Cisco Cyber Threat Defense Solution 1.1

How-To Guide: ASR 1000 Series NetFlow Configuration

Guide

May 2013

Introduction

What is the Cisco Cyber Threat Defense Solution?

The network security threat landscape is ever evolving, but always at the cutting edge are custom-written, stealthy threats that evade traditional security perimeter defenses. The Cisco® Cyber Threat Defense Solution provides greater visibility into these threats by identifying suspicious network traffic patterns within the network interior. These suspicious patterns are then supplemented with contextual information necessary to discern the level of threat associated with the activity.

The Cisco Cyber Threat Defense Solution, jointly developed and offered with Lancope®, leverages Cisco networking technology including NetFlow®, Network Based Application Recognition (NBAR), and the Identity Services Engine to provide visibility and context to allow the identification of suspicious traffic patterns within the network interior. The level of visibility and context provided can allow security analysts to detect targets, potential damage, and threatening behavior such as:

- Network reconnaissance
- Interior network malware proliferation
- Command and control traffic
- Data exfiltration

About This Document

This document describes deployment, implementation, and usage best practices in incorporating Cisco ASR 1000 Series Routers as an effective source of visibility and context as part of the Cisco Cyber Threat Defense Solution. This document assumes that the reader has a working familiarity with the Cyber Threat Defense Solution and has at least read the **Introduction to the Cisco Cyber Threat Defense Solution How-To Documents**.

Design Considerations

Flexible NetFlow support on ASR 1000 Series routers adheres to the platform-independent implementation of NetFlow as documented in IOS guides. NetFlow support on the ASR takes the traditional NetFlow approach of collecting information and generating a NetFlow record for flows that cross a Layer 3 boundary. This makes the ASR a key component in providing visibility into flows that traverse different areas of the network.

Additionally, the ASR 1000 contains software-supported Network-Based Application Recognition (NBAR) fully integrated with NetFlow services. If enabled, NBAR can perform deep packet inspection on packets traversing an interface to recognize and classify the application that is generating the traffic (for supported protocols). The application classification of the traffic set can be exported in a NetFlow record.

Because NetFlow and NBAR are implemented as software services on the ASR 1000 Series, care should be taken when deploying these features, as they can have an impact on device performance.

Configuring NetFlow Export

Procedure 1: Configure the Flow Record.

The flow record configuration defines which data fields will be collected for each flow.

Step 1. Create a flow record using the following key and non-key fields.

```
ASR(config)#flow record CYBER_ASR_RECORD
ASR(config-flow-record)#match ipv4 tos
ASR(config-flow-record)#match ipv4 protocol
ASR(config-flow-record)#match ipv4 source address
ASR(config-flow-record)#match ipv4 destination address
ASR(config-flow-record)#match transport source-port
ASR(config-flow-record)#match transport destination-port
ASR(config-flow-record)#match interface input
ASR(config-flow-record)#collect routing next-hop address ipv4
ASR(config-flow-record)#collect ipv4 dscp
ASR(config-flow-record)#collect ipv4 ttl minimum
ASR(config-flow-record)#collect ipv4 ttl maximum
ASR(config-flow-record)#collect transport tcp flags
ASR(config-flow-record)#collect interface output
ASR(config-flow-record)#collect counter bytes
ASR(config-flow-record)#collect counter packets
ASR(config-flow-record)#collect timestamp sys-uptime first
ASR(config-flow-record)#collect timestamp sys-uptime last
ASR(config-flow-record)#collect application name
```

Taking advantage of the NetFlow version 9 formatting and the ASR's role as a Layer 3 boundary allows the collection of many Layer 3 and 4 fields that are not always available on switch-based implementations of NetFlow, such as Time-To-Live values, TCP flags and next-hop addresses.

Note that the above flow record enables the collection of the name of the application from NBAR using the "**collect application name**" option. If NBAR is not being run, this line may be omitted.

Note: NBAR services can impact the performance of the router; while the collection of the application name is of great value in the Cisco Cyber Threat Defense Solution, enabling NBAR services must be done carefully.

Procedure 2: Configure the Flow Exporter.

The flow exporter configuration defines where flow records will be sent (the FlowCollector), including destination IP address and port.

Step 1. Define the exporter.

```
ASR(config)#flow exporter CYBER_EXPORTER
```

Step 2. (Optional) Add a description.

```
ASR(config-flow-exporter)#description Lancope StealthWatch FlowCollector for
the Cisco Cyber Threat Defense Solution
```

Step 3. Define the source.

```
ASR(config-flow-exporter)#source Loopback 1
```

This setting is the IP address that the switch will use as the source of the NetFlow export records. The best practice is to define a loopback interface (Loopback 1 in the example shown) with an IP address on a management VLAN and use that interface as the source. Note that the loopback interface must be configured before it can be used as a flow export source.

Step 4. Define the destination IP address.

```
ASR(config-flow-exporter)#destination ip-address-of-FlowCollector
```

Step 5. Define the transport protocol.

```
ASR(config-flow-exporter)#transport udp 2055
```

Best Practice: NetFlow is usually sent over UDP port 2055.

Procedure 3: Create the Flow Monitor.

The flow monitor represents the device's memory resident NetFlow database, and links together a flow record and flow exporter configuration.

Step 1. Define the flow monitor.

```
ASR(config)#flow monitor CYBER_MONITOR
```

Step 2. (Optional) Add a description.

```
ASR(config-flow-monitor)#description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution
```

Step 3. Configure the flow record.

```
ASR(config-flow-monitor)#record CYBER_ASR_RECORD
```

Step 4. Configure the exporter.

```
ASR(config-flow-monitor)#exporter CYBER_EXPORTER
```

Step 5. Define the active timeout.

The active timeout refers to how often NetFlow records are generated for flows that are still active. It is recommended that a value of 60 seconds be used.

```
ASR(config-flow-monitor)#cache timeout active 60
```

Step 6. Define the inactive timeout.

The inactive timeout refers to the time period in which flows that are inactive (not transmitting data) but still resident in the cache are timed-out of the cache. It is recommended that a value of 15 seconds be used.

```
ASR(config-flow-monitor)#cache timeout inactive 15
```

Procedure 4: Apply the Flow Monitor to an interface.

The flow monitor should be applied to all routing interfaces and sub-interfaces.

Step 1. Enter interface configuration mode

```
ASR(config)#interface GigabitEthernet 0/0/0
```

Step 2. Apply the Flow Monitor on ingress traffic

```
ASR(config-if)#ip flow monitor CYBER_MONITOR input
```

Procedure 5: Verify.

Step 1. Check the configuration using show commands

```
ASR#show run flow [exporter|monitor|record]
```

Step 2. Verify that NetFlow records are being exported form the appliance and are being received by the FlowCollector. (Refer to the Design and Implementation Guide for details.)

Final Configuration

```
!
flow record CYBER_ASR_RECORD
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 collect routing next-hop address ipv4
 collect ipv4 dscp
 collect ipv4 ttl minimum
 collect ipv4 ttl maximum
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect application name
!
!
flow exporter CYBER_EXPORTER
 description Lancope StealthWatch FlowCollector for the Cisco Cyber Threat
Defense Solution
 destination <ip-address>
 source loopback 1
 transport udp 2055
!
!
flow monitor CYBER_MONITOR
 description Main NetFlow Cache for the Cisco Cyber Threat Defense Solution
 record CYBER_ASR_RECORD
 exporter CYBER_EXPORTER
 cache timeout active 60
 cache timeout inactive 15
!
```

```
!
interface GigabitEthernet0/0/0
 ip address <ip-address> <net-mask>
 ip flow monitor CYBER_MONITOR input
!
```

Additional Information: **NetFlow Configuration Guide, Cisco IOS XE Release 3S (ASR 1000)**
http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/xe-3s/asr1000/nf-xe-3s-asr1000-book.pdf

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.

Printed in USA C07-728138-00 05/13