

Hillstone IPsec VPN Solution

1. Introduction

With the explosion of Internet, more and more companies move their network infrastructure from private lease line to internet. Internet provides a significant cost advantage over private lines and it makes setting up branch offices fast and easy. Now that the connections between offices are over public infrastructure, how to secure data transport between remote sites becomes very crucial. VPN (Virtual Private Networks) technology emerges to address this problem.

IPsec has been the most important VPN technology to interconnect remote endpoints over public network. SSL VPN emerges over the last few years and now is the preferred way to provide remote access VPN solution for employees working away from their office. Still IPsec VPN remains the technology of choice to provide site to site connection between remote offices.

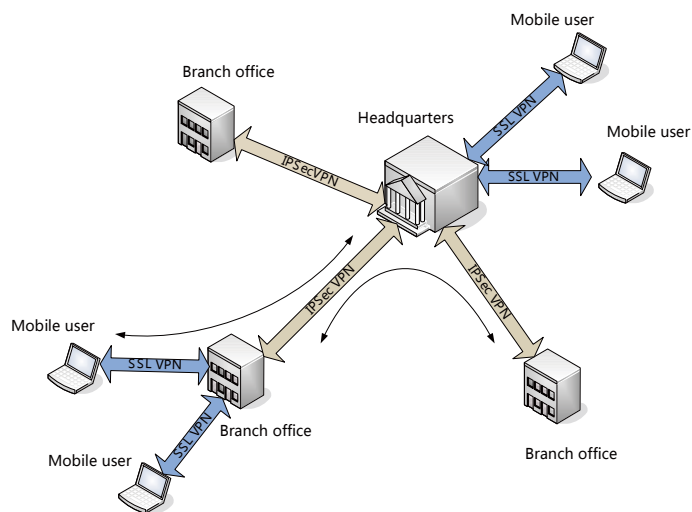


Figure 1: Hillstone IPsec and SSL VPN integrated solution

Hillstone IPsec VPN offers Hub-and-Spoke deployment of both policy and route based VPN that interconnect remote offices. Mobile users can connect using SSL VPN



Hillstone IPSec VPN Solution

into either the branch offices or the headquarters. SSL VPN provides maintenance free deployment that includes auto installation and upgrade. User authentication is integrated. Both SSL VPN and IPSec VPN can be route based to provide ubiquitous access from anywhere to anywhere on the network layer.

IPSec VPN is a mature technology and many hardware acceleration solutions exist. It has higher performance and remains the technology of choice for site-to-site connection of remote offices.

Hillstone IPSec VPN support

- Up to 8Gbps scalable IPSec performance
- Up to 30000 IPSec tunnels
- Standard based implementation that interoperates with major VPN vendors
- Complete crypto suite support up to AES256, Diffie-Hellman group 5
- Preshared Key and PKI support
- Route Based VPN and Policy Based VPN
- Hub-and-Spoke deployment
- Dead Peer Detection (DPD) support
- NAT Traversal support
- Static IP, Dynamic IP and Dial-up peers
- QoS over VPN
- Anti-replay support
- Commit bit support
- Application layer control over VPN
- GRE and GRE-over-IPSec
- L2TP and L2TP-over-IPSec
- Routing protocol over IPSec VPN/GRE/GRE-over-IPSec

2. IKE and IPSec Implementation

IPSec VPN and its corresponding key exchange protocol (IKE) consist of a set of IETF standard documents (RFCs). Standard based implementation means that devices from different manufacturer should and can interoperate with one another. The set of protocols and algorithms have passed much scrutiny on its security aspect.

Hillstone IPSec solution have been tested to interoperate with major international VPN equipment vendors, such as Cisco, Juniper, Netscreen, Watchguard. Hillstone IKE



Hillstone IPSec VPN Solution

stack has been subject to various type of vulnerability scanning and attack tests.

IPSec

Hillstone support complete IPSec parameters and algorithms:

- Encryption Algorithm: DES, 3DES, AES128, AES192, AES256. AES128 usually is computationally faster than 3DES while offers similar strength. AES256 is a much stronger encryption algorithm. All of these algorithms are hardware accelerated on Hillstone platforms. (RFC2405, RFC1851, RFC3602)
- Hash Algorithm: MD5 and SHA-1. Both of these algorithms are hardware accelerated on Hillstone platforms. (RFC2403, RFC2404)
- ESP (RFC2406) and AH (RFC2402): Both IPSec methods are accelerated on Hillstone platforms.
- UDP Encapsulation of IPSec. Hillstone support multiple versions for maximum interoperability draft-ietf-ipsec-udp-encaps-01.txt, draft-ietf-ipsec-udp-encaps-02.txt, RFC3948)
- Anti-Replay detection: Hillstone StoneOS supports standard Anti-Replay detection mechanisms and can dynamically adjust the anti-replay window based on network conditions.

IKE

Hillstone IKE support full series of related RFCs including RFC2401, RFC2407, RFC2408 and RFC2409. A rich set of IKE features is supported.

- IKE Phase 1 support the same and complete set of encryption algorithm and hash algorithm as indicated before.
- Main Mode and Aggressive Mode negotiation.
- Diffie-Hellman group: Group 1, 2 and 5. Support for Group 5 in IKE is crucial for generating keying material for strong algorithms such as AES256.
- Preshared Key and Certificate based (PKI) authentication
- Perfect Forward Secrecy (PFS) group 1, 2, 5 or no PFS: PFS in IKE guarantees that breaking an old set of keys will not jeopardize the secrecy of new keys.
- Dead Peer Detection: automatic detection reachability between the two peers and bring down the security association.
- NAT Traversal negotiation: Hillstone support multiple version for maximum interoperability. (draft-ietf-ipsec-nat-t-ike-01.txt, draft-ietf-ipsec-nat-t-ike-02.txt, RFC3947)



Hillstone IPsec VPN Solution

Other Features

- DF bit: Copy/Set/Clear. Don't Fragment bit in IP header controls how routers handle IP packets that are too large for the interface MTU.
- Manual Configure Phase 2 ID: Problem matching phase 2 ID is the most frequent cause of VPN interoperability problem between vendors. With Hillstone device, administrator has the ability to manually configure Phase 2 ID to match another vendor's device.
- Hillstone device can be configured to be Initiator only or Responder only or both.
- Hillstone device has autoconnect feature that can automatically start IKE negotiation.

High Capacity and Performance

All Hillstone platforms support IPsec acceleration through hardware. Each CPU core has an embedded IPsec processing engine. This ensures that the IPsec performance scales with the number of CPU cores and the engine will not be the bottleneck. IPsec performance can reach 8G on Hillstone top of the line platform.

Through state of the art hardware platform, Hillstone devices support up to 30000 IPsec tunnels. All 30000 IPsec tunnels are setup through IKE negotiations. The scalability nature of the implementation means that VPN throughput for 30000 tunnels is similar to throughput with 1 tunnel. Hillstone device can reach a throughput of 8Gbps.

3. Hillstone Solution

Site-to-Site VPN

For site-to-site VPN, Hillstone support static IP peers where peer IP address is specified. If one site's IP may change over time, FQDN can also be specified. This together with DDNS service, peer IP can be obtained at run time and IKE negotiation can be initiated.

For VPN peer with dynamic IP address, we can configure dynamic IP VPN. IKE authentication can be verified using FQDN ID. One side peer ID must match the local ID configured on the other side, and vice versa.

Route Based VPN

Route based VPN virtualize a VPN tunnel as an interface. In StoneOS it is the tunnel



Hillstone IPSec VPN Solution

interface. This interface can be treated similar as many other interface, and StoneOS can provide many functions that are available to regular interface:

- NAT can be configured on tunnel interface for IP packet. When connecting two networks with conflict IP subnet, both side can use this NAT feature to translate their IP subnet into a non-conflicted network before apply VPN encryption.
- MTU and MSS can be configured on tunnel interface.
- QoS profile can be configured on tunnel interface. User can apply QoS profile such as shaping, policing, priority queue, IP queue etc on the tunnel interface to control traffic inside the VPN tunnel.
- Routing protocol can be configured on tunnel interface. For example, a company can run OSPF between different sites interconnected with VPN.
- For Route Based VPN, P2P/IM control, content filtering can be configured on related firewall policy to achieve the desired effect.
- Route load balance and failover comes naturally. Hillstone support standard ECMP (Equal cost multiple path) and WCMP (weighted ECMP), and this can be between VPN route and regular routes.
- Hillstone support many type of routes: Source based routing (SBR), Source interface based routing (SIBR) and Policy based routing (PBR). All these different type of routing can be applied to tunnel interface and route based VPN.
- StoneOS support GRE and GRE-over-IPSec, multiple IPSec/GRE/GRE-over-IPSec tunnels can be supported on one tunnel interface. OSPF can be supported on the tunnel interface.

Route based VPN can work seamlessly with other network technologies. It separates the networking and security configuration and makes the logic of device management more clearly.

Policy Based VPN

Policy based VPN is VPN applied on top of a firewall policy. This is the traditional VPN scenario. With Policy based VPN, user can apply different profiles that are available to regular firewall policies:

- P2P/IM control can be applied to traffic inside VPN tunnel
- Policy based QoS is available to traffic inside VPN tunnel
- URL and Content filtering can be applied to VPN policy

Hillstone IPSec VPN Solution

Hub-and-Spoke VPN

Many company consists of a headquarter and many branch offices. Interconnect all branch offices with full mesh VPN deployment is not scalable. As the number of branch office increases, the number of VPN tunnels increase as $O(n^2)$. And with adding a branch office, VPN configuration of all other sites needs to be changed, including headquarter and other branch offices. When we are dealing with hundreds to thousands branch offices, VPN tunnels on a branch office devices also runs into hundreds to thousands. All these problems make full-mesh deployment not an acceptable solution.

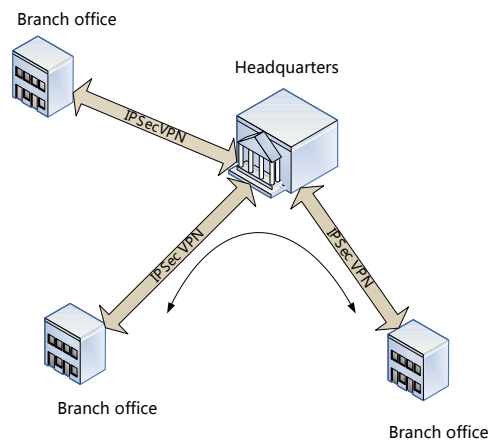


Figure 2: Hub-and-Spoke VPN

Hub-and-Spoke deployment solves this problem by setting up one VPN between each branch office (Spoke) and the headquarter (Hub). The branch office can communicate with each other through the headquarter.

Hillstone support Hub-and-Spoke deployment both in policy based VPN and route based VPN.

Dial-up VPN

In headquarter-branch office scenario, with the increase number of branch offices, configure one VPN in the headquarter for each branch office quickly becomes a tedious problem. Dial-up VPN solves this problem by configure one VPN template in the headquarter. With each branch office connect in, a VPN is automatically created in the headquarter.

Hillstone IPSec VPN Solution

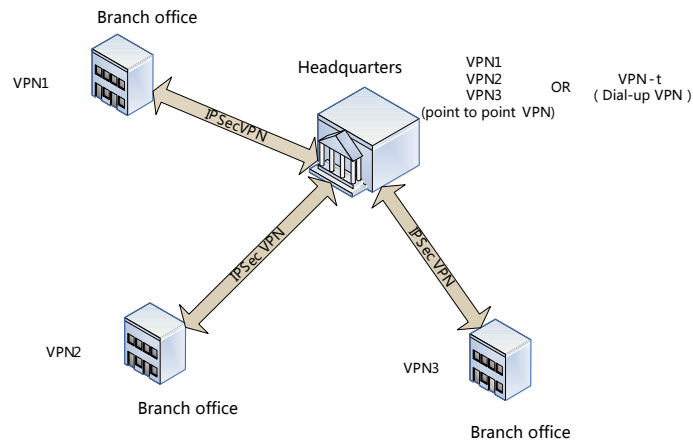


Figure 3: Site-to-Site VPN vs Dial-up VPN

For example, in Figure 3, when connecting the headquarter with 3 branch offices, we need to configure 3 site-to-site VPN. If dial-up VPN is used, we only need to configure one VPN (VPN-t which is the VPN template).

Dial-up VPN can use either preshared key or certificate (PKI) as authentication method. For pre-shared key, Hillstone use special techniques to make sure that each branch office uses different preshared keys and these keys can not be derived from each other.

Hillstone role based access control provides fine grained access control can grant/deny user access base on user' s identity and group information. Dial-up VPN can be combined with role based access control. Each dial-up VPN connection can be associated with a user identity and this can be used to determine what level or access this user can have.

PnPVPN

Traditionally, IPSec VPN is regarded as difficult to configure. On both side of the VPN tunnel there are a series of Phase 1 and Phase 2 parameters. Any discrepancy in the configuration will cause VPN negotiation malfunction. For a company with hundred to thousands branch offices, deploy branch office VPN is a repetitive, tedious and error-prone process. Hillstone PnPVPN is a patent pending technology for fast branch office deployment. It centralizes the configuration management in the headquarters, with each branch office needing only a username and password. The VPN and other configuration

Hillstone IPsec VPN Solution

parameters will be downloaded during negotiation. This greatly reduces the effort for setting up VPN for remote offices.

PnPVPN solution also provides a batch processing capability for branch office devices, which sets up user name and password for many devices at the same time. This further simplifies the deployment effort.

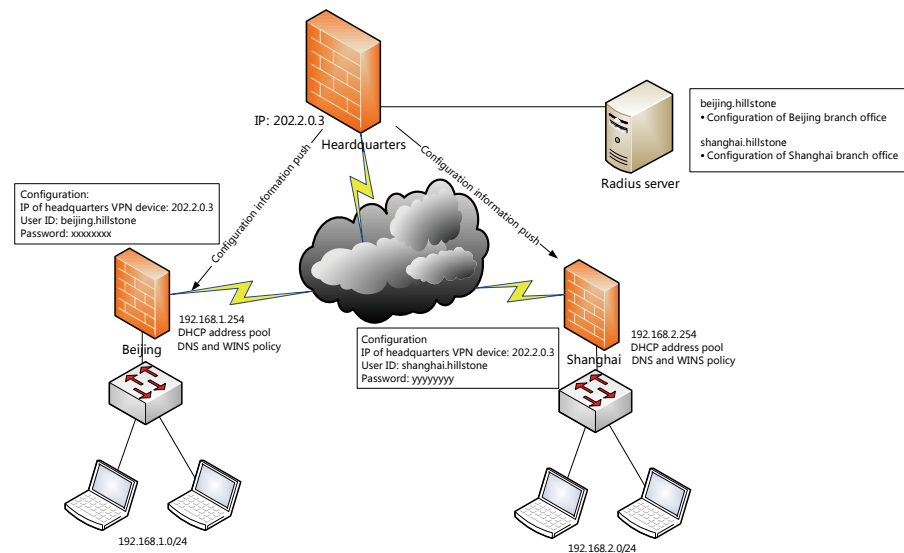


Figure 4: Example of PnPVPN

4. Conclusion

Hillstone support a rich set of IPsec VPN features that tightly integrated VPN with network protocols and feature sets. Flexible deployment scenario, together with SSL VPN, offers a complete VPN solution for ISPs, enterprises and small businesses.