

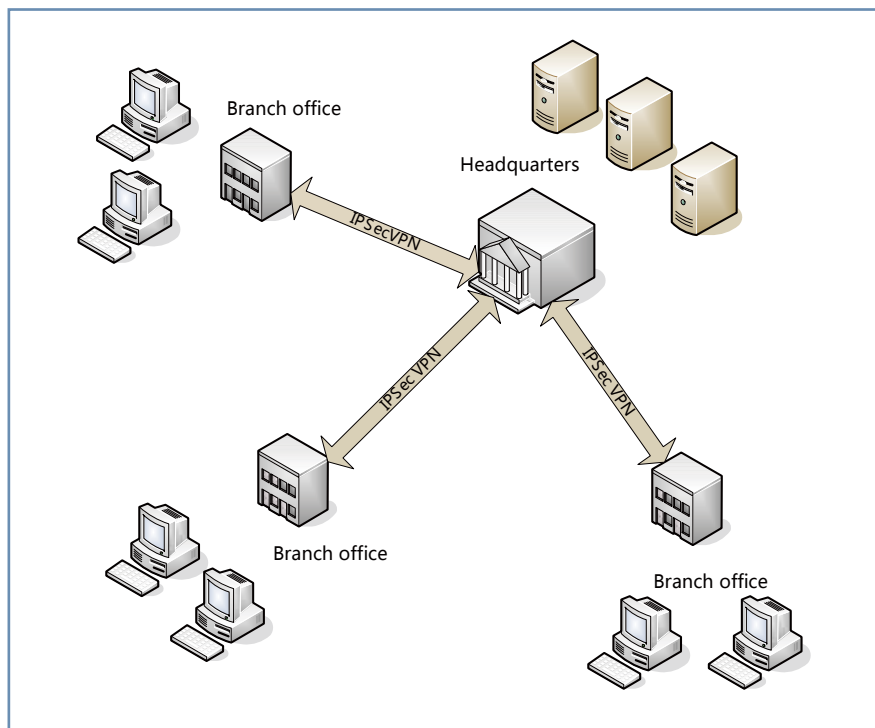
# Hillstone PnPVPN Solution

## Easy Deployment Branch Office VPN

### 1. Introduction

For companies that spread across geographically locations, VPN is the mission critical technology that brings people together. IPsec VPN is the technology of choice to provide site to site connection between remote offices that uses public telecommunication infrastructures. IPsec, together with its key negotiating protocol (IKE) has the major advantage of been standard based and very good interoperability between vendors, if configured properly. But IPsec has also been regarded as hard to configure and deploy, the flexibility of IPsec and IKE provide a maze of configuration options that confuses administrators new to the technology. Furthermore, some enterprises have a large number of remote sites that needs to be connected. For example, gas stations, supermarkets and chain stores. The complexity of VPN configuration multiply by the number of remote sites makes VPN operation a formidable task for the enterprise IT department.

Figure 1: Typical branch office and Headquarter VPN scenario



Hillstone PnPVPN is a patent pending, rapid deployment branch office VPN solution that greatly simplify the process of setting up VPN for branch

office. With a centrally managed database of parameters at the headquarter, a branch office to be setup simply by a username and password, parameters of local configuration can be downloaded when the VPN is established. This greatly reduce the maintenance of branch office connection within the enterprise.

## 2. Difficulties of IKE and IPSec Configuration

IPSec is a IP layer encryption standard that allows any IP traffic to be encrypted and transported over public networks. It is defined by a set of IETF (Internet Engineering Task Force) standard documents (RFCs). Although manually set keys are allowed, the more secure and common case is to use IKE (Internet Key Exchange) protocol. In IKE, keys used for encryption and decryption are negotiated on the fly and different each time. IKE is also defined by a set of IETF RFCs.

To set up IPSec VPN negotiated by IKE protocol, one needs to set up:

- Phase 1 parameters
- Phase 1 proposals defined by a combination of encryption algorithm (such as 3DES), hash algorithm (such as SHA-1) and Diffie-Hellman groups
- Phase 1 ID for local system and remote system
- Preshared key or certificates
- Remote system IP or domain name
- IKE mode (Main mode or Aggressive Mode)
- Phase 2 parameters
- Phase 2 proposals defined by a combination of protocol (ESP/AH), encryption algorithm (such as 3DES), hash algorithm (such as SHA-1) and Diffie-Hellman groups
- Phase 2 ID for local system and remote system (also called traffic selectors)
- VPN policy for allowed traffic

The parameters need to be properly set up at both VPN devices and any discrepancy will cause the malfunction of the VPN tunnel. Another problem is for each branch office, a separate VPN and IKE instance needs to be configured and with hundreds or thousands of branch offices in some enterprises, we will have hundreds to thousands of VPN configurations in the headquarter equipments, and most parameters of these configurations will be the same. It will be much simpler if we can have one configuration that can be a single point of control for all the branch office VPNs.

For branch office setup, there is also repetitive work that needs to

be done on the firewall. There is a need to provide a quick way to push standard configuration to the device.

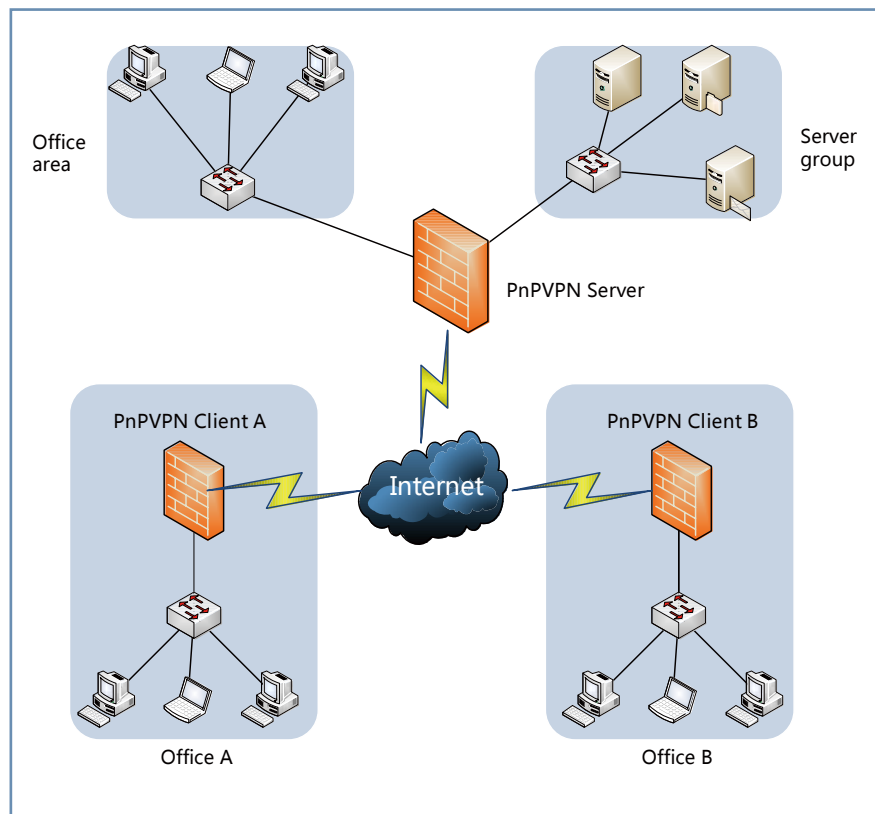
### 3. Overview of PnPVPN

PnPVPN is an acronym for Plug-n-Play VPN. It is composed of 2 parts:

- PnPVPN Server: Often placed in enterprise headquarters, managed by IT engineers from headquarter. Client configurations can be pushed by the server. PnPVPN Server is usually a Hillstone SA/SG series security gateway.

- PnPVPN Client: Usually placed at branch site, can be remotely managed by IT engineers from headquarter. Simple configuration is needed to setup connection to the server, for example, client ID, password and server IP. After negotiation with the server, configuration information can be retrieved, including DNS, WINS, DHCP pool etc. PnPVPN clients can be Hillstone SR series security routers or SA/SG series security gateways.

Figure 2: shows a typical network setup for PnPVPN: ▶



#### PnPVPN work flow

With example in Figure 2, here is a simple workflow:

1. Client sends connection request with client ID and password to the server
2. When server receives the request, it verifies the client ID and password. If the verification is successful, it pushes configuration parameter

to the client, including DHCP parameters, DNS, WINS, policy and routing information.

3. Client receive the information and set up security functionality

4. PCs connect to PnPVPN client can receive IP, mask, gateway from the client and access resources beyond the VPN.

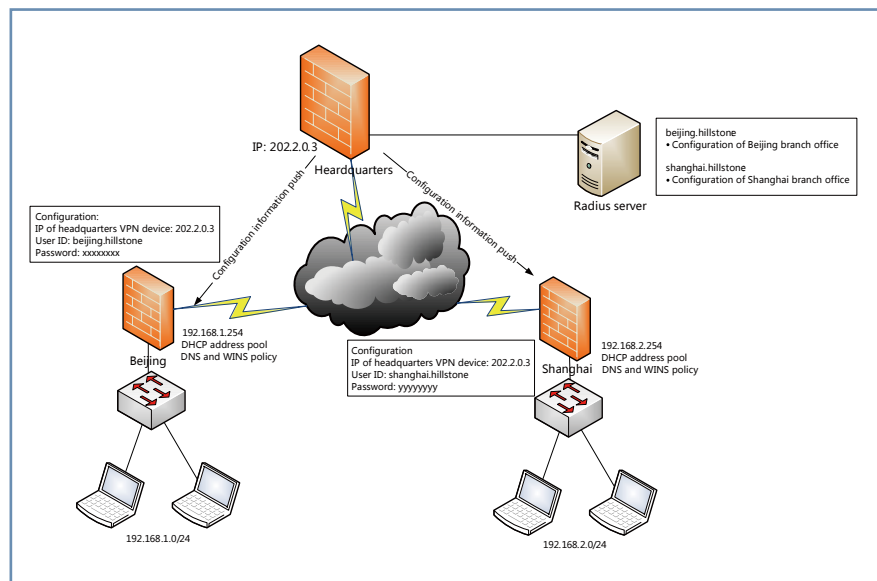
## 4. Hillstone PnPVPN

### Configuration

Hillstone PnPVPN is a rapid deployment VPN solution. The VPN configuration is centrally control from the Headquarter VPN device. The information can either be stored in a Radius user database, or as local user in the Hillstone VPN device. For each remote user, VPN setup can be as simple as 1-2-3, putting in headquarter’s IP or domain name, a user ID and password. The user ID and password is the parameter used to establish IPsec connection with the headquarter device. The headquarter VPN device controls the Phase 1 and Phase 2 parameters for IKE negotiation. If the negotiation is successful, other network parameters are also pushed to the branch office VPN device, this includes:

- DHCP parameters used for branch office networks
- DNS and WINS servers, this will be in addition to the DNS servers each branch office will receive from their local ISP connection.
- Routes
- Policies
- Other configuration

Figure 3: shows an example of PnPVPN operation



These parameters can optionally be saved in the branch office device as configuration after they are pushed. Most of the configuration work are

centrally managed on the headquarter side by the IT administrator there. Hillstone PnPVPN supports storing the information either in a Radius server or as additional parameters in local user database on the VPN device.

Two branch offices are configured on a Radius server (local user on the VPN device is also supported). On the Beijing branch VPN device, we configure the headquarter IP, a user ID and password. Using these parameters, the branch office device can successfully negotiate a VPN connection with the headquarter device. After the connection is established, network parameters are then pushed from the headquarter to the branch office, such as the DHCP pool used for branch office, the company private DNS and WINS servers etc.

### Managing Branch Office Device

Adding and removing a branch office device is very simple. On the headquarter side, the administrator just need to add a user account in the Radius server or device's local user database used for the PnPVPN. A user ID and password pair can be generated. The user ID and password can be physically delivered to the branch office. Or, if the administrator have a remote connection to the branch office device (for example, through HTTPS or SSH), he can perform the PnPVPN client side setup remotely.

### Batch Generation of User ID and Password

To simplify deployment for a larger number of devices at the same time, Hillstone provides a way to batch generate the user IDs and passwords. The administrator can prepare a spreadsheet detailing the name of different sites, user ID, DHCP pool parameters etc, and import it into the headquarter VPN device. The VPN device will automatically create the branch office VPN user entries. These entries can be exported and delivered to each branch offices. Many fields of the imported spreadsheet are optional and can be derived from the site name.

## 5. Conclusion

PnPVPN greatly reduces the setup and maintenance effort of VPN operation for enterprise IT departments. It is suitable for both small and medium enterprises that have a few sites and large enterprises that have hundreds to thousands of branch offices. For small and medium enterprises, PnPVPN provides a simplified way to setup IPsec VPN that do not need a strong IT department to maintain. For large enterprises, it greatly reduces the setup and operation cost by centralizing the configuration and minimal client side configuration.