Next-Generation Firewall with Wildfire

What are Next-Generation Firewalls?

Firewalls define network boundaries. A traditional firewall is designed to police the flow of internet traffic that comes in and out of a network, based on some predefined rules on port, protocol, source and destination IP address.

Traditional in this context means all the features that preceded Next-Generation Firewalls, such as -

- **Packet filtering** - Incoming and outgoing packets are inspected to make sure they fit or satisfy the filters set of rules before they are forwarded or dropped.
- **Virtual Private Network (VPN)** support.
- **Stateless** or **stateful** inspection.

NGFWs (Next-Generation Firewalls) have all of the traditional firewall functions - plus several more. NGFWs have more layers of security built into them, to protect against more sophisticated threats. Crucially, they go beyond the static inspection that traditional firewalls are limited to, instead having application-level control.

To understand this, let us take an example. Consider two airport security agencies. One agency inspects the passengers to make sure they are not on any no-fly lists, they are who they say they are, and that they're going to places the airport actually serves.

The other agency does all of this but also makes sure to inspect the passengers' items, in order to make sure they don't have any dangerous or disallowed items. This agency is able to detect threats that are not as obvious.

A traditional firewall is much like the first agency in the example; it blocks or allows data based on where it is going, where it comes from and whether or not it is part of a legitimate network connection. An NGFW is more like the second agency; it inspects the data on a deeper level to identify and block threats that may be hidden in what seems to be normal traffic.

Why do we need them?

Any firewall, traditional or Next-Generation, is a must as they are the first and primary line of defence against threats outside your own network. It acts as a barrier between your network and the public internet. It continuously monitors and filters incoming and outgoing network traffic to maintain the integrity and security of your infrastructure.

NGFWs take matters a step further as they're able to block a variety of advanced cyber threats, such as malware and application-layer attacks.

Unlike their traditional counterparts, which perform basic traffic filtering, NGFWs operate at Layer 7 of the OSI model, providing a more sophisticated and nuanced approach to network security.

Most internet traffic nowadays flows through the Hypertext Transfer Protocol (HTTP). As users browse the web, their browsers send HTTP requests to servers globally, receiving responses in return.

Additionally, substantial data packets originate from various business applications, such as file transfer protocol or web services like the X API. A Layer 3 firewall, operating at a lower level, may inadvertently permit breaches through these protocols, leaving many vulnerabilities that could be exploited by a malicious opponent.

This is where a Layer 7 firewall becomes indispensable. Unlike their Layer 3 counterparts, Layer 7 firewalls have the capability to inspect not only the protocol but also delve into the application layer, in a process known as payload inspection. While it is possible to have a Layer 3 firewall inspect the protocol and block known threats from certain URLs, if the threat comes from a URL that has not been reported and is socially engineered to hijack your data, things might prove difficult.

How do they work?

1. Packet Filtering: Like traditional firewalls, NGFWs filter network traffic based on predefined rules. These rules specify which packets are allowed or denied based on criteria such as source and destination IP addresses, port numbers, and protocols.

2. Stateful Inspection: NGFWs employ stateful inspection to keep track of the state of active connections. This means the firewall is aware of the state of the connection (e.g., whether it's part of an established session), allowing it to make more informed decisions about whether to permit or deny traffic.

3. Deep Packet Inspection (DPI): NGFWs go beyond traditional firewalls by incorporating deep packet inspection. This involves inspecting the actual content of data packets to identify the applications generating the traffic. This allows the firewall to make decisions based on the specific applications and services rather than just IP addresses and port numbers.

4. Intrusion Prevention System (IPS): NGFWs often include an intrusion prevention system to detect and prevent known and unknown threats. This involves analysing traffic for patterns that match known attack signatures and using heuristics to identify potentially malicious behaviour.

5. Application Awareness and Control: NGFWs can identify and control applications running on the network. This enables administrators to define policies based on specific applications, restricting or allowing access as needed.

6. User and Identity Awareness: NGFWs may integrate with identity management systems to associate network traffic with specific users or groups. This enables more granular control over access based on user identity.

7. VPN Support: Many NGFWs include Virtual Private Network (VPN) capabilities for secure remote access and site-to-site connectivity.

8. Logging and Reporting: NGFWs typically provide extensive logging and reporting capabilities. This allows administrators to monitor network activity, analyse security events, and generate reports for compliance purposes.

9. Threat Intelligence Integration: NGFWs often integrate with threat intelligence feeds to stay updated on the latest threats. This helps in proactively blocking known malicious IP addresses, domains, or signatures.

By combining these features, NGFWs provide a comprehensive security solution that helps organisations protect their networks from a wide range of cyber threats while also allowing for more fine-grained control over network traffic and applications.

SWOT Analysis

Strengths:

- **Deep Packet Inspection (DPI) -** DPI involves inspecting not only the header, but also the body for malware signatures and other potential threats. It compares the contents of each packet to known malicious attacks.
- **Application awareness -** Traditional firewalls analyse traffic at Layers 3 and 4 (OSI model). NGFWs, on the other hand, possess the capability to block or allow packets based on which application they are going to. They do so by analysing traffic at Layer 7, the application layer.
- **Intrusion Prevention -** NGFWs include intrusion prevention systems (IPS) as part of their DPI capabilities. IPSes can use various methods such as signature detection, statistical anomaly detection, and stateful protocol analysis detection to identify and block known and potential threats. This proactive approach to threat detection and prevention is a key strength of NGFWs.
- **Threat Intelligence -** NGFWs can utilise threat intelligence feeds from external sources to stay current on potential attacks and effectively prevent them. Threat intelligence provides information about potential attacks, including the latest malware signatures and IP reputation information. By leveraging threat intelligence, NGFWs can continuously update their defences and block the latest known threats, making them a formidable defence against evolving cyber threats.

Weaknesses:

- **NFGWs do more, so they cost more -** They require more and better resources to handle all the extra work it takes to inspect deeper into packets. Moreover, NFGWs require constant updates to the firewall's security features to keep it up to date for finding and blocking the ever-changing attack threats. This is called a firewall security subscription and it must be renewed periodically which adds another extra cost.
- **NFGWs work harder, so they need more processing power -** Performance issues are likely if the firewall is not to proper specifications for your needs. It is important to properly size your firewall for the speed of your internet circuit and the number of users behind the firewall. Sometimes users find that they need to turn off some security features to get the performance they need. This potential performance issue is not as likely with traditional firewalls.

- **NGFWs are more complex than traditional firewalls** - A traditional stateful firewall may need a quality technical resource to properly configure and maintain, while an NGFW requires even more. An NGFW demands more ongoing configuration and maintenance than a traditional stateful firewall.

Opportunities:

- **Regulatory Compliance** - Increasing regulatory requirements for data protection and privacy create opportunities for NGFW vendors to offer solutions that help organisations comply with various regulations.
- **Advanced Threat Intelligence** - Opportunities exist for NGFWs to leverage advanced threat intelligence, machine learning, and AI to stay ahead of evolving cyber threats.
- **Market Expansion** - The growing demand for advanced security solutions provides an opportunity for NGFW vendors to expand their market presence and cater to a wider range of industries.

Threats:

- **Budget Constraints** - Organisations facing budget constraints may hesitate to implement NGFWs due to their increased cost, limiting their adoption. These organisations may opt for cheaper traditional firewall solutions.
- **Integration difficulties -** Integrating NFGWs into existing network infrastructures may pose a threat, and increase the amount of attack vectors that a malicious opponent may use to breach the network. Integration requires very careful planning.
- **Human error** - NGFWs are extremely effective security tools, however they can still be undermined by the human factor, as users may fall victim to social engineering attacks or fail to follow best-practice security protocols.
- **Evolving cyber-threats** - Cyber threats are dynamic and are ever-evolving. NFGWs need to continuously adapt to new attack vectors and techniques.

Modern Tools Usage:

Palo Alto Networks WildFire is an advanced cloud-based malware prevention service that employs cutting-edge technologies to safeguard against evolving cyber threats. Leveraging a combination of machine learning and crowdsourced intelligence, WildFire specialises in detecting and preventing unknown and highly evasive malware variants.

- **Palo Alto Networks Next-Generation Firewall-**

  Description: An all-inclusive firewall solution with capabilities like application control, intrusion prevention, user and identity awareness, and more that goes beyond conventional firewalls.

  Usage: Installed at the edge of the network to keep an eye on and manage network traffic according to user, content, and application criteria.

- **Wildfire-**

  Description: Palo Alto Networks offers a cloud-based threat analysis solution that analyses unknown files both dynamically and statically in order to detect and stop advanced threats.

  Usage: Integrated with NGFWs to analyse suspicious files, detect malware, and provide threat intelligence for proactive security measures.

- **Panorama-**

  Description: The centralised management platform from Palo Alto Networks allows you to control several NGFWs from a single interface.

  Usage: Enables streamlined policy management, monitoring, and reporting across distributed networks.

- **Global Protect-**

  Description: A Palo Alto Networks VPN (Virtual Private Network) service that offers safe remote access to the company network.

  Usage: Ensures secure communication for remote users and branch offices, extending NGFW protection beyond the traditional network perimeter.

- **Threat Prevention Subscription-**

  Description: Additional subscriptions that enhance threat prevention capabilities by providing access to threat intelligence feeds, URL categorization, and other security services.

  Usage: Augments NGFW and WildFire capabilities with up-to-date threat intelligence and URL filtering.

- **URL Filtering-**

  Description: A Palo Alto Networks VPN (Virtual Private Network) service that offers safe remote access to the company network.

  Usage: Integrated with NGFWs to block access to websites that pose security risks, and often includes categorization based on WildFire verdicts.

- **User- ID-**

  Description: Integrates with identity management systems to associate network activity with specific users.

  Usage: Enhances security policies by allowing granular control over user-specific access and monitoring user behaviour on the network.

- **SSL Decryption-**

Description: Decrypts and inspects SSL/TLS-encrypted traffic to identify threats hidden within encrypted communication.

Usage: Improves visibility and threat detection by analysing encrypted traffic for potential security risks.

- **Auto Focus-**

  Description: A threat intelligence service that provides context around threats and enables targeted threat hunting.

  Usage: Integrates with NGFWs and WildFire to enhance threat detection and response by providing detailed threat intelligence.

- **Cortex XSOAR (formerly Demisto)-**

  Description: A security orchestration, automation, and response (SOAR) platform for incident response and automation.

  Usage: Integrates with NGFWs and WildFire to automate response actions based on identified threats, reducing manual intervention.

- **DNS Security-**

  Description: Monitors and filters DNS requests to prevent access to malicious domains and detect suspicious activities.

  Usage: Integrated with NGFWs to enhance security by blocking access to known malicious domains and identifying potential threats

To defend against a variety of cyber threats, these tools work together to provide a layered and proactive approach to cybersecurity that combines network security, threat analysis, and automation. Organisations' entire security posture and response capabilities are improved by the integration and cooperation of these instruments.

Wildfire

What is Wildfire?

Palo Alto Networks WildFire is an advanced cloud-based malware prevention service that employs cutting-edge technologies to safeguard against evolving cyber threats. Leveraging a combination of machine learning and crowdsourced intelligence, WildFire specialises in detecting and preventing unknown and highly evasive malware variants.

Some of its key Components are:

1. **Cloud-Based Protection:** WildFire operates in the cloud, utilising a centralised and constantly updated threat intelligence platform.
2. **Machine Learning and Crowdsourced Intelligence:**The service harnesses the power of machine learning to analyse and understand patterns associated with malware.Crowdsourced intelligence provides real-time data from a global network of users, enhancing the accuracy and timeliness of threat detection.
3. **Real-Time Prevention:**WildFire operates in real-time, proactively preventing up to 95% of unknown malware variants.The inline prevention mechanism ensures immediate action without compromising business productivity.
4. **Compatibility with Palo Alto Next-Generation Firewalls:**WildFire seamlessly integrates with Palo Alto next-generation firewalls, enhancing their capabilities in threat detection and prevention.
5. **Multi-Technique Approach:**The service employs a multi-technique approach that includes dynamic analysis (sandboxing), static analysis, and machine learning techniques.This comprehensive approach allows WildFire to detect and prevent file-based threats effectively.

Some Benefits of Firewall:

1. **Proactive Threat Prevention:**WildFire proactively prevents unknown threats, reducing the risk of infections and data breaches.
2. **Efficient Integration:**Compatible integration with Palo Alto next-generation firewalls streamlines deployment and ensures a cohesive security infrastructure.
3. **Operational Continuity:**The inline prevention mechanism enables swift action without causing disruptions to business productivity.
4. **Global Threat Intelligence:**Leveraging crowdsourced intelligence provides a global perspective on emerging threats, enabling timely responses.
5. **Adaptability to Evolving Threats:**WildFire's multi-technique approach allows it to adapt to the evolving nature of cyber threats, staying ahead of new and sophisticated attack vectors.

Why use Wildfire?

Adding to the benefits mentioned above, here are some more reasons companies should adapt to wildfire

1. Adaptive Threat Landscape:
Adversaries have access to advanced technologies, including cloud resources and machine learning, enabling the rapid development of sophisticated and polymorphic threats.

WildFire adapts to these advancements, providing dynamic and advanced threat prevention mechanisms.

2. Variability of Malware Attacks:
Many malware attacks are variations of basic attacks with changes to domains or techniques, making them appear as new threats.
WildFire's signatureless capability allows it to block up to 95% of unknown malware variants in real-time, preventing the spread of new and evolving threats.

3. Proliferation of New Threats:
The threat landscape is dynamic, with an alarming rate of 1,000 new threats emerging every five minutes, followed by up to 10,000 variants shortly thereafter.
WildFire provides timely and automated threat analysis to stay ahead of the rapid proliferation of new and unknown threats.

4. Real-Time Prevention:
Inline machine learning-based prevention within WildFire operates in real-time, stopping threats without the need for cloud analysis.
This ensures immediate protection and minimises the risk of organisations becoming the first victims of emerging threats.

5. Reduced Dwell Time:
WildFire's automated and coordinated protection across network, endpoint, and cloud minimises the time it takes to respond to threats.
This reduction in dwell time helps mitigate the potential impact of security incidents.

6. Efficient Security Operations:
By combining dynamic and static analysis, recursive analysis, and Multi-Vector Recursive Analysis (MVRA), WildFire reduces false positives and the workload for Security Operations Centers (SOCs).
SOC teams can focus on actionable events, enhancing overall efficiency in threat detection and response.

7. Cloud-Based Architecture:
WildFire's cloud-based architecture eliminates the need for deploying, managing, patching, and maintaining appliance-based sandboxes.
This reduces Total Cost of Ownership (TCO) while providing scalable and cost-effective threat analysis.

8. Seamless Threat Intelligence Integration:
WildFire seamlessly integrates threat intelligence into the Palo Alto Networks ecosystem.
This automated flow of threat intelligence eliminates the need for manual integrations, ensuring that security tools are always up-to-date.

How does Wild Fire Work?

WildFire employs a holistic approach to cybersecurity, utilising cutting-edge technologies to reduce the ever-evolving landscape of cyber threats.

1. Inline Machine Learning-Based Prevention:
WildFire features an inline machine learning-based engine integrated within both hardware and virtual ML-powered next-generation Firewalls (NGFWs). This unique inline approach allows the prevention of malicious content in common file types without the need for cloud analysis, ensuring real-time protection without compromising user productivity.

2. Signatureless Capability:
A hallmark of WildFire's efficacy is its signatureless capability, a feature that enables the blocking of a substantial percentage of unknown malware variants in real time. This is achieved through the implementation of innovative, signature-independent methods that operate seamlessly within the inline prevention framework.

3. Dynamic and Static Analysis:
WildFire combines dynamic and static analysis techniques to comprehensively scrutinise files and identify potential threats. Dynamic analysis involves the execution of files within a controlled environment, allowing for the observation of their behaviour. Simultaneously, static analysis examines the characteristics of files without actual execution, ensuring a thorough examination of potential risks.

4. Recursive Analysis:
The integration of recursive analysis within WildFire represents a strategic approach to combating highly evasive and memory-resident malware. By iteratively analysing files and their interactions, this technique uncovers concealed layers of threats that may otherwise elude traditional detection methods.

5. Multi-Vector Recursive Analysis (MVRA):
A pioneering aspect of WildFire's methodology is the implementation of Multi-Vector Recursive Analysis (MVRA). This comprehensive approach combines advanced file analysis with URL crawling, allowing WildFire to follow multiple stages of an attack. Even in instances where execution fails in a particular stage, MVRA provides a holistic view of a campaign over multiple stages, effectively thwarting complex, multistage attacks.

6. Protection Against Evolving Threats:
WildFire's multi-technique approach positions it as a formidable defence against evolving threats. It not only addresses known threats but also demonstrates the capability to prevent unknown and highly evasive modern malware variants. This adaptability ensures that WildFire remains a stalwart guardian in the face of the dynamic threat landscape.

Conclusion:
In conclusion, Palo Alto Networks WildFire’s efficacy in advanced threat prevention is rooted in its multifaceted approach. By seamlessly integrating machine learning, dynamic and static analysis, recursive analysis, and MVRA, WildFire not only identifies and prevents known threats but also excels in proactively countering unknown and evolving malware variants.

References

[1] D. Teplinskiy, “Why your business will need next generation firewall (NGFW),” AlphaCIS, https://www.alphacis.com/why-your-business-will-need-next-generation-firewall-ngfw/ (accessed Dec. 15, 2023).

[2] J. Thain, “Next generation firewalls: Do I need one? are they worth it?,” IntegriCom, https://integricom.net/next-generation-firewalls (accessed Dec. 15, 2023).

[3] A. Ot, “Are NGFWs Needed? Why You Need a Next-Generation Firewall,” Datamation, https://www.datamation.com/security/need-for-next-generation-firewalls/ (accessed Dec. 15, 2023).

[4] “What is a next-generation firewall?,” FS Community, https://community.fs.com/article/what-is-a-next-generation-firewall.html (accessed Dec. 15, 2023).

[5] “What is a next-generation firewall (NGFW)?,” Cloudflare, https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/ (accessed Dec. 15, 2023).

[6] “Palo Alto Networks | WildFire | Datasheet.” Available: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/wildfire