* Personal Point-to-Point (PPTP) Virtual Private Network
  + J. Jones, H. Wimmer and R. J. Haddad, "PPTP VPN: An Analysis of the Effects of a DDoS Attack," 2019 SoutheastCon, 2019, pp. 1-6, doi: 10.1109/SoutheastCon42311.2019.9020514.
    - While the client is under attack, it is found that the VPN would not establish a connection. Additionally, if the client is already connected to the VPN and is attacked, the VPN disconnects the client. This is accompanied by near-complete network instability and packet loss which correlates to the notorious insecurity of PPTP.
    - it was conclusively determined that the hping3 DDOS was a critical attack causing nearly full disruption. This is telling of the PPTP VPN’s redundancy and protection against DOS attacks. PPTP VPNs are used still today in small operations and for personal use so that this vulnerability could create unwanted disruption for systems still utilizing this type of VPN or legacy systems.
    - it is shown that a client connected to a PPTP VPN can be disrupted or outright denied connection through a Distributed Denial-of-Service (DDOS) attack
    - Due to their promised security and privacy, VPN software is widely used for business solutions. PPTP VPNs, specifically, are still used in legacy systems that have not been changed because of the lack of need to change a system that still works. This can create problems for companies and cost them profits or even customer trust
    - VPN software should include DOS protection from all directions. Most commercial routers included features that limit the number of network packets that pass through without replies; this technology could also be implemented into VPNs to detect when an abnormal amount of network traffic is being transmitted.
  + S. Narayan, S. S. Kolahi, K. Brooking and S. de Vere, "Performance Evaluation of Virtual Private Network Protocols in Windows 2003 Environment," 2008 International Conference on Advanced Computer Theory and Engineering, 2008, pp. 69-73, doi: 10.1109/ICACTE.2008.187.
    - With prolific development of the Internet, businesses nowadays implement VPN tunnels using different protocols that guarantee data authenticity and security between multiple sites connected using public telecommunication infrastructure.
    - The results indicate that throughput of VPN tunnel and CPU utilization of VPN servers are dependent on the choice of tunneling protocol, algorithm, and window size used in data transmission. We conclude that:
    - VPN tunnel implemented in Windows 2003 environment has the best network performance when PPTP is used as the tunneling protocol (average value =90 Mbps). The values obtained indicate that throughput for PPTP is very close to that of a network without VPN. IPSec is the second best performer while SSL depicts the lowest values (average value =40 Mbps).
    - Choice of a particular tunneling protocol algorithm can affect network performance significantly. In case of SSL, throughput values vary by almost 30% depending on the choice of algorithm.
    - CPU utilization of the VPN server is dependant on the tunneling protocol and the algorithm. While IPSec used the least resource and SSL the most, it is evident the various SSL algorithms consumed CPU resources differently.
  + J. B. R. Lawas, A. C. Vivero and A. Sharma, "Network performance evaluation of VPN protocols (SSTP and IKEv2)," 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN), 2016, pp. 1-5, doi: 10.1109/WOCN.2016.7759880.
    - This research focuses on the performance evaluation of VPN protocols, mainly the Secure Socket Tunneling Protocol (SSTP) and Internet Key Exchange Version 2 (IKEv2). Throughput, jitter, and delay were measured when the packets were sent from the VPN clients to other client in a test-bed environment. After the test-bed environment research, it was found that IKEv2 had significantly better performance than SSTP in relation to throughput, jitter, and delay.
    - The TCP throughput of IKEv2 is slightly higher than SSTP while in UDP, while IKEv2 is slightly less than SSTP, with a less than 1% difference. SSTP TCP throughput ranges from 9Mbps to 89Mbps, while IKEv2 ranges from 10Mbps to 90Mbps. The UDP throughput of SSTP ranges from 5Mbps to 90Mbps while IKEv2 ranges from 6Mbps to 89Mbps.
    - SSTP TCP jitter was 1% higher than IKEv2, while in UDP it was 4% lower than IKEv2.
    - IKEv2 has consistently less delay in TCP and UDP with a 2% difference to SSTP.
    - It was evident that IKEv2 was significantly better than SSTP in relation to throughput, jitter, and delay.
  + S. Narayan, K. Brooking and S. de Vere, "Network Performance Analysis of VPN Protocols: An Empirical Comparison on Different Operating Systems," 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, pp. 645-648, doi: 10.1109/NSWCTC.2009.367.
    - Metrics: throughput, CPU usage and VPN initiation time
    - In Windows environment, there is a clear distinction between VPN network throughput of PPTP, SSL and IPSec protocols, however in Linux that is not the case. SSL when implemented with various algorithms gives the lowest throughput in Windows environment; however IPSec is the least performer in Linux.
    - Linux throughput values range between 65 and 95Mbps while Windows values range from 15 to 95Mbps.
    - Linux operating system uses the highest CPU of the VPN end nodes when compared to Windows Vista and Server 2003.
    - Linux VPN initiation time is significantly higher than the Windows operating systems.
  + Z. Wu and M. Xiao, "Performance Evaluation of VPN with Different Network Topologies," 2019 IEEE 2nd International Conference on Electronics Technology (ICET), 2019, pp. 51-55, doi: 10.1109/ELTECH.2019.8839611.
    - At the same time, the performance of the VPN constructed with Softether protocol is superior to that of the L2TP protocol. Compared with the experimental environment carried out under the local area network [1] [2], our experiment is based on the test results of the VPN network actually deployed and operated in the campus network of Beijing Normal University. The network environment is more complicated than the LAN experimental environment. And more suitable for the actual Internet environment. The experimental results show that the performance of Softether and SSTP/L2TP are basically the same in terms of throughput, which means that in actual use, Softether performance is not lost to SSTP and L2TP.
  + A. A. Jaha, F. B. Shatwan and M. Ashibani, "Performance Evaluation for Remote Access VPNs on Windows Server 2003," 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies, 2008, pp. 582-587, doi: 10.1109/NGMAST.2008.17.
    - This paper has presented an experimental performance evaluation for the wired and the wireless remote access VPNs, namely PPTP, L2TP/IPSec, and Open VPN on windows server 2003 VPN server. From the results that were collected from the testbeds and the user applications requirements, the following conclusion remarks are gained:
    - This work examines and empirically evaluates the remote access VPNs, namely point to point tunneling protocol (PPTP), layer 2 tunneling protocol over Internet protocol security (L2TP/IPSec), and secure socket layer (SSL). We explore the impact of these VPNs on end-to-end user application performance using metrics such as throughput, RTT, jitter, and packet loss. All experiments were conducted using wired and wireless windows XP SP/2 host (VPN client) connected to a windows server 2003 host (VPN server)
    - Due to the smallest overhead packets that have been add by PPTP [12], PPTP has produced the best performance values for both TCP-and UDP-based user applications.
    - In order to have strong security, L2TP/IPSec combines L2TP's tunnel with IPSec's secure channel which increases the overhead packets [12]. So, L2TP/IPSec has produced a good performance values for both TCP-and UDP-based user applications.
    - Because Open VPN was written as a user space daemon rather than a kernel module [13], the Open VPN has produced a low performance values in high traffic environments for both TCP-and UDP-based user applications.
    - The wireless testbed performance values indicate clearly that the deployment of VPNs on a wireless network infrastructure could be considered as an acceptable choice to secure transmission between wireless clients and their wired enterprise network.
* Z. Xu and J. Ni, "Research on network security of VPN technology," 2020 International Conference on Information Science and Education (ICISE-IE), 2020, pp. 539-542, doi: 10.1109/ICISE51755.2020.00121.
  + IPSec VPN, as can be seen from the literal, is a VPN that realizes remote access through the IPSec protocol. It provides a tunnel over a public network for two private networks to transmit data. This tunnel is encrypted to ensure security. The advantage of IPSec.VPN is that it is a net-to-network networking method, which can establish multilevel networking. Fixed networking mode, suitable for inter-institutional networking; Users can have transparent access and do not need to log in. (Pros)
  + IPSec processing modules are independent of the Linux kernel, so there is almost no impact on the kernel, which is its biggest advantage of this framework. However, the introduction of the virtual interface mechanism makes it likely to process one same packet multiple times, which leads to a waste of time and resources, reduces the throughput of the system, increases the response delays and even may lead to loss of data packets. (Cons)
* L. Shif, F. Wang and C. Lung, "Improvement of security and scalability for IoT network using SD-VPN," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1-5, doi: 10.1109/NOMS.2018.8406192.
  + To improve the security and scalability for IoT networks, we propose a Software-Defined Virtual Private Network (SD-VPN) solution, in which each IoT application is allocated with its own overlay VPN. The VPN tunnels used in this paper are VxLAN based tunnels and we propose to use the SDN controller to push the flow table of each VPN to the related OpenvSwitch via the OpenFlow protocol. The SD-VPN solution can improve the security of an IoT network by separating the VPN traffic and utilizing service chaining. Meanwhile, it also improves the scalability by its overlay VPN nature and the VxLAN technology.
  + Currently, the majority of VPN services are provisioned manually. Consequently, it may take a few days to build the VPN services, as a variety of configurations need to be changed. The manual process delays new service implementation and increases operational cost and complexity. As we all know, SDN provides network simplification and automation, it is effective to provision the VPN services via SDN and this is so-called SD-VPN. In other words, instead of creating VPN services manually in advance, SD-VPN creates VPN services automatically when a VPN client joins.
  + The proposed SD-VPN combines SDN and VPN, i.e., it uses characteristics of both SDN and VPN to improve network security in two ways: (i) Traffic separation provided by VPN; and (ii) Network service chaining based on SDN.
  + (1) automated service provisioning reduces the complexity and cost of operation; (2) virtual separation of services with a centralized and in-depth security policy and service chaining can improve the security; and (3) VxLAN and the overlay model are more scalability. All the above benefits are suitable for IoT networks
* K. Ishimura, T. Tamura, S. Mizuno, H. Sato and T. Motono, "Dynamic IP-VPN architecture with secure IPsec tunnels," 8th Asia-Pacific Symposium on Information and Telecommunication Technologies, 2010, pp. 1-5.
  + An IP virtual private network using IPsec (IPsecVPN) has begun to be used as a forwarding base for cloud services. Cloud computing architecture is evolving into an inter-cloud structure that enables many cloud services to connect to each other freely. IPsecVPN applied to cloud services will increase in complexity along with the evolving cloud architecture. In this paper, we discuss the requirements for applying IPsecVPN to cloud services and propose dynamic IP-VPN architecture with secure IPsec tunnels that meets these requirements.
  + In this paper, we described the requirements for IPsecVPN, a technology for composing CUGs on open networks, to be applied to cloud services. We then clarified the problems of the two current IPsecVPN architectures in relationtion to these requirements. To solve these problems, we proposed a MOBIKE extension for establishing dynamic IPsec and a TS extension for detailed packet filtering only with an IPsec tunnel. With these proposals, it is possible for cloud services using IPsecVPN to change into a hybrid-cloud computing architecture or smoothly evolve into an inter-cloud architecture.
  + In our proposed method, both IKE SA and IPsec SA are passed by using MOBIKE. However, to achieve a more efficient IPsec-VPN architecture, in the future we will investigate a method in which only IPsec SA is passed.