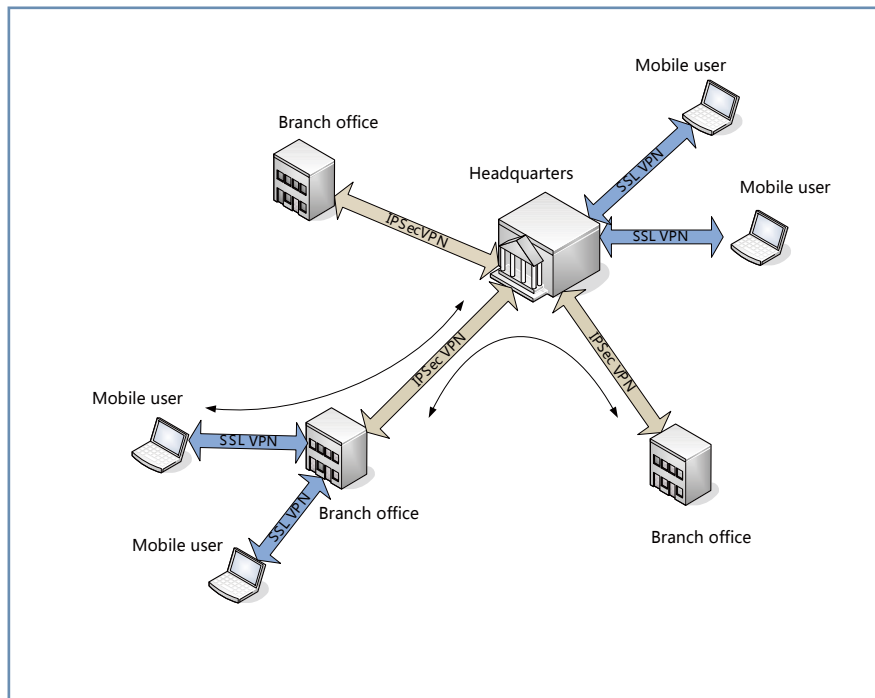


Hillstone SSL VPN Solution

1. Introduction

Evolution of Internet has changed the way companies build their network infrastructure. Places that use to be connected with private lease lines need to add public internet access. Also public connection enjoys a big price advantage. VPN technology emerges that secure connects remote offices and users that either works off site or on business trip. For a long time, IPsec VPN is the technology of choice. It is standard based and offers good interoperability among device vendors. With the emergence of internet and wide distribution of web browsers, a new type of VPN technology emerged and now is the preferred way to provide secure remote access. Hillstone solution support both SSL and IPsec VPN. Hillstone platform operating on the network layer can seamless combine two types of VPN and provide IP layer access while at the same time offers fine grain access control.

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 into either the branch offices or the headquarter. 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. Fine grained role based access can be setup on the device to provide strong control on what resources a certain user can access.

Hillstone SSL VPN support

- Native IP Layer network access, support all IP based application
- Private IP allocation
- Private DNS and WINS provide intranet name resolution
- Control of cryptographic algorithms
- Automatic route distribution
- Support multiple user domains, each with different AAA server
- Support local user database, Active Directory, LDAP, Radius, USB key, two factor authentication
 - Hardware binding for connected users and PCs, support 1 to 1, many to 1, 1 to many and many to many bindings
 - Support security scanning of user PC to determine user level of access.
 - Real-time monitoring of the connected users
 - Role based access control provide fine grained access control, user roles can base on a sophisticated combination of user name, user group and user PC's security profile.
- Support multiple instances of SSL VPN for maximum security
- Support multiple interfaces and IPs for connectivity redundancy.
- User management features.

2. IPSec VPN vs. SSL VPN

IPSec VPN and its corresponding key exchange protocol (IKE) consists 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.

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. However, IPSec VPN is generally considered not easy to use. Deployment requires manual delivery of authentication materials and IDs, many parameters such as authentication and encryption algorithms also need to be manually configured. This is especially problematic for remote users who use PC to connect to the office. VPN client software need to be delivered and installed. This requires a large amount of repetitive work and increase the operating cost of the remote access solution. It is not suitable for large scale remote access deployment.

Furthermore, in remote access scenario, IPSec VPN lacks a natural way of user authentication. Besides using certificate as a way to authenticate the users, several ways were created such as XAUTH or L2TP-over-IPSec to introduce user authentication into IPSec VPN. This increases the complexity of the VPN configuration that was already very hard to understand. SSL VPN was introduced in 2000 and is generally accepted as the way to deploy remote access VPN. It is browser based which means it can be remotely deployed. The ease of use is greatly enhanced. With HTTPS protocol, bidirectional authentication can be easily achieved. The client verify the server through HTTPS server certificate, the server subsequently verify the client through username/password, or with hardware token, multi-factor authentication which combines the two.

SSL VPN's weakness is it is not suitable for site-to-site remote office deployment, because it requires user authentication at connection time. It is initiated from client to server unidirectionally compare to IPSec VPN which can be initiated bidirectionally from either side. SSL VPN is in general much slower than IPSec VPN. Hardware acceleration technology for IPSec is more mature and SSL VPN suffers from connection based technology as we will explain later.

Lastly, all SSL VPNs from different vendors contains proprietary technology. There is no chance of interoperating among vendors. It can be seen that SSL VPN and IPSec VPN are in many ways complimentary. While SSL VPN excels at remote access, IPSec VPN is the better choice of remote office site-to-site interconnection. Hillstone offers both type of VPNs and an complete solution to the customer

3. Evolution of SSL VPN

HTTP and Application Proxy

First generation SSL VPN is a HTTPS proxy. Around turn of the century with the explosion of internet and web based applications. The key technology in this solution is URL rewrite. Beside proxying the initial HTTPS request, the gateway rewrites the private URL in HTTP content into HTTPS URLs. URL rewrite technology is never complete. With the emergence of Javascript, Java Applet, Flash, all can have embedded URL and scripts that can generate additional URL. Support for translation of these URLs varies from vendor to vendor.

SSL VPN vendors gradually add support for different applications over SSL. Application Proxy is a technology that converts different application into HTTPS access. Application support varies from vendor to vendor. Commonly

support applications such as FTP, exchange and windows file access. Some vendors added support for selected Database applications. In many cases, ActiveX or Java applets need to be downloaded to provide UI interaction.

Figure 2: HTTP to HTTPS Proxy ▶

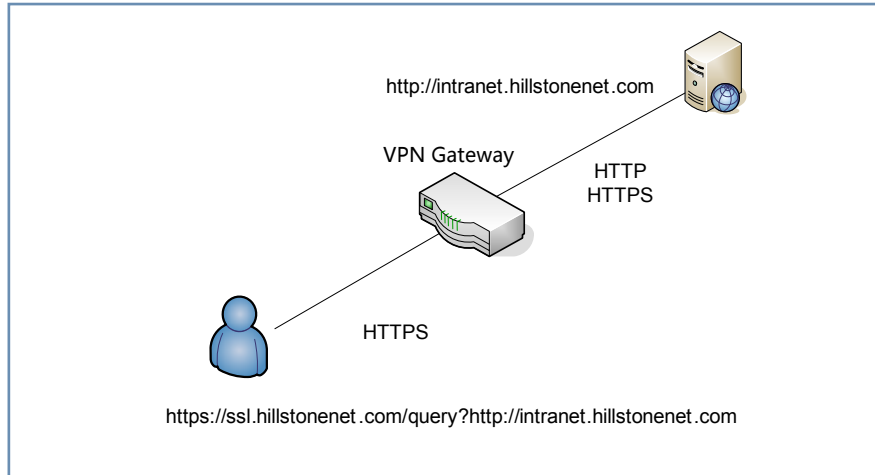
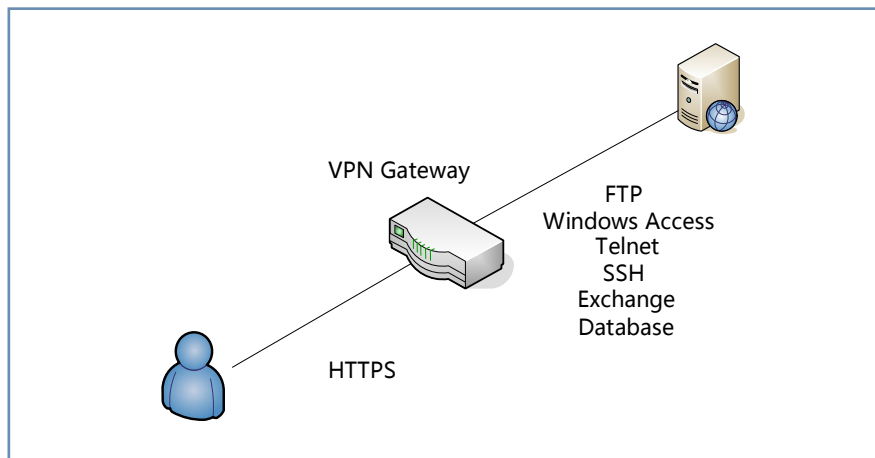


Figure 3: Application Proxy ▶



IP Tunnel

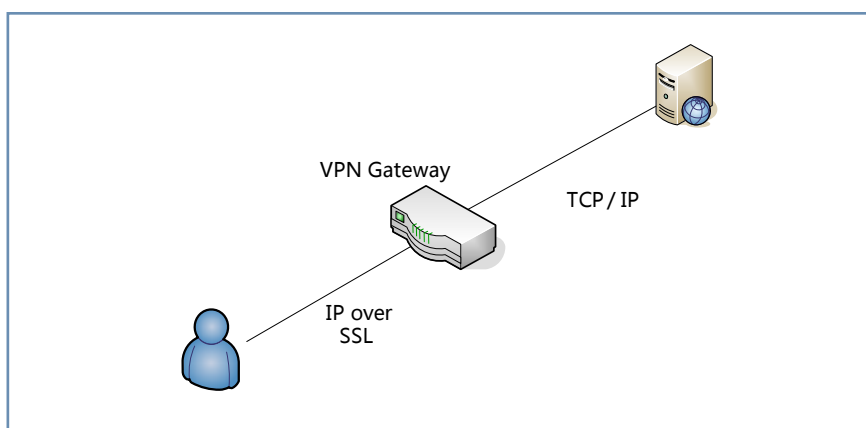
It becomes apparent very soon that adding proxy to support each type of application is not scalable. The second generation SSL VPN added support for all IP based protocols. The technology is called IP tunneling. IP Tunneling works for all IP based applications and solves the problem that user need to write proxy software for each new type of application. This arrangement have a major problem. Encapsulating TCP application inside SSL tunnel introduces a serious TCP-over-TCP problem. On a WAN link with a small number of packet loss, both the application TCP and SSL tunnel's TCP will try to recover from the lost packet. The two TCP mechanisms interfere with each other and introduce drastic performance degradation. Even without the TCP-over-TCP problem, raw SSL data performance is still lower than IPsec performance on similar platforms.

4. Hillstone Secure Connect VPN

SSL Deployment

Hillstone Secure Connect VPN is the next generation SSL VPN solution that combines the benefit of SSL VPN and IPsec VPN. As for other SSL VPN, an ActiveX will be automatically installed the first time user log on to the system. This VPN client is maintenance free and will autoupdate if a new version is detected. Subsequently, the user has 2 ways to log on to the system: either through the web page or through direct starting of the VPN client. The VPN client automatically cache the previous log on parameters including the domain, server IP/port and user name.

Figure 4: IP Tunneling



On the server, client settings are centrally configured. First of all, client will be allocated a private IP upon log on. At the same time, private DNS and WINS are also pushed to the client so that intranet domain names can also be resolved easily.

Routes centrally configured on the device will also be pushed to the client. This allows the client to only specified traffic through the VPN tunnel. Route configuration is very flexible. For example it is easy to achieve the effect that only traffic targeting intranet servers will go through the tunnel, while the user's internet browsing will still go through the regular route to the user's ISP.

Cryptographic algorithm that will subsequently be used in the data channel is also centrally configured and pushed to the client. During SSL exchange, cryptographic materials were exchanged and keys were negotiated between the client and the device.

IPsec Data Channel

Hillstone Secure Connect VPN utilizes IPsec data channel to transport

user data. The connectionless nature of IPSec solves the TCP-over-TCP problem that traditional IP over SSL tunneling has. This greatly improves the performance over high latency, lossy WAN link. IPSec naturally support all IP based applications. Hillstone utilizes hardware IPSec acceleration engine that can achieve much higher VPN performance than SSL encryption solution. Hillstone IPSec support advanced crypto algorithms including 3DES, AES-128, AES-192, AES-256, MD5 and SHA-1, all hardware accelerated.

Role based Access Control

Hillstone introduced role based access control that can provide fine grain control on who can access what device. After log on, a user's roles can be determined by his user name or user groups. A user can have multiple roles. Access policy can be configured such that users with specific roles are permitted or denied access to certain resources. This policy can be specific to certain user or certain group of users. Further more, policies can be configured to apply to users with a combination of roles. Hillstone role based policy supports a rich set of features that is available to all policies:

- QoS: QoS profile can be configured on policy to provide various type of functions
 - IP based QoS
 - Service based QoS
 - Shaping
 - Policing
 - Guarantee bandwidth
 - Priority
 - Marking
 - Low latency
- P2P/IM control
- Content filtering
- Time schedule: allows policy to be turned on/off according to a time schedule.
 - Application security

User Hardware Binding

Hillstone SecureConnect VPN supports hardware binding of users and PCs. This offers an added level of security for customers. The client assigns a unique PCID to each PC and user can be allowed access only if certain binding relationship is satisfied. Supported binding mode are very flexible and includes 1 user to 1 PC, 1 user to multiple PC, multiple user to 1 PC etc. Administrators can setup super users that have no PC restrictions and super PCs that have no user restrictions.

The binding relationship between user and PC can either be manual, or through automatic learning. Administrators can approve user bindings learned manually or through preapproval.

Secure Connect VPN Features

Hillstone Secure Connect VPN supports multiple user domains. Each user domain can have its own AAA server or AAA server list. This way, several groups of users with different authentication needs may use the same SSL VPN portal. Roles can be assigned differently based on domain and this will determine access rights of different groups of users. Secure Connect VPN can authenticate users with Active Directory, LDAP, Radius, USB key, local user database and two factor authentication. Hillstone devices also support multiple instances of SSL VPN for maximum security and versatility. For example, an external SSL VPN portal can be setup for remote access, while an internal portal can be setup for intranet control of Guest LAN or wireless networks.

Common Deployment: Remote Access

Hillstone Secure Connect is an SSL VPN solution and ideal for remote access deployment. This deployment scenario applies for employees that work away from office. Secure Connect enables him to connect to the intranet and if policy allows, all network resource will appear local to him. Role based access control can be applied to control the resources that he can access. The company can integrate user authentication with existing Active Directory or Radius server. Furthermore, the connection is bidirectional. If policy allows, resources inside the intranet can initiate connection to this user's system.

Common Deployment: Intranet Control

Figure 5: Remote Access Solution ▶

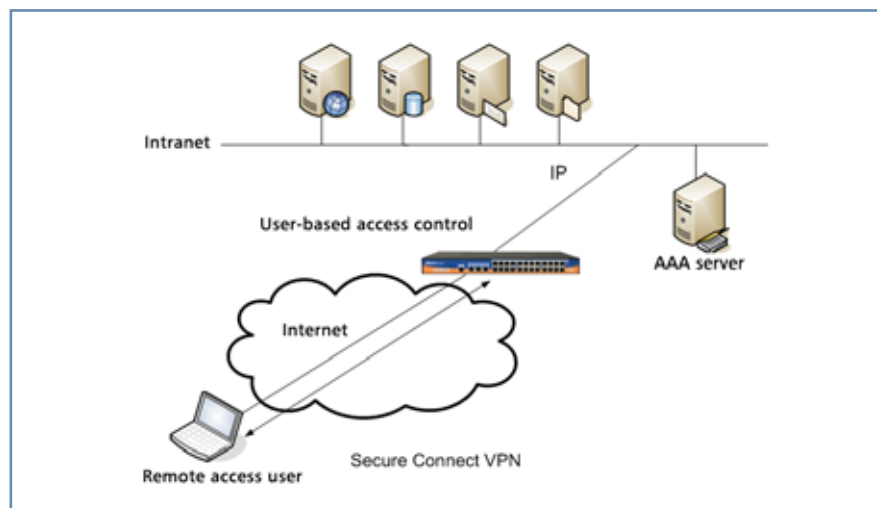
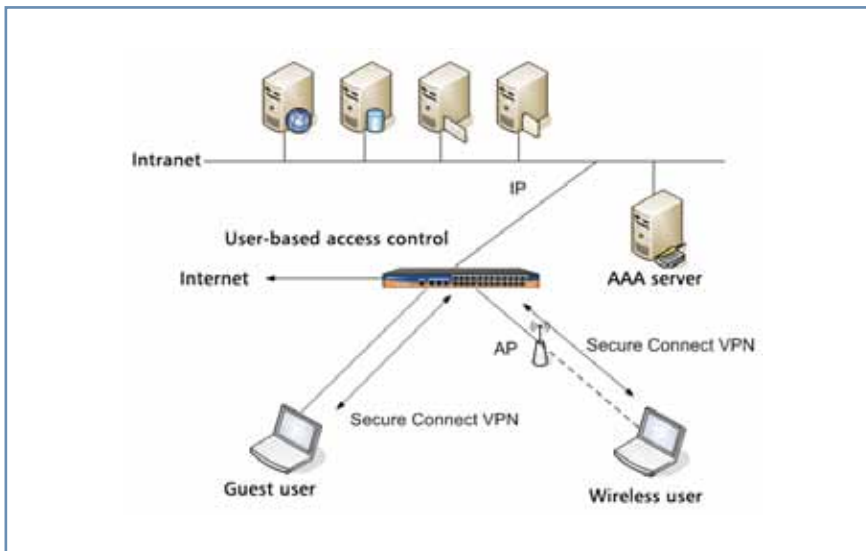


Figure 6: Intranet Control ▶



In this scenario, the company may have a controlling point that is connected to a Guest LAN or a wireless AP. Users can log on using Secure Connect VPN and the device will control the access based on user roles. For example, guest user will only be allowed access to the internet while company wireless users are allowed access to the intranet.

5. Conclusion

Hillstone Secure Connect offers the next generation SSL VPN solution. It uses SSL for VPN deployment while at the same time utilizes IPSec for data transport to avoid the performance bottleneck of SSL VPN. Hillstone’s role base access control provides for fine grained control on internal resources.

Hillstone devices combine state of the art multi-core processors, hardware crypto acceleration, high speed switching fabric that can deliver high performance, high scalable SSL VPN solution.