SecureIQlab™

Bridging the enterprise cloud security gap

Next-Generation Firewall Command & Control Prevention Comparative Report

TEST PERIOD: JULY 2022—SEPTEMBER 2022

LAST REVISION: 11/30/2022

COMMISSIONED BY: PALO ALTO NETWORKS

www.secureiqlab.com

Report Contents:

1. Executive Summary

SecureIQLab tested the ability of next-generation firewalls to block the command-and-control capabilities of the Cobalt Strike attack suite. Six firewalls were tested: The Checkpoint SG5100, Cisco Firepower 4110, Fortinet FG-301E, Fortinet FG-VM04V, Palo Alto Networks PA-460, and Palo Alto Networks PA-VM-Flex.

The test measured the block rate of the tested firewalls against Cobalt Strike in six attack scenarios.

SecureIQLab concludes Palo Alto Networks' new machine learning approach provides superior protection.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products					
	Checkpoint	Cisco	Fortinet		Palo Alto Networks	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
Overall Block Rate	**18.9%**	**13.3%**	**20.0%**	**20.0%**	**99.1%**	**99.1%**

Table 1: Table of Overall Block Rate Results.

2. Introduction

Command-and-control[1] ("C2") attacks include implants that report back to the attacker's server that thereafter issues commands to a compromised machine. A compromised machine will carry out the commands issued from 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.

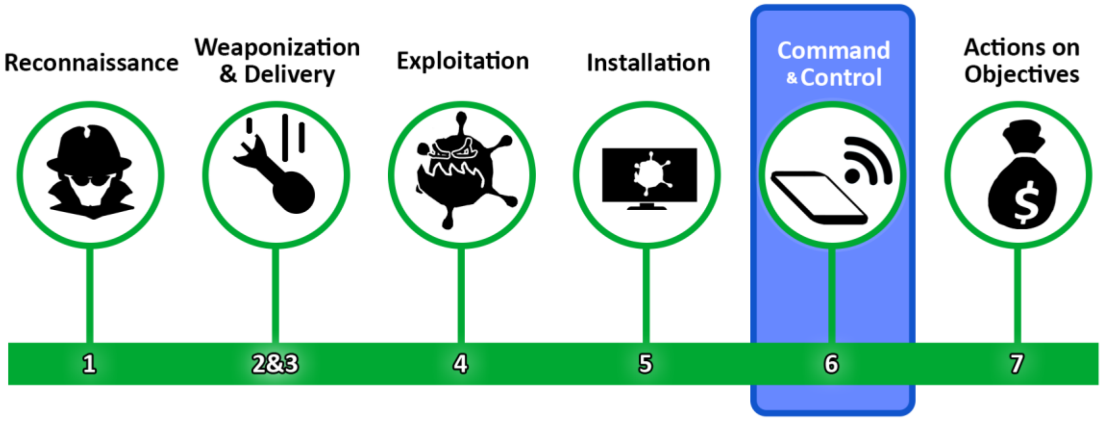


Figure 1: Position of Command and Control in the Lockheed Martin Cyber Kill Chain®.

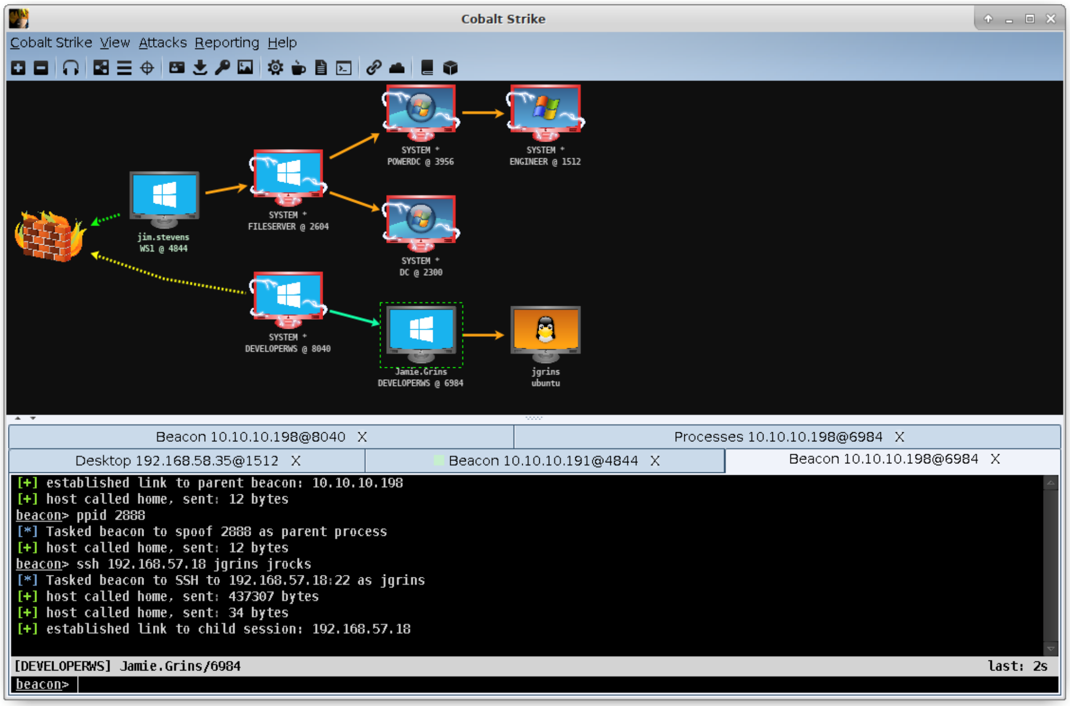
Cobalt Strike is a commercial command-and-control attack suite now owned by Fortra (formerly HelpSystems). Their website states Raphael Mudge created the Cobalt Strike command-and-control framework in 2012 to assist red teams in testing enterprise defense postures against post-exploitation activity.

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.

[1] https://attack.mitre.org/tactics/TA0011/

[2] https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf.



```
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2888
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18

[DEVELOPERWS] Jamie.Grins/6984                                        last: 2s
beacon>
```

Figure 2: Official Screenshot of Cobalt Strike GUI from https://www.cobaltstrike.com/screenshots/.

This test did not cover all of Cobalt Strike's capabilities; instead, it was limited to testing firewalls' ability to block Cobalt Strike's network callback functions.

In order to provide detection of command-and-control network activity between a "team server" and "beacon" (the Cobalt Strike attack server and the implant, respectively), network security products typically utilize traditional IPS signatures to match against specific static strings and/or patterns unique to Cobalt Strike. However, these signatures can be easily evaded with malleable profiles that can create endless combinations of the content that may have been used as Cobalt Strike "fingerprints" in the creation of static IPS signatures. To combat this, in addition to traditional IPS signatures, Palo Alto Networks has launched its Advanced Threat Prevention service that detects and blocks these modifications to typical 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 security solutions in protecting customers against Cobalt Strike command-and-control network activity. This report is intended to indicate protection not only against Cobalt Strike's basic/standard command-and-control network activity, but also to evaluate the relative resiliency of the protection provided by each product when modifications are made in order to evade detection.

Because this report is not intended as a how-to manual for hacking these products, we are omitting or redacting specific details of attacks.

3. Test Environment

Cobalt Strike version 4.6.1 was used in this test, with Debian 5.15.15-2kali1 (2022-01-31) x86_64 GNU/Linux used as the platform to host Cobalt Strike's team server. On the attack side, the Cobalt Strike team server was hosted on the public internet.

The following products and firmware/software versions were tested:

Checkpoint:	SG5100 vR81.10 HF T66 (Hardware)
Cisco:	Firepower 4110 v7.2.0 (Build 82); VDB 357 (Hardware)
Fortinet:	FG-301E v7.2.1build1254(Feature) (Hardware) FortiGate VM04V v7.2.1build1254(Feature) (Virtual)
Palo Alto Networks:	PA-460 v10.2.2 (Hardware) PA-VM-Flex v10.2.2-h1 (Virtual)

Prior to testing, all products' firmware was updated and dynamic security content updates were configured/allowed to happen[3]. Content that updated automatically, for example IPS signatures, continued to be updated during the test.

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.

Publicly available best-practice documentation and admin guides for each product were referred to in an effort 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.

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 profiles (for example, Amazon, Bing, CNN, MSNBC, Wikipedia) through the product as configured.

[3] The Cisco VDB update that occurred mid-testing, release 358, was not applied.

[4] FortiGate firewalls were configured to use proxy-based inspection mode.

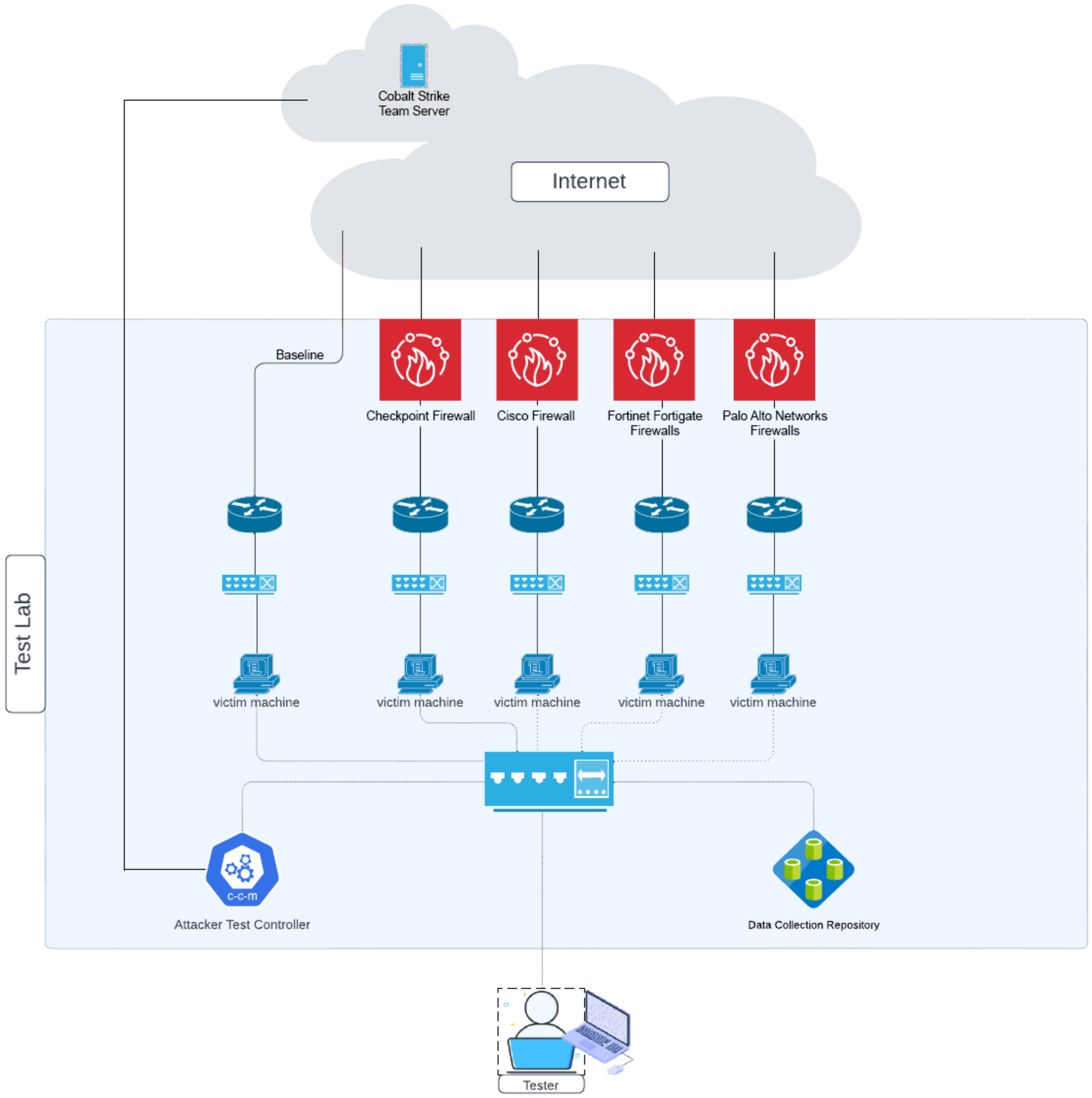


Figure 3: Command-and-Control Testing Environment.

4. Test Procedure

The overall command-and-control test procedure included six main categories of attack scenarios executed using the Cobalt Strike attack framework. Each of the six 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, a stageless 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 Cobalt Strike callback network activity was tested, not the ability to block the initial delivery of the beacon itself; exploitation and delivery of the beacon are assumed to have already taken place.

The types of attacks we evaluated are:

1. **Basic Attack Scenario:** This test was performed to evaluate the product's basic protection against the most commonly available public attack profiles attempting data exfiltration and malware delivery via HTTP. The basic attack scenario included three subcategories: Normal, Crimeware, and APT. Each scenario had a multitude of profiles that were evaluated as a part of the Cobalt Strike attack framework.
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 wherein the traditional threat defenses of the firewall might be rendered ineffective against data exfiltration and malware delivery.
3. **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. The modifications were made to attacks that were previously blocked, to confirm whether the modifications would be sufficient to bypass the defenses. Modifications were made on the different variables that are supported for customization. The variables were modified using data transform language.
4. **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.
5. **HTTPS Attack Scenario:** The purpose of this testing was to confirm if the next-generation firewalls provide the same level of protection when attacks are delivered via HTTPS rather than HTTP.
6. **Hostname Change Attack Scenario:** The purpose of this testing was to confirm if the next-generation firewalls continue to provide the same level of protection when the threat actors adjust/seed/modify the hostname used by a profile in order to evade reputation-based protection.

The tests did not have equal sample sizes. The Custom Attack Scenario, Nonstandard Ports-based Attack Scenario, HTTPS Ports-based Attack Scenario, and the Hostname Change 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 and Random Attack Scenario.

In graphs, where a vendor's two products had the same results, results are presented by vendor rather than by product.

5. Scoring Criteria

Products under test earned blocking credit in two ways: First, by stopping the Cobalt Strike attack at the communication stage, and second, by blocking the attack at the exfiltration and download stage.

The communication stage is when the compromised machine checks in with the Cobalt Strike Team Server and command-and-control is established. Blocking credit at the communication stage was earned by preventing the command-and-control link from establishing.

The exfiltration and download stage is when the compromised machine sends out data or downloads malware, as directed in the communication stage. Blocking credit at the exfiltration and download stage was earned by blocking the exfiltration of system data (output of command output (e.g., 'whoami /all')), blocking output of one or more screenshots, and preventing the download of malware. All three needed to be blocked to earn blocking credit at the exfiltration and download stage.

Some graphs differentiate between blocking credit at the communication stage and blocking credit at the exfiltration and download stages. Where blocking credit is not differentiated, blocking credit was given for blocking at either stage.

6. Overall Block Rate

Overall Block Rate is intended to give a general overview of the capability of products under test to withstand, absorb, and mitigate different variations of Cobalt Strike profiles generated via different tools and third-party-maintained profiles. It includes the results from all the variations of attacks conducted. Overall Block Rate is an unweighted calculation. It is computed by dividing the total number of attacks blocked by all the attacks launched.

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

Equation 1: Formula for Computation of Overall Block Rate.

The higher the Overall Block Rate is, the better the product's ability to withstand attacks. In this test, products' responses to 469 attacks were evaluated.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products					
	Checkpoint	Cisco	Fortinet		Palo Alto Networks	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
Overall Block Rate	18.9%	13.3%	20.0%	20.0%	99.1%	99.1%
Communication stage	17.0%	11.2%	16.6%	16.6%	97.8%	97.4%
Additional Exfiltration and download stage	1.9%	2.2%	3.4%	3.4%	1.3%	1.7%

Table 2: Table of Overall Block Rate Results by Block Stage.

Overall Block Rate is only a general overview because not all attacks are created equal: The composition of the various Cobalt Strike attacks targeting a given network may vary from the composition of the profiles in this test.

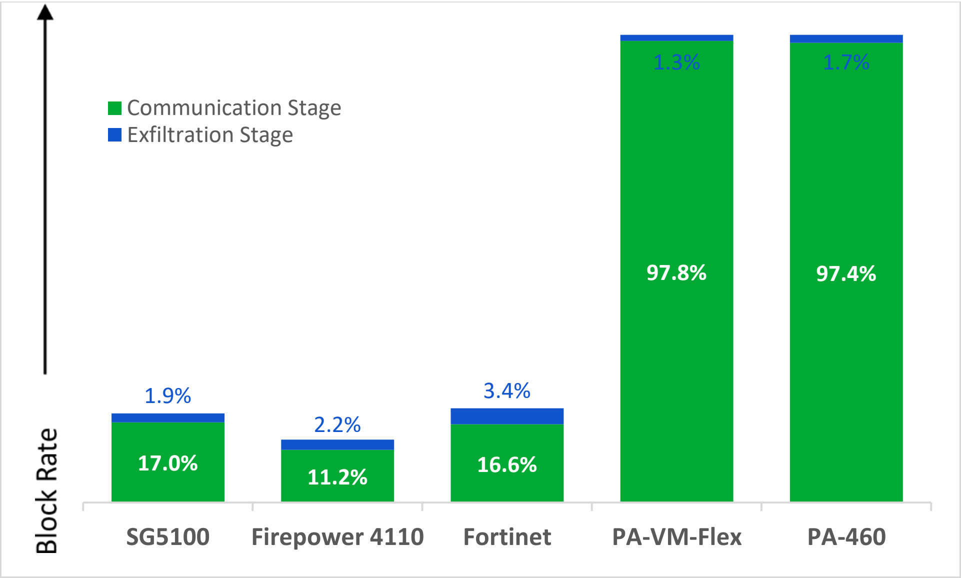


Figure 4: Overall Block Rate by Attack Stage.

7. Comparative Analysis

This section provides a breakdown of results by category. As such, it provides a more detailed analysis of the tested products' performance than the Overall Block Rate.

The summary of key results below shows how the four security vendors' tested products fared during our validation across six main categories of attack scenarios using the Cobalt Strike attack framework. This validation was performed alongside false positive validation during the entire test period. In all cases, results are reported using unweighted percentages of attacks blocked.

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

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

Attack scenarios are broken down into six categories: The Basic Attack Scenario, the Random Attack Scenario, the Custom Attack Scenario, the Nonstandard Ports Attack Scenario, the HTTPS-based Attack Scenario, and the Hostname Change Scenario. Each is discussed further below.

Cobalt Strike Command-and-Control Profile Categories	**Vendors and Products**					
	Checkpoint	**Cisco**	**Fortinet**		**Palo Alto Networks**	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
1. Basic Attack Scenario	**37.2%**	**22.4%**	**30.8%**	**30.8%**	**99.4%**	**99.4%**
Enterprise Attack Profile Set 1	25.9%	3.2%	9.7%	9.7%	100%	100%
Enterprise Attack Profile Set 2	16.7%	0.0%	16.7%	16.7%	100%	100%
Enterprise Attack Profile Set 3	0.0%	0.0%	0.0%	0.0%	100%	100%
Enterprise Attack Profile Set 4	59.0%	46.2%	56.4%	56.4%	97.4%	97.4%
Enterprise Attack Profile Set 5	40.0%	24.3%	32.9%	32.9%	100%	100%
2. Random Attack Scenario	**3.0%**	**2.0%**	**10.0%**	**10.0%**	**99.0%**	**99.0%**
Random Attack Test Set 1	0%	1%	0%	0%	100%	100%
Random Attack Test Set 2	1%	5%	16%	16%	98%	98%
Random Attack Test Set 3	9%	0%	12%	13%	100%	100%
3. Custom Attack Scenario	**28.6%**	**14.3%**	**14.3%**	**14.3%**	**85.7%**	**85.7%**
4. Nonstandard Ports Attack Scenar-io	**100%**	**100%**	**16.7%**	**16.7%**	**100%**	**100%**
5. HTTPS-based Attack Scenario	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
6. Hostname Change Scenario	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**100%**	**100%**

Table 3: Block Rate by Attack Scenario Category ("Overview Table").

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

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 five Enterprise Attack Profile Sets. These sets consisted of attacks that are being used in the wild. These five profile sets each had three categories of profiles, 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 publicly available. Together, this test consisted of 156 Cobalt Strike attack profiles.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products					
	Checkpoint	Cisco	Fortinet		Palo Alto Networks	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
1. Basic Attack Scenario	**37.2%**	**22.4%**	**30.8%**	**30.8%**	**99.4%**	**99.4%**
Enterprise Attack Profile Set 1	25.9%	3.2%	9.7%	9.7%	100%	100%
Enterprise Attack Profile Set 2	16.7%	0.0%	16.7%	16.7%	100%	100%
Enterprise Attack Profile Set 3	0.0%	0.0%	0.0%	0.0%	100%	100%
Enterprise Attack Profile Set 4	59.0%	46.2%	56.4%	56.4%	97.4%	97.4%
Enterprise Attack Profile Set 5	40.0%	24.3%	32.9%	32.9%	100%	100%

Table 4: Overview Table Excerpt, Basic Attack Scenario by Toolset Used to Generate.

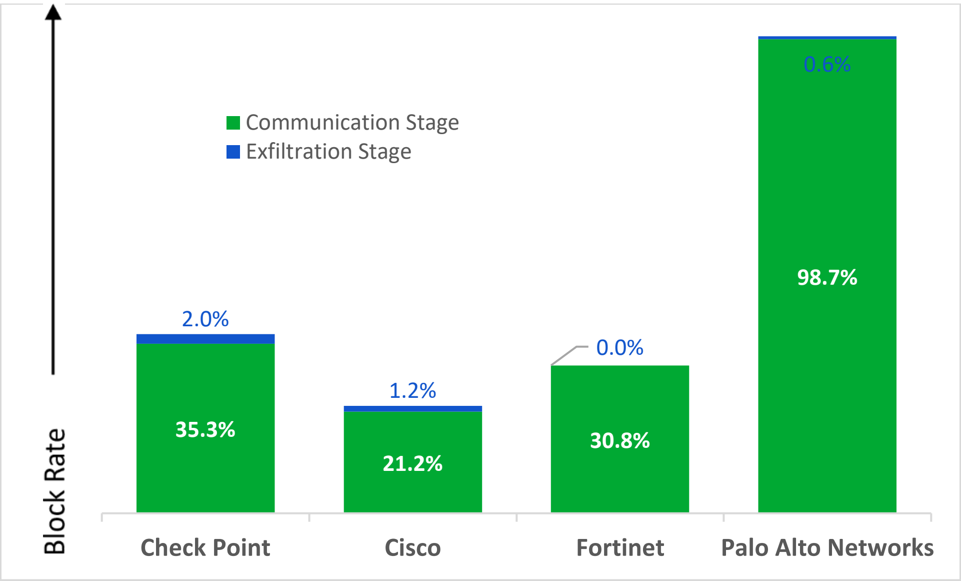


Figure 5: Block Rate for Basic Attack Scenario with Block Type Indicated.

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 five Enterprise Attack Profile Sets just discussed. The following table gives the total block rates by attack type.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products					
	Checkpoint	Cisco	Fortinet		Palo Alto Networks	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
1. Basic Attack Scenario	**47.3%**	**26.0%**	**36.7%**	**36.7%**	**99.7%**	**99.7%**
Normal Operational Attack Set	8.0%	4.0%	9.0%	9.0%	99.0%	99.0%
Crimeware Attack Set	64.0%	51.0%	57.0%	57.0%	100.0%	100.0%
APT Attack Set	70.0%	2.0%	44.0%	44.0%	100.0%	100.0%

Table 5: Basic Attack Scenario Block Rate by Attack Type

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 78 attacks.

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 51 attacks.

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 27 attacks.

The block rate of the tested firewalls by attack subcategory (Normal, Crimeware, APT) is shown visually in the table below. Because the Normal Operational Attack Set, the APT Attack Set, and the Crimeware Attack Set all consist of different numbers of attacks, the percentages in the table below added together and divided by three do not match the overall block rate in the Basic Attack Scenario.

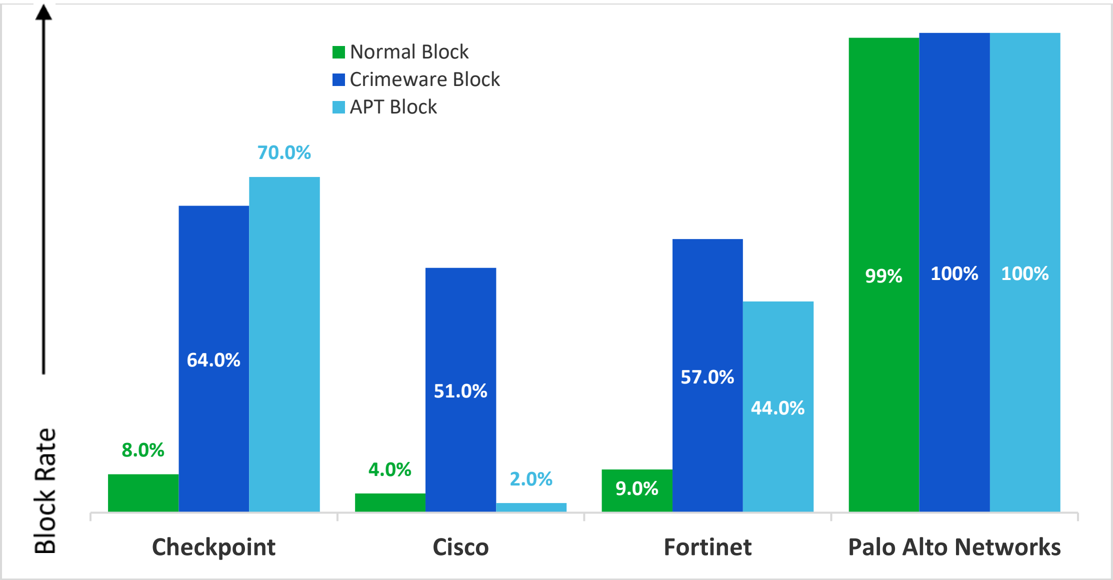


Figure 6: Overall Profile Block Rate for Basic Attack Scenario by Attack Type.

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 285 attack profiles in this test.

The Random Attack Scenario consisted of profiles that were generated by three 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, and Random Attack Test Set 3. The three toolsets used are not named because they are available in the wild, and our test results would show what vendors they are effective against.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products					
	Checkpoint	Cisco	Fortinet		Palo Alto Networks	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
2. Random Attack Scenario	**3.0%**	**2.0%**	**10.0%**	**10.0%**	**99.0%**	**99.0%**
Random Attack Test Set 1	0%	1%	0%	0%	100%	100%
Random Attack Test Set 2	1%	5%	16%	16%	98%	98%
Random Attack Test Set 3	9%	0%	12%	13%	100%	100%

Table 6: Overview Table Excerpt, Random Attack Scenario.

There was a small difference in prevention capability of Fortinet FG-301E and FG-VM04V. Because of rounding, the total percentage blocked for the FG-301E and FG-VM04V firewalls appears the same despite their breakdowns being slightly different. The following graph shows the overall block rate for each vendor within the Random Attack Scenario for each of the three Random Attack Sets. Because the three Random Attack Sets each had a different number of attack profiles, the sum of the percentages in the following graph divided by three does not equal the Random Attack Scenario block rate.

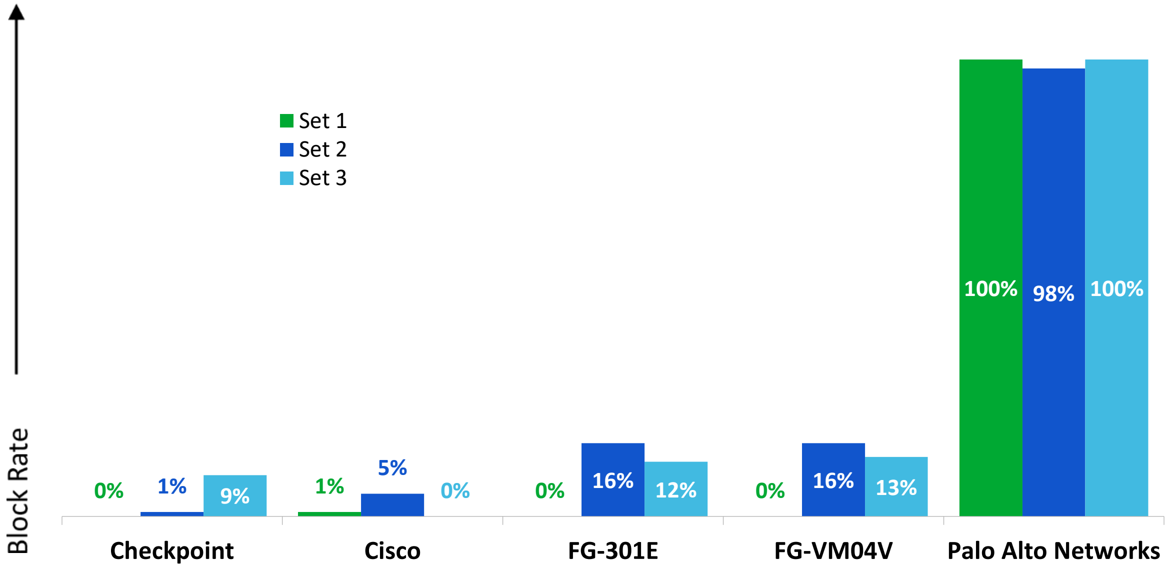


Figure 7: Random Attack Scenario Block Rate by Random Attack Set.

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 started with attacks that were previously blocked in the Basic Attack Scenario or Random Attack Scenario. 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. No attack was blocked by every firewall we tested. Custom Attack Profile 6 (name redacted) was blocked by none.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products					
	Checkpoint	Cisco	Fortinet		Palo Alto Networks	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
3. Custom Attack Scenario	**28.6%**	**14.3%**	**14.3%**	**14.3%**	**85.7%**	**85.7%**

Table 7: Overall Table Excerpt, Custom Attack Scenario.

It is possible to block some of these command-and-control attacks on the Domain Name System (DNS) and Uniform Resource Locator (URL) level. However, threat actors can seed these domains/URLs for a long time to make them look legitimate, and thus the entire attack might bypass these protections. Thus, for this test these capabilities were disabled should they be responsible for a block. That is, to simulate seeding, in some cases the firewalls' DNS and/or URL protections were disabled (e.g., newly observed domain category was set to monitor rather than block).

Because of the individualized nature of the test, the sample size was relatively small. SecureIQLab tested seven Cobalt Strike attack profiles in this test. Each attack was designed to test a specific aspect of the products' ability to block.

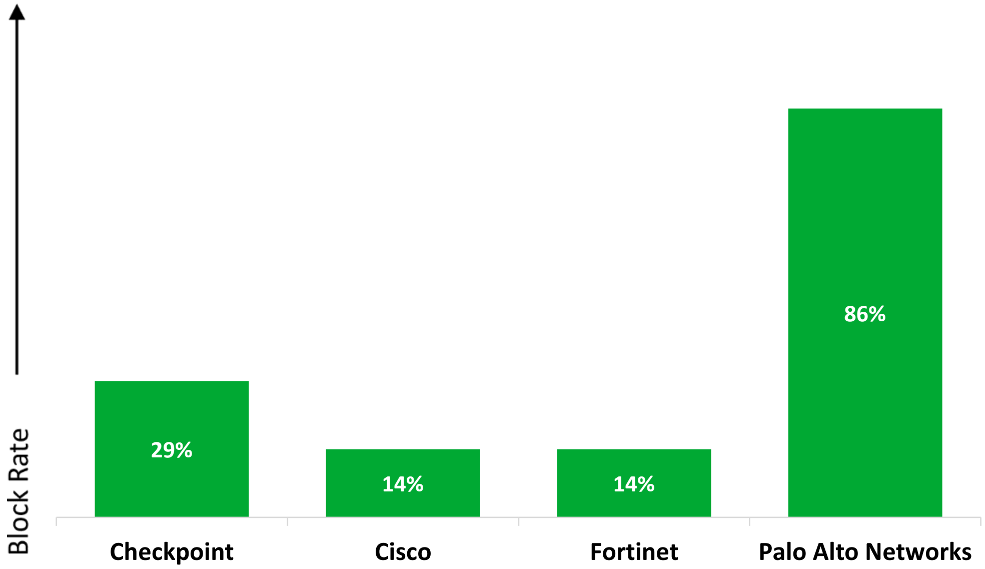


Figure 8: Custom Attack Scenario Block Rate.

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.

Nonstandard Ports 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 a different port to see if the evaluated firewalls maintained their prevention coverage for the same attacks when hosted on different ports. This test included 12 attacks.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products					
	Checkpoint	Cisco	Fortinet		Palo Alto Networks	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
4. Nonstandard Ports Attack Scenario	**100%**	**100%**	**16.7%**	**16.7%**	**100%**	**100%**

Table 8: Overview Table Excerpt, Nonstandard Ports Attack Scenario.

As the data table above shows, the firewalls we tested from Checkpoint, Cisco, and Palo Alto Networks were still able to consistently block the profiles that the firewalls had previously been able to block when attacks using those profiles were relaunched on a nonstandard port.

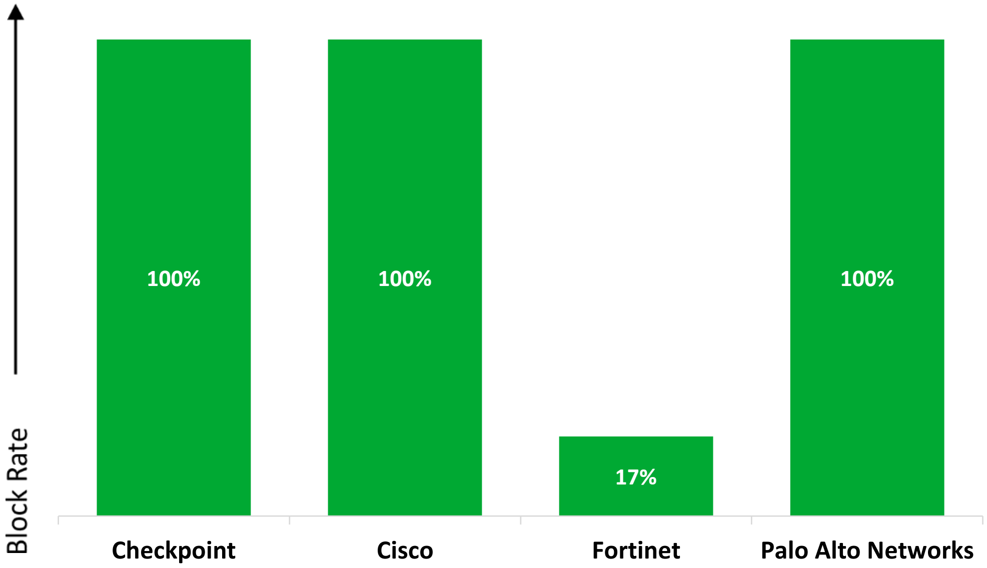


Figure 9: Nonstandard Port Attack Scenario Block Rate.

HTTPS Port-Based Attack Scenario Comparative Analysis

The purpose of this testing is to confirm if the next-generation firewalls provide the same level of protection when attacks are delivered via HTTPS. Over 80% of the Web traffic is SSL driven.

The HTTPS-based Attack Scenario consisted of profiles that used HTTPS rather than HTTP for communication. This included APT and Normal Operational attack profiles. In this test, we tested five Cobalt Strike attack profiles.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products					
	Checkpoint	Cisco	Fortinet		Palo Alto Networks	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
5. HTTPS-Based Attack Scenario	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

Table 9: Overview Table Excerpt, HTTPS-Based Attack Scenario.

Hostname Change Attack Scenario Validation

The Hostname Change Scenario consisted of profiles that were previously blocked by the product under test, except that the hostname being used for the attacks was changed. This test was intended to test coverage for attacks hosted on a different domain/host. A total of four test profiles were used.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products					
	Checkpoint	Cisco	Fortinet		Palo Alto Networks	
	SG5100	Firepower 4110	FG-301E	FG-VM04V	PA-460	PA-VM-Flex
6. Hostname Change Scenario	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**100%**	**100%**

Table 10: Overview Table Excerpt, Hostname Change Scenario.

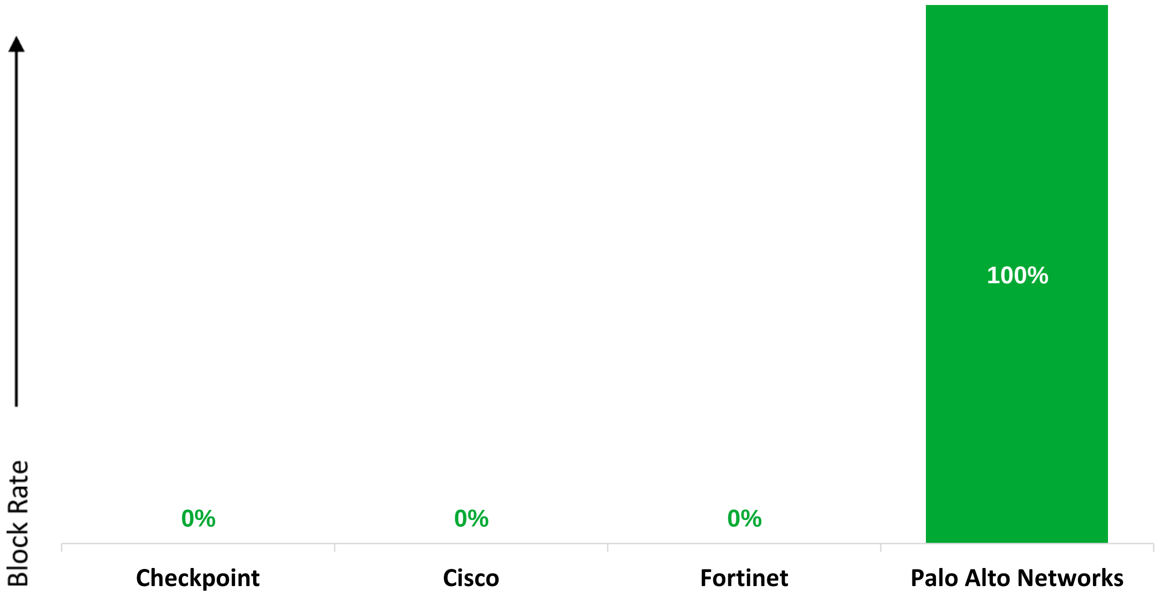


Figure 10: Hostname Change Scenario Block Rate.

8. Conclusion

In the six Cobalt Strike attack suite tests we performed, the Palo Alto Networks firewalls we tested were either the top performer or tied for top performance.

Going through the results of the tests in sequence, the Palo Alto Networks firewalls we tested performed better than the competition in the Basic Attack Scenario. The Palo Alto Networks firewalls managed to block 99.4% of attacks, while the next best performance was Checkpoint's firewall at 37.2%. In the Random Attack Scenario, Palo Alto Networks' firewalls blocked 99.0% of attacks. The next best performance was from Fortinet's firewalls, this time at 10.0% blocked.

Turning to the confirmation tests, in the Custom Attack Scenario the Palo Alto Networks firewalls each blocked 85.7% of attacks. The next best performance was from the Checkpoint firewall, which blocked 28.6% of attacks. The firewalls of Palo Alto Networks, Cisco, and Checkpoint all blocked 100% of attacks in the Nonstandard Ports Attack Scenario. All firewalls continued to block HTTPS-based attacks that were previously tested using HTTP. In the Hostname Change Scenario, only the Palo Alto Networks firewalls blocked attacks.

Overall, Palo Alto Networks performed well against the Cobalt Strike attack profiles we tested. Compared with the other products tested, Palo Alto Networks' machine learning-based model outperformed the competition by a significant margin in most of the Cobalt Strike tests we ran.

9. Appendix

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://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111303&partition=Basic&product=All
- https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202
- https://sc1.checkpoint.com/documents/Best_Practices/CP_R80.20_Best_Practices_for_Threat_Prevention/Content/Topics/Introduction.htm
- https://sc1.checkpoint.com/documents/R81.10/SmartConsole_OLH/EN/Topics-OLH/Home-Page.htm?tocpath=_____1
- https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Welcome.htm
- https://downloads.checkpoint.com/dc/download.htm?ID=103845

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
- https://secure.cisco.com/secure-firewall/v7.2/docs
- https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/031/original/Talos_Cobalt_Strike.pdf

Fortinet:

- https://docs.fortinet.com/document/fortigate/7.2.0/administration-guide/954635/getting-started
- https://docs.fortinet.com/document/fortigate/7.2.0/best-practices/587898/getting-started
- https://docs.fortinet.com/document/fortigate/6.4.0/best-practices/587898/best-practices

Palo Alto Networks:

- https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices

10. 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, LLC.
6001 W. Parmer Lane Ste 370, #970
Austin, TX 78704 USA

+1.512.575.3457

www.secureiqlab.com
info@secureiqlab.com

11. Copyright and Disclaimer

SecureIQLab cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper.

We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the research results cannot be taken by any representative of SecureIQLab. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time.

No one else involved in creating, producing, or delivering research results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, research documents or any related data.

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

SecureIQLab (November 2022)