Modernize your NGIPS

It can be tempting to hold on to older security products you have deployed in your network. Not modernize them when you have the opportunity because you need to cut costs. But continuing to rely on older products may have a detrimental effect to your business.

Your business is changing so your security needs to change too. Security threats will continue to be a problem. Your business will continue to grow and change. All these factors require your security to evolve and stay current with the times to meet the needs of your business.

Be vigilant – As cyberattacks evolve, you need to continually evolve your defenses with the latest levels of protection and threat intelligence to cover new threats and vulnerabilities. It's no secret that today's attackers have the resources, expertise, and persistence to compromise any organization at any time.

Get Fast and reliable performance – The latest hardware offers greater and more dependable performance. Older hardware becomes less and less reliable over time. Don't let outdated hardware slow down your operations or be the reason for network downtime.

Designed and optimized for better security

Performance and Hardware Design

- Sustained throughput performance when IPS threat inspection is enabled
- Reliable hardware dilivers exceptional security inspection and performance
- Fail to Wire provides enhanced network uptime and reliablity

For new features and bug fixes – Your older products may no longer be supported with new software releases, so no new features or bug fixes will be available. Product support may be an issue. Everyday network changes may become a hassle, forcing you to develop workarounds.

Setting the Stage:
Technology-driven business innovation

IT is enabling business growth

- Networks are increasingly complex and distributed
- Security must enable business growth and expansion
- Security needs to evolve and support the business

CXX-XXXXXX-00 XX/XX

How do I begin: It's as easy as 1, 2, 3.

1. Confirm your current IPS model and refresh needs.
2. Review the recommended migration path.
3. Contact your trusted Cisco Security account manager or partner to get started.

Migration Recommendations

FirePOWER 7000, 8000 Series Migration

FirePOWER 7000 8000 Series	Cisco Firepower NGIPS
FirePOWER 8350	Firepower 9300 SM 44
FirePOWER 8360	Firepower 9300 SM 44 - 3 Blade Cluster
FirePOWER 8370	Firepower 9300 SM 44 - 4 Blade Cluster
FirePOWER 8390	Firepower 9300 SM 36 - 6 Blade Cluster
FirePOWER 8120	Firepower 4110
FirePOWER 8130	Firepower 4110
FirePOWER 8140	Firepower 4120
FirePOWER 7050	Firepower 2130
FirePOWER 7110	Firepower 2130
FirePOWER 7115	Firepower 2130
FirePOWER 7120	Firepower 2130
FirePOWER 7125	Firepower 2130

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