Release Notes for the Cisco Cyber Threat Defense Solution Version 1.1

May 24, 2013

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Introduction 3
New Features; Supported Hardware and Software 3
Caveats 4
Related Documentation 4

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Introduction

The Cisco Cyber Threat Defense Solution improves detection and remediation of advanced cyber threats within the Cisco network by combining the following elements:

- Unique interior network traffic telemetry using the scalable unsampled NetFlow capabilities of Cisco Catalyst® switches, Cisco routers, and Cisco NetFlow Generation Appliances, as well as NetFlow Security Event Logging from Cisco ASA 5500 Series Next Generation Firewalls.
- Network traffic analysis capabilities provided by the Lancope StealthWatch products. Cisco has partnered with Lancope to jointly develop and offer the Cisco Cyber Threat Defense Solution.
- Contextual information, including user and device identity from the Cisco Identity Services Engine (ISE), NAT translation from Cisco ASA firewalls, and Network-Based Application Recognition (NBAR) from Cisco routers.

New Features; Supported Hardware and Software

New Features Supported in StealthWatch 6.3

Lancope StealthWatch 6.3 adds the following new capabilities to the Cisco Cyber Threat Defense Solution:

- Support for NetFlow export from Cisco NetFlow Generation Appliances and Cisco ASR 1000 Series routers
- New threat defense dashboards
- NAT stitching for ASA firewalls and ASR 1000 Series routers
- Improved caching of ISE identity information
- Support for redundant ISE Monitoring and Troubleshooting nodes

Solution Components

Tables 1 and 2 list hardware and software components of the Cisco Cyber Threat Defense Solution 1.1.

Table 1. Cisco Catalyst Switches Capable of Line-Rate, Unsampled NetFlow

Model	Hardware Required	Recommended Cisco IOS® Software Version
Catalyst 3560-X and 3750-X	Cisco Service Module	15.0.1-SE
Catalyst 4500 Series	Supervisor Engine 7-E or 7L-E	15.1.1-SG (IOS-XE 3.2 SG)
Catalyst 6500 Series	Supervisor Engine 2T	12.2-50-SY

Additional information regarding Cisco Catalyst switches and Cisco NetFlow can be found at http://www.cisco.com/go/catalyst and http://www.cisco.com/go/netflow.

Table 2. Recommended Software for Different Cisco Platforms

Platform	Recommended Software Version
Cisco Integrated Services Routers	Cisco IOS Software Release 15.1(2)T3
Cisco ASR 1000 Series Aggregated Services Routers	Cisco IOS XE Software Release 3.7S Cisco IOS Software Release 15.2(4)S
Cisco ASA 5500 Series Adaptive Security Appliances	Cisco ASA Software Release 8.4.3
Cisco Identity Services Engine	Cisco ISE Release 1.1.2
Cisco NetFlow Generation Appliance	Cisco NGA Release 1.0 (1)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Caveats

ISE API Performance with Large Numbers of Endpoints

In Cisco ISE Software 1.1, the response time of the ISE Representational State Transfer (REST) API may degrade with large (in excess of 20,000) numbers of endpoints in the ISE session database. Care should be exercised when integrating StealthWatchinto such a deployment.

Release Notes for Component Products

Please consult the product release notes for product-specific caveats regarding any Cisco products integrated with the Cyber Threat Defense Solution (Table 3).

Table 3. Release Notes for Component Products

Component	Release Notes
Cisco Catalyst 3560-X/3750-X with C3KX-SM-10G Service Module	http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/15.0_1_se/release/notes/OL25302.html
Cisco Catalyst 4500 with Supervisor Engine 7-E or 7L-E	http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_24726.html
Cisco Catalyst 6500 with Supervisor Engine 2T-10GE	http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/release/notes/ol_20679.html
Cisco Integrated Service Router G2 Series	http://www.cisco.com/en/US/docs/ios/15_1/release/notes/151-2TCAVS.html
Cisco Aggregated Service Router 1000 Series	http://www.cisco.com/en/US/docs/routers/asr1000/release/notes/asr1k_rn_rel_notes.html
Cisco ASA 5500 Series Adaptive Security Appliances	http://www.cisco.com/en/US/docs/security/asa/asa84/release/notes/asarn84.html
Cisco Identity Services Engine	http://www.cisco.com/en/US/docs/security/ise/1.1.1/release_notes/ise111_rn.html
Cisco NetFlow Generating Appliance	http://www.cisco.com/en/US/docs/net_mgmt/netflow_generation/1.0/release/notes/nga1relnote.html

Related Documentation

Design and implementation guides and other reference materials are available at http://www.cisco.com/go/threatdefense.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C85-728320-00 05/13

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.