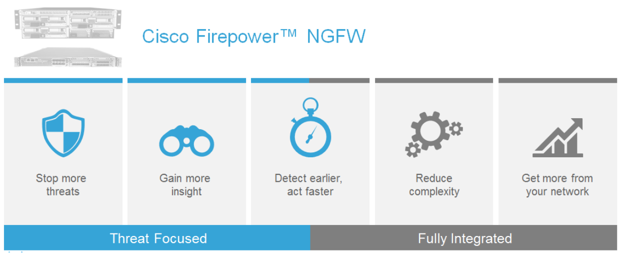
Cisco Security News Digest

8/29/2017 Issue 8

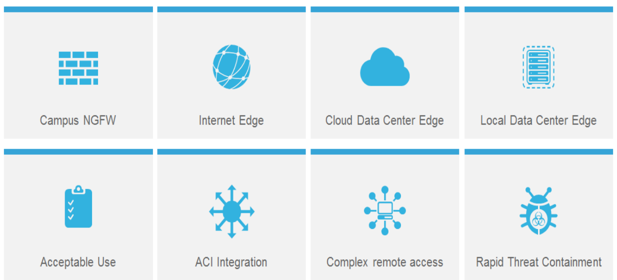
Cisco's threat focused Next - Generation Firewall platform

Cybersecurity attackers are finding new ways to profit criminal economy by morphing and adapting to today's dynamic business environment . Traditional method of keeping the bad guy out with static security controls on filtering ports, protocols or focusing on Web Applications alone are no longer sufficient. The only way to combat today's security threat is to address them holistically across the full attack continuum—before, during and after an attack. Next Generation Firewalls are critical points of security enforcement between different trust zones but in order to combat todays multi dimensional and dynamic threat landscape, NGFW's need to continue protecting before an attack, but also in the event of an attack - scope the incident, contain it and remediate it as well. Cisco's Firepower Next-Generation Firewall (NGFW) is industry's first fully integrated threat focused NGFW combating security threats across the full attack continuum at the perimeter zone. It delivers comprehensive, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection across the network all the way to the endpoint. By combining multiple layers of Security on a single platform, Cisco Firepower NGFW's architecture avoids complexity, provides effective contextual visibility and correlation, minimizes security gaps and lowers cost.

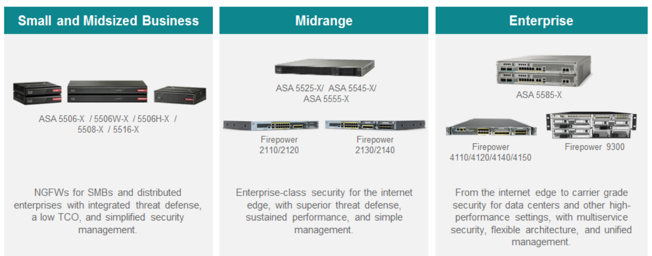
Cisco Firepower NGFW is a complete solution



Business-critical use cases



Cisco has an NGFW solution for every business

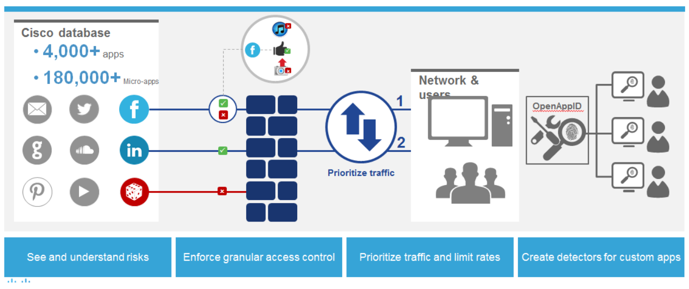

Small and Midsized Business
Midrange
Enterprise
ASA 5506-X / 5506W-X / 5506H-X / 5508-X / 5516-X
ASA 5525-X/ ASA 5545-X/ ASA 5555-X
Firepower 2110/2120
Firepower 2130/2140
ASA 5585-X
Firepower 4110/4120/4140/4150
Firepower 9300

Small and Midsized Business	Midrange	Enterprise
NGFWs for SMBs and distributed enterprises with integrated threat defense, a low TCO, and simplified security management.	Enterprise-class security for the internet edge, with superior threat defense, sustained performance, and simple management.	From the internet edge to carrier grade security for data centers and other high-performance settings, with multiservice security, flexible architecture, and unified management.

Combating and containing security threats are possible only if threats are visible in the first place. Cisco NGFW contextual awareness and Application Visibility and Control (AVC) detects multi-vector threats, eliminates visibility gaps in traditional defenses comprised of disparate point technologies. Cisco Next-Gen Firewall can also provide insight into users, mobile devices, client side applications, system details, vulnerabilities, threats, and URLs. OpenAppID- Cisco's open-source, application-focused detection language will enable you to custom create application detectors in addition to default application database.

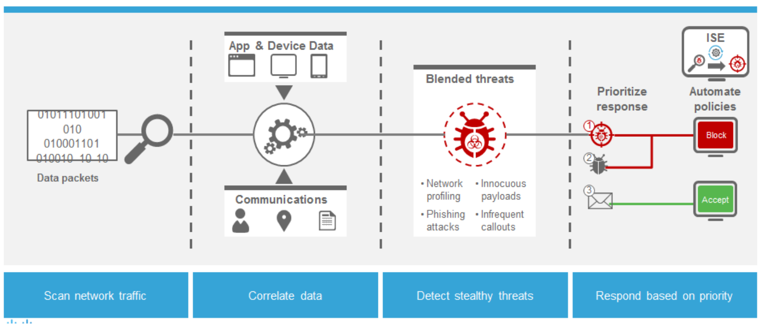
Provide next-generation visibility

Application Visibility & Control



Understand threat details and quickly respond

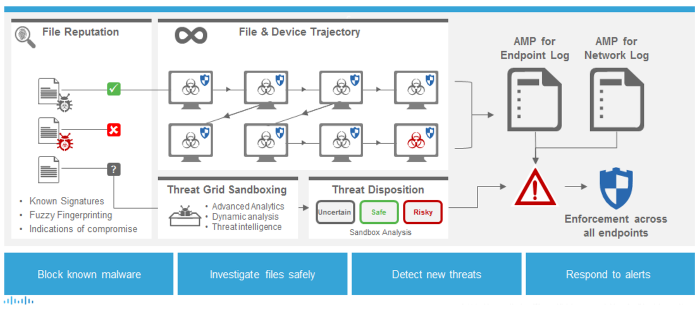
Next-Generation Intrusion Prevention System (NGIPS)



Enormous amount of intrusion event data will result in information overload on IT departments. Actionable and prioritized intrusion events are more valuable in streamlining operations. Intrusion events need to be automatically correlated while minimizing false positives. Cisco's NGIPS functionality continuously scans network traffic and correlates asset information with the vulnerabilities those assets contain and prioritize impacts. NGIPS can automatically determine the appropriate IPS rules to put in place to defend against the risks contained in the environment.

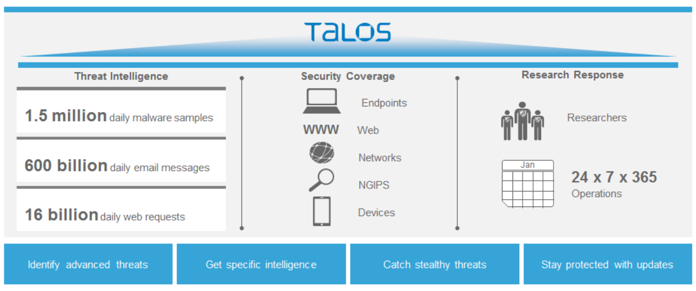
Uncover hidden threats in the environment

Advanced Malware Protection (AMP)



Advanced Malware Protection (AMP) functionality can contain known and unknown malware and breach activity with AMP's large scale analysis and automated models. Dynamic analysis could be done for any unknown files in a secure ThreatGrid sandbox for deeper investigation. Point-in-time signature based protection alone will not address the variants of malware today. With AMP's unique Continuous protection and Retrospection feature, malware detection and response is enabled at malware point of entry, propagation and post infection remediation addressing both during and after attack continuum.

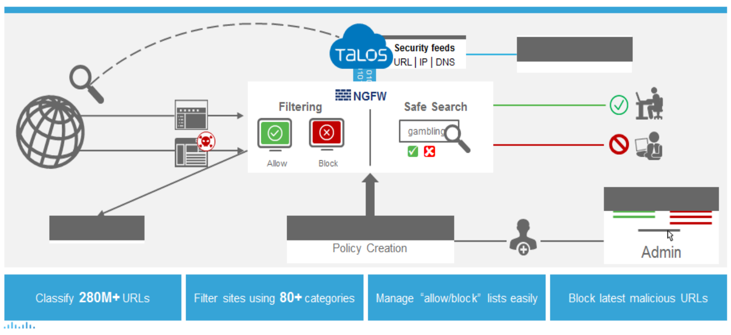
Get real-time protection against global threats


Talos
Threat Intelligence
1.5 million daily malware samples
600 billion daily email messages
16 billion daily web requests
Security Coverage
Endpoints
WWW
Web
Networks
NGIPS
Devices
Research Response
Researchers
Jan
24 x 7 x 365
Operations
Identify advanced threats
Get specific intelligence
Catch stealthy threats
Stay protected with updates

Cisco Talos - feeds intelligence and provides visibility into the most advanced threats before it can harm your network with its reputation scoring , blacklists, industry leading research team.

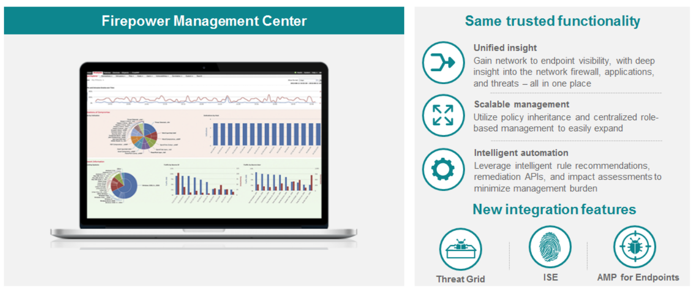
Block or allow access to URLs and domains

Web controls



URL filtering on Cisco NGFW makes it easy to minimize your exposure to web-based threats. Access control can be as broad or specific as needed to restrict access to harmful or inappropriate sites. You can also block sites and subsites based on the category instead of specific name or keyword

Firepower Management Center- Centralized security administration and automation



Same trusted functionality

Unified insight
Gain network to endpoint visibility, with deep insight into the network firewall, applications, and threats – all in one place

Scalable management
Utilize policy inheritance and centralized role-based management to easily expand

Intelligent automation
Leverage intelligent rule recommendations, remediation APIs, and impact assessments to minimize management burden

New integration features

For further details visit : https://www.cisco.com/go/ngfw

For more information on Cisco Security solutions and products, please contact your **Cisco Account Manager**

Suggestions/comments on this newsletter contact
Joby James at joby@cisco.com

Cisco Systems, Inc. 170 West Tasman Drive, San Jose, California 95134