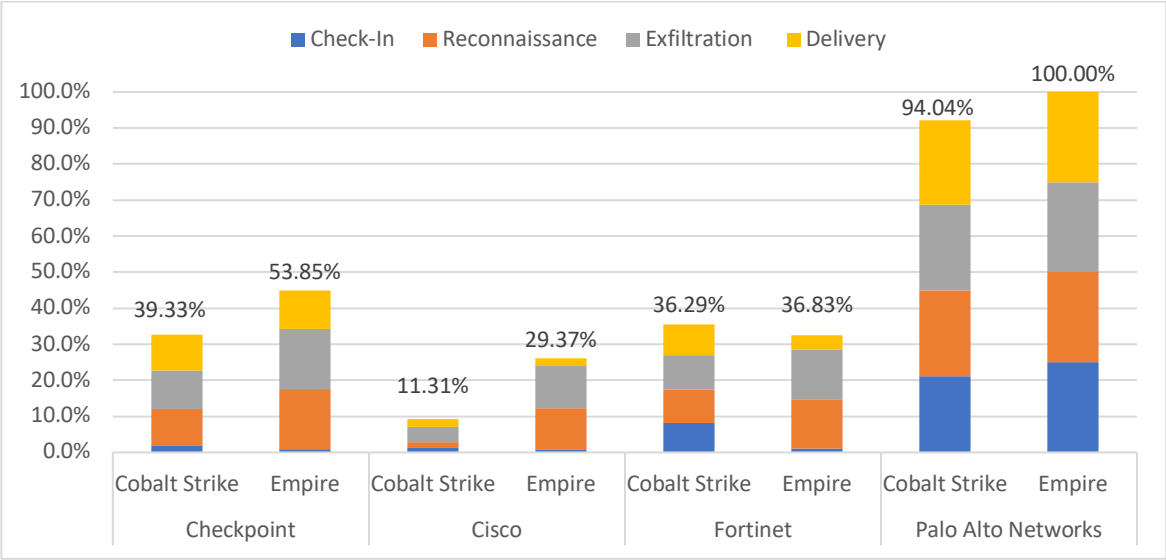

Figure 6. Overall Block Rate by Attack Stage for Cobalt Strike and Empire

©SecureIQLab LLC, 2025. All rights reserved

Overall Block Rate is only a general overview because not all attacks are created equal: The composition of the various attacks targeting a given network may vary from the composition of the profiles in this test. Figure 6 provides an overview of the results. This figure illustrates the contribution of each of the four attack stages to the overall score—5% for the first stage, 15% for the second, 40% for the third, and 40% for the fourth—highlighting the relative post-compromise effectiveness of the firewalls in blocking Empire and Cobalt Strike attacks.

7. Detailed Comparative Analysis

This section breaks down results by category, providing a more detailed analysis of the tested products' performance than the Overall Block Rate.

The summary of key results below shows how the tested products fared during our validation across seven main categories of attack scenarios using the Cobalt Strike attack framework and Empire. This validation was performed alongside false positive validation during the entire test period. In all cases, results are reported using 5% for the first stage, 15% for the second, 40% for the third, and 40% for the fourth weighted percentages of attacks blocked in each stage.

$$Percentage\ of\ attacks\ blocked = \left(\frac{blocked\ attacks}{total\ attacks}\right) \times 100\%$$

Equation 2. The Formula for Computation of Percentage of Attacks Blocked

Attack scenarios are broken down into seven categories: The Basic Attack Scenario, the Random Attack Scenario, the Custom Attack Scenario, the Custom Random Attack Scenario, the Nonstandard Ports Attack Scenario, Modified Base Attack Scenario, and the Testing with additional Policy Scenario. Each is discussed further below.

Cobalt Strike	Vendors and Products			
Command-and Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
1. Basic Attack Scenario	46.86%	18.63%	74.69%	99.71%
Enterprise Attack Profile Set 1	11.40%	4.80%	26.20%	100.00%
Enterprise Attack Profile Set 2	29.06%	16.09%	79.69%	100.00%
Enterprise Attack Profile Set 3	69.42%	31.28%	85.00%	99.53%
Enterprise Attack Profile Set 4	53.33%	17.07%	82.80%	99.60%
2. Random Attack Scenario	42.29%	16.54%	56.50%	92.38%
Random Attack Test Set 1	20.36%	20.00%	82.32%	99.82%
Random Attack Test Set 2	69.67%	13.33%	0.00%	69.83%
Random Attack Test Set 3	70.47%	27.03%	72.97%	99.84%
Random Attack Test Set 4	5.33%	5.33%	71.33%	100.00%
3. Custom Random Attack Scenario	30.21%	6.08%	25.54%	87.49%
Custom Random Attack Test Set 1	20.36%	5.71%	42.54%	99.69%
Custom Random Attack Test Set 2	4.00%	4.00%	35.67%	85.83%
Custom Random Attack Test Set 3	62.88%	8.31%	1.54%	78.50%
4. Custom Attack Scenario	48.43%	13.61%	41.20%	98.84%
5. Nonstandard Ports Attack Scenario	100.00%	100.00%	100.00%	100.00%
Port 53	100.00%	100.00%	100.00%	100.00%
Port 123	100.00%	100.00%	100.00%	100.00%
Port 725	100.00%	100.00%	100.00%	100.00%
6. Modified Base Attack Scenario	40.03%	11.03%	29.97%	95.20%
Change Get to Post	46.98%	20.18%	20.52%	94.51%
Change Host Header	37.23%	8.28%	64.13%	95.89%
Combine 'Change Get to Post' and 'Host Header'	35.89%	4.62%	5.25%	95.20%
7. Testing with additional Policy Scenario	86.93%	80.70%	82.97%	97.72%

Table 5. Block Rate by Attack Scenario Category for Cobalt Strike

©SecureIQLab LLC, 2025. All rights reserved

Empire	Vendors and Products			
Command-and Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
1. Basic Attack Scenario	55.91%	29.94%	46.99%	100.00%
Enterprise Attack Profile Set 1	20.74%	16.30%	27.22%	100.00%
Enterprise Attack Profile Set 2	41.38%	18.45%	29.14%	100.00%
Enterprise Attack Profile Set 3	80.73%	44.27%	66.46%	100.00%
Enterprise Attack Profile Set 4	60.68%	31.49%	50.41%	100.00%
2. Random Attack Scenario	63.17%	48.27%	52.21%	100.00%
Random Attack Test Set 1	46.67%	33.75%	42.29%	100.00%
Random Attack Test Set 2	77.32%	60.71%	60.71%	100.00%
3. Custom Random Attack Scenario	54.12%	19.17%	17.48%	100.00%
Custom Random Attack Test Set 1	46.51%	33.75%	38.28%	100.00%
Custom Random Attack Test Set 2	60.21%	7.50%	0.83%	100.00%
4. Custom Attack Scenario	56.25%	35.50%	46.35%	100.00%
5. Nonstandard Ports Attack Scenario	100.00%	100.00%	65.42%	100.00%
Port 53	100.00%	100.00%	100.00%	100.00%
Port 123	100.00%	100.00%	55.00%	100.00%
Port 725	100.00%	100.00%	41.25%	100.00%
6. Modified Base Attack Scenario	52.15%	30.13%	37.86%	100.00%
Change Get to Post	58.39%	33.65%	45.67%	100.00%
Change Host Header	50.13%	28.12%	35.63%	100.00%
Combine 'Change Get to Post' and 'Host Header'	47.94%	28.61%	32.29%	100.00%
7. Testing with additional Policy Scenario	99.90%	92.42%	91.94%	100.00%

Table 6. Block Rate by Attack Scenario Category for Empire

The following sections contain detailed results for the seven Cobalt Strike profile categories.

7.1. Basic Attack Scenario Comparative Analysis

This test was conducted to evaluate products' basic protection against the most commonly available public attack profiles attempting data exfiltration and malware delivery via HTTP.

The Basic Attack Scenario consisted of four Enterprise Attack Profile Sets. These sets consisted of attacks that were being used in the wild. Each of the three profile sets had three categories: Normal Operational Attack profiles, APT Attack profiles, and Crimeware Attack profiles. They are grouped together as basic attacks because the attack techniques are already known and well-researched by the cybersecurity community and are publicly available. Together, this test consisted of 175 Cobalt Strike attack profiles and 169 attack profiles for Empire.

Cobalt Strike	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Basic Attack Scenario	46.86%	18.63%	74.69%	99.71%
Enterprise Attack Profile Set 1	11.40%	4.80%	26.20%	100.00%
Enterprise Attack Profile Set 2	29.06%	16.09%	79.69%	100.00%
Enterprise Attack Profile Set 3	69.42%	31.28%	85.00%	99.53%
Enterprise Attack Profile Set 4	53.33%	17.07%	82.80%	99.60%

Table 7. Basic Attack Scenario by Toolset Used to Generate in Cobalt Strike

©SecureIQLab LLC, 2025. All rights reserved

Empire	Vendors and Products			
Command-and Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Basic Attack Scenario	55.91%	29.94%	46.99%	100.00%
Enterprise Attack Profile Set 1	20.74%	16.30%	27.22%	100.00%
Enterprise Attack Profile Set 2	41.38%	18.45%	29.14%	100.00%
Enterprise Attack Profile Set 3	80.73%	44.27%	66.46%	100.00%
Enterprise Attack Profile Set 4	60.68%	31.49%	50.41%	100.00%

Table 8. Basic Attack Scenario by Toolset Used to Generate in Empire

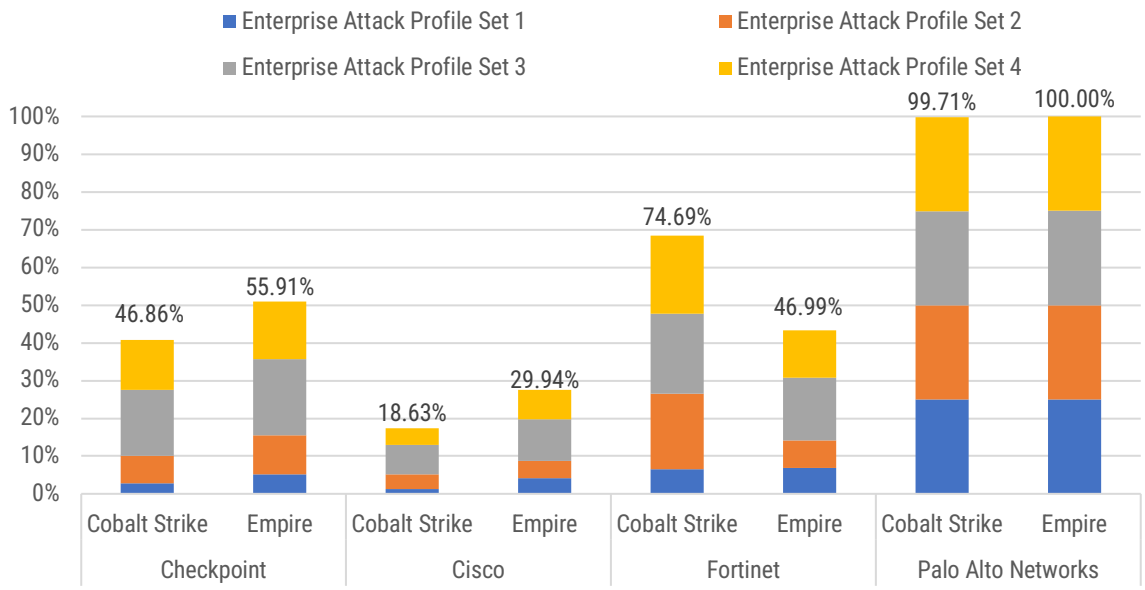

Figure 7. Block Rate for Basic Attack Scenario for Cobalt Strike and Empire

As mentioned above, the attacks in the Basic Attack Scenario can also be organized by attack type into three categories: the Normal Operational Attack Set, the Crimeware Attack Set, and the APT Operation Attack Set. Together, these three sets contain the attacks of the three out of four Enterprise Attack Profile Sets just discussed. The following table gives the total block rates by attack type.

Cobalt Strike	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Basic Attack Scenario	52.77%	20.93%	82.77%	99.67%
Normal Operational Attack Set	45.52%	14.31%	71.03%	99.40%
Crimeware Attack Set	55.35%	27.95%	91.73%	99.91%
APT Attack Set	64.62%	23.09%	93.08%	99.83%

Table 9. Basic Attack Scenario Block Rate by Attack Type – Cobalt Strike

Empire	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Basic Attack Scenario	62.50%	32.50%	50.69%	100.00%
Normal Operational Attack Set	60.31%	34.31%	42.46%	100.00%
Crimeware Attack Set	62.50%	32.60%	61.35%	100.00%
APT Attack Set	67.78%	27.96%	50.00%	100.00%

Table 10. Basic Attack Scenario Block Rate by Attack Type - Empire

©SecureIQLab LLC, 2025. All rights reserved

The Normal Operational Attack Set consisted of attacks that mimicked Amazon, One Drive, and other safe browsing traffic requests and responses. This traffic looks harmless to most users and inspection tools; however, in the test, this traffic included sinister activity masked as part of this harmless traffic. The Normal Operational Attack Set tested the response to 67 attacks for Cobalt Strike and 65 for Empire.

The Crimeware Attack Set consisted of attacks that mimicked known botnets as well as attacks that can hide in non-malicious traffic. An example of a known botnet that was tested was Emotet. Data from this test is useful to expose gaps in coverage to known threats. The Crimeware Attack Set tested the response to 54 attacks for Cobalt Strike and 52 for Empire.

The APT Attack Set consisted of known APT (Advanced Persistent Threat) attacks. For example, one APT threat that was mimicked was The Dukes APT 29. These attacks were included to test the firewalls' ability to prevent attacks similar in modus operandi to high-profile APT attacks. The APT Attack Set tested the response to 29 attacks for Cobalt Strike and 27 for Empire.

The block rate of the tested firewalls by attack subcategory (Normal, Crimeware, APT) is shown visually in the table below.

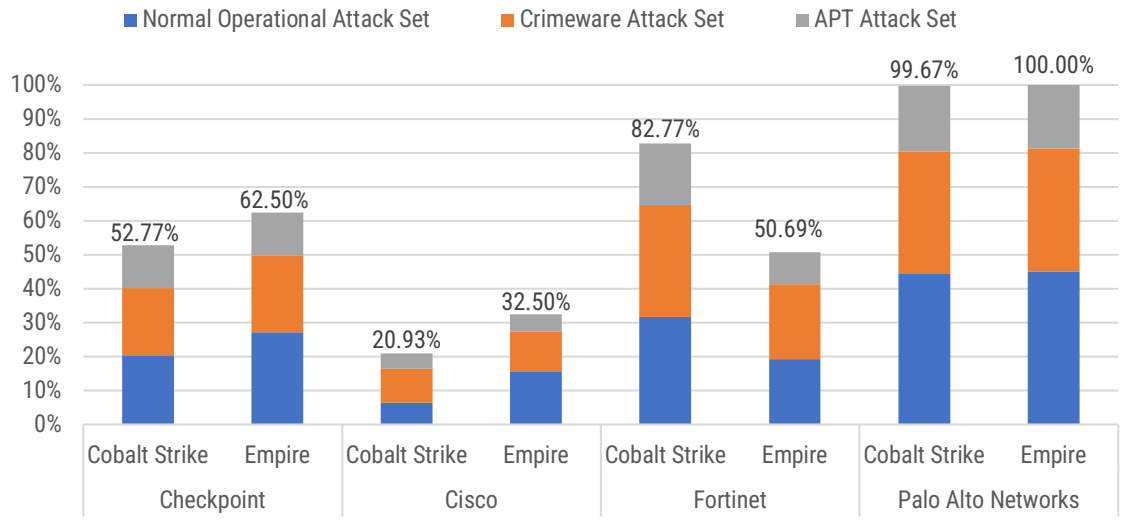

Figure 8. Overall Profile Block Rate for Basic Attack Scenario by Attack Type – Cobalt Strike and Empire

7.2. Random Attack Scenario Comparative Analysis

This test was intended to evaluate the protection when commonly available tools are leveraged to generate "randomized" attack scenarios using Cobalt Strike, increasing the probability of the traditional threat defenses of the firewall being rendered ineffective against data exfiltration and malware delivery via HTTP. SecureIQLab tested 120 attack profiles using Cobalt Strike and 52 attack profiles using Empire in this test.

The Random Attack Scenario consisted of profiles that were generated by four tools that were publicly available and maintained at the time of testing. Each tool was used to generate an attack set, labeled Random Attack Test Set 1, Random Attack Test Set 2, Random Attack Test Set 3, and Random Attack Test Set 4 for Cobalt Strike. In the case of Empire, profiles were generated by 2 tools labeled as Random Attack Test Set 1 and Random Attack Test Set 2.

Cobalt Strike	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Random Attack Scenario	42.29%	16.54%	56.50%	92.38%
Random Attack Test Set 1	20.36%	20.00%	82.32%	99.82%
Random Attack Test Set 2	69.67%	13.33%	0.00%	69.83%
Random Attack Test Set 3	70.47%	27.03%	72.97%	99.84%
Random Attack Test Set 4	5.33%	5.33%	71.33%	100.00%

Table 11. Overview Table Excerpt, Random Attack Scenario – Cobalt Strike

©SecureIQLab LLC, 2025. All rights reserved

Empire	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Random Attack Scenario	63.17%	48.27%	52.21%	100.00%
Random Attack Test Set 1	46.67%	33.75%	42.29%	100.00%
Random Attack Test Set 2	77.32%	60.71%	60.71%	100.00%

Table 12. Overview Table Excerpt, Random Attack Scenario - Empire

The following graph shows the overall block rate for each vendor within the Random Attack Scenario for each of the four Random Attack Sets for Cobalt Strike and two Random Attack Sets for Empire.

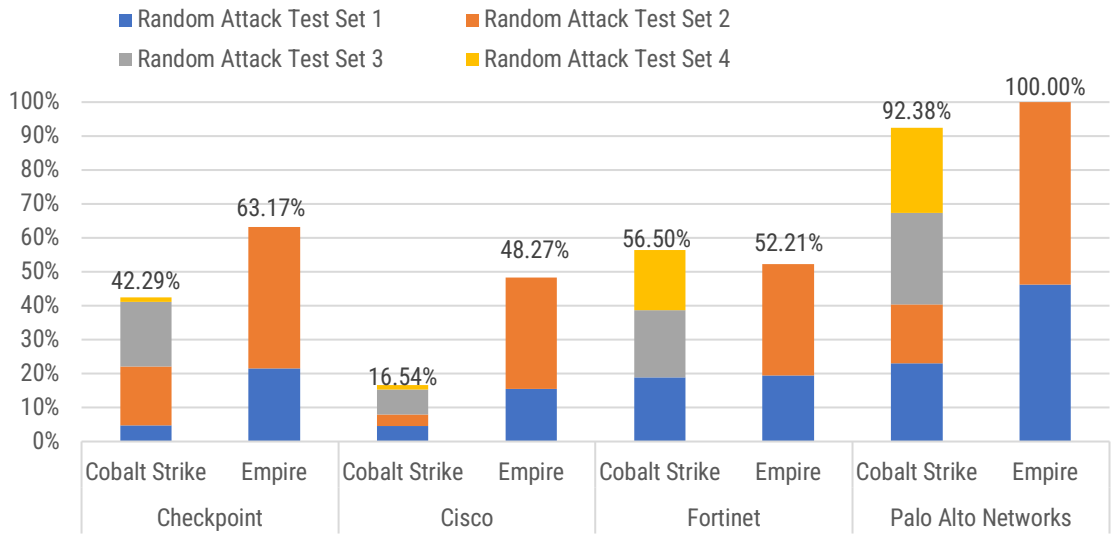

Figure 9. Random Attack Scenario Block Rate by Random Attack Set Cobalt Strike and Empire

7.3. Custom Random Attack Scenario Comparative Analysis

This testing was performed to assess the ability of each product to provide protection when publicly available tools are customized (e.g., replace default wordlists/dictionaries) and used to generate "randomized" profiles, further increasing the probability that traditional static signatures are rendered ineffective. SecureIQLab tested 362 attack profiles using Cobalt Strike and 216 attack profiles using Empire in this test.

Cobalt Strike	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Custom Random Attack Scenario	30.21%	6.08%	25.54%	87.49%
Custom Random Attack Test Set 1	20.36%	5.71%	42.54%	99.69%
Custom Random Attack Test Set 2	4.00%	4.00%	35.67%	85.83%
Custom Random Attack Test Set 3	62.88%	8.31%	1.54%	78.50%

Table 13. Overview Table Excerpt, Custom Random Attack Scenario – Cobalt Strike

Empire	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Custom Random Attack Scenario	54.12%	19.17%	17.48%	100.00%
Custom Random Attack Test Set 1	46.51%	33.75%	38.28%	100.00%
Custom Random Attack Test Set 2	60.21%	7.50%	0.83%	100.00%

Table 14. Overview Table Excerpt, Custom Random Attack Scenario – Empire

©SecureIQLab LLC, 2025. All rights reserved

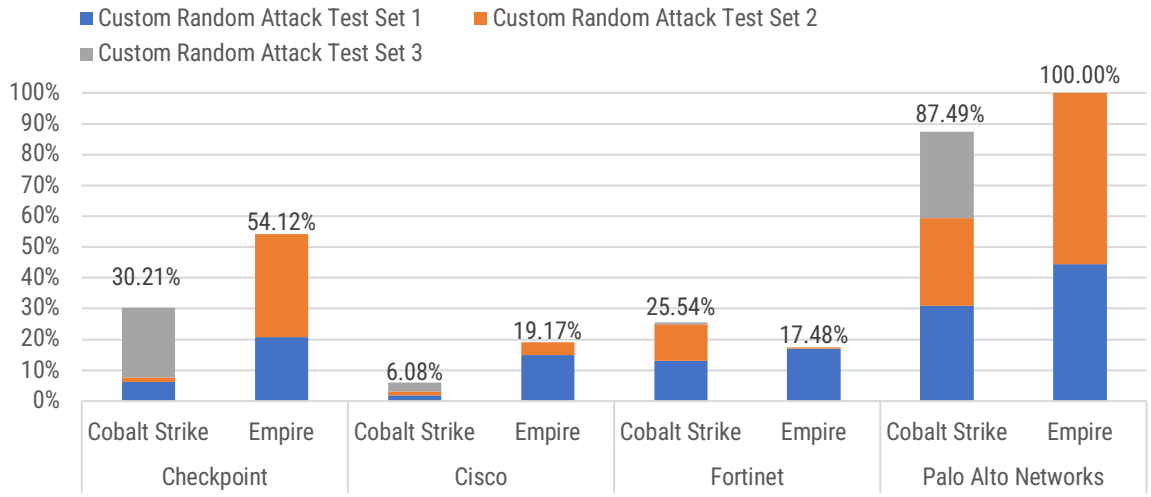

Figure 10. Custom Random Attack Scenario Block Rate by Random Attack Set Cobalt Strike, and Empire

7.4. Custom Attack Scenario Comparative Analysis

This test was intended to evaluate the firewall's protection against intelligently modified attacks from the Basic Attack Scenario and Random Attack Scenario.

The Custom Attack Scenario was intended to model attacks from a more sophisticated actor. We picked the profiles from Basic Attack Scenario, or Random Attack Scenario, or new profile set. We then modified variables inside the profiles which, from data analysis, looked likely to impact block rate. For example, sleep time is a highly customizable variable inside the baseline profile. Increasing this value will force the product under test to wait for more time to inspect the incoming traffic.

Custom Attack Scenario Profile	Vendors and Products			
	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Cobalt Strike	48.43%	13.61%	41.20%	98.84%
Empire	56.25%	35.50%	46.35%	100.00%

Table 15. Overall Table Excerpt, Custom Attack Scenario – Cobalt Strike & Empire

Because of the individualized nature of the test, the sample size was relatively small. SecureIQLab tested 108 Cobalt Strike attack profiles and 100 attack profiles for Empire in this test. Each attack was designed to test a specific aspect of the product's ability to block.

Attackers in the wild may affirmatively target designated vendors. Because we did not tailor the attacks against specific vendors, this test is more useful as an indicator of relative product capabilities than as a measure of absolute protection afforded by a product.

7.5. Nonstandard Ports Attack Scenario Comparative Analysis

The purpose of this testing is to confirm if the tested firewalls can continue to provide protection when attacks are targeting a nonstandard port.

The Nonstandard Ports Attack Scenario consisted of profiles that were hosted via HTTP on a nonstandard port. We used basic attack profiles for this validation. Typically, HTTP traffic is hosted on TCP port 80. We hosted these profiles on different ports to see if the evaluated firewalls maintained their prevention coverage for the same attacks when hosted on different ports. This test included 12 attacks for Cobalt Strike and 4 attack profiles for Empire.

©SecureIQLab LLC, 2025. All rights reserved

Cobalt Strike	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Nonstandard Port Attack Scenario	100.00%	100.00%	100.00%	100.00%
Port 53	100.00%	100.00%	100.00%	100.00%
Port 123	100.00%	100.00%	100.00%	100.00%
Port 725	100.00%	100.00%	100.00%	100.00%

Table 16. Nonstandard Port Attack Scenario Block Rate for Cobalt Strike

Empire	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Nonstandard Port Attack Scenario	100.00%	100.00%	65.42%	100.00%
Port 53	100.00%	100.00%	100.00%	100.00%
Port 123	100.00%	100.00%	55.00%	100.00%
Port 725	100.00%	100.00%	41.25%	100.00%

Table 17. Nonstandard Port Attack Scenario Block Rate for Empire

As the data table above shows, all tested products demonstrated consistent efficacy against attack profiles on nonstandard port for Cobalt Strike. However, only the firewalls from Checkpoint, Cisco, and Palo Alto Networks consistently blocked the previously detected profiles when those attacks were reattempted on a nonstandard port for Empire. Fortinet received 100% on port 53 but a lower block rate for port 123 and port 725. Also, they have a lower block rate over port 80 for Empire as compared to non-standard ports that were tested for larger profile sets.

7.6. Modified Base Attack Scenario Comparative Analysis

The Modified Base Attack Scenario is conducted to assess the ability of each product to provide protection when each of the base profile sets is modified as follows:

- CHANGE GET to POST
  - HTTP “GET” verbs in profiles are changed to “POST”
- CHANGE HOST HEADER
  - HTTP host headers in profiles are changed to use IP address rather than hostname
- COMBINE ‘CHANGE GET to POST’ AND ‘CHANGE HOST HEADER’
  - HTTP “GET” verbs in profiles are changed to “POST”
  - HTTP host headers in profiles are changed to use IP address rather than hostname

Cobalt Strike	Vendors and Products			
Command-and-Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Modified Base Attack Scenario	40.03%	11.03%	29.97%	95.20%
CHANGE GET to POST	46.98%	20.18%	20.52%	94.51%
CHANGE HOST HEADER	37.23%	8.28%	64.13%	95.89%
COMBINE ‘CHANGE GET to POST’ AND ‘CHANGE HOST HEADER’	35.89%	4.62%	5.25%	95.20%

Table 18. Modified Base Attack Scenario for Cobalt Strike

©SecureIQLab LLC, 2025. All rights reserved

Empire	Vendors and Products			
Command-and Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Modified Base Attack Scenario	52.15%	30.13%	37.86%	100.00%
CHANGE GET to POST	58.39%	33.65%	45.67%	100.00%
CHANGE HOST HEADER	50.13%	28.12%	35.63%	100.00%
COMBINE 'CHANGE GET to POST' AND 'CHANGE HOST HEADER'	47.94%	28.61%	32.29%	100.00%

Table 19. Modified Base Attack Scenario for Empire

7.7. Testing with Additional Policy Attack Scenario Comparative Analysis

The purpose of this testing is to set multiple policies as required to adequately determine the efficacy of each product (e.g., a URLF policy that blocks 'unrated/uncategorized' URLs).

Cobalt Strike	Vendors and Products			
Command-and Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Overall Score	86.93%	80.70%	82.97%	97.72%
Check-In	1.99%	3.88%	4.07%	4.77%
Reconnaissance	13.42%	11.86%	12.54%	14.69%
Exfiltration	35.88%	33.24%	33.48%	39.22%
Delivery	35.64%	31.72%	32.88%	39.05%

Table 20. Overall Block Rate for the Policy "Block Unrated/Uncategorized" URLs for Cobalt Strike

Empire	Vendors and Products			
Command-and Control Profile Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Overall Score	99.90%	92.42%	91.94%	100.00%
Check-In	4.98%	4.47%	4.41%	5.00%
Reconnaissance	14.99%	14.11%	14.08%	15.00%
Exfiltration	39.97%	37.65%	37.62%	40.00%
Delivery	39.97%	36.19%	35.83%	40.00%

Table 21. Overall Block Rate for the Policy "Block Unrated/Uncategorized" URLs for Empire

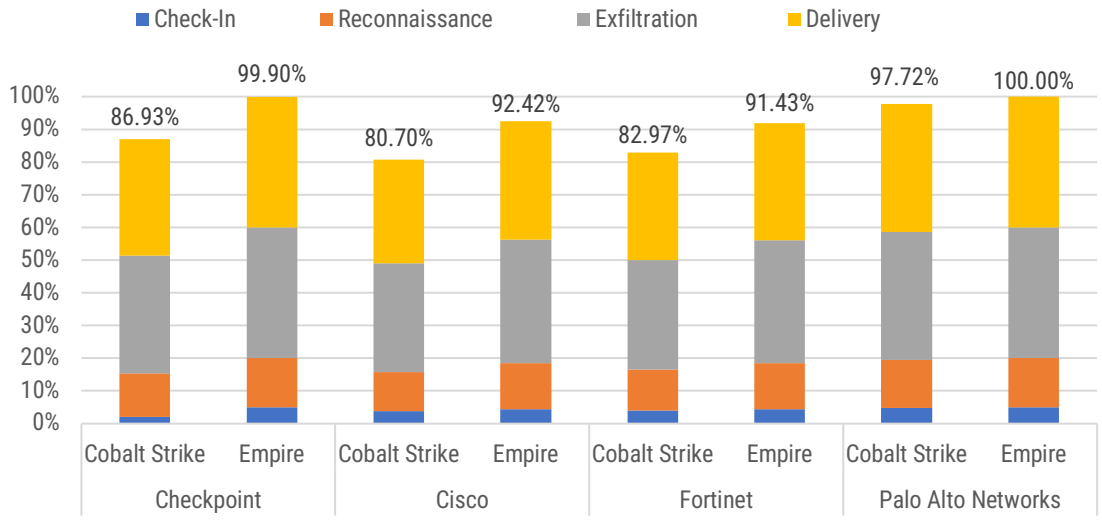

Figure 11. Overall Block Rate for the Policy "Block Unrated/Uncategorized URLs for Cobalt Strike and Empire

©SecureIQLab LLC, 2025. All rights reserved

8. Comparing Policies

The Allow Unrated/Uncategorized URLs policy grants access to URLs that have not yet been assigned a specific category (e.g., business, news, malware, etc.). This can be beneficial for accessing new or less-known sites that have not yet been reviewed by the filtering system. However, it also introduces a security risk, as cybercriminals may exploit newly created or unclassified sites for malicious purposes, such as phishing, malware distribution, or command and control (C2) communications.

The Block Unrated/Uncategorized URLs policy prevents access to URLs that have not yet been classified. This strengthens security by reducing exposure to potentially harmful or unknown sites. However, it may also restrict access to legitimate but newly created websites, leading to accessibility challenges for business or research purposes. For this reason, extensive false positives were performed when the policy was set to 'Block Unrated/Uncategorized' URLs Names for a product.

Vendors and Products	Overall Block Rate- Cobalt Strike	
	Allow Unrated/Uncategorized Policy	Block Unrated/Uncategorized Policy
Checkpoint	39.33%	86.93%
Cisco	11.31%	80.70%
Fortinet	36.29%	82.97%
Palo Alto	94.04%	97.72%

Table 22. Overall Block Rate for both policies – Cobalt Strike

Vendors and Products	Overall Block Rate- Empire	
	Allow Unrated/Uncategorized Policy	Block Unrated/Uncategorized Policy
Checkpoint	53.85%	99.90%
Cisco	29.37%	92.42%
Fortinet	36.83%	91.94%
Palo Alto	100.00%	100.00%

Table 23. Overall Block Rate for both policies – Empire

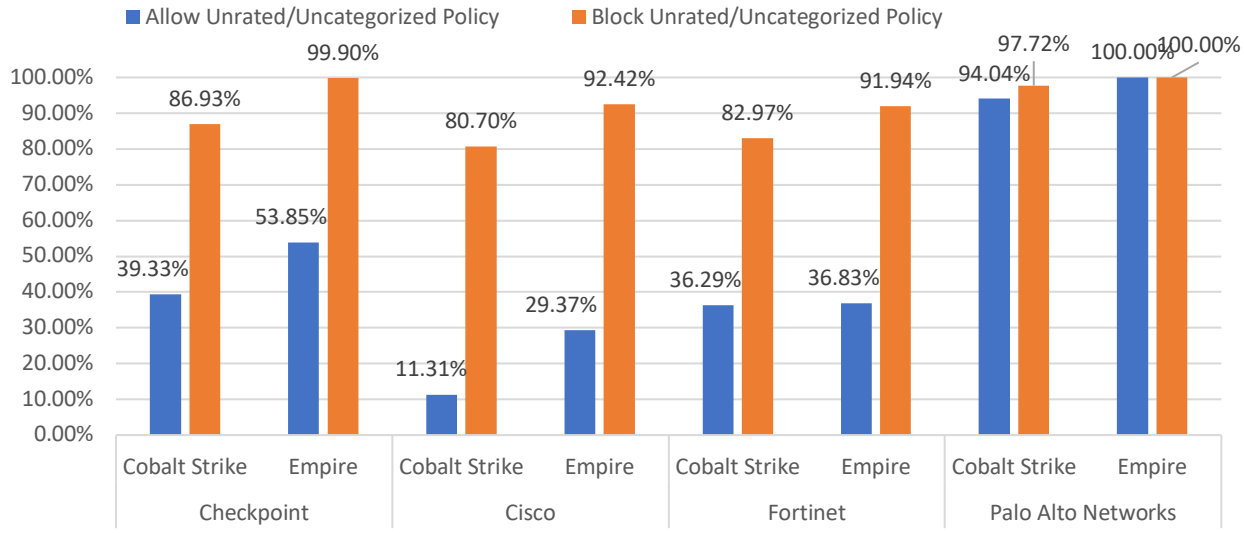

Figure 12. Overall Block Rate for both policies for Cobalt Strike and Empire

9. Threat Mitigation Efficiency Scoring

The *Threat Mitigation Efficiency Score* is intended to measure the ability of the product to identify and respond to the threat campaigns that were delivered as part of the command-and-control Cobalt Strike and Empire testing. The appropriate response and mitigation capabilities of the different solutions were measured to understand how the products under test help improve the overall risk posture and the security efficacy of the organization. It was measured by factoring in the ease of tuning the solution against C2 attacks, the solution's attack response

©SecureIQLab LLC, 2025. All rights reserved

intuitiveness from a policy and security configuration perspective, the comprehensiveness of the data and the enhanced reporting capabilities, and the ease of using data it generates to provide an effective threat detection & response. Threat mitigation efficiency was determined for five different categories: Simplicity of attack mitigation tuning specific to Cobalt Strike and Empire-based threats, speed to tune and respond, which makes it easier to detect and respond to command-and-control based threats, intelligence-driven attack response, customizable analytics dashboard, and enhanced mitigation-centric reporting. During analysis, each of these products were rated high (10 points), medium (6 Points) or a low (3 points) score accordingly.

Overall	Vendors and Products			
Threat Mitigation Efficiency Categories	Checkpoint	Cisco	Fortinet	Palo Alto Networks
	Quantum 6200P	Firepower 1140	FG 600F	PA-460
Attack Mitigation Tuning Efficacy	Medium	Medium	High	High
Speed to Tune and Respond	Medium	Medium	Medium	High
Intelligence-Driven Attack Response	High	High	High	High
Customizable Analytics Dashboard	Medium	Low	Medium	Medium
Enhanced Mitigation- Centric Reporting	Medium	Medium	High	High

Table 24. Threat Mitigation Efficiency Results.

As Table 25 above shows, all participating vendors had some level of medium-to-high threat mitigation efficiency capabilities. The overall *Threat Mitigation Efficiency Scores* were at a high of 92% for the Palo Alto Networks PA-460 and 84% for the Fortinet FG600F. The next at 68% was the Checkpoint Quantum 6200P. Last at 62% were the Cisco Firepower 1140.

$$Threat\ Mitigation\ Efficiency\ Score = \frac{\left(Attack\ Mitigation\ Tuning\ Efficacy + Speed\ to\ Tune\ and\ Respond + Attack\ Response\ Intelligence + Customizable\ Analytics\ Dashboard + Enhanced\ Mitigation\text{-}Centric\ Reporting \right)}{50} \times 100\%$$

Equation 3. Threat Mitigation Efficiency Score Calculation

As shown by Equation 3, the *Threat Mitigation Efficiency Score* was calculated by adding the points awarded for each subcategory, then dividing this number by the maximum potential points (50) and multiplying that number by 100%.

9.1 Attack Mitigation Tuning Efficacy:

Ability to tune the firewall effectively against known and on-going attacks from the Cobalt Strike and Empire frameworks was one of the key metrics that was factored into the overall threat mitigation metric. Business requirements should be aligned with the environment being used. Scoring for this category was performed as follows:

High (10 points): Solution has multiple ready-to-use canned, pre-set configuration policies, response-based signatures, or tuning based on certain key indicators present. Solutions should be able to address different business requirements in line with the attacks resulting from Cobalt Strike and Empire with automated deployment models with zero-to-very minimal professional intervention.

Medium (6 points): Solution has some ready-to-use canned, pre-set configuration policies, response-based signatures, or tuning based on certain key indicators. Solutions should be able to address different business requirements in line with the attacks resulting from Cobalt Strike and Empire with semi-automated deployment models with medium professional intervention.

Low (3 Points): Solution does not have ready-to-use, canned, pre-set response policies, response-based signatures, or tuning based on certain key indicators. Solutions are extremely manual in nature to address different business requirements in line with the attacks resulting from Cobalt Strike and Empire with manual deployment models with maximum professional intervention.

©SecureIQLab LLC, 2025. All rights reserved

9.2 Speed to Tune and Respond:

This goes directly to the time taken to identify, detect and respond to threats from Cobalt Strike and Empire frameworks. Scoring was based on the solution's capability around the following three criteria:

1. Time-to-detect and alert/block on attacks.
2. Time to notify attacks
3. The quality of mitigation and post-attack mitigation reliability.

High (10 points): Solution can showcase all the 3 highlighted metrics above end-to-end.
Medium (6 Points): Solution can showcase at least 2 of highlighted metrics above end-to-end.
Low (3 Points): Solution can showcase at least 1 of the highlighted metrics above end-to-end.

9.3 Intelligence-Driven Attack Response

This applies directly to the core of the solution's response strategy with minimal intervention and simplified workflows. Scoring was based on the solution's capability around the following:

High (10 points): Consolidated high-level summary (single pane of glass) of the threat workflow, and view of a set of command and control-based attack campaigns/profile/threats that are easily categorized (intuitively). Ability to take a proactive response-centric approach is integral to the intelligence-driven model.
Medium (6 Points): High-level summary of the threat workflow but are not easily categorized (intuitively) with basic intelligence built-in around proactive response.
Low (3 Points): No categorization of attack campaigns/profile/threats (intuitively) with no high-level summary of the threat workflow.

9.4 Customizable Analytics Dashboard

This evaluates how customizable the product's dashboard is and whether it allows the customer to choose and represent both the data and incident of interest visually. The threat analytics dashboard should also give the investigators the customization capabilities on-demand and the ability to integrate the data via multiple operational streams.

High (10 points): There is a highly customizable widget-driven dashboard that allows the customer to choose both the data presented and how that data is represented visually (e.g., pie chart, xy plot, bar graph, and so forth). This also provides enhanced API functionality to integrate with third party Power BI or other third-party data visualization platforms.
Medium (6 Points): The product provides some level of API out of the box to integrate with third party data visualization platforms such as Power BI. The product had a widget-driven dashboard that allows customers to choose the data but does not allow the customer to choose how the data is represented visually.
Low (3 Points): Only the default dashboard was available with no API integration.

9.5 Enhanced Mitigation-centric Reporting

This enables the solutions to require a proactive mitigation approach to the Cobalt Strike and Empire-based attacks that answers critical questions like: Which threat actors are most likely to cause an impact in my organization, possible motivation and goals, attack surface, and C2 prevention capabilities with actionable countermeasures that be deployed to improve my organization's cyber defense capabilities.

High (10 points): Solution can showcase Cobalt Strike and Empire threat notifications with context, attack source and timelines with a deep dive into each attribute and artifact of the attack. Present product configuration/vulnerabilities on a unified dashboard with the ability to recommend and advise response/mitigation actions to be taken. Having the ability to identify, alert with search capabilities and give the ability to remediate suboptimal product configurations and conditions.
Medium (6 Points): Cobalt Strike and Empire threat notification with information such as minimum of IP, hostname, geolocation, time, threat disposition with some basic information around why an attack was classified as a threat. Attacks may be searched and filtered via date and other fields with some level of graphical representation, advisory and recommendations.
Low (3 Points): Cobalt Strike and Empire basic threat notification with the ability to search and filter attacks and threats via date and other fields. A minimal graphical representation that is specific to those attacks with no advisory and recommendations. No alert capabilities on suboptimal product configuration or conditions or to act.

©SecureIQLab LLC, 2025. All rights reserved

10. Conclusion

In the seven Cobalt Strike and Empire attack suites tested, the Palo Alto Networks firewall was always the top performer or tied for top performance.

Reviewing the Cobalt Strike test results, the Palo Alto Networks firewall performed better than the competition in the Basic Attack Scenario. The Palo Alto Networks firewall managed to block 99.71% of attacks, while the next best performance was by Fortinet's firewall at 74.69%. In the Random Attack Scenario, Palo Alto Networks' firewall blocked 92.38% of attacks, while the next best performance was from Fortinet's firewall, with 56.50% blocked.

In the Custom Attack Scenario, the Palo Alto Networks firewall blocked 98.84% of attacks. The next best performance was from the Checkpoint firewall, which blocked 48.43% of attacks. The firewalls of Palo Alto Networks, Cisco and Checkpoint and Fortinet all blocked 100% of attacks in the Nonstandard Ports Attack Scenario. The Palo Alto Networks firewalls managed to block 87.49% of attacks in Custom Random Attack Scenario, while the next best performance was Checkpoint's firewall at 30.21%. In the Modified Base Attack Scenario, the Palo Alto Networks firewall blocked 95.20% of attacks.

In the case of the Empire results, the Palo Alto Networks firewall was the top performer with 100% block rate in all of the test scenarios. The next best performance in these scenarios was from the Checkpoint's Firewall with 55.91% in Basic Attack and 63.17% in Random Attack Scenarios. Additionally, Checkpoint's Firewall blocked 54.21% in Custom Random Attack, 52.15% in Modified Base Attack and 56.25% in Custom Attack. On the other hand, Fortinet's firewall blocked 46.99% in Basic Attack and 52.21% in Random Attack whereas in Custom Random Attack it blocked 17.48% and 46.35% in Custom Attack. The firewalls of Palo Alto Networks, Cisco and Checkpoint blocked 100% of attacks whereas Fortinet blocked 65.42% in the Nonstandard Ports Attack Scenario for Empire.

When the policy was changed to block unrated and uncategorized URLs, Palo Alto Networks firewalls managed to block 97.72% of attacks in Cobalt Strike and 100% in Empire. The next best performances were Fortinet with 82.97% blocked for Cobalt Strike and Checkpoint for Empire with 99.90% blocked.

The Threat Mitigation Efficiency was validated to determine how easy a solution was to use when identifying and responding to C2 threats from Cobalt Strike and Empire. The Palo Alto Networks' firewall has the highest Threat Mitigation Efficacy of 92%. Fortinet earned a Threat Mitigation Efficiency score of 84% and Checkpoint earned 68%. Cisco had the lowest Threat Mitigation Scores at 62%.

Overall, Palo Alto Networks performed very well against the Cobalt Strike attack profiles and Empire profiles tested. Compared with the other products tested, Palo Alto Networks' Advanced Threat Prevention model outperformed the competition by a significant margin in the majority of the tests, while providing highest Threat Mitigation Efficiencies.

©SecureIQLab LLC, 2025. All rights reserved

11. Appendix

11.1. Product Staging

The following documentation was referred to during product configuration:

Checkpoint

- https://sc1.checkpoint.com/documents/Best_Practices/IPS_Best_Practices/CP_R80.10_IPS_Best_Practices/html_frameset.htm
- https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuide/CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf
- https://support.checkpoint.com/results/sk/sk111303
- https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_ThreatPrevention_AdminGuide/CP_R81.20_ThreatPrevention_AdminGuide.pdf

Cisco

- https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fdm-config-guide-720.html
- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72.html

Fortinet

- https://docs.fortinet.com/document/fortigate/7.6.2/administration-guide/954635/getting-started
- https://docs.fortinet.com/document/fortigate/7.6.2/cli-reference/84566/fortios-cli-reference
- https://docs.fortinet.com/document/fortigate/7.6.0/best-practices/587898/getting-started
- https://community.fortinet.com/t5/FortiGate/Technical-Tip-Difference-between-Security-Events-and-All-session/ta-p/206881

Palo Alto Networks

- https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices
- https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/wildfire-features/hold-mode-for-wildfire-realtime-signature-lookup
- https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/configure-threat-prevention/configure-inline-cloud-analysis
- https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention
- https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices

Juniper

- https://www.juniper.net/documentation/us/en/software/jweb-srx24.2/help/jweb-srx/topics/topic-map/j-web-security-overview.html
- https://www.juniper.net/documentation/us/en/software/jweb-srx24.2/help/jweb-srx/topics/concept/j-web-security-about-rules-page.html
- https://www.juniper.net/documentation/us/en/software/junos/utm/topics/topic-map/

Versa Networks

- https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration
- https://academy.versa-networks.com/docs/

©SecureIQLab LLC, 2025. All rights reserved

12. About SecureIQLab

SecureIQLab is a cybersecurity testing lab that was founded in 2019. SecureIQLab works with enterprises, governments, and security vendors to bridge the applied intelligence gap that exists between market and technology research. SecureIQLab also provides services to operationalize security and the metrics to help organizations improve their return on security investments.

SecureIQLab
9600 Great Hills Trail
Suite 150W
Austin, TX 78759

+1.512.575.3457

www.secureiqlab.com

info@secureiqlab.com

13. Copyright and Disclaimer

Copyright © 2025 SecureIQLab, LLC. All rights reserved. The content of this report is protected by United States and international copyright laws and treaties. You may only use this report for your personal, non-commercial, informational purposes. Without SecureIQLab's prior written consent, you may not: (i) reproduce, modify, adapt, create derivative works from, publicly perform, publicly display, or distribute this report; or (ii) use this report, the SecureIQLab name, or any SecureIQLab trademark or logo as part of any marketing, promotion or sales activities. THIS REPORT IS PROVIDED "AS IS," "AS AVAILABLE" AND "WITH ALL FAULTS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, SECUREIQLAB EXPRESSLY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING: (a) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND (b) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF THE REPORT, OR THAT USE OF THE REPORT WILL BE ERROR-FREE, UNINTERRUPTED, FREE FROM OTHER FAILURES OR WILL MEET YOUR REQUIREMENTS. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING SENTENCE, YOU ACKNOWLEDGE AND AGREE THAT THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT DEPEND UPON VARIOUS FACTORS, INCLUDING FACTORS OUTSIDE OF SECUREIQLAB'S CONTROL, SUCH AS: (1) THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF INFORMATION AND MATERIALS PROVIDED BY OTHER PARTIES THAT ARE RELIED UPON BY SECUREIQLAB IN PERFORMING PREPARING THE REPORT; AND (2) THE UNDERLYING ASSUMPTIONS MADE BY SECUREIQLAB IN PREPARING THE REPORT REMAINING TRUE AND ACCURATE. YOU ARE SOLELY RESPONSIBLE FOR INDEPENDENTLY ASSESSING THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT BEFORE TAKING OR OMITTING ANY ACTION BASED UPON THE REPORT. IN NO EVENT WILL SECUREIQLAB BE LIABLE FOR ANY LOST PROFITS OR COST OF COVER, OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING DAMAGES ARISING FROM OR RELATING TO ANY TYPE OR MANNER OF COMMERCIAL, BUSINESS OR FINANCIAL LOSS, EVEN IF SECUREIQLAB HAD ACTUAL OR CONSTRUCTIVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE.

For more information about SecureIQLab and the testing methodologies, please visit our website.

SecureIQLab (April 2025)