

CISCO VALIDATED PROFILE

# Routing Standard Branch Vertical

April 2016

---

# Table of Contents

|   |           |
|---|-----------|
| <b>Profile Introduction</b> .....       | <b>1</b>  |
| Cisco Cloud Web Security .....          | 1         |
| VPN .....                               | 2         |
| QoS .....                               | 2         |
| WAN Optimization .....                  | 2         |
| <b>Network Profile</b> .....            | <b>4</b>  |
| Topology Diagram .....                  | 4         |
| Hardware & Feature Specifications ..... | 5         |
| Test Environment .....                  | 6         |
| <b>Use Case Scenarios</b> .....         | <b>7</b>  |
| Test Methodology .....                  | 7         |
| Use Cases .....                         | 7         |
| <b>Appendix A</b> .....                 | <b>10</b> |

# 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 Standard Branch profile outlines a typical deployment in a small & medium branch office. Branches are typically deployed with an Internet link; hence, security is a major concern. Cisco provides a secure branch-in-a-box solution equipped with features described in this document.

## CISCO CLOUD WEB SECURITY

Cisco Cloud Web Security (CWS) provides security and control for the distributed enterprise across one of the top attack vectors: the web. Cisco worldwide threat intelligence and advanced threat defense capabilities help protect users on any device and in any location.

### Defend Against Web-Based Threat

Get near-real-time web protection, plus granular application visibility and control.

Cisco CWS offers:

- Zero-day defense through heuristics engines, signatures, and more in a single cloud-delivered service.
- Analysis of more than 100 TB of security intelligence and 13 billion web requests daily to detect and mitigate threats.
- Granular visibility and control of more than 150,000 applications and micro-applications.

### Identify Breaches and Reduce Total Time to Remediation

Integrations with Advanced Malware Protection (AMP) and Cognitive Threat Analytics (CTA) allow increased visibility and intelligence into malware and breaches that could be present in your network. The integrated solutions provide:

- Advanced security for advanced threats to defeat unknown threats.
- Protection across the attack continuum—before, during, and after an attack.
- Threat scores and identification of the threat to help prioritize the security response.

## Reduce TCO

Moving to an OpEx model lowers complexity for IT while getting more out of your existing Cisco investment:

- Our product's service is built on next-generation tower architecture that boasts 99.999 percent uptime.
- You can integrate with current Cisco infrastructure to reduce bandwidth costs at your branch.
- You can re-direct traffic to the proxy through Cisco firewalls and secure mobility clients.
- Bandwidth and seat-based options are available.

## Protection for Software-as-a-Service Applications

Cisco Cloud Access Security delivers Software-as-a-Service (SaaS) visibility, extended granular control, and intelligent protection. Use it to embrace the benefits of cloud applications while maintaining strict security policies before, during, and after an attack.

## VPN

Remote branch offices are connected with the head office through Internet cloud, and it is very important to protect the data they exchange. Cisco provides the solution for this kind of deployment—a DMVPN where the static secure tunnel is formed between branch and head offices and a dynamic secure tunnel is formed branch-to-branch when required.

## QoS

Bandwidth use is critical, and this can directly impact employee productivity if bandwidth use is not planned properly. Cisco recommends that you configure QoS on the WAN or LAN interface, so that more bandwidth is used for Intranet traffic and critical applications and less bandwidth is used for non-critical & Internet traffic.

## WAN OPTIMIZATION

Cisco Wide Area Application Services (WAAS) is a set of WAN optimization solutions that minimize enterprise bandwidth use and accelerate application performance. You can use it to optimize use of your existing bandwidth, while seeing to it that each application gets the resources it needs to deliver high-quality user experiences across the WAN. Cisco WAN optimization includes TCP optimization and network sequence caching, as well as byte and bit level compressions.

Cisco Intelligent WAN with Akamai Connect helps businesses deliver high-quality digital experiences with minimal bandwidth impact, regardless of device, connectivity, or cloud. It delivers next-generation application optimization to speed up Cisco IWAN by extending the Akamai Intelligent Platform directly into the branch router. This fully integrated solution helps organizations improve customer engagement and employee productivity while reducing network infrastructure costs through lower bandwidth consumption.

**Table 1** Profile feature summary

| Deployment areas                   | Features   |
|------------------------------------|--|
| Security                           | DMVPN, IKEV2, CWS  |
| Services                           | QoS, AVC, FNF, ZBFW, NAT, IP SLA, EEM Script, ACL, EIGRP, WAAS & Single side optimization  |
| IPv6 migration                     | IPv4 only  |
| Network planning & troubleshooting | Flexible NetFlow (FNF)<br>Application Visibility & Control (AVC)<br>Embedded Packet Capture (EPC)<br>MPLS, BGP, WAAS Central Manager (WCM) |
| Network management                 | Cisco Prime, LiveAction  |

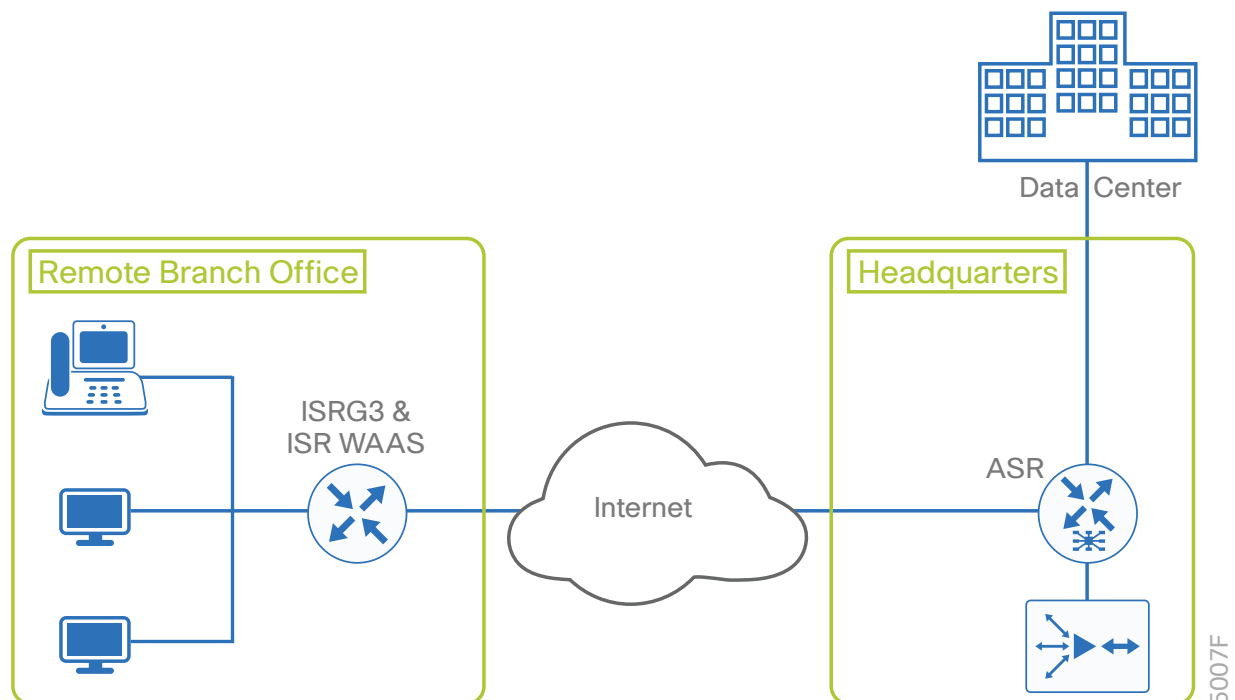
# Network Profile

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

## TOPOLOGY DIAGRAM

Figure 1 shows the topology for Standard Branch profile.

*Figure 1* Topology overview



## HARDWARE & FEATURE SPECIFICATIONS

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

### 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 the 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  |
|------------------------|-------------------------------|---|
| Head office            | ASR1000                       | DMVPN, IKEV2, WCCP  |
| Datacenter WAVE        | WAVE 594                      | TCP & all application optimizations and WCCP                          |
| Branch office          | ISR4451<br>ISR4331<br>ISR4321 | QoS, AVC, FNF, ZBFW, NAT, IP SLA, EEM Script, ACL, EIGRP              |
| ISR-WAAS               | WAAS-OVA                      | TCP & all application optimizations, APPNAV, single-side optimization |

### Hardware Profile

Table 3 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end 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                         |
|----------------|------------------------------------|-------------------------------------|
| Ixia           | IxNetwork and IxExplorer version X | Generate traffic streams            |
| Spirent        | Spirent Test Center                | Generate L7 traffic                 |
| LiveAction     | Version 4.0                        | To collect the FNF statistics       |
| Windows        | Windows 7                          | Generate real-time Internet traffic |
| Windows Server | 2003 server                        | Datacenter Server                   |

## 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** *Standard branch: feature scale validated in this profile*

| Feature              | Scale  |
|----------------------|--|
| ISR4451 as DMVPN HUB | ISR4451, phase 2, 4000 EIGRP neighbor with minimal route, 179 Sec convergence time<br>ISR4451, phase 3, 4000 EIGRP neighbor with minimal route, 242 Sec convergence time |
| ISR-WAAS             | ISR-WAAS 200, 175 bidirectional flows for datacenter, 200 Internet flows with single side optimization & CWS   |
| ISR4451 NAT overload | 26k App mix flows—without single side optimization   |



# Use Case Scenarios

## TEST METHODOLOGY

The use cases listed in Table 5 are executed using the Topology defined 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, specific negative events are triggered during use case testing.

## USE CASES

Table 5 describes the use cases that are executed on the Standard Branch 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              | Remote branch | Network admin wants to upgrade remote branch office DUT to latest CCO image. <ul style="list-style-type: none"> <li>All of the configuration should be migrated seamlessly during the upgrade/downgrade operation.</li> </ul>   |
| 2              | Head office   | Network admin wants to upgrade head office DUT to latest CCO image. <ul style="list-style-type: none"> <li>All of the configuration should be migrated seamlessly during the upgrade/downgrade operation.</li> </ul>            |
| 3              | WAAS          | Network admin wants to upgrade WAAS DUT to latest CCO image. <ul style="list-style-type: none"> <li>All of the configuration should be migrated seamlessly during the upgrade/downgrade operation.</li> </ul>                   |
| Security       |               |   |
| 4              | Secure DMVPN  | Network admin wants to have secure DMVPN between the branch and head offices. <ul style="list-style-type: none"> <li>Configure DMVPN</li> <li>Configure IKEV2, DMVPN will be secure over Internet with IKEV2 profile</li> </ul> |

Table 5 continued

|                              |                          |   |
|------------------------------|--------------------------|---|
| 5                            | DMVPN overlay routing    | <p>Network admin wants to advertise private subnets with EIGRP.</p> <ul style="list-style-type: none"> <li>All private subnets are advertised through EIGRP if the DMVPN session is successful.</li> <li>Branch and head office can communicate each other.</li> </ul>  |
| 6                            | Cisco Cloud Web Security | <p>Network admin wants to protect the branch office from Internet traffic.</p> <ul style="list-style-type: none"> <li>Configure CWS on WAN and LAN interfaces and all Internet traffic is redirected to a CWS tunnel after the CWS tunnels are up.</li> <li>Whitelisted traffic shouldn't be redirected to CWS tunnels.</li> <li>All Internet traffic is blocked or not blocked based on the CWS fail open close config.</li> </ul> |
| 7                            | WAAS                     | <p>Network admin wants to save bandwidth by enabling WAAS.</p> <ul style="list-style-type: none"> <li>Deploy ISR-WAAS OVA on the branch side.</li> <li>Configure APPNAV as redirection method.</li> <li>Deploy WAVE in head office.</li> <li>Enable all TCP optimization in both ISR-WAAS and WAVE.</li> </ul>  |
| Network services             |                          |   |
| 8                            | QoS                      | <p>Network admin needs to enhance user experience by ensuring traffic and application delivery using QoS policies for DMVPN and LAN interfaces.</p> <ul style="list-style-type: none"> <li>Traffic types: VOIP, video, data.</li> <li>Policing and shaping</li> </ul>   |
| 9                            | ZBFW                     | <p>Network admin to secure the traffic using Zone-Based Firewall.</p> <ul style="list-style-type: none"> <li>Inspect traffic based on type of traffic or source/destination address</li> </ul>  |
| 10                           | NAT                      | <p>Network admin wants to enable NAT to reach out Internet from branch.</p> <ul style="list-style-type: none"> <li>Enable NAT on primary ISP connection</li> <li>Enable ip nat inside on LAN and ISR-WAAS interfaces.</li> </ul>  |
| Monitoring & troubleshooting |                          |   |
| 11                           | EPC                      | <p>Network admin should be able to troubleshoot the network by capturing and analyzing the traffic.</p> <ul style="list-style-type: none"> <li>Embedded Packet Capture</li> <li>Wireshark</li> </ul>  |
| 12                           | NetFlow                  | <p>Enable IT admins to determine network resource use and capacity planning by monitoring IP traffic flows using Flexible NetFlow.</p> <ul style="list-style-type: none"> <li>Traffic types: IPv4</li> <li>LiveAction</li> </ul>  |
| 13                           | SNMP                     | <p>Network admin should be able to use SNMP for monitoring.</p> <ul style="list-style-type: none"> <li>SNMP mibwalk</li> </ul>  |

Table 5 continued

|   |                           |  |
|---|---------------------------|--|
| 14                                      | AVC                       | <p>Enable IT admins to determine network resource use and capacity planning by monitoring IP traffic flows using Application Visibility and Control.</p> <ul style="list-style-type: none"> <li>▪ Traffic types: IPv4, HTTP</li> <li>▪ LiveAction</li> </ul>   |
| 15                                      | IPSLA & EEM script        | <p>Network admin should be able to troubleshoot the network by enabling the IPSLA.</p> <ul style="list-style-type: none"> <li>▪ IPSLA Probe from branch to ISP</li> <li>▪ EEM script to change the DMVPN tunnel source</li> </ul>  |
| Simplified management                   |                           |  |
| 16                                      | Manageability             | <p>Simplified network troubleshooting and debugging for IT admins</p> <ul style="list-style-type: none"> <li>▪ Monitor network for alarms, syslogs, and traps</li> </ul>   |
| System health monitoring                |                           |  |
| 17                                      | System Health             | <p>Monitor system health for CPU use, memory consumption, and memory leaks during longevity</p>  |
| System & network resiliency, robustness |                           |  |
| 18                                      | System resiliency         | <p>Verify system level resiliency during the following events:</p> <ul style="list-style-type: none"> <li>▪ WAN/LAN interface flaps</li> <li>▪ DMVPN tunnel interface flaps</li> </ul>   |
| 19                                      | Network resiliency        | <p>Verify that the system holds well during a network-level resiliency</p> <ul style="list-style-type: none"> <li>▪ CWS tunnel IKEV2 session</li> <li>▪ Single side optimization sessions</li> </ul>   |
| 20                                      | Negative events, triggers | <p>Verify that the system holds well and recovers to working condition after the following negative events are triggered:</p> <ul style="list-style-type: none"> <li>▪ Config changes—add/remove config snippets, config replace</li> <li>▪ Routing protocol interface flaps</li> <li>▪ IPSec, IKEv2 events like clear gdoi sessions, clear sa counters</li> <li>▪ QoS events such as adding/removing QoS policy, modifying the ACL, modifying the class map</li> <li>▪ Adding/deleting/appending/prepending ACEs in the KS ACL and issuing rekey</li> </ul> |

# 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](http://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.

© 2016 Cisco Systems, Inc. All rights reserved.

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](http://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)