CISCO VALIDATED PROFILE

Routing
Internet Edge LAN-LAN Vertical

April 2016

Table of Contents

Profile Introduction 1

Network Profile 2

Topology Diagram 3

Hardware & Feature Specifications 3

Test Environment 5

Use Case Scenarios 6

Test Methodology 6

Use Cases 6

Appendix A 8

Profile Introduction

Cisco is transforming the network edge with Cisco ASR 1000 Series Aggregation Services Routers and Cisco 4000 Series Integrated Services Routers (ISRs), new lines of midrange routers that establish a new price-to-performance class offering, benefiting both enterprises and service providers. These routers provide a great opportunity for simplifying the WAN edge and significantly decreasing network operating expenses (OpEx). By efficiently integrating a critical set of WAN edge functions such as WAN aggregation, Internet edge services, firewall services, VPN termination, etc. into a single platform, enterprises can meet their business objectives by facilitating deployment of advanced services in a secure, scalable, and reliable manner while minimizing the total cost of ownership (TCO).

Cisco WAN aggregation solutions distinguish themselves from other solutions by offering multiservice routers with the highest performance, availability, and density for concurrent data, security, voice, and application-acceleration services with maximum headroom for growth. The solutions feature embedded security, performance, and memory enhancements, and high-performance interfaces featuring the latest WAN technologies can help enterprises meet the needs of the most demanding WAN network.

Enterprise Wifi users and devices have been growing exponentially; customers are demanding large-scale Network Address Translation (NAT) deployment for IPv4 address conservation. ASR 1000 is already the popular platform for Internet Edge platforms, providing HundredGig connectivity. On the other hand, customers are fully aware of the NAT44 feature sets on ASR 1000. Additionally, some of the existing platforms currently in their network performing NAT functionality, such as the Cisco Catalyst 6000 Firewall Services Module, are going end-of-sale. Therefore there are strong requirements to consolidate the BGP routing and NAT functionality into a single system on ASR 1000. Security is always a customer priority for their Internet Edge deployments, and the ASR 1000 zone-based firewall (ZBFW) provides effective protection against distributed denial of service attacks.

Table 1 lists the key areas on which the profile focuses:

Table 1 Profile feature summary

Deployment areas	Features
Security	Zone-based firewall, ACL
Network services	NAT44
Efficient network management	LiveAction
System and network resiliency	Box-to-box (B2B) high availability (HA)
Price-performance	Line rate throughput

Network Profile

Cisco ASR 1000 can sustain high rate of firewall and NAT sessions while maintaining a very high number of concurrent sessions inspected all the way up to Layer 7 content. Even with its high adoption in the security domain, ASR 1000 was still lacking compared to internal and external competitive products, because it did not have stateful failover support for firewall and NAT across boxes. Box-to-box HA is a method for achieving high availability of applications such as ZBFW, NAT, VPN, SBC, etc. between ASR 1000 routers.

The NAT Box-to-Box High-Availability Support feature enables network-wide protection by making an IP network resilient to potential link and router failures at the NAT border.

NAT Box-to-Box High-Availability Support leverages services provided by the redundancy group (RG) infrastructure present on the device to implement the high-availability functionality. The RG infrastructure defines multiple RGs to which applications can subscribe to and function in an active-standby mode across different devices. You achieve NAT box-to-box high-availability functionality when you configure two NAT translators, residing across different devices, to an RG and they function as a translation group. One member of the translation group acts as an active translator, and the other members of the translation group act as a standby translator. The active translator is responsible for handling traffic that requires address translation. Additionally, the active translator informs the standby translator about packet flows that are being translated. The standby translator uses this information to create a duplicate translation database that equips the standby translator to take over as the active translator in the event of any failures to the active translator. Therefore, the application traffic flow continues unaffected as the translations tables are backed up in a stateful manner across the active and standby translators.

Currently, you can deploy B2B three different ways:

- LAN-LAN
- LAN-WAN
- WAN-WAN

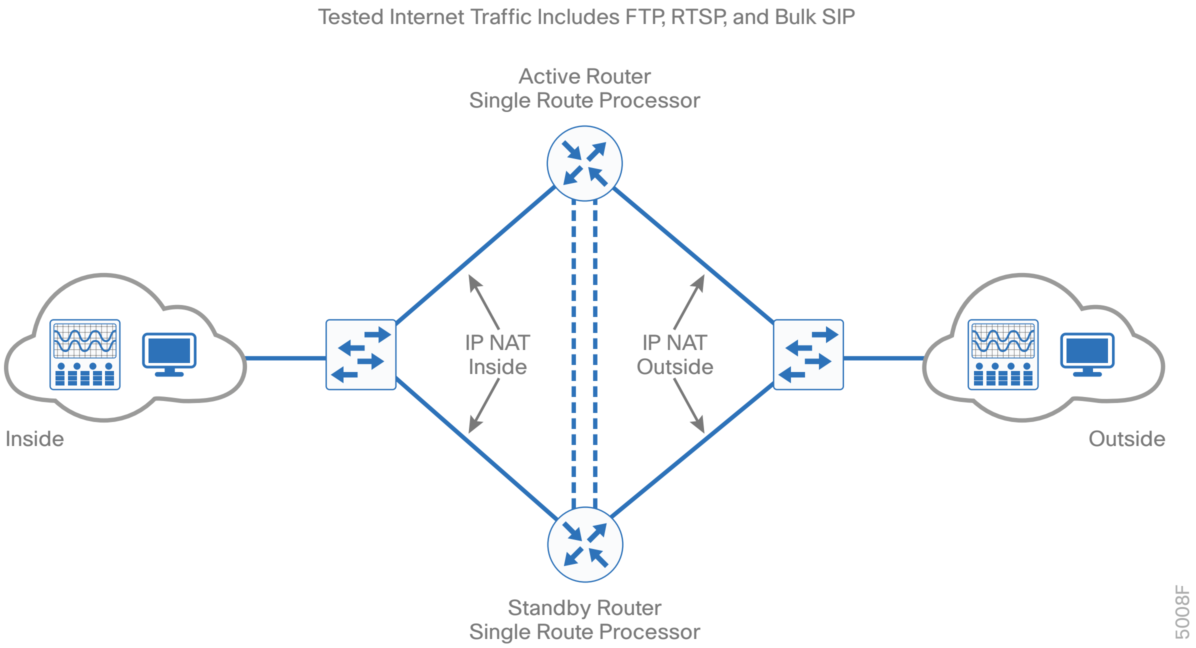
This document focuses on the LAN-LAN deployment.

This is the first time that a Cisco routing platform would offer functionality provided by only an appliance. B2BHA is supported in the ASR 1000 family of routers starting RLS3.1.0. ASR 1000 that supports B2BHA offers stateful failover of zone-based firewall and NAT, as well as secure service including Session Border Controller (RLS3.2S). Redundancy Framework not only supports a large set of application types but is also built to accommodate any existing or custom redundancy protocol.

Based on the research, customer feedback, and configuration samples, this profile is designed with a generic deployment topology that you can easily modify to fit any specific deployment scenario. Refer to the topology for further details.

TOPOLOGY DIAGRAM

Figure 1 *Internet Edge Profile: topology overview*



Disclaimer

100 Gb links were used for profile validation.

HARDWARE & FEATURE SPECIFICATIONS

This section describes the 3-D feature matrix where the hardware platforms are listed along with their place-in-network (PIN) and the relevant vertical deployed.

Key Vertical Features

Table 2 defines the hardware, PIN, and the features deployed. The scale of these configured features, the test environment, the list of endpoints, and the hardware/software versions of the network topology are defined later.

Disclaimer

Refer to appropriate CCO documentation for release/feature support across different platforms.

Table 2 *3-D feature summary with hardware and PIN*

Deployment layer (PIN)	Platforms	Critical vertical features
Edge Device	ASR1013 (RP2 (16GB) / ESP200)	NAT, ZBFW
LAN Device	Nexus 7k	Switching

Hardware Profile

Table 3 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end Government branch Vertical Profile deployment.

This list of hardware, along with the relevant software versions and the role of these devices, complement the actual physical topology defined in Figure 1.

Table 3 *Hardware profile of servers and endpoints*

VM and HW	Software versions	Description
LiveAction	4.0	For network management
Spirent	Test Center 3.95	Generate traffic streams
Ixia	IxLoad and IxExplorer version 6.40	Generate traffic streams

TEST ENVIRONMENT

This section contains describes the features and the relevant scales at which the features are deployed across the physical topology. Table 4 lists the scale for each feature.

Disclaimer

The table below captures a sample set of scale values used in one of the use cases. Refer to appropriate CCO documentation/datasheets for comprehensive scale data.

Table 4 *Internet Edge Profile: feature scale validated in this profile*

Feature	Scale/features
NAT44	8M NAT translations
NAT mode	CGN with PAP and BPA
ZBFW	IPv4 Create 3 FW zones (inside, outside, DMZ). Inspect all traffic from inside>outside, DMZ>outside. Allow only http, smtp from outside>DMZ web & mail server. Allow/inspect SQL/SMTP traffic from web/email server from DMZ>inside.
Traffic pattern	5 Gb from in to out and 100 Gb from out to in

Use Case Scenarios

TEST METHODOLOGY

The use cases listed in Table 5 are executed using the topology shown in Figure 1, along with the test environment shown in Table 4.

Images are loaded on the devices under test via the tftp server using the Management interface.

To validate a new release, the network topology is upgraded with the new software image with an existing configuration composed of the use cases and relevant traffic profiles. Addition of new use cases acquired from the field or customer deployments are added on top of the existing configuration.

During each use case execution, syslog is monitored closely across the devices for any relevant system events, errors, or alarms. With respect to longevity for this profile setup, CPU and memory use/leaks are monitored during the validation phase. Furthermore, to test the robustness of the software release and platform under test, typical networks events are triggered during the use case execution process.

USE CASES

Table 5 describes the use cases that are executed on the Internet Edge Profile. These use cases are divided into buckets of technology areas to show the complete coverage of the deployment scenarios.

These technology buckets are composed of system upgrade, security, network services, monitoring & troubleshooting, simplified management, and system health monitoring, along with system and network resiliency.

Table 5 List of use case scenarios

No.	Focus Area	Use Cases
System upgrade		
1	Software upgrade	Network administrator should be able to perform router upgrade and downgrade between releases seamlessly. ▪ All of the NAT configurations should be migrated seamlessly during the upgrade/downgrade operation. ▪ SW Install, Clean, Expand ▪ All translations should be synced between active and standby.
Network services		
2	ZBFW	Network admin to secure the traffic using zone-based firewall ▪ Inspect traffic based on type of traffic or source/destination address.

Table 5 continued

Monitoring & troubleshooting		
3	NetFlow	Enable IT admins to determine network resource use and capacity planning by monitoring IP traffic flows using Flexible NetFlow ▪ Traffic types: IPv4 ▪ LiveAction
4	Wireshark	Network admin should be able to troubleshoot the network by capturing and analyzing the traffic. ▪ Wireshark–Dataplane & Control Plane Capturing
5	Show CLI	Enable IT admins to determine network resource use and capacity planning by monitoring encrypted traffic flows using show CLI
Simplified management		
6	Prime-Troubleshooting	Simple network troubleshooting and debugging for IT admins ▪ Monitor network for alarms, syslogs, and traps
System health monitoring		
7	System health	Monitor system health for CPU use, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
8	System resiliency	Verify system level resiliency during the following events: ▪ Active RP failure ▪ Active ESP failure ▪ LAN interface flaps ▪ SIP/SPA reload/OIR ▪ Redundancy switchover
9	Negative events, triggers	Verify that the system holds well and all translations are synced to standby after the following negative events are triggered: ▪ Config Changes–add/remove config snippets, config replace ▪ Clear IP NAT translations, NAT mode change ▪ Adding/deleting/expanding NAT pools

Appendix A

You can find example configurations at the following location:

http://cvddocs.com/fw/cvpconfig-routing

Please use the feedback form to send comments and suggestions about this guide.

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, “DESIGNS”) IN THIS MANUAL ARE PRESENTED “AS IS,” WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.