Free report on remote access design plan

Business, Company

Why Fantasy Games network should adopt VPN

VPN has a high potential to provide quality communication services. It also provides savings for company costs. The savings range from 30% to 80% depending on the type of line that was leased. Since Fantasy Games network has offices in many places, it can save vast amount of expenses that would be used on communication by the introduction of a VPN.

VPN also offer good security for the sensitive information that is being shared and stored in Fantasy Games network. This information need to be stored in a safe and only shared in a private. The security of applications and the systems that are running in Fantasy Games network is a matter of great concern. As more operations and business processes are done from the Internet, there is a lot of concern on their security. This has resulted in companies researching on the ways and solutions of overcoming this.

With the increase in mobile devices and persons working remotely over few past decades, the security threats they pose too have risen exponentially. With increase in Brand and blended security threats that apply various vectors of intrusion, these remote working persons and devices are highly at risk. They pose an evolving security threat to the enterprise Network when guru hackers take advantage of the vulnerabilities on these devices as conduits to the enterprise network when these persons come online again. Previous years have seen many new technologies come into the market to counter these security concerns. But with growth in complexity, magnitudes and number of these threats, these solutions seize to function fully to address all the security concerns. Today, gurus in the field conger that the

best alternative for remote access devices security and the networks they make connections to through a VPN or within the scope firewall, is a combined, multi-level approach. These approach offers Authorization that makes sure that only trusted hosts and devices can gain network access. If a device has not logged in via the VPN gateway, it is restricted access or denied. If a device gives authorization details such as username and password, the VPN gateway includes the device to its allowed devices list. It also offers Encryption which counters interception of data traffic by scrambling information. After authorization, a device can incorporate encryption to lock out digital packet sniffing by any middle points on the Internet, factoring in unauthorized hosts.

Remote operation is a key component for all enterprises sizes in today’s dynamic market place. Nevertheless with the great anticipations that come with it there are also many shortcomings that needs to be addressed like reliability and security. Virtual private networks seems to address most of this shortcomings developed with the intention of serving mobile work force, the Virtual private network client offers the critical capability for remote users to kick-start VPN communication with enterprise resources. Road warriors and moving devices require gaining access to mission vital networks via the net often; they make use of unsecured public networks or rather un-trusted local area networks. VPN connections have ability to connect end-home users that require a secure host to carry vital data to required destinations. Mobile L2TP/IPsec VPN Client incorporates the IPsec tunnel mode of ESP to create a safe information exchange environment to a network that is GTA firewall secured. It offers VPN ability to multi-plat formed

remote devices allowing secure peer-to-peer or peer-to-gateway communication via TCP/IP based networks. L2TP/IPsec can be applied with gateway IPsec and firewalls or even other host operating any VPN compatible software. Secure encrypted information exchange can be started in any VPN scenario, such as WLAN, DSL, Dial-up or even NAT.

The remote access design strategy factor in several vital areas first is a software controls policy which will define purely security software controls that are incorporated on remote access based devices. Second is endpoint security management which includes choice of a vendor that provides a detailed endpoint security management with policy enforcement as part of the VPN based remote access approach. This simply is enabling a get true protocol conformity and assurance of endpoint posture security. Third is enforcing corporate policy conformity to familiarize end users that enterprise security policy also covers their remote devices when online on the enterprise network. End point user conformity reporting is critical. Many above approaches give reporting abilities to allow administrators keep track on the connecting end points status. Finally is a periodical policy and reports review, carrying out periodical audits and reviews to identify patterns and behaviors in access infringements. This is mainly for purposes of making sure that the protocols are truly addressing our remote access security demands.

.

References

Bollapragada, V., Khalid, M., & Wainner, S. (2005). IPsec VPN design. New York: Cisco Press.

Feilner, M. (2006). Open VPN: Building and operating virtual private networks. New Delhi: PacktPublishing Ltd.