Beyond Application Visibility and Control: What an NGFW Must Be

What You Will Learn

Modern networks and their components are constantly evolving and traditional next-generation firewalls are not able to provide the level of protection organizations require.

In this paper you will learn:

- Why typical next-generation firewalls that focus primarily on application visibility and control offer an incomplete approach to threat defense
- What organizations need to defeat advanced threats in a resource-constrained environment
- What benefits you can gain with the Cisco Firepower™ Next-Generation Firewall (NGFW), the industry's first fully integrated, threat-focused NGFW

Introduction

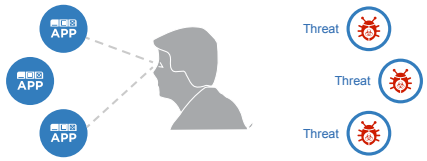
Digital transformation is happening on a massive scale and creating significant opportunities. More than 15 billion devices are now Internet connected, and this number is expected to grow to 500 billion by 2030.[1] This transformation is expected to generate an estimated $19 trillion opportunity for businesses worldwide over the next 10 years.[2] However, it also creates significant opportunities for cybercriminals. The global cybercrime market is currently estimated at $450 billion to $1 trillion.[3]

As modern networks and their components constantly evolve, the attack surface is expanding. Financially motivated attackers are adopting increasingly sophisticated methods to infiltrate networks and steal an ever-increasing volume of digitized assets. Once they infiltrate the network, they are difficult to detect. In fact, the industry median time to detect an advanced threat is approximately 100 days.[4]

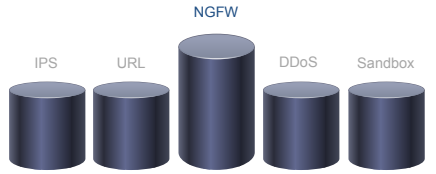
Today's Network Security Challenge

Security is foundational to seizing the emerging business opportunities that the digital economy and new business models create. The introduction of next-generation firewalls (NGFWs) was an important step forward, but typical NGFWs have focused heavily on application access control with scant attention paid to threat defense capabilities. This incomplete approach does little to protect you against the risks posed by sophisticated attackers and advanced malware. Worse, these NGFWs offer limited assistance once an organization does get infected, because they can't help you scope the infection, contain it, and remediate quickly.

Legacy NGFWs are focused too narrowly and are too hard to manage



Focused on apps, not threats



Another silo to manage

Organizations don't have the resources to add more products, or the security staff to manage the extra complexity this fragmented approach creates. In fact, resource constraints are the most commonly cited obstacle to adopting better security.[5] In addition, architectures based on these disconnected security services are brittle, inhibiting business growth due to operational inflexibility.

1. Cisco Internet of Things: http://www.cisco.com/web/solutions/trends/iot/indepth.html
2. http://ioeassessment.cisco.com/learn
3. RSA/CNBC: http://www.cisco.com/web/offer/emear/38586/images/Presentations/P16.pdf
4. Cisco 2016 Annual Security Report
5. Cisco 2016 Annual Security Report

What an NGFW Must Be

Organizations need more from their NGFW platforms. They need a next-generation firewall that:

- Focuses on threat effectiveness and provides protection across the entire attack continuum—before, during, and after an attack
- Fully integrates all the security services and event information into a single view and management platform
- Integrates with existing security investments to provide a sum greater than its parts

A next-generation firewall that meets these requirements not only provides value with precise application control, but also delivers real-world security effectiveness against the threats posed by sophisticated and evasive malware attacks. It allows organizations to streamline operations and to get more from their networks.

Introducing the Cisco Firepower NGFW

The Cisco Firepower Next-Generation Firewall (NGFW) is the industry's first fully-integrated, threat-focused NGFW. It moves beyond traditional NGFWs to provide complete, integrated protection for the entire attack continuum.

With Cisco Firepower NGFW, you now have an integrated security platform that goes far beyond application control. Its powerful correlation of multivector information facilitates the detection of evasive or suspicious activities and identifies hosts that exhibit signs of compromise early on. You can stop more threats, gain greater visibility into the network, detect and mitigate zero-day and targeted threats more quickly, automate critical tasks to better focus your organizational efforts, and get the most from existing resources.

Providing Complete Protection

Cisco Firepower NGFW includes the world's most widely deployed stateful firewalling technology along with next-generation IPS, advanced malware protection, application visibility and control, and reputation-based URL filtering. All these features come in a single appliance. All are managed by a rich, unified management console.

Cisco Firepower NGFW: Providing complete protection across the entire attack continuum

Stop More Threats

Deploy the industry's most effective threat protection for both known and emerging threats. Our NGFW incorporates an integrated sandbox solution and file prevalence and disposition to help identify and halt evasive targeted threats before they can do damage.

Gain More Insight

Gain visibility into the users, hosts, applications, mobile devices, virtual environments, threats, and vulnerabilities that exist in your constantly changing network. This information will help you defend your network. The NGFW automatically correlates threats and your network's vulnerabilities, so your security team can prioritize threats and focus on what matters most.

Detect Earlier and Act Faster

Mitigate advanced threats more quickly to shrink the time to detection and remediation from months to hours. Cisco completes the task in 17.5 hours.[6] Immediately understand the scope of malware infections, the path and behavior of file activity, and implement containment actions even before signatures become available.

Reduce Complexity and Simplfy Operations

Consolidate all security functions into one high-performance platform with a single management interface. The Cisco Firepower Management Center unifies, centralizes, and simplifies policy to ease the burden of administering defense-in-depth security architecture. It automatically analyzes network vulnerabilities and recommends protections to provide a responsive solution for today's dynamic and understaffed environments.

Get More from Your Network

Cisco Firepower NGFW integrates with other Cisco® security solutions such as the Cisco Identity Services Engine (ISE) for identity data and network segmentation, and OpenDNS for Internet-wide domain visibility. Intelligence, context, and policy controls are shared, making this approach effective, agile, and easier and less costly to manage. Automated network segmentation helps you rapidly contain threats. Global DNS and IP threat intelligence from Cisco Talos provide reputational threat indicators for early warning so that network security devices can prepare defenses before an attack arrives.

Cisco Firepower NGFW keeps customers safer, mitigates advanced threats faster, and streamlines operations better. Security becomes a growth engine to help you seize new business opportunities.

Learn More

For more information about the Cisco Firepower Next-Generation Firewall, please visit: www.cisco.com/go/ngfw

6. Cisco 2016 Annual Security Report

C11-736644-00 02/16