White Paper

Transport-Independent Design: Virtualize Your WAN Infrastructure for Any Transport Service

What You Will Learn

Enterprises today face a big bandwidth challenge as carrier-grade access becomes more costly: how to create secure, reliable, and optimized WANs that offer user experiences over any connection—desktop, laptop, and mobile devices—at an affordable cost. In response, nearly half (46 percent) of businesses are migrating, or are planning to migrate, their WAN to the Internet (Nemertes Research, Benchmark 2012–2013 Emerging WAN Trends). The Internet has become a much more stable platform, and the price-to-performance gains are compelling. But using the Internet as bandwidth brings additional concerns, including application performance, flexibility, security, and the cost of operational support.

This paper describes how Transport-Independent Design, a cornerstone of Cisco® Intelligent WAN (IWAN), provides the foundation to address these challenges by virtualizing the WAN in a consistent and secure manner over any transport service.

Delivering an Uncompromised User Experience

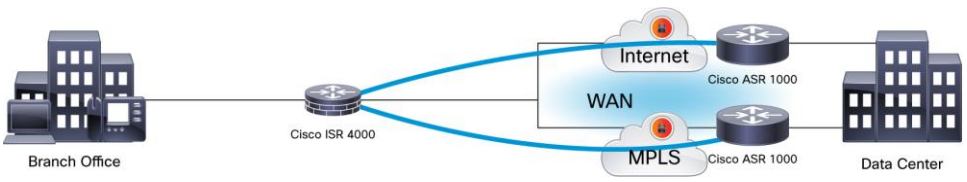
Cisco IWAN enables businesses to deliver an uncompromised experience over any connection. IT organizations can right-size remote and branch-office connections using less-expensive WAN transport service options without affecting performance, security, or reliability. With Cisco IWAN, traffic is dynamically routed based on application, endpoint, and network conditions to deliver the best-quality experience.

Benefits of Transport Independence

Cisco IWAN Transport-Independent Design virtualizes the WAN with a secure IP Security (IPsec) VPN over any transport service offering (refer to Figures 1 and 2). It also:

- Simplifies the WAN with easy multihoming to providers and a consistent design over all transport options
- Offers scalable full-mesh connectivity, including automatic site-to-site IPsec tunnels
- Provides proven robust security, featuring certified strong cryptography and firewall for compliance, and threat protection by design

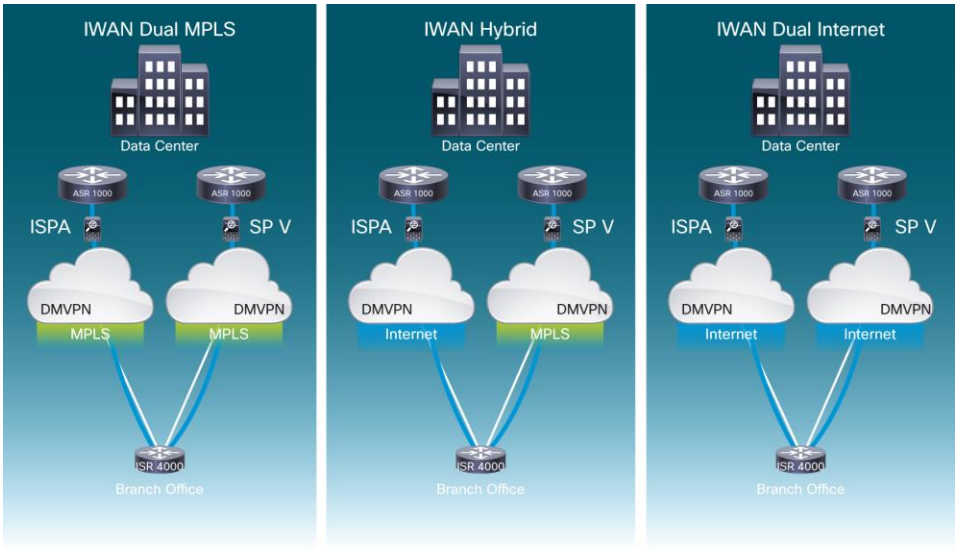
Figure 1. Cisco IWAN Transport-Independent Design



Simplifying the WAN Through Virtualization

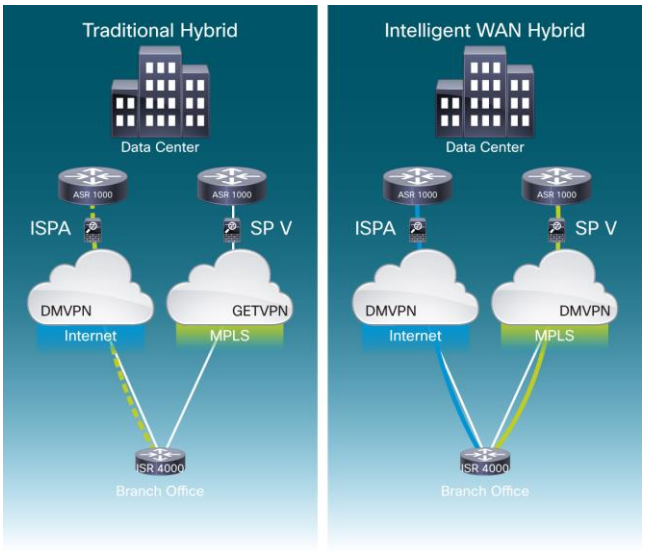
Dynamic Multipoint VPN (DMVPN) is a key building block for Transport-Independent Design. The IWAN Transport-Independent Design uses an IPsec VPN to overlay the provider's WAN transport circuit. This IPsec VPN overlay provides a virtualized WAN design that abstracts (or hides) the complexities associated with mixing various transport options (Multiprotocol Label Switching [MPLS], Internet, fourth generation (4G)/LTE, and so on) together to create a hybrid WAN design (refer to Figure 2). In addition, the Transport-Independent Design gives organizations flexibility regarding transport service types and costs, based on requirements of a given scenario. It can be used over any transport service, including MPLS, Carrier Ethernet, Internet, and 3G or 4G. Dynamic Multipoint VPN (DMVPN) is a key building block for the IWAN Transport-Independent Design. DMVPN is the most widely deployed IPsec VPN technology in the industry. DMVPN supports both hub-and-spoke and full mesh topologies with standards-based and certified cryptography and key management.

Figure 2. Transport-Independent Design Examples



As is evident in Figure 2, the same IWAN design is provided over all the various transport options. This deployment consistency simplifies both the deployment and ongoing support of the WAN. For example, compared to traditional hybrid WAN design (Figure 3), the Cisco IWAN Transport-Independent Design is less complex with fewer technologies and protocols while offering the same advantages and security levels.

Figure 3. Traditional versus Intelligent WAN Design



Traditional Hybrid

- Primary with backup link in active and standby
- Two IPsec Technologies. GETVPN for MPLS and DMVPN for Internet
- Two WAN Routing Domains. For MPLS, eBGP or Static. For Internet, iBGP, EIGRP or OSPF

Intelligent WAN Hybrid

- Both WAN paths are active
- A single IPsec overlay using DMVPN
- A single WAN routing domain using iBGP, EIGRP or OSPF

Securing Intelligent WAN

With Cisco IWAN, IT can deliver high performance with high-security WAN using DMVPN. IT can also enable direct Internet access (DIA) using Cisco Cloud Web Security (CWS) for better software-as-a-service (SaaS) application performance, while protecting all branch-office endpoints and maintaining a centralized InfoSec policy management paradigm.

Cisco IWAN with DMVPN provides data privacy and protection from outside threats over all external networks. Why trust Cisco IWAN?

- **Industry tested and certified:** Our security products and technologies, vetted and proven by security industry experts, are widely deployed with a strong record, meeting or exceeding requirements including Federal Information Processing Standards (FIPS) 140-2, Common Criteria, and Cisco Next-Generation Cryptography (Suite-B).
- **Consistent, robust security posture throughout the solution:** Security is included at every layer of the design.

- **Strong data privacy:** Cisco IWAN uses standards-based IPsec and routing technologies, plus strong NG Cryptography (Internet Key Exchange Version 2 [IKEv2] or ASE-GCM-256) and Public Key Infrastructure (PKI) lifecycle key management.
- Protection from outside threats by:
  - Minimizing exposure by using provider address space and by partitioning and isolating the external interfaces of the router.
  - Using Cisco IOS® Zone-Based Firewall (ZBFW) in Cisco Integrated Services Routers (ISR) and Aggregation Services Routers (ASR); ZBFW uses a default deny-all policy that prohibits traffic between firewall security zones until an explicit policy is applied to allow desirable traffic.

Automated Provisioning for the Branch Office

Cisco's approach to IWAN management is simple, centralized, and automated. Unlike most vendors, Cisco offers customers a variety of management and orchestration tools provided by Cisco and third-party development partners, because one size and type of management and automation tooling does not fit all customer requirements and needs. The current list of management and automation tools designed specifically for IWAN include the following:

- Cisco Application Policy Infrastructure Controller-Enterprise Module (APIC-EM) Software-Defined Networking (SDN) Controller
- Cisco Prime™ Infrastructure
- LiveAction
- Glue Networks

To minimize deployment time and cost to deploy IWAN, zero-touch deployment (ZTD) services provided by APIC-EM, the Cisco Prime solution, or Glue Networks can be used to securely bootstrap a branch-office site (routers, switches, and access points) onto an IWAN. Visualization, monitoring, reporting, and troubleshooting an IWAN are provided as well.

Conclusion

Cisco IWAN Transport-Independent Design, a cornerstone of Cisco IWAN, provides the foundation to address today's remote-site networking challenges by virtualizing the WAN in a consistent and secure manner over any transport service. Cisco IWAN Transport-Independent Design:

- Reduces cost and complexity without compromising security or availability
- Eliminates dependencies on specific transport options
- Simplifies the WAN with a consistent deployment model at all sites
- Scales as business grows, with a variety of platform performance options
- Is a widely deployed, proven, robust validated security
- Reduces deployment time and cost with autoprovisioning

For More Information

To learn more about Cisco IWAN, please visit: http://www.cisco.com/c/en/us/solutions/enterprise-networks/intelligent-wan/index.html.

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 C11-734761-00 05/15