White Paper

Evolving your WAN to Embrace Mobile, Cloud, and Digital Services

Software Define WAN (SD-WAN) technologies within the UK Public Sector.

Summary

The Internet as a WAN service has become a more stable platform, and the price-to-performance gains can be very attractive. Until now, businesses have primarily deployed the Internet as a transport for backup purposes because of perceived performance risks. With the increasing demand for Cloud Services, traffic patterns are changing and there is an emerging requirement for Internet breakout at the network edge closer to communities and end users for Direct Internet Access (DIA).

This whitepaper outlines how public sector WAN's can evolve and embrace Internet connectivity to accommodate the changing needs of the public sector. In order to evolve to a Hybrid WAN architecture, IT needs to ensure that the performance, visibility, and security are still in place. It is targeted at network professionals and other personnel who assist in the design of shared Public Sector WAN Infrastructure and compliments the design patterns and principles issued by GDS Common Technology Services (CTS). The solutions outlined in this guide have been developed in response to:

- Flat or decreasing WAN budgets;
- Changing traffic patterns and increased bandwidth demands;
- Demand for increased flexibility, agility and automation.

Contents

The Evolution of Public Sector WAN Networks

The Public Services Network (PSN) provides UK Public Sector organisations with a standardised ICT environment – a single assured network and a set of network services (voice, unified communications and video) from accredited providers via a simplified procurement process.

PSN is already delivering direct cost savings for the Public Sector through implementation of agreed best practice standards, simpler procurement and the use of shared ICT infrastructure and services. It continues to deliver greater efficiencies and cost savings through its ability to support applications and shared services that will transform how Public Sector organisations are run and how they deliver citizen services.

Cisco has contributed actively to the Cabinet Office PSN programme since 2008 and has been a major technology provider to PSN Service Providers delivering end-to-end solutions via the Crown Commercial Service (CCS) procurement frameworks. Our strong service provider relationships allow those solutions to be delivered as managed services in a cost efficient, timely manner. Cisco helps Public Sector organisations justify the investment in ICT-enabled business transformation that drives operational efficiency and improves citizen services.

The traditional private Wide Area Network (WAN) architecture is evolving, as it was designed to support client/server based applications with predictable traffic flows between clients in remote offices and applications hosted in a central data centre(s). This one-size-fits-all approach is not agile enough to cater for the diverse user needs across the UK Public Sector and the following business drivers and market transitions are shaping a new Hybrid WAN architecture.

A Hybrid WAN approach is needed to address the following user needs:

1. **Cloud Services:** Citizen services and Line-of-business (LoB) applications are increasingly being delivered from public cloud data centres and users are demanding a secure, consistent and reliable experience;
2. **Guest Internet:** The demand for Guest and trusted visitor Internet access;
3. **Real-estate Consolidation**: Multi-tenanted buildings require shared infrastructure that needs to be flexible to allow users to work without restriction;
4. **Location Independent & Mobile Working:** Users are increasingly more mobile;
5. **Shared Services:** Peer-to-peer applications are increasing as full hosted UC and video services are adopted for greater collaboration between agencies;
6. **Application Visibility & Control:** Without application visibility, business critical web-based services cannot be distinguished from general web content.

These changes are shifting the emphasis away from fixed length private MPLS WAN contracts towards Internet connectivity and flexible Over-The-Top (OTT) VPN services.

1. Cloud Services: The Impact on Internet Gateway Architectures

Since the introduction of Public Services Network (PSN), most public sector WAN's have moved over to MPLS L3VPN's supplied by Direct Network Service Provider's (DNSP's). In many cases the PSN Code of Connection (CoCo) requirements have driven the public sector bodies to separate their internal traffic into multiple L3VPN's. Almost all deployments include backhauling Internet traffic across the PSN to a central Data Centre hosting the Internet link and security infrastructure. In the past there were good reasons for choosing the centralised Internet

gateway approach, such as lack of suitable broadband at remote locations and a desire to consolidate the security infrastructure centrally to minimise the attack surface and limit management overhead and operational costs. However, as the nature of work and Internet usage changes and as broadband becomes more prevalent through initiatives such as the Superfast rollouts, many customers, particularly in local government and education are beginning to question the suitability and sustainability of the centralised Internet gateway model.

The central Internet gateway is not only supporting email and outbound web traffic for internal staff, but it is expected to support business critical applications such as public cloud based applications, online citizen facing services (including revenue generating ones like council tax or parking fine payment), remote access VPN's for mobile workers and site-to-site VPN's for homeworkers and suppliers. Some of these changes have been driven by government policy, e.g.:

- **Cloud First** - introduced in May 2013 mandated Central Governments departments and recommended the wider public sector, adopt public cloud services to provide savings and efficiencies and enable quicker delivery of IT services.
- **Digital by Default** - introduced to encourage citizen facing services to be conducted digitally due to the lower costs associated with online transactions when compared to telephone, post or face-to-face meetings.

2. Guest Internet Access: Network policy control

Citizens have increasingly come to expect wireless guest Internet access at all public buildings. This demand is greatest at NHS locations especially those which may involve an extended stay. However, providing guest access for citizens at a hospital or library especially with a centralised delivery model as discussed previously only adds to the pressure on the WAN and security infrastructure. Adding Direct Internet Access (DIA) at the network edge has the advantage of allowing guest Internet access to breakout locally rather than adding to pressure on MPLS links. Once guest access is introduced at the branch office, strong security and application visibility and control is required to ensure business critical public cloud applications are prioritised over guest web traffic. This can be further enhanced by introducing WAN acceleration and local content caching services on the CPE router.

However, as all these services drive the demand for Internet bandwidth in the branch office ever higher and reliance on public cloud delivered applications increases, the disadvantages of the centralised Internet model become ever more apparent. For example, the continual upgrades to MPLS and Internet links and security hardware to keep pace with rapidly increasing Internet usage. The central Internet link also introduces a single point of failure as most public sector organisations are not dual-homed to two ISP's. The single links are also easily susceptible to outages through DoS and DDoS attacks. DNS Amplification attacks against councils and HEFE establishments in particular are now a daily occurrence.

3. Real Estate Consolidation: Shared Workplaces

Any new WAN infrastructure and equipment must have the flexibility and agility to support the introduction of future services, but also support the consolidation, reduction and mergers which are occurring in the public sector at an organisation level but also in terms of buildings, equipment and energy consumption.

Multi-tenant buildings require WAN connectivity which can deliver secure virtualised WAN services over a single shared physical infrastructure.

- The most common of these is MPLS Layer 3 VPN. To support multi-tenant buildings, MPLS L3 VPN's can be extended from an SP's infrastructure into an end-site through the use of VRF-Lite technology on the CPE router and logical segmentation of the WAN link. VRF-Lite allows organisations sharing a building to

split the cost of WAN links while maintaining secure separation between their respective wide-area networks. In addition to virtualised WAN services, the CPE router should also deliver VRF-aware security services such as firewalls and NAT and also support Hierarchical QoS (HQoS). VRF-Aware security services and HQoS allow each tenant to maintain their own security and QoS policies independent of the other tenants. Multi-tenant services via MPLS require all tenants to have their WAN provided by the same service provider so will be most likely adopted in regional aggregated networks.

- Overlay VPN's such as Cisco's DMVPN or IWAN can also provide wide-area connectivity to a shared building. With an overlay service, transport connectivity can be jointly purchased from any provider, e.g. a direct Internet or PSN connection and each tenant installs a VPN router to securely connect their users back to their wider network over the shared transport. Overlay VPN's allow each tenant to maintain control of their connectivity and also enable each tenant to have a different WAN topology that satisfies their own requirements. A limitation of this approach is the inability to dedicate bandwidth on the shared transport link to each tenant organisation. However this can be mitigated by the use of features such as Adapative QoS for DMVPN or Intelligent Path Control in IWAN.

A solution whitepaper for Shared Workplace Infrastructure in the Public Sector is available at http://www.cisco.com/cisco/web/UK/public_sector/new/index.html

4. Location Independent & Mobile Working: The Impact of BYOD

Joint ventures between different agencies to deliver improved service to citizens such as in the social care arena are driving a requirement for inter-agency wireless and wired roaming. To support these initiatives, there is a requirement for workers to be able to work from any public sector building seamlessly. In particular this requires connectivity to their home network resources from a partner organisation's site without resorting to remote access VPN's across wireless guest access, virtual desktops or physically separate computer equipment provided by the host organisation. With, a mutual authentication mechanism in place between participating organisations, technologies such as 802.1X, Cisco ISE, TrustSec, VRF-Lite and DMVPN can help deliver secure network access based on a user's identity and security posture.

Other changes have been due to the more mobile and flexible nature of work and the consumerisation of IT. Bring Your Own Devices (BYOD) such as tablets and smartphones, although restricted from accessing PSN originated data are now permitted to access OFFICIAL data providing suitable controls such as Mobile Device Management (MDM) are in place. The Health & Social Care and Education sectors have seen extensive deployments of tablet devices to support a mobile workforce and student population. All these mobile devices behave as thin-clients and contribute to the pressure on WAN's and central Internet connections by frequently pulling down application, OS and security updates in addition to their regular application traffic.

5. Shared Services

Shared services are typically delivered on a local level by leveraging private circuits with back-to-back firewalls to perform NAT and maintain clear security boundaries between organisations. However, private circuits between partnering organisations do not scale from a cost perspective.

Regional Shared Services VPN's are an attractive solution as they can facilitate collaboration between a greater number of participants and in most cases have a relatively low setup cost as they are delivered using VRF-Lite and unused capacity on existing WAN bearers.

6. Application Visibility & Control

Modern networks are faced with the following challenges when attempting to ensure a good quality experience for their end-users:

Standardisation on HTTP(s) Transport

Applications are increasingly moving to HTTP(s) for their transport protocol, which is being driven by the adoption of cloud-based services and the device agnostic nature of web based applications.

The standardisation on HTTP(s) for transport has made classification of traffic a complex task, as access-lists to classify applications based on OSI layer 3 or 4 fields is challenging, if not impossible and certainly does not scale for public cloud services.

Encrypted Applications

Accurate classification, particularly of HTTP and HTTPS applications now requires deep packet inspection techniques such as Network Based Application Recognition (NBAR2) which look further into the packets or employ heuristic techniques to identify the payload.

Without application visibility, business critical web-based services cannot be distinguished from general web content and application performance can be impaired. However, with application visibility in place, controls can be applied to traffic to ensure the business critical applications take priority. This benefits productivity and also aids in capacity management and could postpone or eliminate costly MPLS bandwidth upgrades.

Choosing the Right WAN Architecture

1. Public Services Network (PSN) Accredited MPLS L3VPN's

MPLS L3VPN services enable a service provider to build virtual WAN networks for their customers on a shared network infrastructure. Aggregating WAN's onto a shared high bandwidth MPLS network is considerably cheaper than each customer building their own WAN network which often results in duplication, geographic overlap and restricts collaboration.

The fundamental building block of the L3VPN technology is the Virtual Route and Forwarding (VRF) table which can be thought of as a virtual router. In a L3VPN, the SP creates VRF's for each customer on their provider edge (PE) routers and attaches the customer sites to the VRF. By default, traffic is not permitted to cross between VRF's unless explicitly configured to do so by the SP. This secure by default behaviour provides segmentation of the shared SP infrastructure. Traffic is MPLS switched between PE routers with the traffic of each customer assigned MPLS labels identifying which VRF the packets belong to. The MPLS labels provide separation of the customer traffic as it crosses the SP's core network.

MPLS L3VPN provides any-to-any connectivity which is ideal for supporting peer-to-peer applications such as VoIP or desktop to desktop video as traffic flows directly between remotes sites. However, the any-to-any routing is only delivered because the customer and SP form a routing relationship at every site which enables the SP to learn the topology of the customer network and route traffic accordingly. This peering introduces additional complexity and is typically limited by the SP to the BGP protocol which many customers will have limited or no experience with.

In contrast to broadband Internet services which are mostly asymmetrical, MPLS services will typically be offered with symmetrical access circuits such as fibre Ethernet or SDSL services which again benefit voice and UC applications.

MPLS SP's also offer performance and availability Service Level Agreement's (SLA's) as well as supporting QoS. The PSN Technical Domain Description (TDD) mandated that all PSN Connectivity providers support 6 Levels of QoS.

Any-to-any routing combined with service level and QoS guarantees offered by MPLS services, makes a PSN accredited MPLS L3VPN an ideal WAN technology for the majority of public sector sites, especially those with bandwidth requirements greater than can be met with broadband services and those with very low Internet usage.

MPLS is future proofed as it supports Multicast and IPv6. In summary, MPLS L3VPN's have been the cornerstone of Public Services Networks since their inception.

2. Internet VPN Service

Until recently, constructing an Internet-based WAN using commercial off the shelf encryption was not possible in the UK Public Sector. But the changes introduced by the Government Security Classification Policy (GSCP) in April 2014 permits OFFICIAL traffic to cross unassured networks, such as the Internet, provided it is protected by **CPA Foundation Grade IPSec VPN**. This regulatory change when combined with the increasing reliability and availability of broadband Internet services now makes Internet-based WAN possible for the 80-90% of UK Public Sector traffic which is now estimated to fall into the OFFICIAL category.

Table 1. Comparing PSN MPLS and Internet VPN's

	PSN MPLS L3VPN	Internet VPN
Assurance	PSN Assured	None
Security	Limited to PSN members only No Internet access Data sovereignty guaranteed	Open Data sovereignty uncontrolled
Service Levels	SLA backed	Availability SLA only
Quality of Service	Supported	None
Connectivity	Wired	Wired & Wireless options
Suppliers	Restricted to DNSP's	Unrestricted

The quick lead time and short contracts on commercial broadband services can support the UK Government's real-estate rationalisation and consolidation programmes by:

- extending connectivity to temporary sites or new builds well in advance of the installation of a primary MPLS service,
- avoiding the financial commitments of a 3 or 5 year WAN contract at sites where closure is a possibility,
- supporting flexible working initiatives by extending secure connectivity to homeworkers with Cisco Virtual Office (CVO)

Internet Based WAN utilising wireless connectivity such as unlicensed microwave, satellite and 3G/4G mobile services enables great flexibility and agility and can be employed to:

- provide secure connectivity for temporary or mobile locations, e.g. ad-hoc vaccination centres during a pandemic
- provide resilience for a wired primary connection
- restore connectivity to a site suffering an extended outage on their primary connection

Internet based WAN can also aid greater productivity and efficiencies from smarter working by:

- extending network connectivity into non-public sector buildings to assist with the efficient delivery of services, e.g. residential care homes where NHS and Local Authority Social Care staff attend regularly.

3. Direct Internet Access

A solution to the ever increasing growth and reliance on Internet services is to introduce Direct Internet Access (DIA) into branch offices. DIA has many advantages over backhauling Internet traffic. Firstly, from a commercial perspective adding a broadband service to a branch provides:

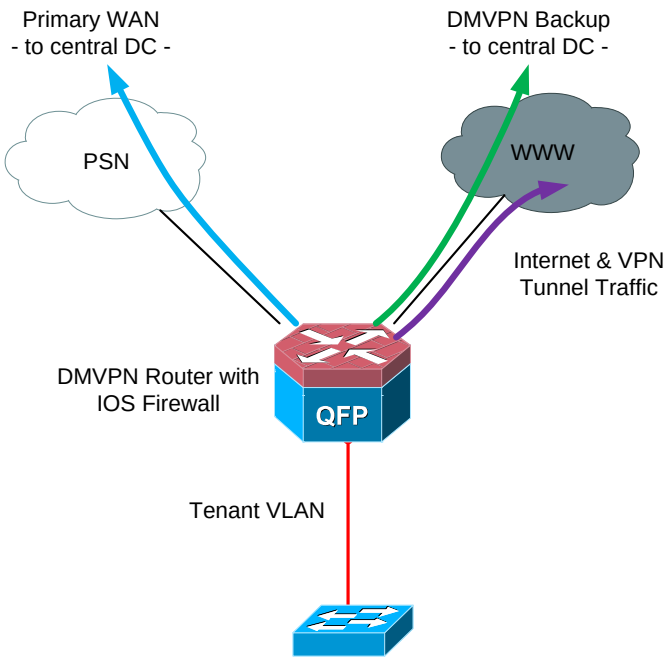
- **Supplier independence** – PSN MPLS and broadband Internet services can be procured from suppliers on Lot1 of the RM1045 Network Services framework;
- **Bandwidth at lower cost** – the price per Megabit (Mb) for broadband services is significantly lower than the MPLS equivalent;
- **Shorter Contracts** – broadband Internet contracts are much shorter allowing greater flexibility for customers;
- **Avoid MPLS Upgrades** – by offloading non-critical branch traffic from the MPLS WAN and central Internet pipe, bandwidth upgrades can be avoided and the performance of business critical applications improved

From an operational perspective, DIA at branch provides:

- **Transport Independence** – PSN MPLS services are delivered over wired connections only and typically are Ethernet fibre or copper-based FTTC or xDSL offerings. Internet connectivity can include these options but also offer wireless options such as 3G/4G, satellite or unlicensed microwave which can extend connectivity to rural, temporary or mobile locations.
- **An Efficient Path to Cloud Applications** – traffic from branch users to cloud applications goes direct rather than indirectly over the MPLS WAN and central Internet connection. This improves the user experience when using cloud-based applications.
- **Improved performance of on-premise/private cloud applications** - in a hybrid WAN which combines MPLS and DIA services, the performance of on-premises business critical apps is improved by reducing the utilisation on the MPLS circuit through offloading non critical traffic onto the DIA path
- **Supplier Resilience** – If each branch has its own local Internet access, a failure or outage of the central Internet connection will have minimal impact on the branch especially in accessing public cloud services. For most local government organisations the council Internet access “piggybacks” on the education service Internet provided by JANET so moving the branches to commercial ISP’s introduces a level of carrier resilience.
- **Security** - the branch router requires only a single public IP which is typically supplied from the ISP’s address range using DHCP. Providing the IP is not registered in DNS, the branch is hidden from would be attackers among all the ISP’s other customers.

The main disadvantage of DIA at branch is the need to replicate the security controls at the central DC into each branch which increases the management overhead. But whereas the security controls at the central DC are likely to be separate devices, in the branch all the security functions (Stateful ZBFW, IDS/IPS & Cloud Web Security) can be performed by only a single device, the ISR router.

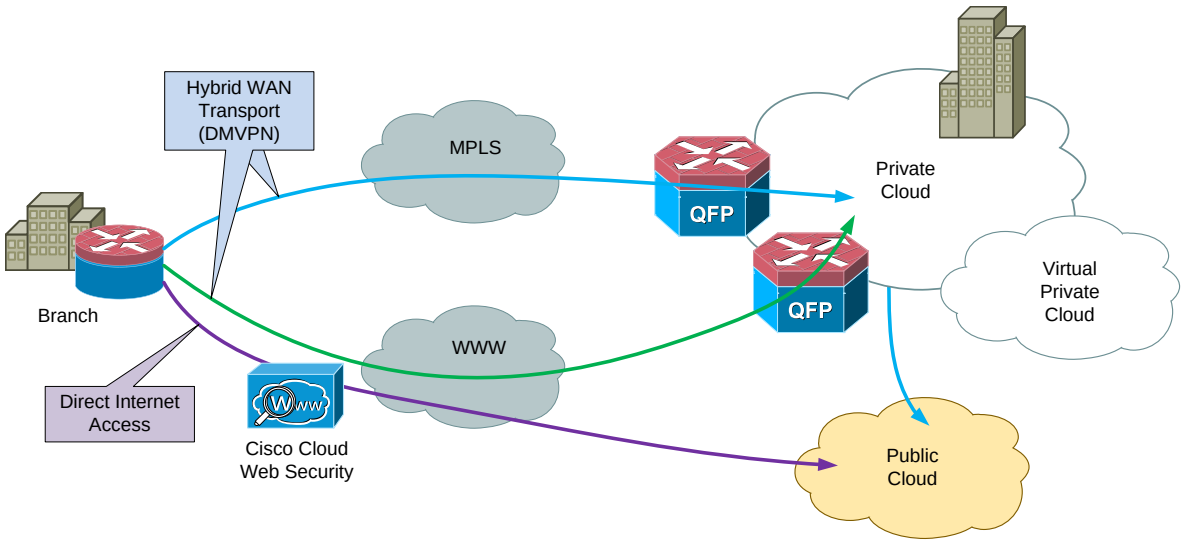
Figure 1. Direct Internet Access schematic



4. Hybrid WAN Architecture

Once a DIA service is added to a branch for local Internet breakout then a DMVPN network over the Internet can be combined with the primary MPLS circuit to create a Hybrid WAN. In the most basic form of Hybrid WAN, the Internet DMVPN offers a secondary resilient path as backup to the primary MPLS service with failover controlled by dynamic routing protocol. However, the true benefits of a Hybrid WAN are experienced when the two connections are used simultaneously in an active/active configuration using Cisco's Intelligent WAN technology.

Figure 2. Hybrid WAN with MPLS & Internet Transport and DIA



5. Which WAN Solution is Right for Me?

The choice between MPLS and Internet WAN can be influenced by the ratio of Internet traffic to on premise generated at each location. For sites, where the majority of traffic is Internet such as a library, it would be sensible to opt for DIA with corporate traffic carried in an overlay VPN. In contrast to this, sites with low Internet use may prefer to remain on MPLS for the performance and availability service level guarantees offered by the service provider.

Table 2. WAN Profiles

Branch Type	Example	Resilient WAN	Internet Usage	UC Usage	Feasible Options
SOHO	Leisure Centre	No	Low	Yes	Internet WAN
	Primary School	No	High	Yes	Internet WAN & DIA & Intelligent Caching
Small	GP Surgery	Yes	High	Yes	Hybrid IWAN & DIA & Intelligent Caching
Medium	Fire Station	No	Low	Yes	MPLS
	Secondary School	No	High	Yes	Internet WAN & DIA & Intelligent Caching
	Police Control Room	Yes	Low	Yes	Dual MPLS WAN
	Health Centre	Yes	High	Yes	Hybrid IWAN & DIA & Intelligent Caching
Campus	Central Government	No	Low	Yes	MPLS
	HEFE College	No	High	Yes	Internet WAN & DIA & Intelligent Caching
Large	Contact Centre	Yes	Low	Yes	Dual MPLS IWAN
	Hospital Trust	Yes	High	Yes	Dual MPLS IWAN + DIA & Intelligent Caching
Data Centre	Data Centre	Yes	High	Yes	Dual MPLS + Dual Internet IWAN

Cisco's Intelligent WAN (IWAN)

Cisco's Intelligent WAN (IWAN) consists of four components:

1. Transport Independence
2. Intelligent Path Control
3. Application Optimisation
4. Secure Connectivity - CPA Foundation Grade IPsec VPN

1. Transport Independence

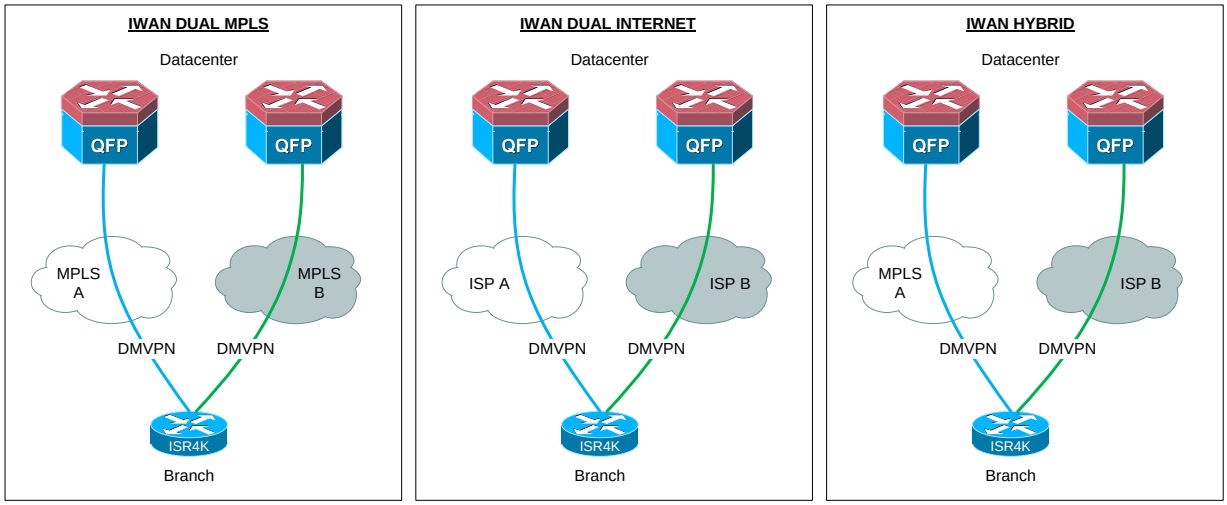
IWAN is an overlay VPN service which has Foundation Grade CPA assured Dynamic Multipoint VPN (DMVPN) as its foundation. DMVPN provides transport independence and simplifies the network by:

- Offering a platform which is agnostic to the underlying carrier network, ie. MPLS or Internet
- Allows the use of many different connectivity types such as Ethernet, xDSL, 3G/4G, etc… allowing the consumer to select the most appropriate connectivity for each branch
- Presenting a consistent configuration to the operator regardless of the underlying connectivity

IWAN can be deployed in one of three models:

- Dual MPLS
- Dual Internet
- Hybrid – MPLS & Internet

Figure 3. IWAN Models



All three models feature:

- Active / Active WAN paths
- One DMVPN for each transport network
- A single WAN Routing Domain (iBGP or EIGRP)

In a Hybrid IWAN deployment, DMVPN has the flexibility to enable IPsec protection on the Internet path and disable IPsec on the MPLS path (assuming the MPLS is a PSN Assured service).

2. Intelligent Path Control

Intelligent Path Control – is based on Performance Routing v3 and can:

- **Improve application availability and performance** - PfRv3 uses the application classification and real-time performance data provided by NBAR2 and Performance Monitor to dynamically adjust the routing of individual applications to ensure their performance requirements are met and outages or brownouts are avoided. This is more advanced than standard routing based on the reachability and metrics of destination network prefixes, e.g. with Intelligent Path Control a voice call may be rerouted because delay, jitter or packet loss on the primary path are causing a degradation in call quality even though the primary network path is still available. With standard routing, as long as the primary path is available the voice calls would continue to use it and call quality would suffer
- **Enables utilization of all WAN bandwidth** - PfRv3 load-shares by default, i.e. it actively tries to maintain an equal split of traffic across all links. By putting resilient links into a building in an active/standby configuration the customer pays for twice as much bandwidth as is actually needed but has half of it idle waiting for an outage on the primary. By load-sharing with PfRv3, both links are actively forwarding traffic.
- **Lower WAN costs** - PfRv3 enables the offloading of non-business critical applications from the MPLS connections onto the lower cost Internet paths. This frees up bandwidth on the MPLS connections for business critical applications that require the performance SLA and QoS provided by MPLS services

The load-sharing capability of IWAN also offers a potential solution to sites that are bandwidth limited through:

- distance from xDSL services

- high excess construction charges for installation of Ethernet fibre services

In these cases IWAN could be used in place of proprietary L1/L2 xDSL bonding mechanisms to aggregate multiple xDSL services at L3.

Despite the improvement in uptime and availability of Internet broadband connections, the lack of SLA's and QoS on Internet services can remain a barrier to some organisations adopting Internet-based WAN's for critical public services. Similarly, QoS is not yet available on any production 4G LTE network. However, the Intelligent Path Control incorporated into IWAN can mitigate the lack of QoS on Internet and 4G networks by dynamically shifting applications to the best performing path to maintain application performance.

3. Application Optimisation

Application Visibility – uses a form of Stateful Deep Packet Inspection called **NBAR2** to identify and classify applications as they traverse the network and **Performance Monitor** which collects and reports performance metrics of the applications. Application Visibility when combined with QoS mechanisms can ensure business critical web or cloud-based applications have priority over web browsing or guest Internet traffic across the network.

- **NBAR2** is invaluable as it is no longer practical or possible to classify applications based on Access Control Lists (ACL's) as:
    - the applications are moving to the cloud so the destination IP address is variable.
    - applications are all standardising on HTTP/S for transport. Distinguishing between business critical applications and web browsing is no longer possible using L4 port information alone.
    - Applications are increasingly adopting encryption such as HTTPS
- **Performance Monitor** – is embedded into the router and:
    - collects performance metrics such as bandwidth usage, response time and latency of TCP applications and jitter, delay, latency and loss of RTP applications such as voice
    - can export the performance data to external management platforms in NetFlow v9 or IPFIX formats for use in capacity management or traffic analysis reporting
- **Application Acceleration** – WAAS embedded into the ISR4000 router as ISR-WAAS or for greater scalability as vWAAS running on a UCS-E server module
    - TCP Optimisation
    - Data Redundancy Elimination (DRE)
    - Compression
    - Application Specific Optimisation – eg. packet multiplexing
- **WAN Offload** – Akamai Connect
    - Intelligent Caching – dynamic content inc Youtube videos, Apple OS
    - Pre-positioning

4. Security

As a minimum, securing a Hybrid or Dual Internet IWAN branch requires:

- **CPA Foundation Grade IPSec enabled DMVPN**: with strong cryptography to provide confidentiality and integrity to OFFICIAL data crossing the Internet.
- **IOS Zone Based Firewall:** to secure the Internet facing edge
- **Front Door VRF and Inside VRF:** to segregate internal networks from the Internet

Security at the branch can be further enhanced by the CPE router by employing:

- **FirePower Threat Defense for ISR**: installed on a dedicated UCS-E server module within the ISR 4000 or G2 series routers. It provides Next Generation IPS, URL Filtering, Application Visibility and Advanced Malware Protection (AMP);
- **Snort IDS/IPS for ISR**: runs on a dedicated services CPU core in the ISR4000 router. Snort provides basic IDS/IPS protection;
- **Cloud Web Security:** the ISR router transparently redirects HTTP requests to the Cisco Cloud Web Security proxy servers. CWS provides content filtering, threat based analytics and Advanced Malware Protection;
- **OpenDNS**: provides content filtering

Dynamic Multipoint VPN (DMVPN)

Dynamic Multipoint VPN is a Cisco IOS feature that combines standards based protocols, GRE, NHRP and IPsec together to form a solution that can deliver very large-scale overlay VPN networks with relatively simple configuration and little operational overhead.

Table 3. DMVPN key features

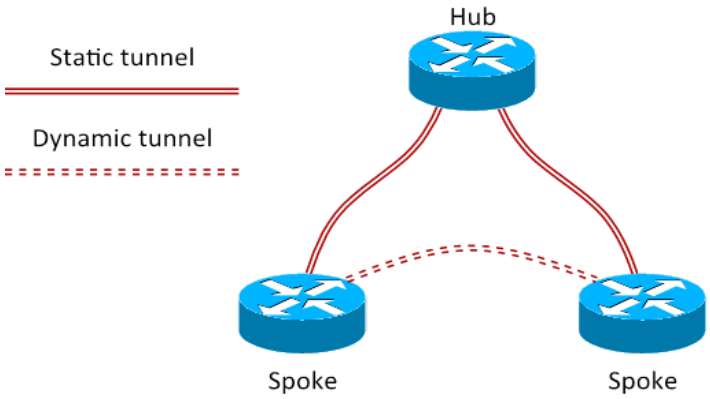
Modes	Encryption	IP Features	
Hub & Spoke	**CPA Assured**	**BGP, EIGRP, RIP, OSPF**	**IPv6 (Payload/Transport)**
Dynamic Full mesh	**Interim, Foundation, PRIME**	**VRF, MPLS, QoS**	**TrustSec Security Group Tags**

Routers participating in a DMVPN network are classed as “Hubs” or “Spokes”. Hubs are typically placed in the Data Centers closest to the applications. Hubs have Multipoint GRE (mGRE) interfaces through which they maintain permanent tunnels and routing adjacencies with each of the spokes. Spokes can be added to a DMVPN network without requiring any additional configuration on the hub.

In hub and spoke DMVPN deployments, all spoke-to-spoke traffic passes through the hub. But in dynamic full-mesh deployments, only the first packets in a spoke-to-spoke flow are routed through the hub. The hub reacts to the first packets in the spoke-to-spoke flow by sending NHRP indirect messages to the spokes which instruct them to create a dynamic on-demand tunnel. Subsequent packets in the flow are then routed directly between the spokes via the on-demand dynamic tunnel.

DMVPN is fully VRF-aware. This allows DMVPN tunnels to be sourced from and attached to VRF’s on a Cisco router as well as the global/default routing table. Cisco routers can join multiple DMVPN networks with each in a separate VRF if required. This flexibility allows multiple customers in a shared building to share a DMVPN router with each tenant constructing a different overlay topology to suit their individual requirements.

Figure 4. DMVPN Static and Dynamic Tunnels



DMVPN can also take advantage of Front VRF (fVRF) and Inside VRF's (iVRF) which allow the tunnel source interface and the tunnel interface to be in different VRF's. The tunnel source interface is placed in the fVRF and the GRE encapsulation/decapsulation process forms a secure "conduit" through to the tunnel interface placed in an iVRF. This allows the Internet to be used as a tunnel transport network safely as the Internet connection is placed in a separate VRF to the internal corporate networks.

CPA Foundation Grade IPSec Requirements

Internet based DMVPN must use one of the following CESG approved IPsec profiles. At time of writing, the guidance[1] states:

- Foundation profile is suitable for protection of OFFICIAL until 31st December 2021. This will be reviewed on an annual basis
- The use of "PSN Interim" profile is acceptable only until 31st December 2018
- All VPN deployments should migrate to Foundation or End-State PRIME by 1st January 2018.

Table 4. CESG Foundation and PRIME cipher suites

Algorithm	Foundation	End-State PRIME
Encryption ESP	AES-CBC 128	AES-GCM 128
Key Exchange	IKEv1	IKEv2
Hash	HMAC-SHA256-128	HMAC-SHA256-128
Diffe-Hellman	Group 14	Group 19
Authentication	RSA X.509v3	ECDSA 256bit X.509v3
Certificate Enrollment/Re-Enrollment	SCEP	EST

[1] CESG document – Network Encryption at OFFICIAL v2.3
[2] Performance data for the ISR4000, ISR G2, ASR1000 and selected 800 series models using the Foundation profile are available under a non-disclosure agreement (NDA). Please contact your Cisco Account Manager for further details.

Simplified WAN Management

In-house vs managed service – drawbacks of self-management are the perception that WAN's have:

- complex routing and QoS configurations requiring advanced technical (CCNP/CCIE) skills to design, build and operate. For instance, most MPLS VPN services require a BGP peering between the customer and SP networks.
- a lack of automation, e.g. a change to the QoS policy to support a new application requires a configuration change to made manually on every WAN router

This has led to many organisations adopting managed service contracts for their WAN over retaining WAN management in-house. However, the emergence of Software Defined WAN's (SD-WAN's) which hide the complexity of WAN operation behind the user friendly GUI of a controller offer to simplify WAN operation in the same way the introduction of Wireless LAN Controller's drastically simplified wireless LAN operation.

Cisco offers two management products, Prime Infrastructure 3.0 and the APIC-EM SDN Controller which work in conjunction to simplify, automate, orchestrate and monitor an Intelligent WAN.

Cisco Prime Infrastructure's IWAN management capabilities include:

- **Out-of-the-box support:** for technologies such as Intelligent WAN (IWAN), Application Visibility and Control (AVC), Zone-Based Firewall, and Cisco TrustSec® 2.0 Identity-Based Networking Services, it helps you get the most from your Cisco devices as quickly as possible.
- **Deep application Visibility:** PI configures and uses embedded Cisco instrumentation and industry-leading technologies for application visibility and network policy optimization. These technologies include NetFlow, Network-Based Application Recognition 2 (NBAR2), Simple Network Management Protocol (SNMP) and more.
- **Simplified deployment of Cisco Validated Designs:** PI includes guided workflows based on Cisco's Validated Designs and best practices that radically simplifies the deployment and management of Cisco IWAN devices and services. The workflow speeds up provisioning of services such as Dynamic Multipoint VPN (DMVPN) and Performance Routing (PfR) and simplifies quality-of-service (QoS) configuration and monitoring. The PfR monitoring dashboard provides visibility into how application path optimization is working on and aids troubleshooting of route change events driven by IWAN.
- **APIC-EM Integration:** Integration with the Enterprise SDN Controller (APIC-EM), provides the ability to automate new device deployment using Zero Touch Provisioning capabilities (https based PnP agent) in the Cisco network devices. In addition, PI can request the APIC-EM PKI (Public Key Infrastructure) Service to securely deploy a router with PKI for an IWAN deployment with DMVPN.

The Open Networking User Group has defined a Software Defined WAN (SD-WAN) as consisting of 10 mandatory elements. The following table details how Cisco IWAN meets those requirements.

Table 5. Open Networking User Group (ONUG) SD-WAN Components

	ONUG Requirement	IWAN
1	**Any Hardware:** Deploy CPE in physical or virtual form factor on commodity hardware	ASR1000, ISR4000, CSR1000v
2	**Zero-Touch Deployment:** With minimal configuration changes for agility in provisioning and deployment	APIC-EM ZTD, PI 3.0 PNP
3	**Highly Secure Hybrid WAN:** Dynamic traffic engineering across a public or private WAN based on application policy, and aware of network availability or degradation	NGE, DMVPN, PfRv3
4	**Active-Active Architecture:** Remote sites connect to applications through a public or private WAN	DMVPN, PfRv3
5	**High Availability and Resilient WAN:** Optimal for client user experience	PfRv3
6	**Layer 2 and 3 Interoperability:** With a directly connected switch and/or router	Broad range of L2 & L3 LAN interface modules, Onboard PoE, vWLC
7	**Visibility, Prioritization, and Steering Applications:** Specifically business-critical and real-time applications per security, corporate governance, and compliance	PfRv3
8	**Management Dashboard**: By site, application, and VPN performance level	APIC-EM, PI 3.0 and ecosystem of 3rd parties, eg. LiveAction, Glue Networks
9	**Open North-Bound API for Controller:** For access and management, forward specific log events	Northbound REST API on APIC-EM
10	**FIPS 140-2 Validation Certification:** For cryptography modules and encryption with automated certificate lifecycle management and reporting	

Note: The PKI element of the APIC-EM IWAN app is not robust enough for use in public sector IWAN deployments at present

Agility & Efficiency

Akamai Connect

Cisco's IWAN with Akamai Connect combines technology from Cisco such as security, WAN Optimization, path selection, and application visibility and control; with Akamai's caching and application optimization technology inside the Cisco ISR.

Customers can receive access to information instantly, inside a branch office, uplifting their experience with video, cloud/mobile apps, and social media.

Cisco's IWAN with Akamai Connect provides businesses with a secure, cost effective way to migrate their traditional WAN to an agile Hybrid WAN giving IT the ability to truly leverage mobile, cloud, and digital.

Scalability

As application delivery shifts from local installations to private or public cloud delivery and the number of network devices and video usage increases, WAN bandwidth upgrades will inevitably be required. In many instances this will require CPE hardware to be swapped with associated expense of a field engineering visit for both the service provider and the customer. Performance on-demand licensing on the ISR4000 router allows the performance of the CPE to be doubled (or tripled in the ISR4331) with the application of a license key and avoids downtime for the customer and a costly truck-roll.

Virtualisation & Green IT

Public sector bodies are increasingly aware of the benefits of Green IT both for environmental and financial reasons and are adopting virtualisation technology for operational flexibility benefits and to maximise the utilisation of assets. New CPE router models can assist with these goals firstly from being energy efficient, but also by allowing the consolidation of multiple devices into a single unit to save on rack space, cabling, power, cooling and management costs. For instance, at small sites such as GP surgeries, local switches can be consolidated into the CPE chassis through Etherswitch modules and local servers can be virtualised onto UCS-E server modules where necessary or warranted.

For More Information

Read more about the Cisco Intelligent WAN solution, or contact your local Cisco account representative.

Additional details are available on Akamai Connect.

The Government Digital Service (GDS) hosts details of the Common Technology Services (CTS) blueprints online.

Disclaimer

Cisco's policy is one of continuous improvement and the specifications and information regarding the products in this document are subject to change without notice. All statements, information, and recommendations in this document are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products. The software license and limited warranty terms are set forth in the information pack shipped with the products and are incorporated herein by this reference

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 CXX-XXXXXX-XX 10/11