At-a-Glance

Benefits

- **Stop more threats,** both known and unknown, with the industry's most effective threat protection
- **Rapidly detect, contain, and remediate** advanced malware attacks
- **Gain more insight** into and protection over the users, applications, devices, and vulnerabilities in your network
- **Enable "virtual patching"** of network vulnerabilities through vulnerability-targeted IPS rules until permanent fixes can be deployed
- **Choose a passive or inline deployment** with fail-to-wire network interfaces

Cisco Firepower NGIPS

Integrated Network Threat Appliances

Network Security for the Threats You Face

It's no secret that today's advanced attackers have the resources, expertise, and persistence to compromise any organization at any time. As attackers become more sophisticated and exploit a growing set of attack vectors, traditional defenses are no longer effective.

Safeguarding your network assets and data from today's threats requires detailed visibility into all your network layers and resources. This is a particular challenge with dynamic IT applications and in hybrid data center environments where users, hosts and workloads are constantly changing.

Fortunately, there is a solution – Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS) threat appliances.

Cisco Firepower NGIPS provides the contextual awareness you need to properly evaluate the users, hosts, files, and applications running in your network or wherever they may execute. This deep visibility enables you to more rapidly detect advanced threats and mount an agile defense.

The Cisco Firepower NGIPS threat appliance provides industry leading threat efficacy against both known and unknown threats. Threats are stopped using:

- Over 30,000 IPS rules that identify and block attack traffic targeting a vulnerability in your network
- A tightly integrated defense against advanced malware attacks incorporating advanced analysis of network and endpoint activity
- Reputation-based IP, URL and DNS security intelligence that reduces risks by identifying known malicious sites
- An integrated sandboxing technology that uses hundreds of behavioral indicators to identify zero-day and evasive attacks
- Indications of Compromise (IoC) that identify possibly compromised hosts through the correlation of multiple events from multiple sources

In independent tests conducted by NSS Labs, a leading security research and advisory authority, Cisco Firepower NGIPS has consistently achieved high marks for its security effectiveness, superior throughput, evasion free protection and class-leading low Total Cost of Ownership.

In addition, Cisco Firepower NGIPS delivered the fastest time to detection (TTD) of all the solutions tested. It was able to detect over 96% of advanced threats in less than 5 minutes. Providing fast TTD drastically reduces the exposure window and enables you to stop infections before they can spread or do damage.

Cisco Firepower Management Center delivers unified management over Firepower NGIPS, Firepower NGFW and Firepower Threat Defense for ISR deployments. This results in consistent policy and less complexity, correlating the views of your extended enterprise in a single console, from branch to datacenter to cloud, across network and endpoint.

Next Steps

To learn more about Cisco Firepower NGIPS threat appliances, please visit http://www.cisco.com/go/ngips.

To learn more about the Cisco Advanced Malware Protection capability, please visit http://www.cisco.com/go/amp.

To learn more about Cisco's Talos Security Intelligence and Research team, please visit http://www.talosintelligence.com/.

Get Better Protection Against Today's Threats

Cisco Firepower NGIPS threat appliances deliver:

- **Real-time contextual awareness:** Gain deep insight into your network devices, applications, users, operating systems, files, and more. Use this information to better understand network behavior, identify out-of-compliance situations, and evaluate intrusion events.
- **Advanced threat protection:** Protect against the latest threats and advanced malware with industry-leading threat prevention as validated by independent third- party testing and thousands of satisfied customers around the world. Address known and unknown threats through a fully integrated advanced malware protection and sandbox solution. Discover, track, and block the progression of suspicious files and malware to prevent the spread of outbreaks and reinfection.
- **Intelligent security automation:** Identify the threats that matter the most by automatically correlating intrusion events with the target's vulnerabilities. Implement better security by analyzing your network's weaknesses and generating the appropriate protection policies to put in place. Speed up forensic analysis by linking users to events and rapidly contain threats with an automated remediation workflow and integration with Cisco's Identity Services Engine (ISE) solution.
- **World-class security intelligence:** Cisco's Talos Security Intelligence and Research team detects and correlates threats in real time using the largest threat detection network in the world. Their efforts result in vulnerability-focused IPS rules and embedded IP-based, URL-based, and DNS-based security intelligence for Firepower NGIPS.
- **High performance and scalability:** Cisco Firepower 4100 Series and 9300 appliances provide high throughput, modular design, and carrier-class scalability with purpose-built appliances. They incorporate a low-latency, single-pass design.
- **Granular application control and URL filtering:** Reduce the surface area for attack through precise control of more than 4000 applications and hundreds of millions of URLs in over 80 categories.

C45-737897-00 10/16