# HP Dynamic Virtual Private Network (DVPN) Solution

Simplifies your WAN connectivity across a distributed enterprise

## Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>The traditional VPN overlay model</td>
<td>2</td>
</tr>
<tr>
<td>Our solution: HP DVPN</td>
<td>3</td>
</tr>
<tr>
<td>What is DVPN?</td>
<td>3</td>
</tr>
<tr>
<td>HP FlexNetwork Architecture and DVPN</td>
<td>3</td>
</tr>
<tr>
<td>HP DVPN is ideal for</td>
<td>5</td>
</tr>
<tr>
<td>Features and benefits</td>
<td>5</td>
</tr>
<tr>
<td>Components</td>
<td>6</td>
</tr>
<tr>
<td>Secure tunnel establishment</td>
<td>6</td>
</tr>
<tr>
<td>Products supporting HP DVPN</td>
<td>7</td>
</tr>
<tr>
<td>HP DVPN and routing</td>
<td>7</td>
</tr>
<tr>
<td>Hub-and-spoke topology</td>
<td>8</td>
</tr>
<tr>
<td>Features</td>
<td>8</td>
</tr>
<tr>
<td>Full-Mesh (FM) topology</td>
<td>9</td>
</tr>
<tr>
<td>Features</td>
<td>9</td>
</tr>
<tr>
<td>Conclusion</td>
<td>9</td>
</tr>
<tr>
<td>It's time to rethink your network</td>
<td>10</td>
</tr>
</tbody>
</table>
Introduction

As enterprises grow, more remote branch and regional offices are being opened across the globe to scale up the business. As a result, a large portion of the enterprise workforce is now working remotely, away from the corporate office. Virtual private networks (VPNs) provide this workforce with secure access to business-critical resources within the enterprise network. It enables users in remote sites to be productive without compromising the security of the enterprise network.VPNs are critical for helping ensure the confidentiality, integrity, and availability of the information across distributed enterprise networks. There are two ways in which they are used: to connect two geographically separated locations that are not physically connected to each other—site-to-site VPN; and where individual users connect to a remote LAN—end-to-site VPN. In this white paper you will learn about simplifying site-to-site VPN with the HP DVPN solution.

Traditional private line and legacy WAN circuits at each branch or remote site are costly. A site-to-site VPN enables enterprises to securely connect remote users to corporate resources via low cost ISP transport, high-speed broadband links (such as T3, E3, T1, E1, xDSL), and so on. But site-to-site VPN is complex and hard to manage and deploy on a large scale, especially across multiple sites. Imagine how much time and effort would be required for an administrator to set up the site-to-site VPN configuration for each router deployed across the distributed enterprise. Even with the enormous benefits of VPN technology, there are significant operational challenges such as complexity and scalability to implement this technology, especially in a large corporation. This white paper discusses the unique HP approach to solving the challenges around deploying simple, secure, and cost-effective WAN connectivity in a large distributed enterprise.

The traditional VPN overlay model

In the overlay model, a VPN is deployed on a public network infrastructure and utilizes the same security, management, and quality of service policies that are applied in a private network. Routers in the overlay (figure 1) can be directly connected by logical links over the public network or the Internet. Enterprises running overlays have the flexibility to build their networks, independent of the underlying WAN transport they selected.

The best example of an overlay VPN is a site-to-site IPsec VPN deployment for a large enterprise that is connecting multiple remote branch and regional offices to its corporate headquarters or data center. There are scalability and support concerns with this approach when connecting multiple remote branches due to the large number of manually configured tunnels. With a traditional site-to-site IPsec VPN, there is additional complexity related to routing protocol configuration, the need for generic routing encapsulation (GRE) tunnels in addition to the IPsec tunnels; matching encryption options for each endpoint; and supporting other IP protocols—which can keep even the most tech-savvy administrators busy for days. As a result, enterprises are looking to reduce complexity around deploying secure WAN connectivity, reduce time to service by automating connectivity, and deliver an agnostic solution with standards-based encryption to secure communication between branch or regional offices and corporate headquarters.

In recent years, government regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Payment Card Industry—Data Security Standard (PCI-DSS) have mandated strong encryption to secure data while in transmission on public and private IP networks. A site-to-site VPN is a secure way of connecting to a private LAN from a remote branch or regional office to access information at the corporate headquarters or data centers.
Figure 1: Traditional enterprise IPsec VPN architecture

Our solution: HP DVPN

What is DVPN?

A hub-and-spoke VPN architecture allows multiple remote branch and regional offices (spokes) to establish site-to-site IPsec VPN tunnels to secure connectivity to the headquarters or data centers (hub). HP Dynamic VPN (DVPN) is not a protocol, but an architecture. HP DVPN helps enterprises simplify the configuration and management of IPsec VPN tunnels. HP DVPN policies share security access, management, and quality of service (QoS) policies to easily connect thousands of remote branch and regional offices to the corporate headquarters or data centers. Administrators no longer need to login to each VPN device to manually set up site-to-site VPN tunnels at each branch or regional office, corporate headquarters, and data centers. HP DVPN is an innovation to simplify secure WAN connectivity for the enterprise.

HP DVPN is a complete and cost-effective solution that is ideal for the hub-and-spoke topology, the most common topology for enterprises, where you also have an option for mesh connectivity. HP DVPN is a complete solution that spans across various domains such as routing, security, and address management.

HP FlexNetwork Architecture and DVPN

HP FlexNetwork Architecture is the industry’s leading end-to-end architecture comprising the HP FlexFabric for a converged and secured data center; HP FlexCampus for unified campus; and HP FlexBranch for simplified branch office solutions. HP FlexManagement provides the visibility and operational simplicity across the entire architecture with a single management platform. This architecture is open, scalable, secure, agile, and delivers a consistent experience across all three solution domains. HP DVPN simplifies the interconnectivity between data center, campus, and branch either with a hub-and-spoke or a full-mesh topology, further enhancing our proven FlexNetwork Architecture. Find out more about the HP FlexNetwork Architecture at [hp.com/networking/FlexNetwork](http://hp.com/networking/FlexNetwork).
The HP DVPN architecture interconnects the FlexFabric, FlexCampus, and FlexBranch building blocks of the HP FlexNetwork Architecture. HP DVPN solution can connect up to 3,000 sites into a single DVPN domain. The solution can be scaled to very large networks by connecting up to 10 DVPN domains (using the HP 6600 router series).

- HP DVPN provides a mechanism to automatically setup IPsec VPN tunnels over the Internet. Benefit from the simplicity and automation of deploying IPsec VPNs with HP DVPN. HP DVPN also offers a lower cost, and yet, is a highly effective solution when compared to Multi-Protocol Label Switching (MPLS) WAN.
- HP DVPN is an architecture designed for hub-and-spoke topologies. Customers can also implement a full-mesh topology with HP DVPN.
- HP DVPN creates dynamic site-to-site IPsec VPN tunnels while simplifying configuration and management. HP DVPN uses standards-based protocols to provide a complete solution for your organization.
- The VPN configuration on the hub is dynamically updated whenever a new spoke is added or deleted.
- In short, HP DVPN provides highly automated, secure WAN connectivity with little management overhead.

Figure 3: A simple graphical representation of the HP DVPN solution
HP DVPN is ideal for

- Payment Card Industry-Data Security Standard (PCI-DSS) requirements to securely connect retail sites that have ATMs and POS systems to data centers for encrypted payment card processing
- Enterprises connecting multiple remote branches and regional offices to the corporate headquarters
- Sites moving away from expensive MPLS-based VPNs, private line, or legacy links (ATM, Frame Relay) to low cost, broadband access links (such as T3, E3, T1, E1, xDSL, etc.) via IPsec tunnels
- Enterprises that want a backup for the MPLS WAN
- Sites where government regulations have mandated traffic encryption for private IP networks

Features and benefits

- HP DVPN helps eliminate the need for static configurations per spoke—simplifying management and deployment. The hub or spoke can be assigned a different address every time a router comes up when using DHCP or PPPoE. Using a static configuration makes this very complex and time consuming in a large network.
- HP has defined a simple protocol called VPN Address Management (VAM) that helps simplify management and configuration challenges in an automated way.
- Dynamic Key Exchange for IPsec is achieved using standards-based Internet Key Exchange (IKE). This helps prevent issues that are caused by long-lasting manual keys as well as key rollovers—highly essential for enterprise security. Perfect Forward Secrecy (PFS) is an optional feature in IPsec IKE protocol. It helps ensure that a session key derived from long-term public and private keys will not be compromised if one of the private keys is compromised in the future. In other words, when keys are generated for a session, the new key is not dependent on the current key. With this, even if one key is compromised, no other keys can be derived as a result of that. HP DVPN performs a new Diffie–Hellman (DH) exchange every time a new key is derived.
- AAA server (authentication, authorization, and accounting) is used to authenticate the digital identity of users/devices and, if applicable, authorize what level of rights or activities a user/device can perform. The accounting part tracks aspects of authorized or unauthorized activities and is used for auditing purposes. In the HP DVPN solution, AAA is used purely for authentication of sites and devices—making HP DVPN a highly secure and reliable architecture.
- HP DVPN supports the use of Network Address Translation (NAT) on the tunnel interface and can operate behind a NAT gateway.
- HP DVPN routing protocols—such as OSPF, RIP, and BGP—can run natively over the DVPN tunnels. This means that the IT operator does not have to perform complex configurations and tweaks to make routing work on the DVPN tunnels.
- HP DVPN QoS support manages delay, bandwidth, and packet loss parameters on a network. The DVPN architecture supports Differentiate Services Code Point (DSCP)-based QoS with intelligent header manipulations. 1
- Support for primary and secondary VAM servers and hubs with a backup interface feature or active secondary connection to a different DVPN domain that offers enhanced redundancy. HP DVPN solves the scaling and configuration complexity inherent in overlay VPN, while reducing connectivity costs.
- As a module of Intelligent Management Center (IMC), Branch Intelligent Management System (BIMS) provides secure network management to the branch router using CPE WAN Management Protocol (CWMP) (TR-069) over SSL. It centrally manages zero-touch deployments for branch routers and solves the problem of effectively managing dynamically assigned IP addresses by service providers. BIMS also provides resource, service, configuration, alarm, and system management functions. It significantly improves network management efficiency.
- As a module of IMC, IPsec VPN Manager (IVM) provides HP DVPN service management with wizards that guide administrators during the configuration of new DVPN domains. It allows administrators to select device roles in a topology view and modify device settings; provides automatic discovery function for the DVPN domain; grants DVPN domain device management to allow device configuration comparisons with Network Management Server (NMS) configuration, helping identify configuration differences. IVM also offers support for QoS policy configuration and deployment (QoS module needed); provides branch traffic monitoring as well as branch-to-hub detection of tunnel connectivity.

---

1 The way DSCP QoS works is that it's classified as packets into categories. The benefit of rewriting inner packet to outer packet is when the inner packet and associated DSCP values are encapsulated into an IPsec packet. This way, the IPsec packet retains the DSCP values, allowing it to be treated based on QoS policies across the network path.
Components

The five main components of HP DVPN architecture are:

- **VAM server** (up to two VAM servers can be present in a DVPN domain to provide redundancy)
  - Receives registration information from DVPN nodes: A VAM server is the central entity managing all the addresses on behalf of the DVPN. It receives address mapping on behalf of the DVPN nodes and maintains these mappings.
  - Provides the public IP address of a peer to help setup secure tunnels: Though the server runs on a router, the VAM server can be a physically separate device from the hub router that forwards DVPN data traffic.

- **VAM client**
  - Registers its private IP address, public IP address, and VAM ID with the VAM server: The VAM clients are entities that register their addresses with the VAM servers and also perform peer address resolution using the server. The hubs, as well as the spoke routers, are VAM clients.

- **Hub** (up to two per domain to provide redundancy)
  - This component is the central device, located either in the data center or in the campus. A spoke can connect to two different hubs for redundancy purposes. An important consideration here is that both hubs are in a redundant configuration and can be active-active, which means both can forward data traffic at the same time. This feature was pioneered in the HP routers and can help balance traffic between the multiple active hubs.

- **Spoke**
  - The spoke is the gateway for the branch office or other remote location and helps forward data traffic to the hub. The hub and spoke establish IPsec tunnels between each other.

- **Authentication server**
  - The AAA server is used to authenticate the VAM clients. It requires reachability to the VAM server.

Secure tunnel establishment

- **VAM tunnel connection initialization (figure 4):** Once the spoke router (VAM client) is connected to the network, it initiates a connection with up to two VAM servers to negotiate VAM protocol packet encryption and integrity validation algorithms, generate keys, and acknowledge the negotiated result. The tunnel between the VAM client and VAM server is established at this phase.

- **VAM client registration (figure 5):** In this phase, the VAM server authenticates the VAM client (locally or using AAA). After the client has successfully authenticated, the client registers its information (public and private IP address, and VAM ID). In return, the VAM server sends the VAM client the hub’s corresponding registration information (public/private IP, and VAM ID).

- **Spoke-to-hub and hub-to-hub tunnel establishment (figure 6):** In this phase, the VAM client has the hub information and establishes a permanent tunnel with the hub. If there are two hubs in the DVPN domain, the VAM client establishes a permanent tunnel with both hubs. In DVPN domains with two hubs, a permanent tunnel is also required between the hubs. Data can be forwarded across the permanent tunnel at this point.

*Figure 4: VAM tunnel setup | Figure 5: VAM client authentication/registration | Figure 6: Hub/spoke IPsec tunnel setup*

*Note: The HP DVPN architecture provides modular design that is easy to comprehend and deploy.*
Products supporting HP DVPN

Refer to the table below to understand which HP DVPN component can operate on which networking products.

### Table 1

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware</th>
<th>Software version</th>
<th>Visual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoke/VAM client</td>
<td>All MSR routers</td>
<td>R1508—September 2007</td>
<td></td>
</tr>
</tbody>
</table>
| Hub/VAM client      | 6600 router series, All MSR routers | R2603 (for 6600)—July 2011  
R1508 MSR—September 2007 |        |
| VAM server          | 6600 router series, All MSR routers | R2603 (for 6600)—July 2011  
R1508 MSR—September 2007 |        |
| IMC Platform (Standard or Enterprise) | Server Wintel/Linux | IMC IPsec VPN Manager v5.1 (E0201L01)—February 2012  
IMC BIMS v5.1 (E0201)—February 2012 |        |

**Note:** We do not recommend configuring the hub as the VAM server in a DVPN domain unless it is a very small scale DVPN deployment and cost is a primary consideration. All HP MSR and 6600 series routers can be configured as a VAM server.

### HP DVPN and routing

- Support for BGP routing with up to 3,000 DVPN tunnels
- Supports OSPF
- For full-mesh topologies, we recommend using the OSPF broadcast interface type on the hub and spoke tunnel interfaces.

**Note:** For OSPF in small scale deployments, HP DVPN solution provides an “Instant-On enterprise” solution at the hub, so that you never have to reconfigure the hub whenever a new spoke is added. Visit [http://h17007.www1.hp.com/gr/en/products/routers/index.aspx](http://h17007.www1.hp.com/gr/en/products/routers/index.aspx) to learn more about HP routing solutions.

---

2 **Note:** 6600 router series can also be a spoke/VAM client for R2603—July 2011
Hub-and-spoke topology

Features

- The HP DVPN overlay is a non-broadcast multiple-access (NBMA) network and is configured as one subnet
- Spokes do not have direct connectivity with other spokes; all spoke-to-spoke traffic must traverse the hub router
- HP DVPN is optimized for hub-and-spoke topology

The hub-and-spoke topology has been enhanced to scale to a larger number of spoke routers per hub. We currently support 3,000 VPN (spoke) tunnels per 6600 series (hub) with BGP. This topology is also called the star topology, where all spokes are connected to each other through the hub router and there is no direct connection between the spokes.

---

NBMA means the network has multiple (more than two) end points, even though there is no generic address to send a broadcast address to all end points.
**Full-Mesh (FM) topology**

**Features**

- The HP DVPN overlay is an NBMA network just like the hub-and-spoke topology and is configured as one subnet
- In a FM topology or partial-mesh topology, direct connectivity between spokes is possible which makes the data flow direct between spoke sites, eliminating the hub as a step in the data path
- HP DVPN can support full mesh as well as partial mesh, but on a smaller scale than it does for hub-and-spoke

In this topology, every spoke is directly connected to every other spoke and can send data directly to the other spoke without traversing other routers in the network. This is in contrast to the hub-and-spoke topology.

**Conclusion**

HP DVPN is a simple, lightweight architecture that can support up to 3,000 spokes per DVPN domain. HP DVPN solution is highly scalable and automates complex site-to-site VPN configuration to securely connect remote branches and regional offices with the corporate headquarters and data center locations over any IP-based transport. HP’s innovative solution is based on standards-based protocols such as IPsec and offers highly secure connectivity. HP DVPN is architecturally superior as it separates the functions of the control plane and data-forwarding plane onto separate hardware allowing for greater scalability. HP DVPN solution enables distributed enterprises to reduce cost, complexity, and time to securely connect branches, regional offices, headquarters, and data centers.
It’s time to rethink your network

Build a simpler, yet superior WAN architecture with HP DVPN. Visit hp.com/networking/dvpn for more information.

Get connected

hp.com/go/getconnected

Current HP driver, support, and security alerts delivered directly to your desktop