CISCO VALIDATED PROFILE

Routing MACsec Enterprise/Federal Security Vertical

April 2016

Table of Contents

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.

This profile examines how recent network enhancements and innovation can be used to optimize and simplify the overall deployment, functionality, and operation of networks requiring high-speed encryption beyond what IPsec can deliver. Customers showing an immediate interest in these high-speed solutions are Campus and Data Center Interconnect deployments, the secure government agencies, scientific and research community, financial companies, and service providers interested in securing customer traffic without sacrificing performance and packet size agility.

Education and government network environments combine the technology requirements of large enterprises with a specialized set of demands that include:

- **Security**—Universities need to protect personal, academic, and copyrighted information. Security rich features-MKA and MACsec are deployed.
- **Performance and scalability**—While IPsec solves most encryption requirements, one of the limitations of IPsec has been the performance, specifically as it relates high-speed links that require line-rate performance, regardless of the packet size, and speed.

Table 1 summarizes the key areas on which this profile focuses.

Table 1   Enterprise profile feature summary

Deployment areas	Features
Security	MKA, MACsec
Network services	EoMPLS,VPLS,OTV,EVPN,VxLAN
Price-Performance	Line rate encryption throughput

Network Profile

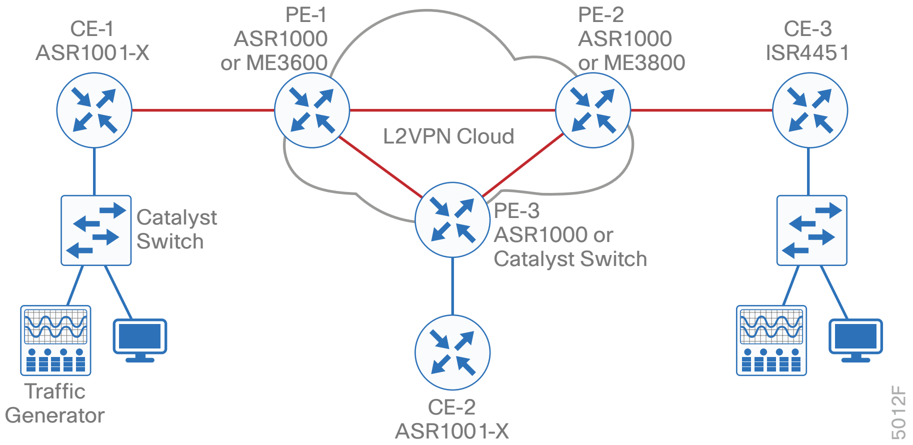
Based on the research, customer feedback, and configuration samples, this profile is designed with a generic deployment topology that you can easily modify to fit any specific deployment scenario. This profile caters both to government and larger university campus deployments.

For larger university campus deployments (covering larger geographical areas, larger scales, and heavier use of resources), this profile uses the classic 3-tier architecture of Access, Distribution and Core.

TOPOLOGY DIAGRAM

Figure 1 shows the topology used for the validation of the profile.

Figure 1 *Topology overview*



Site-1 (the left-portion of the topology) represents a deployment using Cisco ASR 1001-X Router as CE along with Cisco ME 3600 Series Ethernet Access Switch in the Core layer.

Site-2 (the right portion of the topology) represents a deployment with Cisco 4451-X Integrated Services Router in the Distribution layer and Cisco ME 3800X Series Carrier Ethernet Switch Router in the Core layer.

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

Table 2 3-D feature summary with hardware and PIN

Deployment layer (PIN)	Platforms	Critical vertical features
Access	CE1: ASR1001-X CE2: ISR4451	MKA MACsec CDP LLDP Multicast
Core	Core1: ASR1K/Catalyst/ME switches	BGP, OSPF VPLS OTV VxLAN EVPN

Hardware Profile

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

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

Table 3 Hardware profile of servers and endpoints

VM and HW	Software versions	Description
Spirent	Spirent TestCenter	Generate traffic streams

TEST ENVIRONMENT

This section 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.

Table 4 Education Profile: feature scale validated in this profile

Feature	Scale
GigEthernet	8 MKA sessions
TenGigEthernet	32 MKA sessions
VLANs	32
Static routes	32 IPv4

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.

With respect to the longevity for this profile setup, the CPU and Memory use are monitored overnight, as well as during the weekends, along with any mem-leak checks. In order to test the robustness, certain negative events are triggered during the use case testing.

USE CASES

Table 5 describes the use cases that were executed on this 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	Upgrade	Network administrator should be able to perform router upgrade and downgrade between releases seamlessly. ▪ All of the MACsec configuration should be migrated seamlessly during the upgrade/downgrade operation. ▪ SW Install, Clean, Expand
Security		
2	E-line mode	Secure: CE–CE link, DC Interconnect ▪ Ethernet Service ▪ Point to point PW service (no MAC address lookup)
3	E-LAN mode	Secure: CE–CE link, DC Interconnect and targets more branch network deployment option. ▪ VLAN Based E-LAN (Point-to-MultiPoint)
Network services		
4	E0MPLS	Point to point PW service (no MAC address lookup)
5	VPLS	VLAN-based E-LAN (Point-to-MultiPoint) ▪ Verify MACsec works over VPLS

Table 5 continued

6	OTV	OTV extends Layer 2 applications across distributed data centers ▪ Verify MACsec works with OTV
7	VxLAN	VXLAN is a Layer 2 overlay scheme over a Layer 3 network. ▪ Verify MACsec works with VxLAN
8	EVPN	Ethernet VPN (EVPN) and Provider Backbone Bridging EVPN (PBB-EVPN) are next generation solutions that provide Ethernet multipoint services over MPLS networks. ▪ Verify MACsec works with EVPN
9	L2 QoS	MACsec works with existing Layer 2 QoS Configuration (Class of Service).
Monitoring & troubleshooting		
10	Debug MKA/ MACsec	Network admin should be able to troubleshoot the network by using relevant debug MKA/MACsec CLIs.
11	Show CLI	Enable IT admins to determine network resource use and capacity planning by monitoring encrypted traffic flows using show CLI
System health monitoring		
12	System health	Monitor system health for CPU use, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
13	System resiliency	Verify system-level resiliency during the following events: ▪ Online insertion and removal (OIR) ▪ Power failure
14	Negative events, triggers	Verify that the system holds well and recovers to working condition after the following events are triggered: ▪ Config changes–add/remove config snippets, Default-Interface configs ▪ Link flaps, re-routes. ▪ Clear Counters, Clear mka session, Clear Routes, and change access-control mode ▪ SAK re-keys (packet drops in core network hence very frequent peer loss)

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.