Document ID: 118521

Updated: Dec 04, 2015

Contributed by Nazmul Rajib, Cisco TAC Engineer.

Related Products

- Cisco FirePOWER 7000 Series Appliances
- Cisco FireSIGHT Management Center
- Cisco FireSIGHT Management Center Virtual Appliance

Contents

Introduction

When you migrate a Sourcefire appliance from Version 4.10 to Version 5.2, some of the configurations, policies, and features are migrated. After you or upgrade your appliance from 5.2 to any latest version, the terminologies change, as the Version 5.3.1.1 introduces the ability to manage Cisco ASA with FirePOWER Services using a FireSIGHT Management Center. This article provides you a guideline about the new features and terminologies.

Migration from 4.10.x to 5.2

> **Note**: In order to migrate a Sourcefire appliance to Version 5.2, it must be running software version 4.10.3.5 or higher.

Key 5.2.x Features

Software Version 5.2 introduces the following new features:

Features Supported in 5.2.x *	Series 2 Appliances	FirePOWER Appliances

Improved User Interface / Dashboards	Yes	Yes
Expanded Application Classification	Yes	Yes
Enhanced IPS Events/Policy (See notes)	Yes	Yes
FireSIGHT (RNA/RUA Bundled)	Yes	Yes
Threat Prevention / IPS	Yes	Yes
Custom Reporting	Yes	Yes
Full IPv6 Support (GUI/Policy/FireSIGHT)	Yes	Yes
Application Control / URL Filtering		Yes
IP Reputation Blocking		Yes
File Type / Malware Cloud Lookup & Blocking		Yes
Geolocation		Yes
Routing, Switching, NAT		Yes
Site-to-Site VPN		Yes

Additional licenses may be required to enable the new features in 5.2.x.

Migration of Various Features, Configurations and Policies

Feature	4.10.3.5	5.2.0
License Related	Real-time Network Awareness (RNA)	FireSIGHT license is required to enable this feature. Legacy RNA & RUA licenses may be supported. However, Sourcefire does not recommend exceeding the User limits that are matched to the hardware capabilities of Defense Centers.
	Real-time User Awareness (RUA)	
	Intrusion Prevention System (IPS)	PROTECT license is required for series 3 managed devices.
IPS Related	Intrusion Policies	Access rules are created for applied intrusion policies. All intrusion policies are migrated.
	Local Intrusion Rules	All local rules are migrated. Can be enabled using the Access Control rules.
	RNA Detection Policies	Network Discovery and Access Control rules will be created for applied RNA detection policies.
RNA Related	RNA Settings in the System Policies	RNA related system policy settings will be migrated to Network Discovery. No other system policy will be migrated.
	Netflow Devices in System Settings	Netflow devices will be migrated to Network Discovery. No other system setting information will be migrated.
Traffic Related	Compliance Policies	Compliance policies, rules and traffic profiles will be migrated.
	White List	White lists will not be migrated.
	PEP Policies*	Access Control rules will be created for applied PEP policies.
Interface Related	Interface Sets and Detection Engine	Security Zones will be created for interface sets which are used by a detection engine with an applied policy of any type.

** PEP was a feature in Version 4.10.3 that allowed you to create rules to block or send traffic directly through some 3D Sensors with no further inspection.*

Migration from 5.2 to 5.3.1.1 or Higher

Changes to Terminology

Previous Terminology	Version 5.3.1 Terminology
Sourcefire 3D System	FireSIGHT System
Sourcefire Defense Center	FireSIGHT Management Center / Defense Center

Sensor / Managed Device	FireSIGHT Managed Device

New Terminologies on 5.3.1 or Higher

New Terminology	Description
ASA FirePOWER Module	Refers to the hardware and software modules installed on compatible Ci ASA hardware
Cisco ASA with FirePOWER Services	Refers to ASA device with the ASA FirePOWER module installed

Related Documents

- **Supported Features and Capabilities of Various Hardware Models of FireSIGHT System**
- **Cisco Firepower Compatibility Guide**
- **Technical Support & Documentation - Cisco Systems**

Related Cisco Support Community Discussions

The Cisco Support Community is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers.

Refer to Cisco Technical Tips Conventions for information on conventions used in this document.