Technical Whitepaper

Technical Considerations of Telecommuting

We Do IT RIGHT!

Executive Summary:

Corporate devices that are connected back to the corporate network via Virtual Private Networks (VPN) leave critical vulnerabilities unaddressed, unattended, and potentially with access to your network through compromised End User Devices. In 2017 alone, Diverse Concepts, Inc. (DCi) has worked several incidents for our customers where corporate end user devices were infected by command and control malware on a home network and replicated into a corporate network through an inadequately protected VPN connection.

DCi advocates for secure telework through deployed hardware, network segregation, and defense-in-depth approaches all of which can be accomplished using Aruba® Remote Access Points (RAPs) in conjunction with a campus-wide Secure Wireless Network.

Point of Contact:

Roy E. White
Roy.White@dciits.com
443.698.1053

DCi Proprietary Information

A LITTLE ABOUT US

Headquartered in Millersville, MD, Diverse Concepts is a rapidly expanding small business. Diverse Concepts Inc. (DCi), formed in June 2002, is a professional IT consultancy firm specializing in the area of systems/network engineering, end-to-end support and computer forensics. DCi is a reliable and reputable partner that understands the Federal contracting environment as well as the Commercial contracting environment and can bring an immediate competitive advantage as well as relevant expertise to your firm at a competitive price.

DCi Diverse Concepts, Inc.
IT SERVICES

MARYLAND MBE MINORITY BUSINESS ENTERPRISE

Table of Contents

About Telecommuting

Introduction

Today, the average commercial employee is not only encouraged but is expected to work from home for a portion of their work week. For some employers, work from home is more tangential but for most employers, it has become critical to allow and encourage telecommuting. According to GlobalWorkplaceAnalytics.com, "50% of the US workforce holds a job that is compatible with at least partial telework" (Latest Telecommuting Statistics). The report goes on to state that "80% to 90% of the US workforce says they would like to telework at least part time" (Latest Telecommuting Statistics).

While there are employee satisfaction and morale implications to implementing a telecommute program, the undeniable truth is that cost savings remain a driving force regardless of whether the consideration is being made by private industry or by a government agency. Teleworkers require fewer traditional office resources than on-site workers resulting in savings on required office space, power, space, cooling, office amenities, and other utilities since those costs are shifted from the employer to the employee. The employee, in return, sees new benefits such as reduced commuting costs (sometimes 20-40% or more).

Telecommuting, because of its very nature, brings with it a distinct set of benefits and drawbacks. This whitepaper will focus strictly on the technology side of those tradeoffs.

About Telecommuting

Benefits

Telecommuting has been embraced in organizations across a wide range of industries. Both employees and employers have favored telecommuting because of its benefits over the traditional office space environment. With a well-designed telecommuting solution, employees and employers both stand to gain. Benefits include:

- **Improved Employee Productivity**
  Employees who telecommute (and their supervisors) have reported that they are more effective at home than when they work out of the office.
- **Schedule Flexibility**
  Telecommuters are more productive when they can schedule their actual work time during their most effective periods and around the other demands in their lives.
- **Reduced Absenteeism**
  Telecommuters can work in bad weather, when children are home from school for illness/closings, and in other instances where regular employees might instead take a personal or sick day.
- **Increased Time Available for Work**
  Telecommuters have increased time to work by eliminating the stress and time it takes to commute to and from the office.

- **Improved Employee Retention and Attraction**
  Employees who have experienced the benefits of telecommuting programs tend to prefer these work arrangements and seek out similar opportunities.
- **Office Space Savings and Overhead Reductions**
  Organizations with a large number of telecommuters have actually reduced their office space requirements, and, consequently, their rents, by insisting that telecommuting employees share desks and other resources at their company facilities.
- **Eliminating Office Distractions**
  An employee's work day in an office environment can include unscheduled meetings, the noise and commotion of people moving around the office, and the interruptions from visitors in their work area. Telecommuting eliminates many office distractions and allows the employees to be more productive.

The benefits of telecommuting extend to both employers and employees. As organizations embrace a telecommute solution, life improves for everyone.

Drawbacks

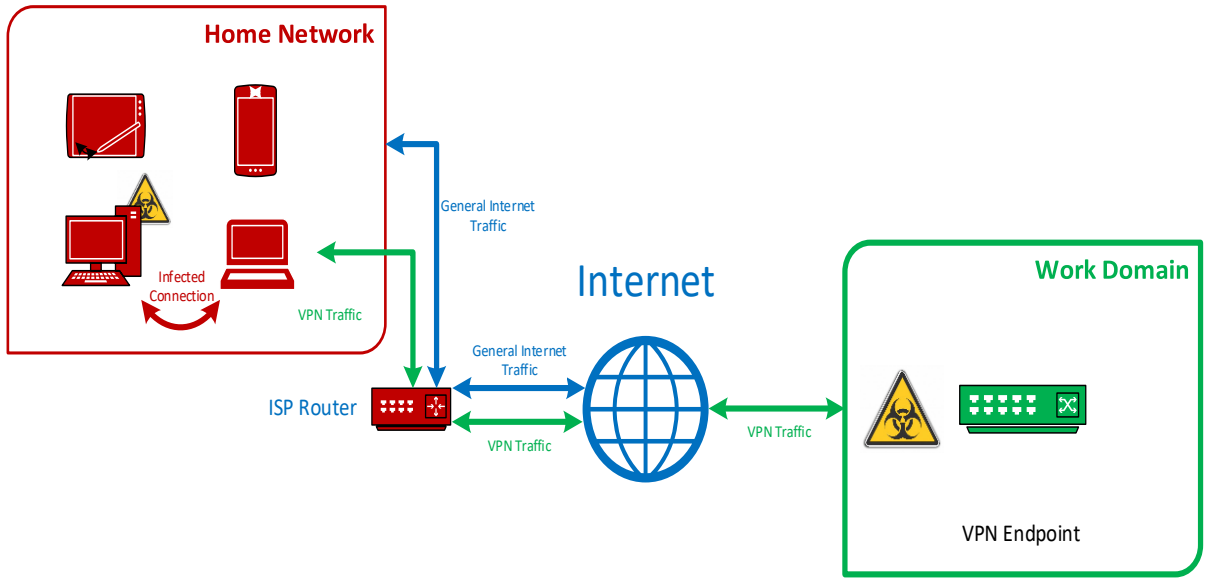
One of the largest challenges that organizations face with regards to telecommuting is ensuring that corporate network security posture is not reduced, compromised, or vulnerable to the increased presence of devices outside of the corporate network. This environment is much tougher for Chief Information Officers (CIOs)/Chief Technical Officers (CTOs) because of the large number of variables that are beyond their ability to control or even influence.

An example of environmental factors beyond the control of a typical company are things such as WiFi Hotspots at places like the local coffee shop, home networks in an employee's house, or wireless guest networks at client locations. Despite the best efforts of a CIO and his/her team, every time a device connects to an unknown network there are risks and threats that exist potentially exploiting any number of vulnerabilities. For this reason, the telecommuting employee presents some of the most challenging problems for corporate management when there is a focus on security.

Other technical/non-technical considerations are data-loss prevention, employee dishonesty, and the inability to directly supervise an employee. While no single solution exists such that personal, professional, technical, and policy solutions can be deployed at the click of a button, a well-planned and executed telecommute solution should be able to address most, if not all, of these concerns.

VPN

Virtual Private Networking (VPN) is a fantastic technology that provides users that are physically outside of a corporate network the ability remotely access resources as if he/she was in the office. Virtual Private Networking, depending on its implementation, can range from non-secure to moderately secure, in an overall sense. While DCi takes no issue with regards to security of the actual VPN tunnels, the issues begin with the End User Devices such as take-home laptops, tablets, and phones.



The traditional Virtual Private Network Connection (VPN) can be exploited such that a trusted VPN workstation is on a home network with countless other devices that may lack virus protection, security updates, and could be under control by nefarious cyber actors.

Figure 1. Traditional VPN Architecture

When an End User Device is within the confines of the corporate firewall, there is a relatively high level of confidence that the device is safe from external threats since the corporate networks generally have a layered security approach with multiple firewalls, intrusion detection systems, mail receivers in a Demilitarized Zone (DMZ) to facilitate virus scanning/spam filtering before they are permitted into the network, and a cadre of other services. However, when a laptop connects at the free WiFi hotspot, the device's only layers of protection are locally installed virus scanners and/or software firewalls built into or installed on the device. While a software firewall is better than no firewall at all, there is a reason that corporate networks are not protected by them.

PPTP VPN

Point-to-Point Tunneling Protocol (PPTP) is a VPN technology that allows for encryption but was truly designed to allow a user to access only a handful of interfaces. By its design and, as implied by its name, it was intended to provide connectivity from one point to another such as we web-interface, intranet website, a Terminal Services Gateway, or a Citrix® Storefront for Virtual Desktop Infrastructure (VDI). This technology, while it allows for encryption of the datagrams inside of it, leaves a certain amount of data in the clear regardless of what level of encryption is configured.

PPTP uses Generic Routing Encapsulation (GRE) tunnels forward data from one end of the VPN to the other. Within the GRE tunnel, Point-to-Point Protocol (PPP) handles the IP datagram that is destined for a host on the distant end. PPP is where the encryption can occur.

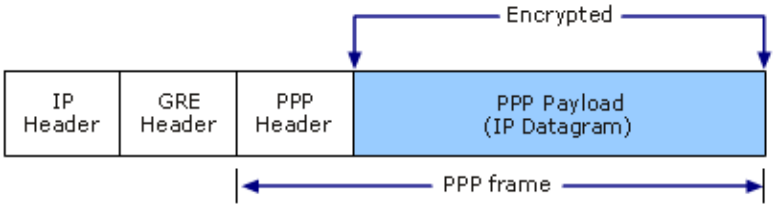


Figure 2. Structure of a PPTP Packet Containing an IP Datagram (VPN Tunneling Protocols)

L2TP VPN

Layer 2 Transport Protocol (L2TP) was designed to allow for Layer 2, switched, network traffic to pass within its tunnels. By virtue of its very design a L2TP VPN connection is, in much the same way, a connection to any other Layer 2 switch within the confines of a corporate network. This is not to say that the corporate network is, or should be, configured to treat these clients identically to those inside the corporate network but they could be. The vast majority of all VPNs place VPN endpoints within subnets that are scrutinized a little more, limit access to certain resources, and/or implement Network Access Protection, which will be discussed a little later.

L2TP does not in and of itself provide for any encryption of traffic within its tunnel but, like PPTP, relies on an underlying network protocol suite to provide data protection. L2TP implements Internet Protocol Security (IPSec) which can be configured with a variety of authentication, key exchange, and encryption algorithms.

Within an L2TP datagram protected by IPSec, the only two portions of the datagram which are visible to an outsider, are the IP header and the IPSec Encapsulating Security Payload (ESP) Header, neither of which is very revealing about the endpoints other than their Internet Protocol (IP) address and which encryption algorithms are being used. Unlike PPTP, the PPP Header and the L2TP headers are completely protected.

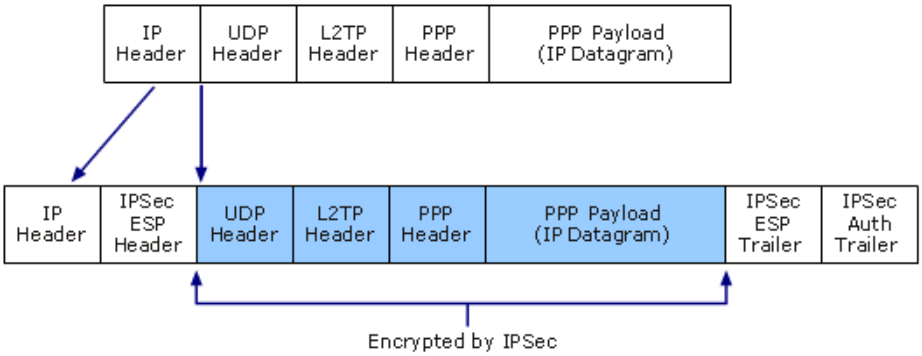


Figure 3. Encryption of L2TP Traffic with IPsec ESP (VPN Tunneling Protocols)

SSL or SSTP VPN

Secure Socket Layer (SSL) VPN or Secure Socket Tunneling Protocol (SSTP), is the newest of the three major VPN types and utilizes the SSL suite of the Hyper Text Transfer Protocol Secure (HTTPS) suite to protect datagrams similar to how website transactions can be protected by HTTPS. By design, SSTP allows the traversal of datagrams through a firewall and/or proxy server using TCP port 443, which is identical to that of HTTPS web traffic.

Like L2TP and PPTP, SSTP implements PPP which makes the same authentication methods available. The use of SSTP VPNs, while becoming more popular, is not as pervasive as L2TP or PPTP.

According to Microsoft®, "All three tunnel types carry PPP frames on top of the network protocol stack. Therefore, the common features of PPP, such as authentication schemes, Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) negotiation, and Network Access Protection (NAP), remain the same for the three tunnel types" (VPN Tunneling Protocols).

NAP

As stated in the Microsoft® Developer Network, NAP is a set of operating system components that provide a platform for protected access to private networks. The NAP platform provides an integrated way of evaluating the system health state of a network client that is attempting to connect to or communicate on a network and restricting the access of the network client until health policy requirements have been met" (Network Access Protection).

While, in concept, this seems like a beneficial technology that is absolutely necessary to protect the corporate network and enforce system health checking before allowing devices into a network through connections such as VPNs, unfortunately, Microsoft® has removed support for NAP from all operating systems beginning with Server 2016 and Windows 10. A typical health check might be to verify that antivirus software is installed and its virus definitions are current or that a system scan was performed recently.

Now that industry no longer has NAP available for endpoint security/health enforcement, there is now a requirement to use Microsoft® System Center Configuration Manager (SCCM) or other third party tools to perform these functions.

Remote Desktop / Virtual Desktop Infrastructure

Many organizations make Virtual Desktops available through either Microsoft® Terminal Services Application Servers or through third party software such as Citrix®. While this type of deployment provides a lot of benefits, it also brings its own challenges, administration, and overhead. Virtual Desktops are among the most secure methods of remote access, if properly implemented, because they keep data transfer within the datacenter, the virtual machines are generally very locked down and are static state systems where the user's image is destroyed at logoff and the machine reverts to a fresh state as if the user had never logged in.

The biggest problem with Remote Desktop / Virtual Desktop Infrastructure comes down to protecting the interface in such a way as to not allow outsiders the ability to try to exploit user accounts to either brute force or deny service to authorized users. For that reason, most Remote Desktop / Virtual Desktop Infrastructure solutions that are used by the teleworker, still require that underlying VPN or other secure data transport to be established prior to use.

Aruba® Remote Access Points (RAPs)

Aruba® Remote Access Points (RAPs) are hardware devices that a teleworking employee takes home with them, connects them to their home network, and the setup is complete. The RAP is configured by a network administrator or by using a service such as Aruba® Activate to push initial connection profiles so that the RAPs know how to connect back to the Aruba® infrastructure that is installed at the corporate office. Aruba® RAPs can be configured to authenticate with an Aruba® Wireless LAN Controller (WLC) by using username/password, factory certified certificates, or even corporate certificates from an internal corporate Certificate Authority (CA).

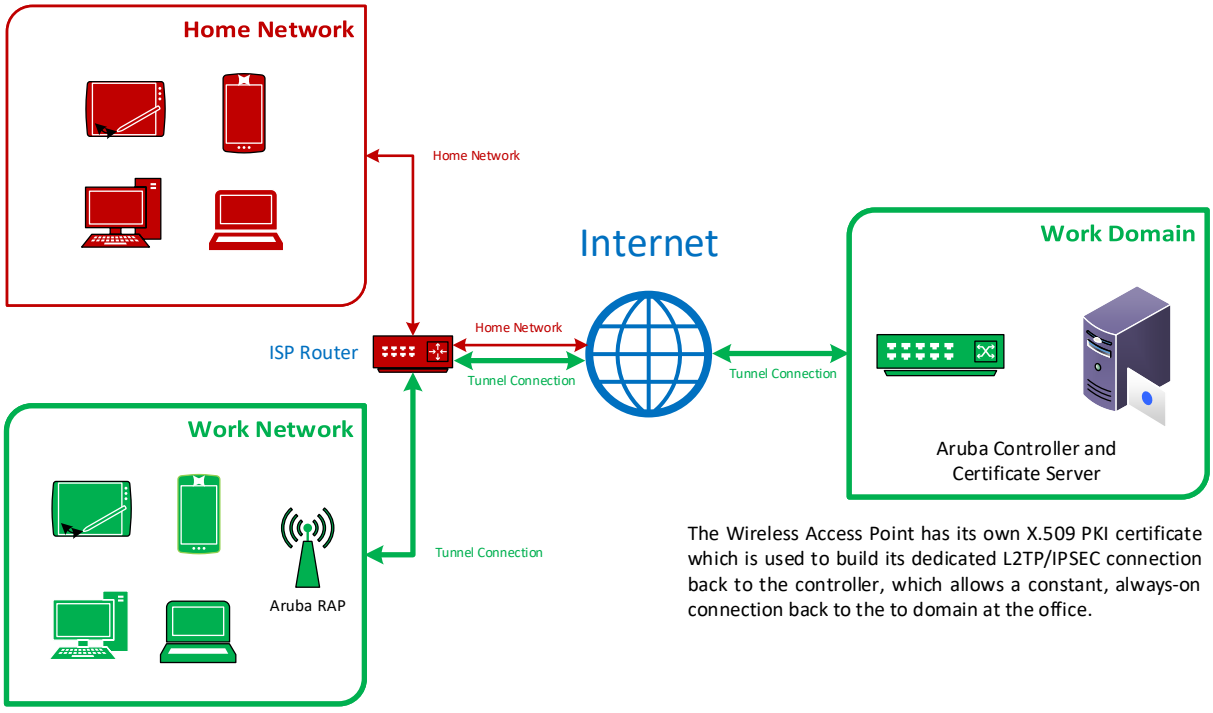


Figure 4. Remote Connectivity via Aruba Remote Access Point (RAP)

When the Aruba® RAP starts up, it builds an L2TP/IPSec Tunnel back to the WLC and sets up a GRE tunnel for user traffic within the outer L2TP/IPSec tunnel. Once the tunnels are complete, the Aruba® RAP pulls its configuration profile from the WLC, configures its radios, and broadcasts applicable Service Set Identifiers (SSIDs). Security actually goes further in that the user's session can be encrypted using WiFi Protected Access 2 (WPA2)-Enterprise via Extensible Authentication Protocol-Transport Level Security (EAP-TLS) from client to WLC in essence providing two layers of encryption for user data traversing between the RAP and the WLC in the corporate office.

From a user experience perspective, the RAP is a plug-and-play device that provides corporate WiFi within the user's house. In many cases, corporate devices are already configured to connect to the corporate WiFi while at work so when the device goes home with the employee, it already knows the network and simply reconnects itself to the corporate network.

What does this mean for the user? As soon as the employee turns on his/her corporate laptop, the device connects itself to the network. He/she logs into the laptop using domain credentials just as if he/she was at the office. The user experience is seamless and identical to that of the user sitting at his/her desk within the corporate office. There are no special buttons to press, no RSA tokens to use, or separate credentials to remember.

What does this mean for the CIO? Well, it means several things:

1. There is no need for the employee at home to connect their work laptop to their home network thereby eliminating those threat vectors
2. The laptop, as soon as it is turned on and sees the secure corporate WiFi connects and is online and can be administered as if it were sitting on the employee's desk back at the office
3. Web traffic from a corporate laptop is FORCED to follow corporate policy regarding whether traffic is tunneled back to the corporate network for inspection/enforcement or if it can be Split-Tunneled out from the RAP to facilitate faster internet access speeds/reduce burdens on corporate WAN connections.
    a. Many VPN clients claim the ability to enforce network traffic flow back to corporate networks but are susceptible to malware on the device that can prevent traffic from flowing correctly. The Aruba® RAP is a hardened hardware device that sits between the user's computer and their home network and it enforces the policies pushed down by the network administrator
    b. Some companies issue converged Session Initiation Protocol (SIP) phones for employees to place on a desk in their home office to provide identical calling experience to when he/she is in the corporate office. The network administrator may want, or need, to authorize SIP traffic to be split-tunneled out of the RAP to go straight out to the internet to eliminate call quality issues that may arise from requiring that SIP session to be tunneled back to corporate and then out to the internet. This enforcement can be done on a per-port, per service, or even per source/destination basis. In other words, the Network Administrator can trust the corporate VoIP provider to allow traffic to be split-tunneled out but require all other SIP traffic to come back to the corporate network for inspection.
4. WPA2-Enterprise session maintains encryption all the way back to the WLC within the corporate datacenter which eliminates eavesdropping/man-in-the-middle concerns when EAP-TLS is configured for bidirectional certificate-based authentication. By protecting the session from end-to-end, the network administrator maintains superior control over data that is authorized to enter the datacenter because the Aruba® WLC has 100% control over data introduction to the network as it performs the decryption. This applies to all traffic regardless of whether originating from a RAP or from a wireless connection to a campus Access Point (AP).

Technical Comparison

	PPTP	L2TP/IPSec	SSTP	Aruba RAP
Offers Secure Remote Access	✓	✓	✓	✓
Offers Strong Encryption	✓	✓	✓	✓
Offers Identical User Experience (Office vs. Home)	✗	✗	✗	✓
No Special Software to Install	✗	✗	✗	✓
Hardware Firewall Enforcement for Teleworking Employee	✗	✗	✗	✓
Compatible with Remote Desktop / VDI	✓	✓	✓	✓
Licensing	**Per User**	**Per User**	**Per User**	**Per AP**
Allows a computer to be 802.1X authenticated to the network prior to logon for remote management, patching, and administration	✗	✗	✗	✓
Always on Connectivity	✗	✗	✗	✓
Zero-Touch User Configuration	✗	✗	✗	✓
Supports additional devices other than a single Personal Computer (PC) (e.g. Voice Over IP (VoIP) Phones, Network Printers, etc.)	✗	✗	✗	✓

Conclusion

By implementing our secure Aruba® telecommute solution, businesses can attract the modern day employee who is looking to juggle their home and office life through convenience and flexibility. Further, the state of our current global cyber climate requires a secure telecommute solution for employees working at home. When looking at the number of risks, vulnerabilities, and threats that pervade every aspect of technical integration, it is time that companies remove their assets from uncontrolled home networks of their employees. A VPN, alone, can no longer be the standard solution for the telecommuting employee because the threat vectors outside of the VPN are the areas of greatest concern.

DCi's solution fully mitigates the threat vectors from the home network by completely removing the devices from the home network and directly connecting those devices back into the corporate network where they belong.

References

Congressional Budget Office. (2010). *Cost Estimate: H.R. 1722 Telework Improvements Act of 2010.*

GlobalWorkplaceAnalytics.com. (n.d.). *Latest Telecommuting Statistics*. Retrieved October 2, 2017, from GlobalWorkplaceAnalytics.com: http://globalworkplaceanalytics.com/telecommuting-statistics

Microsoft. (n.d.). *Network Access Protection*. Retrieved October 9, 2017, from Microsoft Developer Network: https://msdn.microsoft.com/en-us/library/windows/desktop/aa369712(v=vs.85).aspx

Microsoft. (n.d.). *VPN Tunneling Protocols*. Retrieved October 9, 2017, from Microsoft Technet: https://technet.microsoft.com/en-us/library/cc771298(v=ws.10).aspx