aep™ NETWORKS

The **specialist** in network and application access security

WHITE PAPER

Choosing an Effective Teleworker Access Solution

AEP application layer SSL VPN provides secure remote access for teleworkers

Organizations are pursuing teleworker programs that will enable them to increase their operational efficiency, preserve human capital, comply with government regulations, and be prepared in times of emergency. In order to effectively gain the benefits of these programs, organizations realize they must implement secure remote access for their teleworkers. This white paper reviews the essential points[1] *to consider when evaluating SSL VPN (secure socket layer virtual private network) solutions for teleworker access.*

[1] Based upon research published by Frost & Sullivan, in partnership with AEP Networks. The evaluation criteria originally appeared in the white paper entitled “Secure Remote Access: The 10 Most Important Considerations for Choosing an Effective SSL VPN Solution,” by Jason Wright, Frost & Sullivan.

Access Control Management

Precise access control is critical to limit the risk of inappropriate access to sensitive information

With a teleworker solution in place that enables secure remote access to information, organizations can extend their hours of service, increase team expertise on projects, and in general promote virtual collaboration among staff. However, teleworker access that is too broad can raise the risk of inappropriate access to sensitive information assets and can put privacy and confidentiality requirements in jeopardy.

Teleworker access control management therefore must be able to balance the requirement to protect with the need to share specific information in order to get the job done. When compared to other remote access alternatives that give carte blanche access to all network resources upon the establishment of a session, there are significant advantages to AEP Networks' granular policy control that limits the individual applications that specific users may access.

The establishment of a granular access policy for network resources provides an equally beneficial advantage in granular audit capabilities. Audit logs that clearly illustrate what applications were accessed and what information was exchanged during an individual session provide an infinitely more powerful and detailed view of the activities occurring during a session. Granular auditing capabilities are becoming increasingly important to meeting regulatory requirements.

Flexible group management capabilities simplify administration and strengthen controls

Access control management becomes increasingly important as various types of teleworkers are granted access to network resources. Whereas remote access has historically been provided only to select users, access can now appropriately be provided to all employees as well as contractors, partners, suppliers and customers when administrators can control and review what these users are doing during sessions. In government deployments, various access policies based on agency affiliation or clearance levels can be assigned. The ability to assign users to various groups simplifies management, but perhaps more importantly is the ease with which groups and roles can be added, removed or changed with the AEP solution.

Data Encryption

Consider SSL VPN solutions that use the 256-bit government approved AES standard for increased protection

Perhaps the most obvious criteria for a teleworker access solution is the need to maintain the privacy of traffic as it is communicated between two points. While 128-bit encryption may be suitable for some use cases, those requiring stronger protection will need solutions like AEP's with NIST[2] approved 256-bit AES encryption.

Those needing stronger protection and wanting to minimize risk should consider solutions such as AEP's that constantly change session keys. Utilizing dynamic session keys, a technique that changes the values used to encrypt the data between two points frequently, ensures that even in the unlikely event that a session key is compromised only a small fraction of the data that is being transmitted will be decipherable.

Authentication and Identity Management

Using a strong authentication system is critical when accessing sensitive information

Those evaluating teleworker access solutions should be particularly concerned with the strong authentication options that a solution provides. There can be inherent security risks with some teleworking solutions that do not have the strong authentication that is integrated into the AEP solution. With some solutions for example, gaining access to information resources can be as simple as entering a URL address and password from a browser. While this simplicity is an advantage for users, those with malicious intent can also leverage it. Providing a window of access by merely entering a Web address almost invites hackers to attempt to guess passwords to gain access.

[2] U.S. National Institute of Standards and Technology

When access is provided to less sensitive applications, a two-factor authentication rollout may not be required, but if more sensitive information is made available to remote users, a strong authentication system becomes critical.

The AEP Networks strong authentication options have the advantage of focusing on authenticating users as opposed to devices, a definite advantage for teleworker environments. One very effective two-factor authentication system approach included in the AEP solution involves the use of software tokens. These tokens are essentially a digital certificate that is stored on a user's computer. During the authentication process, the user enters their authorization code, and the client or gateway automatically checks for the presence of a software token. If found, the token is verified along with the authorization code to provide a second factor of authentication. Other strong authentication options which AEP supports include the popular one-time password generating tokens from vendors such as RSA and Secure Computing, as well as USB authentication keys from vendors such as Aladdin and Rainbow Technologies. Additional authentication mechanisms such as smart cards and biometrics are less popular but are effective authentication options as well.

As the volume of users, applications and data increase in a teleworker deployment, a scalable identity management system becomes increasingly important. AEP Networks offers an integrated two-factor authentication system that provides better-than-password-only security and eliminates the need for resource intensive integration activities. In addition, AEP self-registration capabilities can simplify administration and expedite the deployment process.

Interoperability

Understand how the teleworker solution will interact with your existing network architecture and applications

An important consideration in the deployment of a remote access teleworker solution is how well the solution interoperates with the existing network architecture and its applications. Administrators should consider what type of infrastructure changes are involved in deploying a remote access solution and whether or not costly systems integration work will need to occur. Does the remote access solution work with any Web enabled application or is integration needed? Is performance acceptable over terrestrial and wireless communication circuits? Gathering this type of information will prevent administrators from making subsequent discoveries that can increase deployment time and resources.

Careful consideration should also be given to the direction of the network's communications infrastructure. If network roadmaps include the deployment or continued use of wireless devices, WLAN, increased bandwidth, or satellite-based connectivity, then consideration of how the solution will integrate with these technologies must be given. The AEP solution has the ability to provide end-to-end, high-performance secure remote access solutions seamlessly over wired, wireless and satellite networks.

Of particular importance in an effective teleworker solution is the ability of a remote access solution to operate in the end user's environment—typically a desk or laptop computer, wireless PDA, or public Internet access point. Many SSL VPN solutions only support certain browser versions with specified configurations. This can cause problems when users deviate from the required settings, use a shared Internet kiosk or unexpectedly download a browser patch or upgrade. This problem also arises when the solution is extended to extranet users where browser and operating environment cannot be dictated. Solutions such as AEP's technology that are browser independent can greatly reduce time and resources spent.

Working as a proxy device residing just behind a network firewall allows AEP's gateway to serve as a perimeter device. From this configuration, the device merely has to be made aware of the various applications and servers it is providing access to. The lack of network architectural reconfiguration that this type of solution requires means that applications and servers do not have to be moved into the DMZ in order to provide Web-enabled access to these resources.

Application Access

Understand the benefits and trade-offs of "clientless" and thin client access methods as they relate to your environment

While nearly all SSL VPN remote access solutions provide access to Web-enabled applications, the level of interoperability with applications that are not Web enabled varies among vendors. Administrators should clearly understand which applications can

be supported by a particular solution, and understand what access scenario must be used to support non-Web enabled applications. AEP technology supports access to all TCP/IP based applications not just those that are Web enabled.
A number of vendors, including AEP, have introduced multiple connection scenarios to provide deeper levels of teleworker access to network resources. These additional options often include the use of a dynamic, temporary, Java-based client that is quickly downloaded and executed upon connection to facilitate access to non-Web enabled applications. The differences between these dynamic thin clients and the use of a pure clientless environment are negligible from a user standpoint because the thin clients are downloaded without any user interaction. However, the differences between the levels of access and security that can be achieved with each type of client can be considerable.

Selected SSL VPN vendors, including AEP, have gone a step further to offer a permanent client that can be used to provide a network-layer connection for the fullest level of network connectivity. These thin and permanent clients provide the user with the original view of the application instead of forcing a user to use the Web-enabled version of the application. As with AEP, some permanent intelligent clients serve as part of an integrated two-factor authentication system, thereby providing strong user security.

Organizations evaluating teleworker solutions should understand the difference between these various clients and the access provided by each. Additionally, considerations should be given concerning whether the network will use Web based versions of applications or native versions of the applications to gauge the need and use of thin or permanent clients.

Endpoint Security

Evaluate end point security capabilities that include the ability to ensure security applications are running before allowing connectivity

Endpoint security has become a chief concern among administrators, and an increasingly important element of teleworker solutions. Endpoint security is critical because a compromised device can so easily translate into a compromised network. If an endpoint becomes the victim of a keystroke-logging Trojan, then the URL of the gateway, the username, and the password can all be captured and used at the attacker's leisure.

Endpoint security features that are becoming popular include the ability to verify that firewall and/or anti-virus applications are running on the endpoint before allowing the establishment of a session. If no such application is found, the user can for example be redirected to a site that the application can be downloaded from.

If the network already has deployed endpoint firewall and/or anti-virus programs, then it is important that the teleworker solution vendor supports or partners with these endpoint security companies in order to provide a smooth integration path.

Are You Experienced?

Request customer references and review vendor deployments in networks that resemble your own

A reasonable degree of product maturity and vendor experience in providing teleworker remote access solutions helps assure that technical bugs and interoperability issues will be limited.

Those evaluating teleworker solutions should look to vendors who specialize in developing solutions for their grade of network. Understanding the types of customers that the vendor supports, as well as the size of existing deployments can provide assurance that the vendor's product will meet the needs of extensibility and scalability as the technology takes on an increasing role in the remote access needs of large networks. One way to effectively evaluate a vendor's competencies is to request customer references and review deployments in networks that resemble those of the potential buyer.

TCO – The Real Cost of Deployment

Consider all costs associated with moving to, integrating with and operating a teleworker access solution

AEP Networks' teleworker solution provides many TCO (total cost of ownership) advantages over other remote access alternatives. AEP's cost-effective teleworker solution is easy to implement and maintain, and it operates across a broad range of hardware and software environments.

There can be hidden costs when solutions are incomplete and require additions to be fully functional. As noted earlier, two-factor authentication and endpoint security -- both of which are included in the AEP solution -- come highly recommended when deploying SSL VPN, and become still more highly recommended as an increasing number of applications and users are added to the deployment. Adding either of these capabilities can represent significant additional expense and should be factored in to the overall cost of ownership.

In order to understand the true cost of a solution, buyers need to consider more than the purchase price of software and equipment. Other important TCO points to consider include the simplicity of end user operation, user training costs, minimal infrastructure changes and integration chores. The main value proposition of the AEP solution is its ability to provide a simple means to securely connect remote end users and allow administrators to forego the pain of purchasing, configuring, deploying, and subsequently maintaining a traditional client. Because AEP technology operates at the application layer, architectural changes required of the network are minimal. Even adding users or changing access rights is so simple that remote access can now be offered at a reasonable cost to all employees instead of only senior management or selected field personnel.

Conclusion

Secure remote access is a fundamental requirement for effective teleworker programs. Organizations can use the essential evaluation points in this white paper to help them select the best SSL VPN solution for their teleworker access needs.

Contact AEP Networks

Corporate Headquarters	Government Solutions Group
AEP Networks 347 Elizabeth Ave., Suite 100 Somerset NJ 08873 Toll-Free: 1-877-638-4552 Tel: +1 732-652-5200	AEP Networks 40 West Gude Drive, Suite 200 Rockville, MD 20850 Toll-Free: 1-800-495-8663 Tel: +1 240-399-1200
Europe	**Asia-Pacific**
AEP Networks Focus 31, West Wing, Cleveland Road Hemel Hempstead Herts HP2 7BW U.K. Tel: +44 1442 458 600	AEP Networks 2107 Tower 2 Lippo Centre 89 Queensway Hong Kong Tel: +852 2845 1118
Japan	
JOYO Bldg 6-22-6 Shimbashi Minato-ku Tokyo 105-0004 Japan Tel: 81-3-3432-3336	