# Direct Internet Access White Paper

## Introduction

Digital innovation is overwhelming the branch and WAN. More specifically, 80 percent of employees and customers work in or are served in branch offices*, which is leading to a 73 percent growth in mobile devices from 2014 to 2018**. These mobile devices are accessing a significantly larger number of cloud applications (such as Office 365, salesforce.com, and Google apps) and as a result, demand for bandwidth and related costs will increase by 20 to 50 percent per year through 2018. The increased surface area and complexity of cyber attacks, and the subsequent increase in time required to mitigate these attacks, have made the branch a prime target for advanced threats. Gartner predicts that 30 percent of advanced threats will target branch offices by 2016 (up from 5 percent in 2013). The need for secure connectivity and security everywhere is as important as ever.

You may already be familiar with these trends, and your organization might be suffering from the lack of bandwidth and rising costs. Additionally, your security department might not allow you to take the proper steps to address these problems. One way to help your organization overcome these challenges is to use direct Internet access (DIA) with Cisco® Intelligent WAN. This white paper will give you the confidence to move to DIA and secure your branch, preparing your organization for future growth and innovations.

### Direct Internet Access

DIA is a component of the Cisco Intelligent WAN solution in which certain Internet-bound traffic or public cloud traffic from the branch can be routed directly to the Internet. DIA helps reduce IT spending, ensure better application experiences, and provide guest Wi-Fi at the branch.

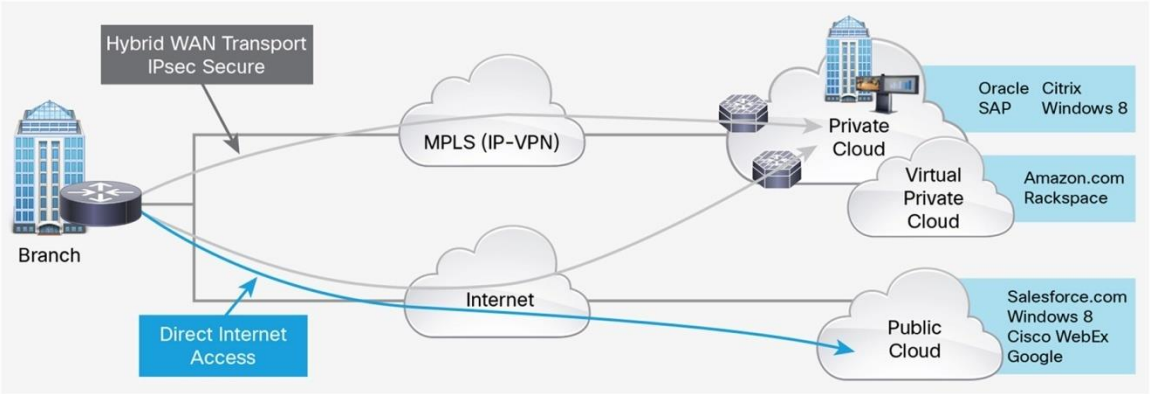
In a traditional hub-and-spoke architecture, all the traffic is routed to headquarters. The primary advantages of DIA are reduced bandwidth requirements at headquarters, fewer network hops (WAN hops are reduced from four to two) and reduced latency (roughly 50 percent improvement) due to direct routing and better optimization (Figure 1). The increased reliability of the Internet for WAN transport makes DIA desirable in branch deployments.

* Tech Target, Branch Office Growth Demands New Devices, 2013

** US The Census Bureau of the Department of Commerce, 2015

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

**Figure 1.** Internet-Based Secure WAN Transport and Direct Internet Access at the Branch




Sending traffic directly from the branch to the Internet creates additional security challenges because the traffic bypasses security tools deployed at headquarters. Therefore, you need to deploy security features at the branch.

## Overview

Tables 1 and 2 summarize the challenges and benefits of using DIA.

**Table 1.** Challenges Involved in Using Direct Internet Access

| Threat Risks | Operational Risks |
|---|---|
| • Increased attack surface<br>• Lack of appropriate security protection at the branch<br>• Lost visibility into DIA traffic | • Additional sensors to manage, additional rack space costs<br>• Overwhelming number of false positives<br>• Inability to zero in on key threats quickly<br>• Loss of revenue-generating square footage due to increased footprint |

**Table 2.** Benefits of Using Direct Internet Access

| Benefits |
|---|
| • Highly secure WAN transport for private and virtual private cloud access, and for branch-to-headquarters connectivity<br>• Uses local Internet path for public cloud and Internet access<br>• Increased WAN transport capacity and cost-effectiveness<br>• Improved application performance (right flows to right places)<br>• Reduced bandwidth consumption |

## Use Cases

### Guest Wi-Fi

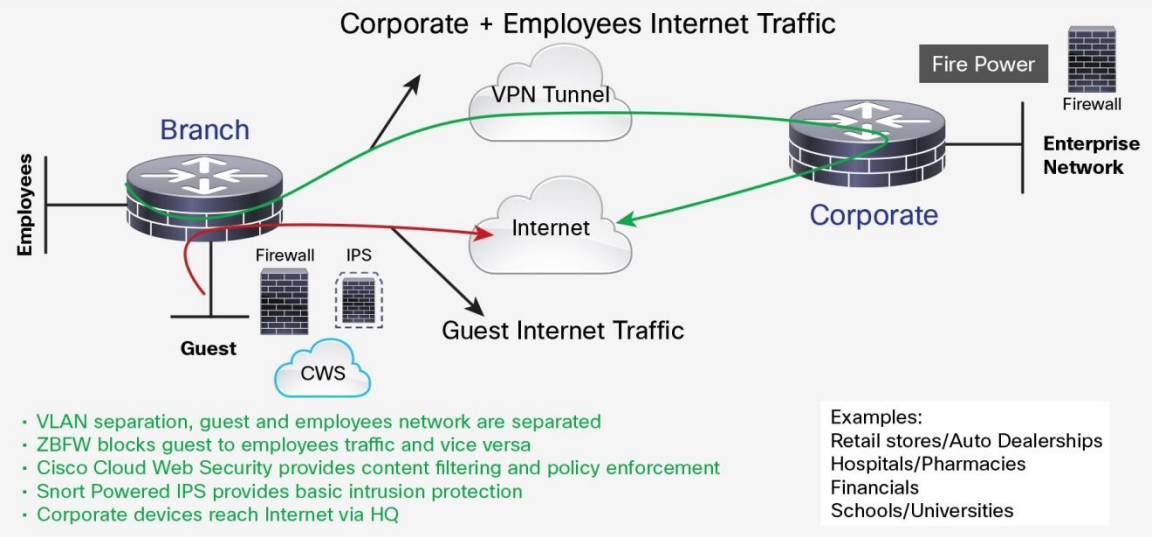
With guest Wi-Fi, guest traffic is routed directly to the Internet while corporate traffic is backhauled to headquarters to help maintain high guest user satisfaction. It is critical that guest traffic does not pose a threat to the corporate environment. Policies should be created to segment guests from corporate traffic, and content-filtering policies should be deployed to ensure appropriate use of the Wi-Fi network and avoid liability.

### Partial DIA Guest Internet Access

With partial DIA, only select types of traffic or applications use the local Internet path (Figure 2). For example, an organization will be able to redirect certain traffic to the public cloud or partner sites. A combination of technologies, such as firewall, content inspection, filtering, and malware protection, provide multilayered protection against unauthorized network access, web-based threats, and malware.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

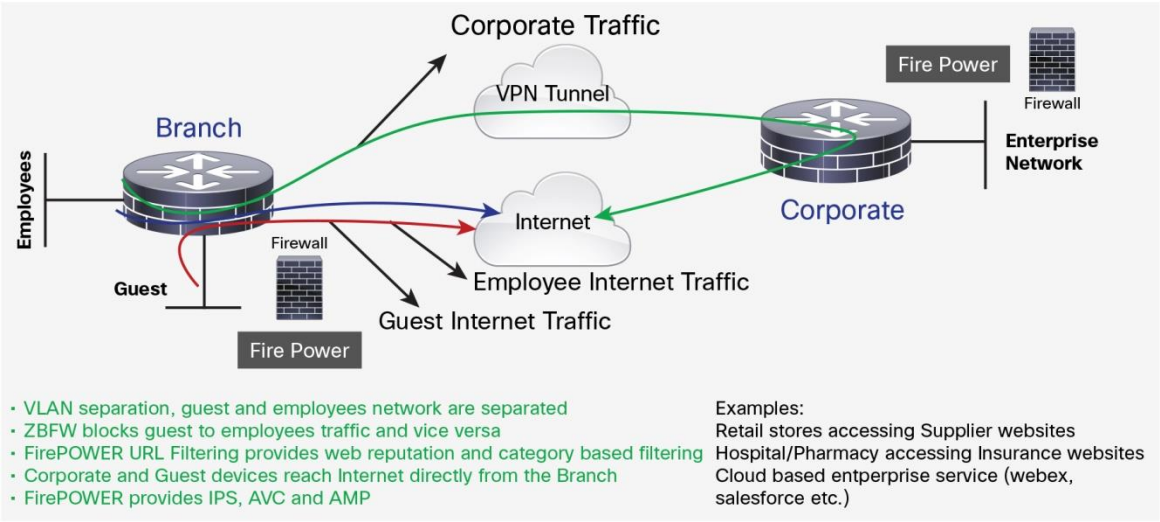
**Figure 2.** Example of Partial Direct Internet Access




## Full DIA

With full DIA, all types of traffic or applications are routed to the Internet via the local path (Figure 3). Security needs at the branch resemble those at the headquarters, and enterprise-class protection is required to protect against enterprise-class threats. A full threat defense stack that includes firewall, content security, intrusion detection and prevention, advanced malware protection, and application visibility and control provides the best protection against increasingly sophisticated cyber attacks.

**Figure 3.** Example of Full Direct Internet Access




© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

## Security Requirements and Components

To better prepare yourself for these DIA use cases, you can take advantage of the breadth of Cisco's industry-leading branch security portfolio, which provides comprehensive protection with the following best-in-class products and solutions:

**Cisco® zone-based firewall (ZBFW)** provides perimeter control and stateful inspection to help ensure your network's availability and the security of your company's resources. Cisco's ZBFW protects the network infrastructure against network-layer and application-layer attacks, viruses, and worms.

**Snort®** is an open-source intrusion prevention system capable of real-time traffic analysis and packet logging, providing integrated threat defense and helping ensure compliance with regulations and Payment Card Industry (PCI) requirements.

**Cisco Cloud Web Security (CWS)** provides industry-leading content filtering with web and file reputation, inspection, and Advanced Malware Protection (AMP) in all the scenarios where web filtering and web-based protection are required. Now, on the Cisco 4000 Series Integrated Services Routers (ISRs), traffic is redirected to a CWS proxy located in one of our data centers around the world for inspection using the industry-standard Generic Routing Encapsulation (GRE) over IPsec Tunnel. GRE over IPsec Tunnel creates a highly secure, encrypted tunnel for your traffic and provides data confidentiality. Traffic does not have to be backhauled to headquarters over expensive Multiprotocol Label Switching (MPLS) circuits in order to keep it secure. The solution supports tens of thousands of nodes with direct point-to-point connections and consistent policy enforcement across all sites to protect all branch office endpoints from threats.

**Cisco FirePOWER™ Threat Defense** offers industry-leading multilayered threat protection with real-time contextual awareness, full-stack visibility, and lower cost of ownership through intelligent security automation. Cisco FirePOWER Threat Defense for ISR includes Cisco Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control, AMP for Networks, and reputation-based URL filtering.

## Solution Management

Even with the breadth of Cisco's branch security portfolio, there are centralized policy management solutions to automate and simplify your overall branch security solution, depending on your organization's needs.

**Intelligent WAN app on Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)** provides centralized automation of policy-based application profiles.

**Cisco Prime™** provides integrated comprehensive and centralized on-premises network management. It includes Cisco Policy Management with monitoring and reporting.

- **Live Action** is an application-aware network performance management tool as well as a quality-of-service (QoS) control tool.
- **Glue Networks** is a cloud-based automation and orchestration platform for hybrid WANs.

**CWS** provides its own cloud-based management portal, which contains granular application visibility and control

Cisco FirePOWER Threat Defense is managed by **Cisco FireSIGHT™ Management Center,** which is the centralized point of event and policy management for all Cisco FirePOWER Threat Defense sensors.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

## Certifications

Cisco router platforms are validated by third-party labs to help ensure that they meet the requirements of major security certification programs. This helps to ensure that Cisco platforms can meet the security requirements of enterprise customers. Cisco router platforms are validated against these major certification programs:

1. **Federal Information Processing Standard (FIPS) Publication 140-2:** U.S. and Canadian government computer security standard used to accredit cryptographic modules.
2. **The Common Criteria (CC) for Information Technology Security Evaluation:** An international standard for computer security certification that defines different. Evaluation Assurance Levels (EALs) for evaluating security equipment. CC product certifications are recognized by 26 nations.
3. **Suite B Cryptographic Algorithms specified by the National Institute of Standards and Technology (NIST):** Used by the National Security Agency's Information Assurance Directorate in solutions approved for protecting National Security Systems. Suite B includes cryptographic algorithms for encryption, key exchange, digital signature, and hashing.

Refer to http://www.cisco.com/go/securitycert for more details about security certifications.

## Conclusion

In summary, Cisco's router security portfolio provides the comprehensive level of security, privacy, and data integrity seen in private WANs, giving confidence to enterprise and government organizations to use the public Internet as a highly secure WAN transport for their branch communication needs. Organizations can use DIA and continue to experience a high level of performance and security while saving money and securing their network.

## References


1. DIA blog post: http://blogs.cisco.com/enterprise/branch-direct-internet-access-is-your-branch-office-secure
2. Branch security webinar: https://grs.cisco.com/grsx/cust/grsEventSite.html?EventCode=12710&LanguageId=1&KeyCode=000967521&_ga=1.204571280.1061921375.1442595323
3. Intelligent WAN DIA design guide: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/intelligent-wan/cvd-iwan-diadesignguide-mar15.pdf
4. Intelligent WAN security white paper: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/intelligent-wan/white-paper-c11-732762.html
5. Gartner – Optimize Enterprise Networks to Improve SaaS Performance
6. Gartner – Bring Branch Office Network Security Up to the Enterprise Standard
7. Router security page: http://www.cisco.com/go/routersecurity


© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 C11-736660-00 02/16

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.