Configuration guide

HP ADVPN with multiple configuration options

Table of contents

Introduction

The HP Auto Discovery VPN (ADVPN) solution provides a mechanism to automatically setup overlay IPsec VPN tunnels using address management, to provide inexpensive IP circuit connectivity over the public Internet or Wide Area Network (WAN) for hub and spoke and full mesh topologies. HP ADVPN is especially useful when branch offices have dynamic public IP addresses and secure connectivity to the corporate network is required. This offers enterprises considerably reduced WAN connectivity costs when compared to peer-to-peer MPLS VPN and considerably simplified configuration and management when compared to overlay IPsec VPN.

The HP ADVPN solution is based on the HP Comware 7 operating system and is the second generation of the HP Dynamic VPN (DVPN) solution, which is based on the HP Comware 5 operating system. HP ADVPN is compatible with HP DVPN solutions, with a hybrid system having the properties of HP DVPN.

This guide describes how to configure HP ADVPN using HP MSR Series next generation routers in a hub-spoke architecture where the required VPN address management (VAM) server co-resides on the same hubs that are used to connect the spoke (branch) connections and OSPF is used for routing. It also uses local authentication and authorization, when RADIUS, as an external authentication, is not available. The intended audience is HP Solution Architects, HP Technical Consultants, and HP partners and customers who want to become familiar with the HP ADVPN technology in a lab environment.

Background information

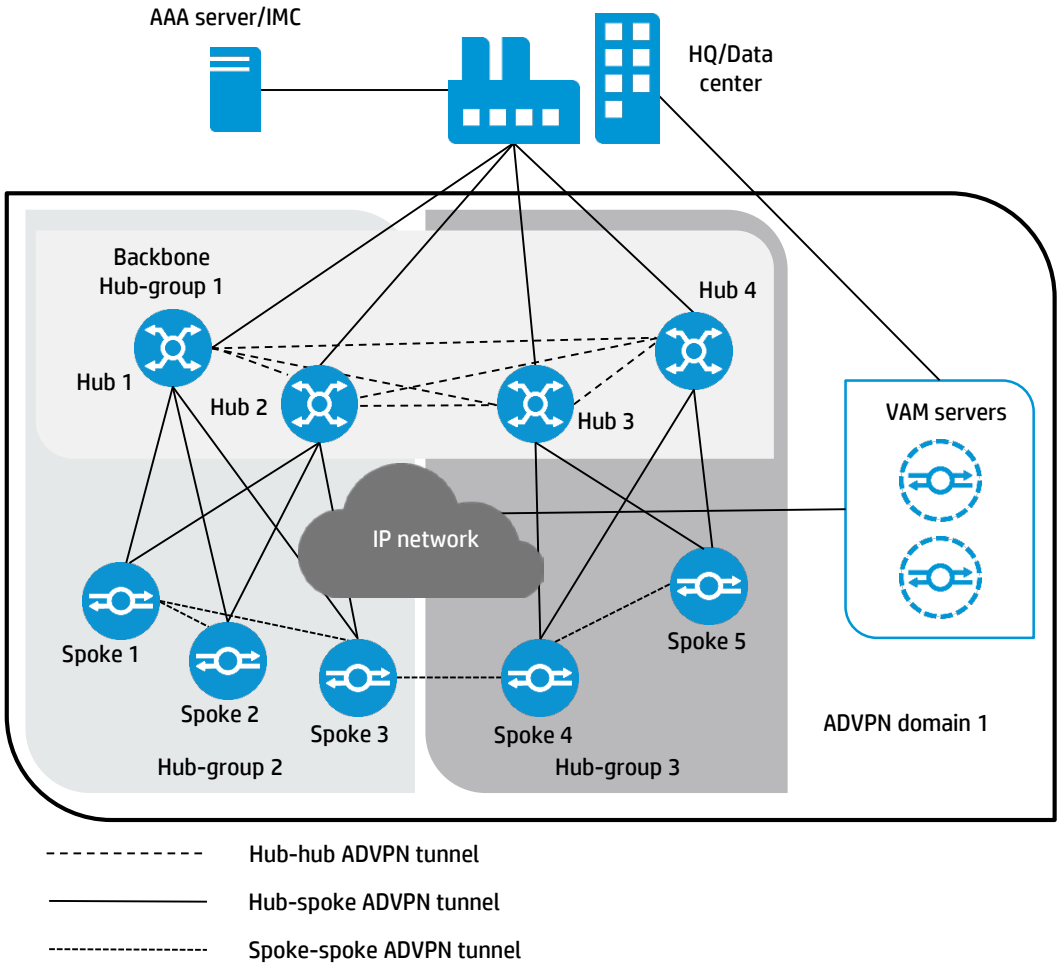
HP ADVPN Architecture

The HP ADVPN solution provides a mechanism to automatically setup overlay IPsec VPN tunnels using address management, to provide inexpensive IP circuit connectivity over the public Internet, for both hub-spoke topology and full mesh (spoke-to-spoke) topologies. This offers enterprises a considerably reduced WAN connectivity cost as compared to an MPLS WAN. However, it can also be run on top of a carrier provided MPLS connection, giving the customer an end-to-end encryption solution, which is easy to configure and maintain. HP ADVPN can run over any L3 topology, both public and private in a secure format. HP ADVPN provides an architecture that allows dynamic and secure communications, while reducing the management overhead that typical IPsec tunnels require.

HP ADVPN is an architecture and not a protocol. The HP ADVPN architecture is optimized for hub and spoke topologies. In the spoke-to-spoke topology, the traffic travels directly between the spokes bypassing the hubs, thus reducing the load on the hubs, which otherwise can very quickly become bottlenecks. HP ADVPN employs the client/server model. HP ADVPN supports two tunnel encapsulation modes: UDP and GRE. In this configuration guide, focus will be placed on a hub-to-spoke configuration with the VAM servers residing on the same routers that are also performing the hub functionality. Using this configuration eliminates the need to have additional routers acting as VAM servers. However, it is recommended that the VAM servers reside on separate routers to eliminate processing overhead when used in a production environment.

HP ADVPN can be incorporated into the HP FlexNetwork architecture, where HP MSR routers are used at the edge of the branch network and connect back to the HP FlexCampus and HP FlexFabric data center environments. This gives customers options on how they want to connect their branch offices to their corporate network, possibly utilizing the Internet for either primary or backup connections, providing redundancy at a lower cost point advantage.

Figure 1. Architecture of the HP ADVPN solution



Components of HP ADVPN

VAM

VAM is a major protocol used in the HP ADVPN solution. It collects, maintains, and distributes dynamic information to help set up an internal secure tunnel conveniently. When forwarding a packet for a subnet, the device first obtains its next hop on the private network through a routing protocol and the public network address associated with this next hop; then encapsulates the packet with the public address as the destination address of the tunnel; and finally sends the packet down the tunnel to the destination.

VAM server

A VAM server is the central entity managing all the addresses on behalf of the HP ADVPN solution. It receives address mappings on behalf of the HP ADVPN nodes and maintains these mappings. To re-emphasize an interesting point here, though the VAM server runs on a router, the VAM server can be a physically separate router from the one that forwards HP ADVPN data traffic. Two VAM servers can be present in an HP ADVPN domain, which provides redundancy by creating a primary/secondary VAM server environment.

VAM client

The next component is the VAM client. The VAM clients are entities which register their private and public addresses with the VAM servers and also perform peer address resolution using the server. The hub, as well as the spoke routers, acts as a VAM client.

- Hub

  A hub is a type of VAM client. As a central device of the HP ADVPN solution, it is the exchange center of routing information. A hub in a hub-spoke network is also a data forwarding center.

- Spoke

  A spoke is a type of VAM client. Usually acting as the gateway of a branch office, a spoke does not forward data received from other HP ADVPN nodes.

Hub-group

A hub-group is a structure that allows the HP ADVPN solution to accommodate more VAM clients, which allows the HP ADVPN solution to scale. This structure solves the problem that one hub cannot manage all clients, for example, because of a routing protocol's limit to neighbors. An HP ADVPN domain can contain multiple hub-groups. Each hub-group has one or multiple hubs and spokes.

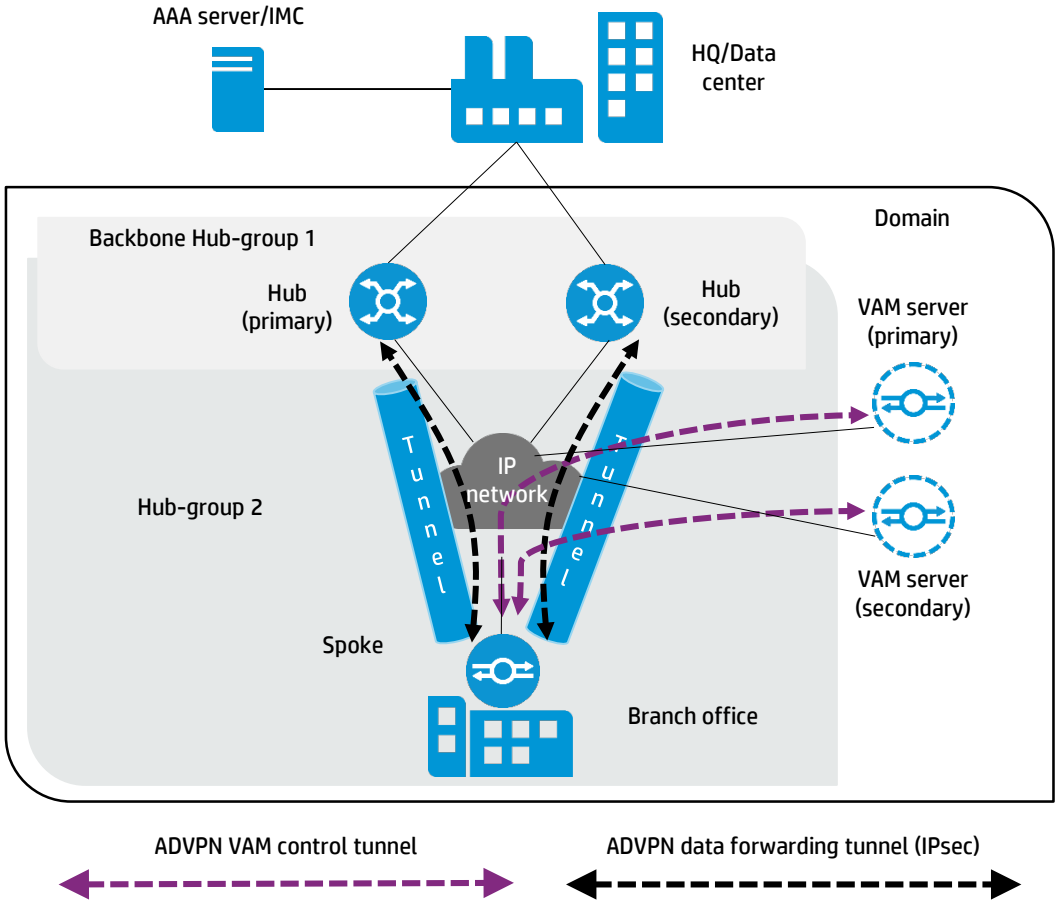
AAA Server

An Authentication, Authorization, and Accounting (AAA) server can be optionally used for user authentication and accounting.

Hub-spoke structure

In a hub-spoke HP ADVPN topology, each spoke establishes a permanent tunnel with the hub, but no tunnel can be established between two spokes, and data between spokes has to be forwarded through the hub. The hub is used as both the routing information exchange center and the data forwarding center.

Figure 2. HP ADVPN solution hub and spoke topology



Requirements

Readers of this document should be familiar with features and configuration of the HP MSR Series next generation routers and HP Comware switches that support OSPF and BGP.

The following hardware is required:

- Qty 1, HP MSR3024 Router Series (hub 1/VAM server 1)
- Qty 1, HP MSR4060 Router Series (spoke 1)
- Qty 1, HP MSR3044 Router Series (hub 2/VAM server 2)
- Qty 1, HP 5500-EI-24G-PWR Switch Series (HQ LAN)
  - Any switch that supports OSPF, BGP, and PoE may be used
- Qty 1, HP 6602 Router Series (WAN)
  - Any router or switch that supports OSPF and BGP may be used

The following software is required:

- HP MSR Router Series software version CW710-R0106P08
- HP 5500-EI-24G Switch Series software version CW520-R2208-s168

The following tools are required:

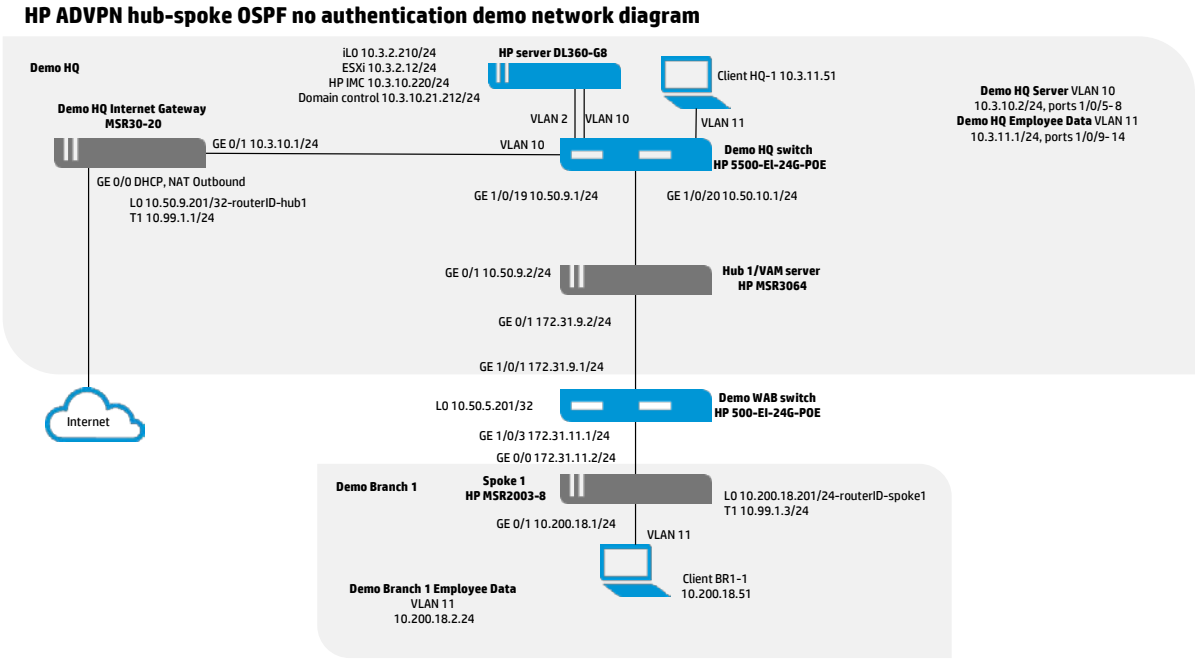
- Qty 2, laptop running Windows® 7 Professional (1 for HQ, 1 for branch)
- System console cable for switches and routers
- Tools for the laptop:
  - USB to DB9 serial adaptor cable
  - PuTTY utility
  - FTP client
  - Web browser (IE 10 is recommended; Safari, Chrome, or Firefox can be used)

ADVPN single hub configuration

Network diagram

Figure 3 illustrates the connectivity for this configuration.

Figure 3. Network diagram for HP ADVPN hub-spoke local authentication demonstration environment



Configure

Getting started

Login to router using CLI

With PuTTY running and connected to the device, you will see text as output on the display.

- Press `Enter` once to display a “username:” prompt
- The default username/password for new Comware 5 or Comware 7 device is “admin” with no password
- The default username/password for a device that may have been previously configured in the HP FlexBranch Demo environment is “admin” with a password of “admin”
- Enter the username and press Enter
- Enter the password and press Enter
- You will be in monitor<prompt> mode.

Save current configuration

If you have a device with a previous configuration, it is recommended to save the current configuration to a file name other than startup.cfg and then reset to factory defaults. Then you can begin your configuration knowing that the previous configuration will not conflict with the new configuration.

- Save the device configuration:

```
save
save configuration? y
Press RETURN
```

File management commands

These are miscellaneous HP MSR Router Series commands that may come in handy.

- To view the files on the flash:

```
dir flash:/
```

- To copy a file:

```
copy startup.cfg backup.cfg
```

- To rename a file:

```
rename startup.cfg clean.bak
```

- To delete a file:

```
delete <filename>
```

- To move into a directory or storage device:

```
cd <directory>
cd <storage device>
```

- To create a directory:

```
mkdir <directory>
```

- To delete a directory:

```
rmdir <directory>
```

- To delete files from the recycle bin to make room on the flash drive:

```
reset recycle-bin
```

Use the "?" key to receive contextual help on the display, use the tab key for command auto-fill and use "display this" for contextual view of the configuration.

Backup configuration

Backup the current configuration, follow these steps:

- From the device system console, where 'clean.bak' is an example:

```
rename startup.cfg clean.bak
```

Reset to factory defaults or previously saved configuration

If a device fails or you want to use it in a different scenario, you can restore the factory-default configuration for the device.

This command does the following:

- Deletes all configuration files (.cfg files) in the root directories of the storage media.
- Deletes all log files (.log files in the folder /logfile).
- Clears all log information (in the log buffer), trap information, and debugging information.
- Restores the parameters for the BootWare to the factory-default settings.

After this command is executed, only the items required for fundamental device operation are retained, including the .bin files, the MAC addresses, and the electronic label information.

To restore the factory-default configuration for the device, execute the following command in user view:

```
restore factory-default
```

This command takes effect after a device reboot.

Alternatively, you can delete both main and backup next-startup configuration files. From the device system console in monitor mode <prompt>:

```
reset saved-configuration backup
reset saved-configuration main
```

After the file is deleted, the device uses factory defaults at the next startup.

- All configuration files must end with .cfg
- To set the device to a previously saved configuration:

```
rename clean.bak startup.cfg
```

- Or you can enter (for example):

```
startup saved-configuration demo.cfg
```

- Display the current startup configuration:

```
display startup
```

- Reboot the device:

```
reboot
```

This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]: n

This command will reboot the device. Continue? [Y/N]: y

Determine software revision

The next thing to do is make sure each device is at the software release required for this configuration. In this procedure, you will compare the software revision that is shown on the device against the required software release.

Determine the current release running on the device:

```
display version
```

Determine the latest supported release of the device:

- Use your laptop connected to a network with Internet access
- Go to the HP Customer Care—Product Support website
  - In the box that says “Enter your product number”:
    - For example, enter “MSR3044”
  - Expand “Networking”, and click on the model you have
  - Click on “Downloads and software”
  - Click on the arrows under “Select” for the model you have

The latest supported software revision is the version with a status of “Current”. If the latest supported software revision is newer than the version currently running on the device you are using, we recommend that you upgrade the device.

- Click on the arrows under “Select” for the version with a status of “Current”
- Save the software image file to your laptop
  - The zip file will contain the software image file for the router and the release notes

Upgrade software

Before starting the configuration, upgrade the device to the software required for this demo configuration. There are two options you can use to copy the device software to the device:

- Copy the device software to a USB stick, then copy it from the USB storage device to the device:
  - Insert the USB storage device into the laptop using any free USB port
  - Copy the software image file from the laptop to a USB storage device
  - Use the Windows® function to “Safely Remove Hardware and Eject Media”
  - Remove the USB storage device from the laptop
  - Insert the USB storage device into HP MSR Router Series USB port 0
  - Copy the software .bin file from the USB storage device to the device

```
copy usba0:/<filename.extension>
```

  - Remove the USB storage device from the HP MSR Router Series
- Setup a temporary management IP address and download it using FTP:
  - Connect the laptop to the Demo HQ data VLAN using DHCP or give your laptop a static IP address

- Use your laptop ftp client and connect to the device:
  - Login as user “admin”, password “admin”
- Put software image file from laptop to the device.
- After the software .bin file has been transferred to the HP MSR Router Series, use the system console to assign the new image file as the main file, which will cause the router to boot using this new software:

```
dir
boot-loader file <filename> main
```

For MSR4000 Series, the command is:

```
boot-loader file <filename> all main
save
reboot
```

Configure basic device attributes

All devices requiring basic configurations will be using these basic device attributes. Refer to this section when setting up a new router. There is a hyperlink within the spoke/hub router sections that will lead you back to this area.

Configure administrator permissions

The system provides 19 predefined user roles. All these user roles have access to all system resources (interfaces, VLANs, and VPNs), but their command access permissions differ. Refer to the device fundamentals configuration guide for additional information on predefined roles and permissions matrix.

As an example the Fundamentals Configuration Guide and other guides for the MSR4000 Router series can be found here. The local-user “admin” is added and configured with a password of “admin” and “network-admin” user role:

```
local-user admin
password simple admin
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator (default)
```

Configure services

Next we will start the telnet and ftp services that are used to administer and manage the device. Setup of the SSH server allows an administrator to login to the device securely using SSH login. This includes creating a public key and enabling the SSH server.

- Follow these steps to setup services for local-user admin:

```
service-type ftp
```

- The “ftp” parameter has to be alone, but the others can be combined into a single command:

```
service-type ssh telnet terminal
quit
```

- Use these commands to create an RSA key pair:

```
public-key local create rsa
```

Press `Enter` **for** `1024`

- Use these commands to enable services:

```
telnet server enable
ftp server enable
sftp server enable
ssh server enable
```

Configure DNS

Setup router to resolve DNS to the demo HQ domain controller:

```
dns resolve
dns server 10.3.10.212
dns proxy enable
dns domain lync2013.hpntmedemo.com
```

- DNS resolve is not used in Comware v7

Configure time, day, year, and NTP
Setup device to synchronize time with the demo HQ domain controller:

```
ntp-service unicast-server 10.3.10.212
```

- Confirm time:

```
display clock
```

- Optionally, when NTP is not available, you can use the "clock" command to set the time and time zone:

```
clock timezone "Eastern Time(US,Canada)" minus 05:00:00
```

Configure terminal access permissions
Enable scheme authentication for user lines VTY 0 through VTY 4:

```
user-interface vty 0 4
user privilege level 3
authentication-mode scheme
idle-timeout 60 0
quit
```

Configure ISP domain
By default, the default ISP domain is the system-defined ISP domain **system**. The commands below are an example of how to create and configure an ISP domain named "hpntmedemo".

- Setup the basic domain configuration using these commands:

```
domain hpntmedemo
```

- These commands are not available within the 7.1.049 0106P08, but they are there by default:

```
access-limit disable
state active
idle-cut disable
self-service-url disable
```

- Display domain hpntmedemo and you should see the following:

```
<HUB1>dis domain hpntmedemo

Domain: hpntmedemo
  State: Active
  Access limit: Disabled
  Access count: 0
  Default authentication scheme:  local
  Default authorization  scheme:  local
  Default accounting     scheme:  local
  Authorization attributes:
    Idle-cut: Disabled
  Session time: Exclude idle time

quit
```

- Make this the default ISP domain:

```
domain default enable hpntmedemo
```

Configure SNMP
- Setup the basic SNMP configuration using these commands:

```
snmp-agent sys-info version all
snmp-agent sys-info location Demo_Rack_1
snmp-agent community read public
snmp-agent community write private
```

Configure LLDP

- Setup the basic LLDP configuration using these commands:

```
lldp enable
```

Configure port security

- Setup port security using these commands:

```
port-security enable
```

Configure quality of service

- Setup a basic quality of service (QoS) configuration using these commands:

```
traffic behavior dscp-46
remark dscp ef
remark dot1p 6
quit
qos policy dscp-46
classifier dscp-46 behavior dscp-46
quit
```

Demo HQ LAN switch

In this configuration, the demo HQ switch is an HP 5500-EI-24G-POE switch running HP Comware 5 software, which supports Layer 3 connectivity and the OSPF and BGP routing protocols. In this demo, we will only use OSPF for both the LAN and the WAN environments. Different OSPF networks will be created to separate the routing from the WAN. The demo HQ network is separate from the WAN network and is only connected through routing or tunnel protocols.

To begin this configuration, use telnet or SSH to connect to the device (via IP or serial system console port) and press `ENTER` to get to an HP Comware user-view command prompt:

```
<HP>
```

Start the configuration by getting to a HP Comware system-view command prompt:

```
system-view
```

Configure basic device attributes click here to access common commands

Configure system name

- Set the system name:

```
sysname DEMO-HQ
```

Configure DHCP relay (optional)

- Enable DHCP so that clients get IP address from domain controller:

```
dhcp enable
dhcp relay server-group 1 ip 10.3.10.212
```

- In Comware v7, the `dhcp relay` is applied within the interface menu.
- Enable DHCP relay inside the physical or VLAN interface to enable DHCP relay support:

```
interface vlan XX
     dhcp relay server-address 1 ip 10.3.10.212
```

Configure Local DHCP for LAN switch only
The steps in this section are not required for this configuration, but are described for completeness.

Optionally, you can configure the device to be able to provide DHCP services to local clients when connectivity to the demo HQ domain controller is not available:

```
dhcp enable
dhcp server ip-pool data-vlan-dhcp-pool
network 10.3.11.0 mask 255.255.255.0
gateway-list 10.3.11.1
option 42 ip-address 10.3.11.1
quit
dhcp server forbidden-ip 10.3.11.1 10.3.11.49
dhcp server forbidden-ip 10.3.11.71 10.3.11.255
```

Save configuration

- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done:

```
save
```

- Copy this as the "Demo HQ basic" configuration:

```
copy startup.cfg hpadvpn-demo-hq-basic.cfg
```
copy flash:/startup.cfg to flash:/hpadvpn-demo-hq-basic.cfg? [Y/N]: `y`

Configure network interfaces

Configure Demo HQ Management VLAN (optional)
Setup the Demo HQ Management VLAN:

```
sys
vlan 2
description Demo HQ Management VLAN
quit
```

- Enter the interface view for this VLAN:

```
interface vlan-interface 2
description Demo HQ Management VLAN Interface
```

- Assign an IP address to this VLAN:

```
ip address 10.3.2.1 24
quit
```

Configure Demo HQ Server VLAN
Setup the Demo HQ Server VLAN:

- In this configuration, the default gateway for this VLAN is 10.3.10.1/24, which is on the Internet gateway router.

```
vlan 10
description Demo HQ Server VLAN
quit
```

- Enter the interface view for this VLAN:

```
interface vlan-interface 10
description Demo HQ Server VLAN Interface
```

- Assign an IP address to this VLAN:

```
ip address 10.3.10.2 24
quit
```

Configure demo employee data VLAN

- Setup the demo HQ employee data VLAN:

```
vlan 11
description Demo HQ Employee Data VLAN
quit
```

- Enter the interface view for this VLAN:

```
interface vlan-interface 11
description Demo HQ Employee Data VLAN Interface
```

- Assign an IP address to this VLAN:

```
ip address 10.3.11.1 24
quit
```

- Enable DHCP Relay for this VLAN so that clients get IP address from domain controller:

```
dhcp select relay
dhcp relay server-select 1
quit
```

Configure interface to hub 1

Configure the interface to demo hub 1:

- Configure the interface from demo HQ switch-to-demo hub 1
  - Your switch port numbers could be different if using something other than the HP 5500 switch. Substitute accordingly.

```
interface GigabitEthernet 1/0/19
description Interface to Demo Hub 1
port link-mode route
ip address 10.50.9.1 24
quit
```

Configure LAN ports for demo HQ switch

- Configure LAN ports for VLAN 2

```
interface gigabitethernet 1/0/1 to interface gigabitethernet 1/0/4
description LAN port in VLAN 2 Management network
port link-mode bridge
port access vlan 2
quit
```

- Configure LAN ports for VLAN 10

```
int gigabitethernet 1/0/5 to interface gigabitethernet 1/0/8
description LAN port in VLAN 10 Server network
port link-mode bridge
port access vlan 10
quit
```

- Configure LAN ports for VLAN 11

```
int gigabitethernet 1/0/9 to interface gigabitethernet 1/0/14
description LAN port in VLAN 11 User network
port link-mode bridge
port access vlan 11
poe enable
quit
```

- Apply voice QoS policy

```
qos apply policy dscp-46 inbound
quit
```

Configure routing

Configure OSPF

Configure OSPF:

```
ospf 1
area 0.0.0.0
```

- Add the demo HQ network to OSPF:

```
network 10.3.0.0 0.0.255.255
```

- Add the network with the hub 1 to OSPF:

```
network 10.50.0.0 0.0.255.255
quit
```

Save configuration

- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done:

```
save
```

- Copy this as the "Demo HQ OSPF" configuration:

```
copy startup.cfg hpadvpn-demo-hq-ospf.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-hq-ospf.cfg? [Y/N]: y
```

Verify

- On the demo HQ switch:
  - Verify the overall configuration:

```
display current-configuration
```

  - Verify the configuration for a particular interface:

```
sys
interface gigabitethernet 1/0/1
display this
```

  - Verify the demo HQ server iLO port **can** be pinged:

```
ping 10.3.2.210
```

  - Verify the demo HQ server ESXi hypervisor **can** be pinged:

```
ping 10.3.2.12
```

  - Verify the demo HQ domain controller **can** be pinged:

```
ping 10.3.10.212
```

  - Verify the demo HQ client **can** be pinged:

```
ping 10.3.11.51
```

  - Verify the interface from demo HQ switch-to-demo hub 1 **cannot** be pinged:

```
ping 10.50.9.2
```

  - Verify the interfaces from demo hub 1-to-demo WAN **cannot** be pinged, starting with hub 1 interface then WAN switch interface:

```
ping 172.31.9.2
ping 172.31.9.1
```

  - Verify the interfaces from demo WAN-to-demo spoke 1 **cannot** be pinged, starting with WAN interface then spoke 1 interface:

```
ping 172.31.11.1
ping 172.31.11.2
```

Demo WAN switch

In this configuration, the demo WAN switch is also an HP 5500-EI-24G Switch Series running HP Comware v5 software, which supports Layer 3 connectivity and the OSPF and BGP routing protocols. For this configuration, the demo HQ network uses OSPF and the WAN uses OSPF.

In most cases, the WAN environment is not controlled by the customer. The customer would be given an assigned IP address to connect to the WAN environment, and would be given instructions on how to connect and configure the edge router for connectivity. Therefore, although basics are listed for the lab configuration, most commands could be ignored, such as DHCP and DNS, since the provider would be responsible for WAN configuration.

To begin this configuration, use telnet or SSH to connect to the device (via IP or serial system console port) and press ENTER to get to an HP Comware user-view command prompt:

```
<HP>
```

Start the configuration by getting to a HP Comware system-view command prompt:

```
system-view
```

Configure basic device attributes click here to access common commands

Configure system name

- Set the system name:

```
sysname DEMO-WAN
```

Save configuration

- It is highly recommended to save the router configuration before you are done:

```
return
save
```

- Copy this as the "WAN basic" configuration:

```
copy startup.cfg hpadvpn-demo-wan-basic.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-wan-basic.cfg? [Y/N]: y
```

Configure network interfaces

Configure WAN interface to hub 1

Configure the WAN interface to demo hub 1:

- Configure the interface from demo WAN-to-demo hub 1

```
sys
interface GigabitEthernet 0/0/1
description WAN interface to Demo Hub1
ip address 172.31.9.1 24
quit
```

Configure WAN interface to spoke 1-ADVPN client

Configure the WAN interface to demo spoke 1:

- Configure the interface from demo WAN-to-demo spoke 1:

```
interface GigabitEthernet 1/0/2
description WAN interface to Demo Spoke 1
ip address 172.31.11.1 24
quit
```

Configure WAN interface to hub 2

Configure the WAN interface to demo hub 2:

- Configure the interface from demo WAN-to-demo hub 2

```
sys
interface GigabitEthernet 1/0/3
description WAN interface to Demo Hub2
ip address 172.31.10.1 24
quit
```

Configure WAN interface to spoke-DVPN client
Configure the WAN interface to demo spoke:

- Configure the interface from demo WAN-to-demo spoke-DVPN spoke:

```
interface GigabitEthernet 1/0/4
description WAN interface to Demo Spoke-DVPN client
ip address 172.31.12.1 24
quit
```

Configure routing
Configure OSPF
OSPF will connect to the hubs and spokes only. The WAN switch/router will not be able to connect to the customer LAN segments.

Configure OSPF:

```
ospf 1
area 0.0.0.0
```

- Add the WAN network with hub 1 to OSPF:

```
network 172.31.0.0 0.0.255.255
quit
```

Save configuration
- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done:

```
save
```

- Copy this as the "Demo WAN OSPF" configuration:

```
copy startup.cfg hpadvpn-demo-wan-ospf.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-wan-ospf.cfg? [Y/N]: y
```

Verify
- Connect demo hub 1 port GE 0/1 to the demo WAN switch port GE 1/0/1.
- Connect demo spoke 1 port GE 0/0 to the demo WAN switch port GE 1/0/2.
- Connect demo hub 2 port GE 0/1 to the demo WAN switch port GE 1/0/3.
- Connect demo spoke-DVPN client port GE 0/0 to the demo WAN switch port GE 1/0/4.
- On the demo WAN switch:
  - Verify the overall configuration:

    ```
    display current-configuration
    ```

  - Verify the demo HQ domain controller **cannot** be pinged:

    ```
    ping 10.3.10.212
    ```

  - Verify the interface from demo HQ switch-to-demo hub 1 **cannot** be pinged:

    ```
    ping 10.50.9.2
    ```

HP ADVPN demo hub 1/VAM server 1 router configuration

In this configuration, the demo hub 1/VAM server 1 is an HP MSR3064 Router running HP Comware v7 software. In this HP ADVPN configuration, this router hosts the primary VAM server and primary hub using local authentication in a hub-spoke structure using IPsec over UDP ADVPN tunnels. There is no secondary server/hub 2 in this example.

To begin this configuration, use telnet or SSH to connect to the device (via IP or serial system console port) and press ENTER to get to an HP Comware user-view command prompt:

```
<HP>
```

- Start the configuration by getting to a HP Comware system-view command prompt:

```
system-view
```

Configure basic device attributes click here to access common commands

Configure system name

- Set the system name:

```
sysname HUB1
```

Save configuration

- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done.

```
save
```

- Copy this as the "basic" configuration

```
copy startup.cfg hpadvpn-demo-hub1-basic.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-hub1-basic.cfg? [Y/N]: y
```

Configure network interfaces

Configure interface to demo WAN

- Configure the interface from demo hub 1-to-demo WAN:

```
interface GigabitEthernet 0/0
description Interface from Demo Hub1 to Demo WAN
port link-mode route
combo enable copper
ip address 172.31.9.2 24
undo shutdown
quit
```

Configure interface to demo HQ

- Configure the interface from demo hub1-to-demo HQ switch:

```
system-view
interface GigabitEthernet 0/1
description Interface from Demo Hub1 to Demo HQ LAN switch
port link-mode route
ip address 10.50.9.2 24
undo shutdown
quit
```

Configure loopback 0

```
interface loopback0
ip address 10.50.9.201 32
```

Save configuration

- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done:

```
save
```

- Copy this as the “network” configuration:

```
copy startup.cfg hpadvpn-demo-hub1-network.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-hub1-network.cfg? [Y/N]: y
```

Configure routing

Configure OSPF

Setup OSPF between hubs and with demo HQ:

```
system-view
ospf 1
area 0.0.0.0
network 10.50.0.0 0.0.255.255
quit
quit
```

Setup OSPF for the WAN:

```
ospf 2
area 0.0.0.0
network 172.31.0.0 0.0.255.255
quit
quit
```

Save configuration

```
return
save
```

- Copy this as the “Demo Hub1 OSPF” configuration:

```
copy startup.cfg hpadvpn-demo-hub1-ospf.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-hub1-ospf.cfg? [Y/N]: y
```

Verify

- Verify the overall configuration:

```
display current-configuration
```

- Verify the demo hub 1 interface to demo HQ switch **can** be pinged:

```
ping 10.50.9.1
```

- Verify the demo HQ domain controller **can** be pinged:

```
ping 10.3.10.212
```

Configure AAA for VAM server 1

Configure VAM clients for local authentication

- Setup spoke users:

Note that there is no RADIUS configuration required because we are using local authentication. Also note that there is no need to specify the local "hub 1" user because it is local (co-resident hub/VAM server). Adding the local-user hub 2 assumes you have a secondary VAM server running on another router. In this configuration guide, we are only configuring the primary VAM server, so the local-user hub 2 would not be required.

- Setup hub 2 VAM client user and password:

```
local-user hub2 class network
password simple abc
service-type advpn
quit
```

- Setup spoke VAM client user and password:
  - A single local-user could be used for all spokes, however, there will be a spoke user defined for a DVPN to ADVPN configuration later in this document. So to keep the DVPN spoke ID unique from the ADVPN spoke ID, two different local-users are created.

```
local-user spoke class network
password simple abc
service-type advpn
quit

local-user spoke1 class network
password simple abc
service-type advpn
quit
```

When creating a local user, you have to be sure to create it with the "class network" at the end of the name. Otherwise, it will default and create a local-user *name* class manage, which is not what is required for ADVPN configurations. If the manage class is used, you will not see the option for ADVPN under the service-type list. In this example, you can see the distinction between creating the local-user test without the designated class, and one with the class network added.

If you decided to create the local-user test again, but this time with the class network at the end, you will then see two different local-users with the name of test. This will cause issues and is not recommended.

Local-user with no class distinction:

```
[HUB1]local-user test
New local user added.
[HUB1-luser-manage-test]dis this
#
local-user test class manage
 authorization-attribute user-role network-operator
#
return
 [HUB1-luser-manage-test]service-type ?
  ftp       FTP service
  http      HTTP service type
  https     HTTPS service type
  pad       X.25 PAD service
  ssh       Secure Shell service
  telnet    Telnet service
  terminal  Terminal access service
```

Local-user with class network distinction:

```
[HUB1]local-user test class network
[HUB1-luser-network-test]service-type ?
 advpn       ADVPN service
 lan-access  LAN access service
 portal      Portal service
 ppp         PPP service
```

Configure VAM server 1

- Create ADVPN domain demo-advpn-domain1:

```
vam server advpn-domain demo1 id 1
```

- Create the backbone hub-group:

```
hub-group 0
```

- Setup hub private address:

```
hub private-address 10.99.1.1
```

- Setup spoke private networks in this hub-group:

```
spoke private-address network 10.99.1.0 255.255.255.0
quit
```

- Set the pre-shared key:

```
pre-shared-key simple abc
```

- Use authentication-method chap domain <name> when you are using local-user <name> class network for local authentication with a user id and password:

```
authentication-method chap domain hpntmedemo
```

VAM server with no authentication

- Remove "`authentication-method chap domain hpntmedemo`".
- Replace with "`authentication-method none`".
- `Set the encryption parameters:`

```
encryption-algorithm des-cbc
```

- Enable the VAM server for the ADVPN domain:

```
server enable
quit
```

Configure VAM client hub 1

Setup VAM client with local authentication:

- Create VAM client:

```
vam client name Hub1
```

- Setup ADVPN domain for the VAM client:

```
advpn-domain demo1
```

- Set the pre-shared key:

```
pre-shared-key simple abc
```

- Setup the VAM client user name and password:

```
user hub1 password simple abc
```

- Setup the primary and secondary VAM servers:

```
server primary ip-address 172.31.9.2
```

- If a secondary VAM server were used:

```
server secondary ip-address X.X.X.X
```

- Enable VAM client:

```
client enable
quit
```

Configure VAM client hub 1 with no authentication.

- Remove the "`user hub1 password simple abc`" out of VAM client configuration.

Configure an IPsec profile

Configure IKE

Setup IKE:

- Configure IKE keychain:

```
ike keychain demo-ike-keychain1
pre-shared-key address 0.0.0.0 0.0.0.0 key simple abc
quit
```

- Configure IKE profile:

```
ike profile demo-ike-profile1
keychain demo-ike-keychain1
quit
```

Configure IPsec profile

Setup IPsec:

- Configure IPsec transform set:

```
ipsec transform-set demo-ipsec-tran1
encapsulation-mode tunnel (default setting)
esp encryption-algorithm des-cbc
esp authentication-algorithm sha1
quit
```

- Configure IPsec profile:

```
ipsec profile demo-ipsec-profile1 isakmp
transform-set demo-ipsec-tran1
ike-profile demo-ike-profile1
quit
```

Configure routing for ADVPN private network

Configure OSPF

Add the ADVPN private network to OSPF:

```
ospf 1
area 0.0.0.0
network 10.99.1.0 0.0.0.255
quit
quit
```

Configure ADVPN tunnel

Tunnel Interface used to transport both the IPsec data traffic and the VAM client information.

```
interface tunnel 1 mode advpn udp
description HP ADVPN Tunnel 1 on Demo Hub1
ip address 10.99.1.1 255.255.255.0
ospf network-type p2mp
source GigabitEthernet 0/0
tunnel protection ipsec profile demo-ipsec-profile1
vam client Hub1
undo shutdown
quit
```

Save configuration

- Return to user-view prompt:

```
exit
```

- It is highly recommended to save the router configuration before you are done:

```
Save
```

Copy configuration

- Copy this as the “Demo Hub1 OSPF final” configuration:

```
copy startup.cfg hpadvpn-demo-hub1-ospf-final.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-hub1-ospf-final.cfg? [Y/N]: y
```

Verify

- Verify the overall configuration:

```
display current-configuration
```

- Verify the demo hub 1 ADVPN tunnel interface can be pinged:

```
ping 10.99.1.1
```

- Display IPv4 private-to-public address mappings for VAM clients registered on the VAM server, and refer to the example output shown in the next figure:

```
display vam server address-map
```

Figure 4. Example output of Hub 1/VAM server 1 display address map command

```
[HUB1]dis vam server address-map
ADVPN domain name: demo1
Total private address mappings: 3
Group      Private address  Public address              Type   NAT  Holding time
0          10.99.1.1        172.31.9.2                 Hub    No   3H 59M 52S
0          10.99.1.3        172.31.11.2                Spoke  No   3H 57M 32S
0          10.99.1.4        172.31.12.2                Spoke  No   3H 55M 20S
```

- Display IPv4 private networks for VAM clients registered on the VAM server, and refer to the example output shown in the next figure:

```
display vam server private-network
```

Figure 5. Example output of Hub 1/VAM server 1 display private network command

```
<HUB1>dis vam server pri
<HUB1>dis vam server private-network
ADVPN domain name: demo1
Total private networks: 0
```

- Display ADVPN domain statistics on the VAM server, and refer to the example output shown in the next figure:

```
display vam server statistics
```

Figure 6. Example output of =hub 1/VAM server 1 display server statistics command

```
[HUB1]dis vam server stat
Total ADVPN number: 1
Total spoke number: 2
Total hub number  : 1

ADVPN domain name      : demo1
Server status          : Enabled
Holding time           : 4H 7M 10S
Registered spoke number: 2
Registered hub number  : 1
Packets received:
  Initialization request        : 3
  Initialization complete       : 3
  Register request              : 3
  Authentication information    : 0
  Address resolution request    : 0
  Network registering request   : 0
  Update request                : 0
  Logout request                : 0
  Hub information response      : 2
  Data flow information response: 0
  Keepalive                     : 245
  Error notification            : 0
  Unknown                       : 0
Packets sent:
  Initialization response       : 3
  Initialization complete       : 3
  Authentication request        : 0
  Register response             : 3
  Address resolution response   : 0
  Network registering response  : 0
  Update response               : 0
  Hub information request       : 2
  Data flow information request : 0
  Logout response               : 0
  Keepalive                     : 245
  Error notification            : 0
```

- Display FSM information for VAM clients, and refer to the example output shown in the next figure:

  `display vam client fsm`

Figure 7. Example output of hub 1/VAM server 1 display VAM client fsm command

```
<HUB1>dis vam client fsm
Client name      : Hub1
Status           : Enabled
ADVPN domain name: demo1
  Primary server: 172.31.9.2
    Private address: 10.99.1.1
    Interface      : Tunnel1
      Current state           : ONLINE (active)
      Client type             : Hub
      Holding time            : 4H 40M 16S
      Encryption-algorithm    : DES
      Authentication-algorithm: HMAC-SHA1
      Keepalive               : 180 seconds, 3 times
      Hub number              : 1
```

- Display statistics for VAM clients, and refer to the example output shown in the next figure:

  `display vam client statistics`

Figure 8. Example output of hub 1/VAM server 1 display VAM client statistics command

```
<HUB1>dis vam client stat
Client name: Hub1
 Status     : Enabled
  Primary server: 172.31.9.2
   Packets sent:
      Initialization request        : 1
      Initialization complete       : 1
      Register request              : 1
      Authentication information    : 0
      Address resolution request    : 0
      Network registration request  : 0
      Update request                : 0
      Logout request                : 0
      Hub information response      : 1
      Data flow information response: 0
      Keepalive                     : 94
      Error notification            : 0
   Packets received:
      Initialization response       : 1
      Initialization complete       : 1
      Authentication request        : 0
      Register response             : 1
      Address resolution response   : 0
      Network registering response  : 0
      Update response               : 0
      Hub information request       : 1
      Data flow information request : 0
      Logout response               : 0
      Keepalive                     : 94
      Error notification            : 0
      Unknown                       : 0
  Secondary server:
   Packets sent:
      Initialization request        : 0
      Initialization complete       : 0
      Register request              : 0
      Authentication information    : 0
      Address resolution request    : 0
      Network registration request  : 0
      Update request                : 0
      Logout request                : 0
      Hub information response      : 0
      Data flow information response: 0
      Keepalive                     : 0
      Error notification            : 0
   Packets received:
      Initialization response       : 0
      Initialization complete       : 0
      Authentication request        : 0
      Register response             : 0
      Address resolution response   : 0
      Network registering response  : 0
      Update response               : 0
      Hub information request       : 0
      Data flow information request : 0
      Logout response               : 0
      Keepalive                     : 0
      Error notification            : 0
      Unknown                       : 0
```

- Display IPv4 ADVPN tunnel information, and refer to the example output shown in the next figure:

  `display advpn session`

Figure 9. Example output of hub 1/VAM server 1 display ADVPN session command

```
<HUB1>dis advpn session
Interface          : Tunnel1
Number of sessions: 1
Private address      Public address       Port  Type  State        Holding time
10.99.1.3            172.31.11.2          18001 H-S   Success      4H 39M 37S
```

Demo ADVPN spoke 1 router

In this configuration, the demo spoke 1 is an HP MSR4060 router running HP Comware v7 software. In this HP ADVPN configuration, this router is a spoke in a hub-spoke structure using IPsec over UDP ADVPN tunnels.

To begin this configuration, use telnet or SSH to connect to the device (via IP or serial system console port) and press ENTER to get to an HP Comware user-view command prompt:

```
<HP>
```

Start the configuration by getting to a HP Comware system-view command prompt:

```
system-view
```

Configure basic device attributes click here to access common commands

Configure system name

- Set the system name:

```
sysname SPOKE1
```

Save configuration

- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done:

```
save
```

- Copy this as the “basic” configuration:

```
copy startup.cfg hpadvpn-demo-spoke1-basic.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-spoke1-basic.cfg? [Y/N]: y
```

Configure network interfaces

Configure interface to demo WAN

- Configure the interface from demo spoke 1 to demo WAN:

```
interface GigabitEthernet 2/0/0
description Interface from Demo Spoke 1 to Demo WAN
port link-mode route
combo enable copper
ip address 172.31.11.2 24
undo shutdown
quit
```

Configure local loopback interface for demo spoke 1

- Configure a loopback address to identify demo spoke 1 router:

```
interface loopback 0
description Loopback interface to identify this router – Demo Spoke1
ip address 10.200.18.201 32
quit
```

Save configuration

- It is highly recommended to save the router configuration before you are done:

```
return
save
```

- Copy this as the “network” configuration:

```
copy startup.cfg hpadvpn-demo-spoke1-network.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-spoke1-network.cfg? [Y/N]: y
```

Configure routing

Configure OSPF

- Setup OSPF between hubs and with demo HQ:

```
system-view
ospf 1
area 0.0.0.0
network 10.200.0.0 0.0.255.255
quit
quit
```

- Setup OSPF for the WAN:

```
ospf 2
area 0.0.0.0
network 172.31.0.0 0.0.255.255
quit
quit
```

Save configuration

```
return
save
```

- Copy this as the “Demo Spoke1 OSPF” configuration:

```
copy startup.cfg hpadvpn-demo-spoke1-ospf.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-spoke1-ospf.cfg? [Y/N]: y
```

Verify

- Verify the overall configuration:

```
display current-configuration
```

- Verify the demo spoke 1 loopback interface **can** be pinged:

```
ping 10.200.18.201
```

- Verify the demo HQ domain controller **cannot** be pinged:

```
ping 10.3.10.212
```

Configure VAM client spoke 1

Setup VAM client:

- Create VAM client:

```
vam client name Spoke1
```

- Setup ADVPN domain for the VAM client:

```
advpn-domain demo1
```

- Set the pre-shared key:

```
pre-shared-key simple abc
```

- Setup the primary VAM server:

```
server primary ip-address 172.31.9.2
```

- Setup the VAM client user name and password:

```
user spoke1 password simple abc
```

- Enable VAM client:

```
client enable
quit
```

Configure VAM client spoke 1 with no authentication.

- Remove the take the" user spoke password simple abc" out of VAM client configuration.

Configure an IPsec profile

Configure IKE

Setup IKE:

- Configure IKE keychain:

```
ike keychain demo-ike-keychain1
pre-shared-key address 0.0.0.0 0.0.0.0 key simple abc
quit
```

- Configure IKE profile:

```
ike profile demo-ike-profile1
keychain demo-ike-keychain1
quit
```

Configure IPsec profile

Setup IPsec:

- Configure IPsec transform set

```
ipsec transform-set demo-ipsec-tran1
encapsulation-mode tunnel
esp encryption-algorithm des-cbc
esp authentication-algorithm sha1
quit
```

- Configure IPsec profile

```
ipsec profile demo-ipsec-profile1 isakmp
transform-set demo-ipsec-tran1
ike-profile demo-ike-profile1
quit
```

Configure routing for ADVPN private network

Configure OSPF

Add the ADVPN private network to OSPF:

```
ospf 1
area 0.0.0.0
network 10.99.1.0 0.0.0.255
quit
quit
```

Configure ADVPN tunnel

Tunnel interface used to transport both the IPsec data traffic and the VAM client information:

```
interface tunnel 1 mode advpn udp
description HP ADVPN Tunnel 1 on Demo Spoke1
ip address 10.99.1.3 255.255.255.0
vam client spoke1
ospf network-type p2mp
source GigabitEthernet 2/0/0
tunnel protection ipsec profile demo-ipsec-profile1
undo shutdown
quit
```

Save configuration

- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done:

```
save
```

Copy configuration

- Copy this as the "Demo Spoke1 OSPF final" configuration:

```
copy startup.cfg hpadvpn-demo-spoke1-ospf-final.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-spoke1-ospf-final.cfg? [Y/N]: y
```

Verify

- Verify the overall configuration:

```
display current-configuration
```

- Verify the demo spoke 1 ADVPN private network **can** be pinged:

```
ping 10.99.1.3
```

- Verify the demo hub 1 ADVPN private network **can** be pinged:

```
ping 10.99.1.1
```

- Verify the demo hub 2 ADVPN private network **cannot** be pinged:

```
ping 10.99.1.2
```

- Verify the demo HQ domain controller **can** be pinged:

```
ping 10.3.10.212
```

- On hub 1, display IPv4 private-to-public address mappings for VAM clients registered on the VAM server, and refer to the example output shown in the next figure:

```
display vam server address-map
```

Figure 10. Example output of hub 1/VAM server 1 display address map command

```
<HUB1>dis vam server address-map
ADVPN domain name: demo1
Total private address mappings: 3
Group      Private address  Public address              Type   NAT  Holding time
0          10.99.1.1        172.31.9.2                 Hub    No   4H 47M 7S
0          10.99.1.3        172.31.11.2                Spoke  No   4H 44M 47S
0          10.99.1.4        172.31.12.2                Spoke  No   4H 42M 35S
```

- On hub 1, display IPv4 private networks for VAM clients registered on the VAM server:

```
display vam server private-network
```

- On hub 1, display ADVPN domain statistics on the VAM server:

```
display vam server statistics
```

- On hub 1, display FSM information for VAM clients:

```
display vam client fsm
```

- On hub 1, display statistics for VAM clients:

```
display vam client statistics
```

- On hub 1, display IPv4 ADVPN tunnel information, and refer to the example output shown in the next figure:

```
display advpn session
```

Figure 11. Example output of hub 1/VAM server 1 display ADVPN session command

```
<HUB1>dis advpn session
Interface         : Tunnel1
Number of sessions: 1
Private address      Public address       Port  Type  State        Holding time
10.99.1.3            172.31.11.2          18001 H-S   Success      4H 39M 37S
```

- On spoke 1, display FSM information for VAM clients, and refer to the example output shown in the next figure:

```
display vam client fsm
```

Figure 12. Example output of spoke 1 display VAM client fsm command

```
<SPOKE1>dis vam client fsm
Client name      : spoke1
Status           : Enabled
ADVPN domain name: demo1
  Primary server: 172.31.9.2
    Private address: 10.99.1.3
    Interface      : Tunnel1
      Current state           : ONLINE (active)
      Client type             : Spoke
      Holding time            : 4H 46M 23S
      Encryption-algorithm    : DES
      Authentication-algorithm: HMAC-SHA1
      Keepalive               : 180 seconds, 3 times
      Hub number              : 1
```

- On spoke 1, display statistics for VAM clients:

  ```
  display vam client statistics
  ```

- On spoke 1, display IPv4 ADVPN tunnel information, and refer to the example output shown in the next figure:

  ```
  display advpn session
  ```

Figure 13. Example output of spoke 1 display ADVPN session command

```
<SPOKE1>dis advpn se
Interface         : Tunnel1
Number of sessions: 1
Private address      Public address       Port  Type  State        Holding time
10.99.1.1            172.31.9.2           18001 S-H   Success      4H 46M 40S
```

Demo Internet gateway router (optional)

In this configuration, the demo Internet gateway is an HP MSR30-20 router running HP Comware v5 software. This device provides Internet connectivity for the demo HQ server VLAN.

To begin this configuration, use telnet or SSH to connect to the device (via IP or serial system console port) and press ENTER to get to an HP Comware user-view command prompt:

```
<HP>
```

Start the configuration by getting to a HP Comware system-view command prompt:

```
system-view
```

Configure basic device attributes click here to access common commands

Configure system name

- Set the system name:

  ```
  sysname DEMO-INTERNET-GW
  ```

Save configuration

- Return to user-view command level:

  ```
  return
  save
  ```

- Copy this as the “basic” configuration:

  ```
  copy startup.cfg hpadvpn-gw-basic.cfg
  copy flash:/startup.cfg to flash:/hpadvpn-gw-basic.cfg? [Y/N]: y
  ```

Configure access control lists

Setup ACLs for internet gateway

Setup ACL rule to permit IP traffic from source 10.3.0.0/24 network:

```
acl number 2001
rule 0 permit source 10.3.0.0 0.0.255.255
quit
```

Configure network interfaces

Configure interface to demo HQ switch

- Configure the demo HQ switch-facing interface—this becomes the default gateway for the demo HQ network so that the servers can reach the Internet

```
interface GigabitEthernet 0/0
description Interface to Demo HQ switch
port link-mode route
ip address 10.3.10.1 24
quit
```

Configure interface to Internet

- Configure the interface to Internet:

```
interface GigabitEthernet 0/1
description Interface to Internet
port link-mode route
```

- Enable outbound NAT using rules in ACL 2001:

```
nat outbound 2001
```

- Obtain an IP address from the next hop:

```
ip address dhcp-alloc
quit
```

Configure routing

Configure OSPF

```
ospf 1
area 0.0.0.0
```

- Add the demo HQ network to OSPF:

```
network 10.3.0.0 0.0.255.255
quit
```

Save configuration

- Return to user-view command level:

```
return
save
```

- Copy this as the "OSPF" configuration:

```
copy startup.cfg hpadvpn-gw-ospf.cfg
copy flash:/startup.cfg to flash:/hpadvpn-gw-ospf.cfg? [Y/N]: y
```

Verify

- Connect demo HQ server iLO port to the demo HQ switch port GE 1/0/1 in VLAN 2.
- On the demo Internet gateway router:
  - Verify the overall configuration:

```
display current-configuration
```

  - Verify the demo HQ switch interface **can** be pinged:

```
ping 10.3.10.2
```

  - Verify the demo HQ Domain Controller **can** be pinged:

```
ping 10.3.10.212
```

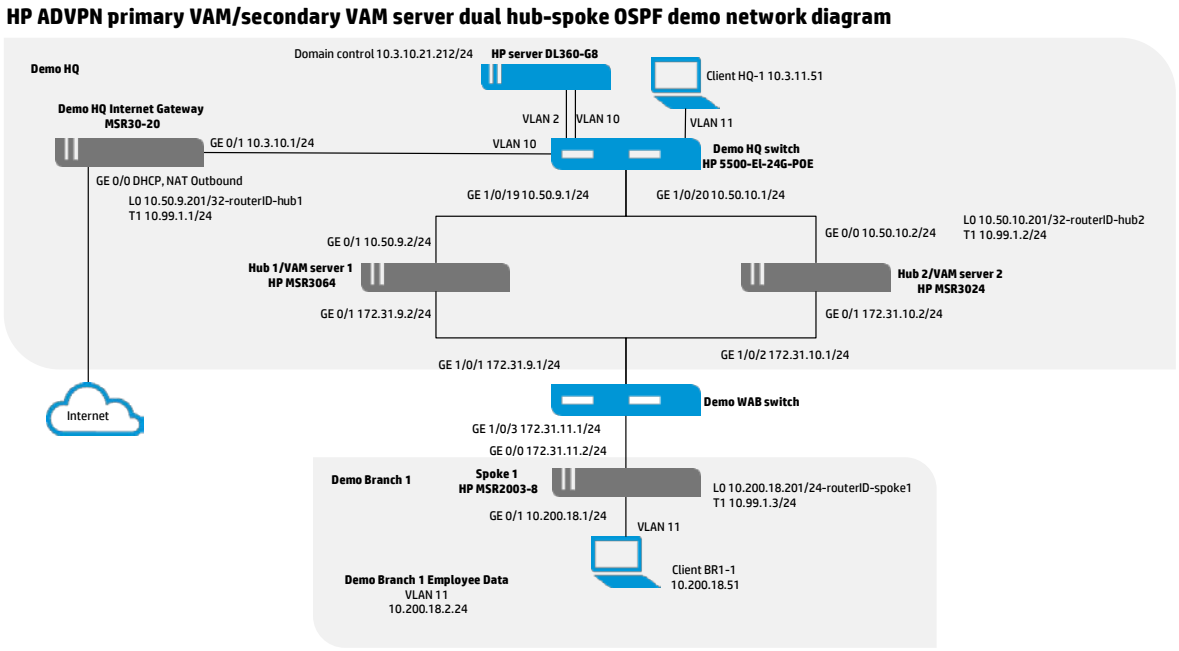
– Verify the Internet **can** be pinged:

```
ping google.com
```

ADVPN primary/secondary VAM server configuration

In this configuration, we are adding a second hub and a secondary VAM server to the ADVPN environment.

Figure 14. Network diagram with primary and secondary VAM servers



HP ADVPN demo hub 1/VAM server 1 router

Using the existing hub 1/VAM 1 configuration, modify both the VAM server and the VAM client on hub 1, by adding the IP address of the secondary VAM server and hub 2 public address. Also add hub 2 local-user and password.

Configure VAM clients for local authentication

- Setup spoke users:

  Note that there is no RADIUS configuration required because we are using local authentication. Also note that there is no need to specify the local "hub 1" user because it is local (co-resident hub/VAM server). Adding the local-user hub 2 adds the hub where the secondary VAM server is running on another router.

- Setup hub 2 VAM client user and password:

```
local-user hub2 class network
password simple abc
service-type advpn
quit
```

Configure VAM server 1

- Create ADVPN domain demo-advpn-domain1:

```
vam server advpn-domain demo1 id 1
```

- Create the backbone hub-group:

```
hub-group 0
```

- Setup hub private address:

```
hub private-address 10.99.1.1
```

- Setup secondary hub private address:

```
hub private-address 10.99.1.2
```

- Setup spoke private networks in this hub-group:

```
spoke private-address network 10.99.1.0 255.255.255.0
quit
```

- Set the pre-shared key:

```
pre-shared-key simple abc
```

- Use authentication-method chap domain <name> when you are using local-user <name> class network for local authentication with a user id and password:

```
authentication-method chap domain hpntmedemo
```

- Set the encryption parameters:

```
encryption-algorithm des-cbc
```

- Enable the VAM Server for the ADVPN domain:

```
server enable
quit
```

VAM server with no authentication

- Remove “authentication-method chap domain hpntmedemo”.
- Replace with “authentication-method none”.

Configure VAM client hub 1

Setup VAM client with local authentication:

- Create VAM client:

```
vam client name Hub1
```

- Setup ADVPN domain for the VAM client:

```
advpn-domain demo1
```

- Set the pre-shared key:

```
pre-shared-key simple abc
```

- Setup the VAM client user name and password:

```
user hub1 password simple abc
```

- Setup the primary and secondary VAM servers:

```
server primary ip-address 172.31.9.2
   server secondary ip-address 172.31.10.2
```

- Enable VAM client:

```
client enable
quit
```

Configure VAM client hub 1 with no authentication.

- Remove the “`user hub2 password simple abc`” out of VAM client configuration.

HP ADVPN demo hub 2/VAM server 2 router

To begin this configuration, use telnet or SSH to connect to the device (via IP or serial system console port) and press ENTER to get to an HP Comware user-view command prompt:

```
<HP>
```

Start the configuration by getting to a HP Comware system-view command prompt:

```
system-view
```

Configure basic device attributes refer to previous configuration listed here

Configure system name

- Set the system name:

```
sysname HUB2
```

- Copy this as the "basic" configuration:

```
copy startup.cfg hpadvpn-demo-hub2-basic.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-hub2-basic.cfg? [Y/N]: y
```

Configure network interfaces

Configure interface to demo WAN

- Configure the interface from demo hub 2 to demo WAN:

```
interface GigabitEthernet 0/0
description Interface from Demo Hub2 to Demo WAN
port link-mode route
combo enable copper
ip address 172.31.10.2 24
undo shutdown
quit
```

Configure interface to demo HQ

- Configure the interface from demo hub 2-to-demo HQ switch:

```
system-view
interface GigabitEthernet 0/1
description Interface from Demo Hub2 to Demo HQ LAN switch
port link-mode route
ip address 10.50.10.2 24
undo shutdown
quit
```

Configure Loopback 0

```
interface loopback0
ip address 10.50.10.201 32
```

Save configuration

- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done:

```
save
```

- Copy this as the "network" configuration:

```
copy startup.cfg hpadvpn-demo-hub2-network.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-hub1-network.cfg? [Y/N]: y
```

Configure routing

Configure OSPF

- Setup OSPF between hubs and with demo HQ:

```
system-view
ospf 1
area 0.0.0.0
network 10.50.0.0 0.0.255.255
quit
quit
```

- Setup OSPF for the WAN:

```
ospf 2
area 0.0.0.0
network 172.31.0.0 0.0.255.255
quit
quit
```

- Save configuration:

```
return
save
```

- Copy this as the "Demo Hub2 OSPF" configuration:

```
copy startup.cfg hpadvpn-demo-hub2-ospf.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-hub2-ospf.cfg? [Y/N]: y
```

Verify

- Verify the overall configuration:

```
display current-configuration
```

- Verify the demo hub 2 interface to demo HQ switch can be pinged:

```
ping 10.50.10.1
```

- Verify the demo HQ domain controller can be pinged:

```
ping 10.3.10.212
```

Configure AAA for VAM server 2 (secondary)

Configure VAM clients for local authentication

- Setup spoke users:

  Note that there is no RADIUS configuration required because we are using local authentication. Also note that there is no need to specify the local "hub2" user because it is local (co-resident hub/VAM server). Adding the local-user hub 1 adds the hub where the primary VAM server is running on another router.

- Setup hub 1 VAM client user and password:

```
local-user hub1 class network
password simple abc
service-type advpn
quit
```

- Setup spoke VAM client user and password:

A single local-user could be used for all spokes, however, there will be a spoke user defined for a DVPN to ADVPN configuration later in this document. So to keep the DVPN spoke ID unique from the ADVPN spoke ID, two different local-users are created.

```
local-user spoke class network
password simple abc
service-type advpn
quit

local-user spoke1 class network
password simple abc
service-type advpn
quit
```

When creating a local user, you have to be sure to create it with the “class network” at the end of the name. Otherwise, it will default and create a local-user *name* class manage, which is not what is required for ADVPN configurations. If the manage class is used, you will not see the option for ADVPN under the service-type list.

In this example, you can see the distinction between creating the local-user test without the designated class, and one with the class network added.

If you decided to create the local-user test again, but this time with the class network at the end, you will then see two different local-users with the name of test. This will cause issues and is not recommended.

Local-user with no class distinction:

```
[HUB1]local-user test
New local user added.
[HUB1-luser-manage-test]dis this
#
local-user test class manage
 authorization-attribute user-role network-operator
#
return
 [HUB1-luser-manage-test]service-type ?
  ftp       FTP service
  http      HTTP service type
  https     HTTPS service type
  pad       X.25 PAD service
  ssh       Secure Shell service
  telnet    Telnet service
  terminal  Terminal access service
```

Local-user with class network distinction:

```
[HUB1]local-user test class network
[HUB1-luser-network-test]service-type ?
 advpn       ADVPN service
 lan-access  LAN access service
 portal      Portal service
 ppp         PPP service
```

Configure VAM server 2

- Create ADVPN domain demo-advpn-domain1:

```
vam server advpn-domain demo1 id 1
```

- Create the backbone hub-group:

```
hub-group 0
```

- Setup hub private address:

```
hub private-address 10.99.1.1
```

- Add secondary address:

```
hub private-address 10.99.1.2
```

- Setup spoke private networks in this hub-group:

```
spoke private-address network 10.99.1.0 255.255.255.0
quit
```

- Set the pre-shared key:

```
pre-shared-key simple abc
```

- Use authentication-method chap domain <name> when you are using local-user <name> class network for local authentication with a user id and password:

```
authentication-method chap domain hpntmedemo
```

- Set the encryption parameters:

```
encryption-algorithm des-cbc
```

- Enable the VAM server for the ADVPN domain:

```
server enable
quit
```

VAM server with no authentication

- Remove “authentication-method chap domain hpntmedemo”.
- Replace with “authentication-method none”.

Configure VAM client hub 2

Setup VAM client with local authentication:

- Create VAM client:

```
vam client name Hub2
```

- Setup ADVPN domain for the VAM client:

```
advpn-domain demo1
```

- Set the pre-shared key:

```
pre-shared-key simple abc
```

- Setup the VAM client user name and password:

```
user hub2 password simple abc
```

- Setup the primary and secondary VAM servers:

```
server primary ip-address 172.31.9.2
server secondary ip-address 172.31.10.2
```

- Enable VAM client:

```
client enable
quit
```

Configure VAM client hub 2 with no authentication

- Remove the “user hub2 password simple abc” out of VAM client configuration.

Configure an IPsec profile for hub 2, similar to hub 1 previously configured

Configure IKE

Setup IKE:

- Configure IKE keychain:

```
ike keychain demo-ike-keychain1
pre-shared-key address 0.0.0.0 0.0.0.0 key simple abc
quit
```

- Configure IKE profile:

```
ike profile demo-ike-profile1
keychain demo-ike-keychain1
quit
```

Configure IPsec profile

Setup IPsec:

- Configure IPsec transform set:

```
ipsec transform-set demo-ipsec-tran1
encapsulation-mode tunnel (default setting)
esp encryption-algorithm des-cbc
esp authentication-algorithm sha1
quit
```

- Configure IPsec profile:

```
ipsec profile demo-ipsec-profile1 isakmp
transform-set demo-ipsec-tran1
ike-profile demo-ike-profile1
quit
```

Configure routing for ADVPN private network

Configure OSPF

Add the ADVPN private network to OSPF:

```
ospf 1
area 0.0.0.0
network 10.99.1.0 0.0.0.255
quit
quit
```

Configure ADVPN tunnel on hub 2

Tunnel Interface used to transport both the IPsec data traffic and the VAM client information:

```
interface tunnel 1 mode advpn udp
description HP ADVPN Tunnel 1 on Demo Hub2
ip address 10.99.1.2 255.255.255.0
ospf network-type p2mp
source GigabitEthernet 0/0
tunnel protection ipsec profile demo-ipsec-profile1
vam client Hub2
undo shutdown
quit
```

Save configuration

- Return to user-view prompt:

```
exit
```

- It is highly recommended to save the router configuration before you are done:

```
Save
```

Copy configuration

- Copy this as the “Demo Hub1 OSPF final” configuration:

```
copy startup.cfg hpadvpn-demo-hub2-ospf-final.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-hub2-ospf-final.cfg? [Y/N]: y
```

Verify

- Verify the overall configuration:

```
display current-configuration
```

- Verify the demo hub 1 ADVPN tunnel interface can be pinged:

```
ping 10.99.1.1
```

- Display IPv4 private-to-public address mappings for VAM clients registered on the VAM server, and refer to the example output shown in the next figure:

```
display vam server address-map
```

Figure 15. Example output of hub 2/VAM server 2 display address map command

```
[Hub2]dis vam server ad
ADVPN domain name: demo1
Total private address mappings: 3
Group      Private address  Public address              Type   NAT  Holding time
0          10.99.1.1        172.31.9.2                 Hub    No   0H 16M 4S
0          10.99.1.3        172.31.11.2                Spoke  No   0H 16M 4S
0          10.99.1.4        172.31.12.2                Spoke  No   0H 15M 11S
```

- Display IPv4 private networks for VAM clients registered on the VAM server, and refer to the example output shown in the next figure:

  ```
  display vam server private-network
  ```

Figure 16. Example output of hub 2/VAM server 2 display private network command

```
<Hub2>dis vam server pri
ADVPN domain name: demo1
Total private networks: 0
```

- Display ADVPN domain statistics on the VAM server, and refer to the example output shown in the next figure:

  ```
  display vam server statistics
  ```

Figure 17. Example output of hub 2/VAM server 2 display server statistics command

```
<Hub2>dis vam server stat
Total ADVPN number: 1
Total spoke number: 2
Total hub number  : 1

ADVPN domain name      : demo1
Server status          : Enabled
Holding time           : 1H 35M 43S
Registered spoke number: 2
Registered hub number  : 1
Packets received:
  Initialization request        : 774
  Initialization complete       : 774
  Register request              : 774
  Authentication information    : 774
  Address resolution request    : 0
  Network registering request   : 0
  Update request                : 0
  Logout request                : 1
  Hub information response      : 5
  Data flow information response: 0
  Keepalive                     : 83
  Error notification            : 0
  Unknown                       : 0
Packets sent:
  Initialization response       : 774
  Initialization complete       : 774
  Authentication request        : 774
  Register response             : 6
  Address resolution response   : 0
  Network registering response  : 0
  Update response               : 0
  Hub information request       : 29
  Data flow information request : 0
  Logout response               : 0
  Keepalive                     : 83
  Error notification            : 768
```

- Display FSM information for VAM clients, and refer to the example output shown in the next figure:

  `display vam client fsm`

Figure 18. Example output of hub 2/VAM server 2 display VAM client fsm command

```
<Hub2>dis vam client fsm
Client name      : hub2
Status           : Enabled
ADVPN domain name: demo1
  Primary server: 172.31.9.2
    Private address: 10.99.1.2
    Interface      : Tunnel1
      Current state           : ONLINE (active)
      Client type             : Hub
      Holding time            : 1H 20M 6S
      Encryption-algorithm    : AES-CBC-256
      Authentication-algorithm: HMAC-SHA1
      Keepalive               : 180 seconds, 3 times
      Hub number              : 1
  Secondary server: 172.31.10.2
    Private address: 10.99.1.2
    Interface      : Tunnel1
      Current state           : OFFLINE
      Client type             : Unknown
      Holding time            : 0H 0M 0S
      Encryption-algorithm    : Unknown
      Authentication-algorithm: Unknown
      Keepalive               : 0 seconds, 0 times
      Hub number              : 0
```

- Display statistics for VAM clients, and refer to the example output shown in the next figure:

  ```
  display vam client statistics
  ```

Figure 19. Example output of hub 2/VAM server 2 display VAM client statistics command

```
[Hub2]dis vam client stat
Client name: hub2
 Status      : Enabled
  Primary server: 172.31.9.2
   Packets sent:
      Initialization request         : 70
      Initialization complete        : 2
      Register request               : 2
      Authentication information     : 2
      Address resolution request     : 0
      Network registration request   : 0
      Update request                 : 0
      Logout request                 : 1
      Hub information response       : 3
      Data flow information response: 0
      Keepalive                      : 34
      Error notification             : 0
   Packets received:
      Initialization response        : 2
      Initialization complete        : 2
      Authentication request         : 2
      Register response              : 2
      Address resolution response    : 0
      Network registering response   : 0
      Update response                : 0
      Hub information request        : 3
      Data flow information request  : 0
      Logout response                : 0
      Keepalive                      : 34
      Error notification             : 0
      Unknown                        : 0
  Secondary server: 172.31.10.2
   Packets sent:
      Initialization request         : 1149
      Initialization complete        : 1137
      Register request               : 1137
      Authentication information     : 1137
      Address resolution request     : 0
      Network registration request   : 0
      Update request                 : 0
      Logout request                 : 0
      Hub information response       : 0
      Data flow information response: 0
      Keepalive                      : 0
      Error notification             : 0
   Packets received:
      Initialization response        : 1137
      Initialization complete        : 1137
      Authentication request         : 1137
      Register response              : 0
      Address resolution response    : 0
      Network registering response   : 0
      Update response                : 0
      Hub information request        : 0
      Data flow information request  : 0
      Logout response                : 0
      Keepalive                      : 0
      Error notification             : 1137
      Unknown                        : 0
```

- Display IPv4 ADVPN tunnel information, and refer to the example output shown in the next figure:

```
display advpn session
```

Figure 20. Example output of hub 1/VAM server 1 display ADVPN session command

```
[HUB1]dis vam ser address-map
ADVPN domain name: demo1
Total private address mappings: 3
Group      Private address  Public address              Type   NAT  Holding time
0          10.99.1.2        172.31.10.2                Hub    No   0H 2M 41S
0          10.99.1.3        172.31.11.2                Spoke  No   0H 2M 41S
0          10.99.1.4        172.31.12.2                Spoke  No   0H 1M 28S
```

Figure 21. Example output of hub 2/VAM server 2 display ADVPN session command

```
[Hub2]dis vam ser add
[Hub2]dis vam ser address-map
ADVPN domain name: demo1
Total private address mappings: 3
Group      Private address  Public address              Type   NAT  Holding time
0          10.99.1.1        172.31.9.2                 Hub    No   0H 21M 13S
0          10.99.1.3        172.31.11.2                Spoke  No   0H 21M 13S
0          10.99.1.4        172.31.12.2                Spoke  No   0H 20M 20S
```

Demo ADVPN spoke 1 router

In this configuration, the demo spoke 1 is an HP MSR4060 router running HP Comware v7 software. In this HP ADVPN configuration, this router is a spoke in a hub-spoke structure using IPsec over UDP ADVPN tunnels.

To begin this configuration, use telnet or SSH to connect to the device (via IP or serial system console port) and press ENTER to get to an HP Comware user-view command prompt:

```
<HP>
```

Start the configuration by getting to a HP Comware system-view command prompt:

```
system-view
```

Configure basic device attributes refer to previous configuration listed here

Configure system name

- Set the system name:

```
sysname SPOKE1
```

Save configuration

- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done:

```
save
```

- Copy this as the “basic” configuration:

```
copy startup.cfg hpadvpn-demo-spoke1-basic.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-spoke1-basic.cfg? [Y/N]: y
```

Configure network interfaces

Configure interface to demo WAN

- Configure the interface from demo spoke 1 to demo WAN:

```
interface GigabitEthernet 2/0/0
description Interface from Demo Spoke 1 to Demo WAN
port link-mode route
combo enable copper
ip address 172.31.11.2 24
undo shutdown
quit
```

Configure local loopback interface for demo spoke 1

Configure a loopback address to identify demo spoke 1 router:

```
interface loopback 0
description Loopback interface to identify this router – Demo Spoke1
ip address 10.200.18.201 32
quit
```

Save configuration

- It is highly recommended to save the router configuration before you are done:

```
return
save
```

- Copy this as the "network" configuration:

```
copy startup.cfg hpadvpn-demo-spoke1-network.cfg
```

copy flash:/startup.cfg to flash:/hpadvpn-demo-spoke1-network.cfg? [Y/N]: `y`

Configure routing

Configure OSPF

Setup OSPF between hubs and with demo HQ:

```
system-view
ospf 1
area 0.0.0.0
network 10.200.0.0 0.0.255.255
quit
quit
```

Setup OSPF for the WAN:

```
ospf 2
area 0.0.0.0
network 172.31.0.0 0.0.255.255
quit
quit
```

Save configuration

```
return
save
```

- Copy this as the "Demo Spoke1 OSPF" configuration:

```
copy startup.cfg hpadvpn-demo-spoke1-ospf.cfg
```

copy flash:/startup.cfg to flash:/hpadvpn-demo-spoke1-ospf.cfg? [Y/N]: `y`

Verify

- Verify the overall configuration:

```
display current-configuration
```

- Verify the Demo Spoke1 loopback interface CAN be pinged:

```
ping 10.200.18.201
```

- Verify the Demo HQ domain controller CANNOT be pinged:

```
ping 10.3.10.212
```

Configure VAM client spoke 1

Setup VAM client:

- Create VAM client:

```
vam client name Spoke1
```

- Setup ADVPN domain for the VAM client:

```
advpn-domain demo1
```

- Set the pre-shared key:

```
pre-shared-key simple abc
```

- Setup the primary VAM server:

```
server primary ip-address 172.31.9.2
server secondary ip-address 172.31.10.2
```

- Setup the VAM client user name and password:

```
user spoke1 password simple abc
```

- Enable VAM client:

```
client enable
quit
```

Configure VAM client spoke 1 with no authentication

- Remove the take the" user spoke password simple abc" out of VAM client configuration.

Configure an IPsec profile

Configure IKE

Setup IKE:

- Configure IKE keychain:

```
ike keychain demo-ike-keychain1
pre-shared-key address 0.0.0.0 0.0.0.0 key simple abc
quit
```

- Configure IKE profile:

```
ike profile demo-ike-profile1
keychain demo-ike-keychain1
quit
```

Configure IPsec profile

Setup IPsec:

- Configure IPsec transform set:

```
ipsec transform-set demo-ipsec-tran1
encapsulation-mode tunnel
esp encryption-algorithm des-cbc
esp authentication-algorithm sha1
quit
```

- Configure IPsec profile:

```
ipsec profile demo-ipsec-profile1 isakmp
transform-set demo-ipsec-tran1
ike-profile demo-ike-profile1
quit
```

Configure routing for ADVPN private network

Configure OSPF

Add the ADVPN private network to OSPF:

```
ospf 1
area 0.0.0.0
network 10.99.1.0 0.0.0.255
quit
quit
```

Configure ADVPN tunnel

Tunnel Interface used to transport both the IPsec data traffic and the VAM client information.

```
interface tunnel 1 mode advpn udp
description HP ADVPN Tunnel 1 on Demo Spoke1
ip address 10.99.1.3 255.255.255.0
vam client spoke
ospf network-type p2mp
source GigabitEthernet 2/0/0
tunnel protection ipsec profile demo-ipsec-profile1
undo shutdown
quit
```

Save configuration

- Return to user-view prompt:

```
return
```

- It is highly recommended to save the router configuration before you are done:

```
Save
```

Copy configuration

- Copy this as the "Demo Spoke1 OSPF final" configuration:

```
copy startup.cfg hpadvpn-demo-spoke1-ospf-final.cfg
copy flash:/startup.cfg to flash:/hpadvpn-demo-spoke1-ospf-final.cfg? [Y/N]: y
```

Verify

- Verify the overall configuration:

```
display current-configuration
```

- Verify the demo spoke 1 ADVPN private network can be pinged:

```
ping 10.99.1.3
```

- Verify the demo hub 1 ADVPN private network can be pinged:

```
ping 10.99.1.1
```

- Verify the demo hub 2 ADVPN private network can be pinged:

```
ping 10.99.1.2
```

- Verify the demo HQ domain controller can be pinged:

```
ping 10.3.10.212
```

- On hub 1, display IPv4 private-to-public address mappings for VAM clients registered on the VAM server, and refer to the example output shown in the next figure:

```
display vam server address-map
```

Figure 22. Example output of hub 1/VAM server 1 display address map command

```
<HUB1>dis vam server address-map
ADVPN domain name: demo1
Total private address mappings: 3
Group      Private address  Public address                Type   NAT  Holding time
0          10.99.1.1        172.31.9.2                    Hub    No   4H 47M 7S
0          10.99.1.3        172.31.11.2                   Spoke  No   4H 44M 47S
0          10.99.1.4        172.31.12.2                   Spoke  No   4H 42M 35S
```

- On hub 1, display IPv4 private networks for VAM clients registered on the VAM server:

  `display vam server private-network`

- On hub 1, display ADVPN domain statistics on the VAM server:

  `display vam server statistics`

- On hub 1, display FSM information for VAM clients:

  `display vam client fsm`

- On hub 1, display statistics for VAM clients:

  `display vam client statistics`

- On hub 1, display IPv4 ADVPN tunnel information, and refer to the example output shown in the next figure:

  `display advpn session`

Figure 23. Example output of hub 1/VAM server 1 display ADVPN session command

```
<HUB1>dis advpn session
Interface         : Tunnel1
Number of sessions: 1
Private address      Public address       Port  Type  State        Holding time
10.99.1.3            172.31.11.2          18001 H-S   Success      4H 39M 37S
```

- On spoke 1, display FSM information for VAM clients, and refer to the example output shown in the next figure:

  `display vam client fsm`

Figure 24. Example output of spoke 1 display VAM client fsm command

```
<SPOKE1>
<SPOKE1>dis vam client fsm
Client name      : spoke
Status           : Enabled
ADVPN domain name: demo1
  Primary server: 172.31.9.2
    Private address: 10.99.1.3
    Interface      : Tunnel1
      Current state           : ONLINE (active)
      Client type             : Spoke
      Holding time            : 8H 28M 11S
      Encryption-algorithm    : DES
      Authentication-algorithm: HMAC-SHA1
      Keepalive               : 180 seconds, 3 times
      Hub number              : 1
  Secondary server: 172.31.10.2
    Private address: 10.99.1.3
    Interface      : Tunnel1
      Current state           : ONLINE
      Client type             : Spoke
      Holding time            : 8H 28M 11S
      Encryption-algorithm    : DES
      Authentication-algorithm: HMAC-SHA1
      Keepalive               : 180 seconds, 3 times
      Hub number              : 1
```

- On spoke 1, display statistics for VAM clients:

  ```
  display vam client statistics
  ```

- On spoke 1, display IPv4 ADVPN tunnel information, and refer to the example output shown in the next figure:

  ```
  display advpn session
  ```

Figure 25. Example output of spoke 1 display ADVPN session command

```
<SPOKE1>dis advpn se
Interface          : Tunnel1
Number of sessions: 1
Private address      Public address       Port  Type  State        Holding time
10.99.1.1            172.31.9.2           18001 S-H   Success      4H 46M 40S
```

Verify

VAM server commands available

- dis vam server statistic

Figure 26. VAM server statistics

```
<HUB1>dis vam server stat
Total ADVPN number: 1
Total spoke number: 2
Total hub number  : 1

ADVPN domain name      : demo1
Server status          : Enabled
Holding time           : 8H 55M 7S
Registered spoke number: 2
Registered hub number  : 1
Packets received:
  Initialization request        : 4575
  Initialization complete       : 4575
  Register request              : 4575
  Authentication information    : 4575
  Address resolution request    : 0
  Network registering request   : 0
  Update request                : 0
  Logout request                : 0
  Hub information response      : 2
  Data flow information response: 0
  Keepalive                     : 531
  Error notification            : 0
  Unknown                       : 0
Packets sent:
  Initialization response       : 4575
  Initialization complete       : 4575
  Authentication request        : 4575
  Register response             : 4
  Address resolution response   : 0
  Network registering response  : 0
  Update response               : 0
  Hub information request       : 2
  Data flow information request : 0
  Logout response               : 0
  Keepalive                     : 528
  Error notification            : 4571
```

- Display VAM server address-map all shows connection to both VAM clients registered (hub 2 and spoke)
- Display VAM client fsm
  - This will show the active connections to the VAM server. Here MSR#1-HUB1 is the primary VAM server, but has a client connection to the MSR#2-HUB2 VAM server as well

Figure 27. Display vam client fsm

```
<HUB1>dis vam client fsm
Client name      : Hub1
Status           : Enabled
ADVPN domain name: demo1
  Primary server: 172.31.9.2
    Private address: 10.99.1.1
    Interface      : Tunnel1
      Current state           : OFFLINE
      Client type             : Unknown
      Holding time            : 0H 0M 0S
      Encryption-algorithm    : Unknown
      Authentication-algorithm: Unknown
      Keepalive               : 0 seconds, 0 times
      Hub number              : 0
  Secondary server: 172.31.10.2
    Private address: 10.99.1.1
    Interface      : Tunnel1
      Current state           : ONLINE (active)
      Client type             : Hub
      Holding time            : 8H 51M 27S
      Encryption-algorithm    : DES
      Authentication-algorithm: HMAC-SHA1
      Keepalive               : 180 seconds, 3 times
      Hub number              : 1
```

- Display VAM client address-map

ADVPN/DVPN compatibility mode using a primary/secondary VAM server configuration

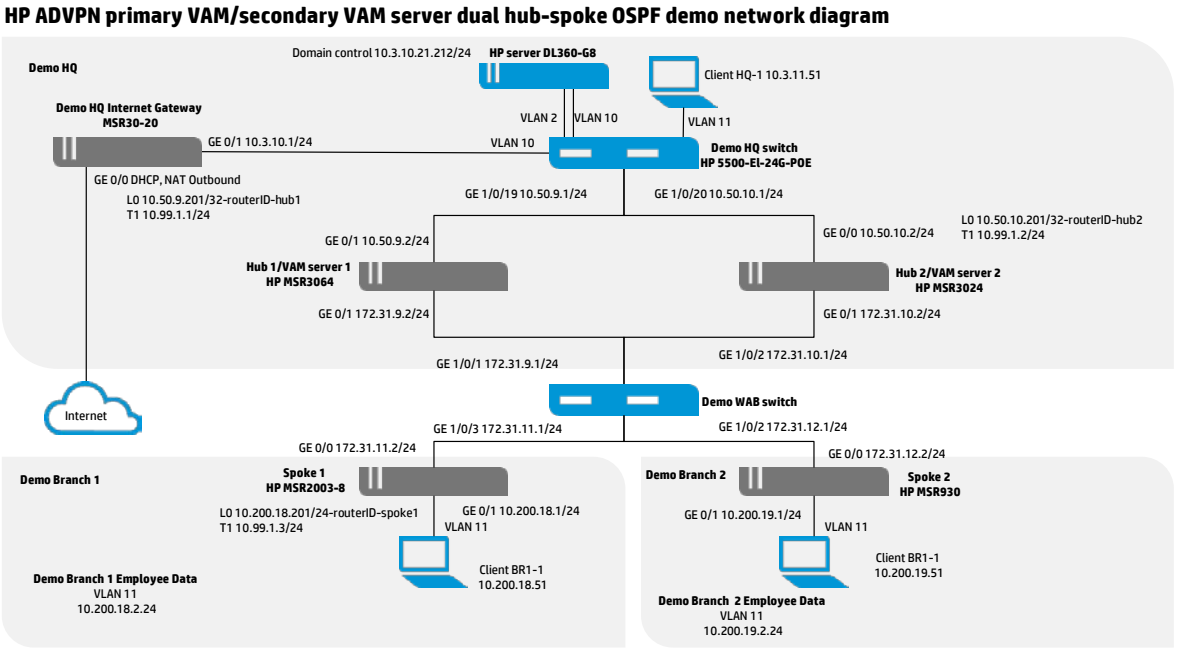
There may be customers that are currently using the DVPN configuration with MSR routers using HP Comware v5, that want to slowly migrate to the HP MSR Series next gen routers using the ADVPN configuration that is supported on HP Comware v7.

Note that when this configuration is used, the DVPN routers will only work in the hub-spoke model, since the HP Comware v5 DVPN routers will not be part of the HP Comware v7 ADVPN hub-group environment.

This configuration details how a customer can use HP Comware v7 VAM servers and connect to HP Comware v5 branch routers. Using the previous configuration for the ADVPN primary/secondary VAM server configuration, only one change is required to the hub/VAM server configurations.

Within the interface tunnel configuration for both hub 1/VAM 1 and hub 2/VAM 2, you will add the following:

Figure 28. ADVPN primary and secondary VAM server configuration



Hub 1/VAM server 1

```
interface Tunnel1 mode advpn udp
 description HP ADVPN Tunnel 1 on Demo Hub 1
 ip address 10.99.1.1 255.255.255.0
 ospf network-type p2mp
 source GigabitEthernet0/1
 tunnel protection ipsec profile demo-ipsec-profile1
```

- Use the compatible advpn0 command

```
vam client hub1 compatible advpn0
```

Hub 2/VAM server 2

```
interface Tunnel1 mode advpn udp
 description HP ADVPN Tunnel 1 on Demo Hub 1
 ip address 10.99.1.2 255.255.255.0
 ospf network-type p2mp
 source GigabitEthernet0/1
 tunnel protection ipsec profile demo-ipsec-profile1
```

- Use the compatible advpn0 command

```
vam client hub2 compatible advpn0
```

With this addition to the ADVPN hubs/VAM servers, MSR93x, and other HP Comware v5 routers that are using DVPN will be able to connect to a HP MSR's next gen router that is configured for ADVPN. No changes are made to the ADVPN spokes or the DPVPN spokes.

MSR930 DVPN spoke configuration

VAM client configuration

```
vam client name spoke1
 client enable
 server primary ip-address 172.31.9.2
 server secondary ip-address 172.31.10.2
 user spoke1 password simple abc
 vpn demo1
 pre-shared-key simple abc
```

IPsec configuration

```
ike peer vpn1
 pre-shared-key simple abc
#
ipsec transform-set vpn1
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm sha1
 esp encryption-algorithm des
#
ipsec profile vpn1
 ike-peer vpn1
 transform-set vpn1
interface Tunnel1
 ip address 10.99.1.4 255.255.255.0
```

Interface tunnel configuration

```
tunnel-protocol dvpn udp
 source GigabitEthernet0/0
 ospf network-type p2mp
 ipsec profile vpn1
 vam client spoke1
```

Verify

- Ping from MSR930 router to 10.50.9.201 (hub 1)

Figure 29. Ping various IP addresses

```
[MSR930-spoke1]ping 10.50.9.201
  PING 10.50.9.201: 56  data bytes, press CTRL_C to break
    Reply from 10.50.9.201: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 10.50.9.201: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.50.9.201: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.50.9.201: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.50.9.201: bytes=56 Sequence=4 ttl=255 time=1 ms
```

- Ping from MSR930 router to 10.50.10.201 (hub 2)

```
[MSR930-spoke1]ping 10.50.9.201
  PING 10.50.9.201: 56  data bytes, press CTRL_C to break
    Reply from 10.50.9.201: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 10.50.9.201: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.50.9.201: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.50.9.201: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.50.9.201: bytes=56 Sequence=4 ttl=255 time=1 ms
```

- Ping from MSR930 router to 10.3.10.2 (LAN Switch)

```
[MSR930-spoke1]ping 10.200.18.201
  PING 10.200.18.201: 56  data bytes, press CTRL_C to break
    Reply from 10.200.18.201: bytes=56 Sequence=0 ttl=254 time=1 ms
    Reply from 10.200.18.201: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 10.200.18.201: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.200.18.201: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.200.18.201: bytes=56 Sequence=4 ttl=254 time=1 ms
```

- Ping from MSR930 router to 10.200.18.201 (MSR2003-spoke)

```
[MSR930-spoke1]ping 10.200.18.201
  PING 10.200.18.201: 56  data bytes, press CTRL_C to break
    Reply from 10.200.18.201: bytes=56 Sequence=0 ttl=254 time=1 ms
    Reply from 10.200.18.201: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 10.200.18.201: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.200.18.201: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.200.18.201: bytes=56 Sequence=4 ttl=254 time=1 ms
```

Figure 30. Display dvpn se all for DVPN tunnel information

```
[MSR930-spoke1]dis dvpn se all
 Interface: Tunnel1  VPN name: demo1  Total number: 2

  Private IP:    10.99.1.2
  Public IP:     172.31.10.2
  Session type:  Spoke-Hub
  State:         SUCCESS
  Holding time: 0h 30m 4s
  Input:  706 packets,  705 data packets,  1 control packets
          65 multicasts,  0 errors
  Output: 571 packets,  570 data packets,  1 control packets
          68 multicasts,  1 errors

  Private IP:    10.99.1.1
  Public IP:     172.31.9.2
  Session type:  Spoke-Hub
  State:         SUCCESS
  Holding time: 9h 21m 22s
  Input:  1337 packets,  1336 data packets,  1 control packets
          1212 multicasts,  0 errors
  Output: 1932 packets,  1931 data packets,  1 control packets
          1255 multicasts,  4 errors
```

Figure 31. Display VAM client fsm

```
[MSR930-spoke1]dis vam client fsm
 Client name: spoke1
 VPN name:  demo1
 Interface: Tunnel1
 Resend interval(seconds): 5
 Client type: Spoke
 Username: spoke1

 Primary server:   172.31.9.2
   Current state:  ONLINE
   Holding time:   0h 36m 45s
   Encryption-algorithm:     DES
   Authentication-algorithm: SHA1

 Secondary server: 172.31.10.2
   Current state:  ONLINE
   Holding time:   9h 30m 12s
   Encryption-algorithm:     DES
   Authentication-algorithm: SHA1
```

MSR2003 ADVPN spoke configuration

VAM client configuration

```
vam client name spoke
 advpn-domain demo1
 server primary ip-address 172.31.9.2
 server secondary ip-address 172.31.10.2
 pre-shared-key simple abc
 user spoke password simple abc
 client enable
```

IPsec configuration

```
ipsec transform-set demo-ipsec-tran1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec profile demo-ipsec-profile1 isakmp
 transform-set demo-ipsec-tran1
 ike-profile demo-ike-profile1
#
ike profile demo-ike-profile1
 keychain demo-ike-keychain1
#
ike keychain demo-ike-keychain1
 pre-shared-key address 0.0.0.0 0.0.0.0 key simple abc
```

Interface tunnel configuration

```
interface Tunnel1 mode advpn udp
 description HP ADVPN Tunnel 1 on Demo Spoke 1
 ip address 10.99.1.3 255.255.255.0
 ospf network-type p2mp
 source GigabitEthernet0/1
 tunnel protection ipsec profile demo-ipsec-profile1
 vam client spoke
```

Verify

Figure 32. Ping various IP addresses

- Ping 10.50.9.201

```
[MSR2003-spoke]ping 10.50.9.201
Ping 10.50.9.201 (10.50.9.201): 56 data bytes, press CTRL_C to break
56 bytes from 10.50.9.201: icmp_seq=0 ttl=255 time=0.593 ms
56 bytes from 10.50.9.201: icmp_seq=1 ttl=255 time=0.399 ms
56 bytes from 10.50.9.201: icmp_seq=2 ttl=255 time=0.394 ms
56 bytes from 10.50.9.201: icmp_seq=3 ttl=255 time=0.370 ms
56 bytes from 10.50.9.201: icmp_seq=4 ttl=255 time=0.412 ms
```

- Ping 10.50.10.201

```
[MSR2003-spoke]ping 10.50.10.201
Ping 10.50.10.201 (10.50.10.201): 56 data bytes, press CTRL_C to break
56 bytes from 10.50.10.201: icmp_seq=0 ttl=253 time=0.639 ms
56 bytes from 10.50.10.201: icmp_seq=1 ttl=253 time=0.454 ms
56 bytes from 10.50.10.201: icmp_seq=2 ttl=253 time=0.423 ms
56 bytes from 10.50.10.201: icmp_seq=3 ttl=253 time=0.445 ms
56 bytes from 10.50.10.201: icmp_seq=4 ttl=253 time=0.440 ms
```

- Ping 10.3.10.2

```
[MSR2003-spoke]ping 10.3.10.2
Ping 10.3.10.2 (10.3.10.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.3.10.2: icmp_seq=0 ttl=254 time=1.509 ms
56 bytes from 10.3.10.2: icmp_seq=1 ttl=254 time=1.326 ms
56 bytes from 10.3.10.2: icmp_seq=2 ttl=254 time=2.008 ms
56 bytes from 10.3.10.2: icmp_seq=3 ttl=254 time=1.330 ms
56 bytes from 10.3.10.2: icmp_seq=4 ttl=254 time=1.464 ms
```

- Ping 10.200.19.201

```
[MSR2003-spoke]ping 10.200.19.201
Ping 10.200.19.201 (10.200.19.201): 56 data bytes, press CTRL_C to break
56 bytes from 10.200.19.201: icmp_seq=0 ttl=254 time=1.086 ms
56 bytes from 10.200.19.201: icmp_seq=1 ttl=254 time=0.966 ms
56 bytes from 10.200.19.201: icmp_seq=2 ttl=254 time=0.926 ms
56 bytes from 10.200.19.201: icmp_seq=3 ttl=254 time=0.915 ms
56 bytes from 10.200.19.201: icmp_seq=4 ttl=254 time=0.999 ms
```

Figure 33. Display advpn se

```
[MSR2003-spoke]dis advpn se
Interface         : Tunnel1
Number of sessions: 1
Private address      Public address       Port  Type  State        Holding time
10.99.1.1            172.31.9.2           18001 S-H   Success      0H 36M 9S
```

Figure 34. Display vam client fsm

```
[MSR2003-spoke]dis vam client fsm
Client name      : spoke
Status           : Enabled
ADVPN domain name: demo1
  Primary server: 172.31.9.2
    Private address: 10.99.1.3
    Interface      : Tunnel1
      Current state           : ONLINE
      Client type             : Spoke
      Holding time            : 0H 36M 24S
      Encryption-algorithm    : DES
      Authentication-algorithm: HMAC-SHA1
      Keepalive               : 180 seconds, 3 times
      Hub number              : 1
  Secondary server: 172.31.10.2
    Private address: 10.99.1.3
    Interface      : Tunnel1
      Current state           : ONLINE (active)
      Client type             : Spoke
      Holding time            : 9H 43M 15S
      Encryption-algorithm    : DES
      Authentication-algorithm: HMAC-SHA1
      Keepalive               : 180 seconds, 3 times
      Hub number              : 1
```

Troubleshoot

If the configuration cannot be verified, follow these steps to troubleshoot:

- Make sure that your routing is setup between your MSRs and WAN switch.
- Confirm via pings and OSPF peer statements that you have a valid connection between all hardware.
- Without ADVPN involved, you should be able to ping from the spoke 1's public interface to the public interface of the hub 1, hub 2, and WAN switch.

After that has been confirmed:

- Make sure that the IKE and IPsec configurations are the same throughout. These are common configurations that all MSRs share.

Confirm that the local-user names are exactly the same between the hub 1, hub 2, and spoke 1.

On spoke 1, confirm that you are using the correct IP addresses of the primary and secondary VAM servers within your VAM client and that the pre-shared-key is the same.

Use simple passwords until you are sure that they match and then you can always go back and change the passwords to cipher for security reasons.

- Clear IPv4 private-to-pubic address mappings for VAM clients registered to VAM server:

```
reset vam server address-map advpn-domain demo1
```

- Clear ADVPN domain statistics on VAM server:

```
reset vam server statistics advpn-domain demo1
```

- Delete IPv4 ADVPN tunnels:

```
reset advpn session statistics interface tunnel 1
```

- Clear statistics for IPv4 ADVPN tunnels:

```
Reset vam server statistics
```

Resources

Visit hp.com/networking for information on how the HP FlexNetwork Solution helps transform the networking experience.

- For information on the HP VSR1000 Series, click “Products” tab, then on “Routers”, and then on “HP VSR1000 Series”

For more information on the HP MSR Series of routers and other HP FlexBranch content, refer to information available on the HP Networking Resource Finder Technical Documentation tab and selecting “Routers” under “Products, Solutions, and Industries.”

- Look for the “HP VSR1000 Series technical overview” white paper for a brief overview

At the HP Customer Care—Product Support website, use the model name of the HP VSR1000 Series routers, for example “VSR1000” in the HP product name field. For these resources:

- Refer to the product manuals for details on supported commands and configurations
- Click “Knowledge Base”, then click “Manuals” in the pull-down menu
- Refer to the release notes for details on supported features, software and hardware versions, limitations, and known issues
- Find software

Learn more at
hp.com/networking

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-7939ENW, May 2015