The Optimal Solution Choice of Remote Access Connection to Corporate Network

Jelena Jardas Antonić
Faculty of Economics Rijeka
University of Rijeka
Ivana Filipovića 4, 51000 Rijeka, Croatia
jjjardas@gmail.com

Daniel Antonić
City of Rijeka
Institute of Informatics
Korzo 16, 51000 Rijeka, Croatia
danijel.antonic@rijeka.hr

Abstract. *Lately, there have been various tendencies to reconcile the need of every employee to have access to information, anywhere and at any time, and at the same time keeping data security unthreatened. In this paper, the authors attempted to offer the best solution to information security and functionality when accessing a corporate network. The analysis based on the multicriterial approach enables the optimal choice among the most frequently used remote access technologies, such as VPN, Remote Desktop Connection and Direct Access to Published Services on Public Network as well as the access via Network Access Control. The goal of this analysis is aimed at facilitating and offering the most secure access to data to all employees and customers without compromising information security of the mother firm. This analysis incorporates the use of several authentication methods and the optimal choice, by using the AHP method, will be implemented.*

Keywords. Remote Access Connection, Corporate Network, Remote Desktop Connection, AHP.

1 Introduction

Today's attacks on corporate networks have become more dangerous then ever before. They no longer pose a threat just to the company budget but also have an impact on the productivity and continuity of the business activity and therefore on the company-customer relation. Any company willing to maintain the reputation and business activity it has achieved on individual markets should be aware of this problem and make further efforts in confronting this issue. In doing so, the only logical solution is to implement an integrated network system protecting it from such attacks and thus protecting its investments, making the network a strategic advantage. By implementing such a system, it increases its efficiency in network protection, since it eliminates the possibility of duplicated resources. In such a process the IT staff will be able to redirect its efforts and automate key functions giving access to customers and partners and at the same time denying access to potential threats. In other words, the trust of the customers and partners grows with the rise of the awareness of the company management for the need of network protection, which results in return on investment and increased productivity.

The fundamental component of intelligent networking is the tendency to integrate network security functions at all levels of the network infrastructure. A network built through intelligent networking is more adjustable, better integrated and more resistant to attacks and through this synergy it increases its overall value.

The next logical issue lies in how to keep the existing network secure and how to determine if the implemented network meets present security standards. Individuals representing the potential threat for an individual network are very creative and productive since they are driven by the most motivating force – challenge. They abuse the weaknesses of individual products implemented within the system and like "ordinary" criminals that seek and exploit loopholes in law, the newly fledged criminals look for loopholes in the security systems. The challenge lies in the need to prove that everything presented as completely secure actually has a flaw which can be used to hack in such an information system. In order to prevent computer criminals from exploiting the loopholes in networking infrastructures, "patches" are designed to close such holes. On the opposite side of this criminal activity, we have administrators whose task is to protect these networks by quickly "patching" up holes and upgrading new security technologies. Apart from securing the computers and servers, due to technological development, IT administrators protect a whole range of new devices such as POS terminals, building management systems and physical alarm systems. Business activity is based on numerous elements integrated within the network and as a result the higher the number of these elements, the bigger the threat of possible damage. The objective is to find a solution for such threats in general since, due to the increased number and variety of individual daily attacks, dealing with individual threats would be highly impractical. We believe that better efficiency

will be achieved also through the use of automated solutions to possible threats [3].

2 PROTECTION AND PRODUCTIVITY

Intelligent networking is supported by an overall approach in which there is no room for traditional focusing of administrators on preventing threats within the network environment. Most of the work is done by the system itself through detection and alarming. It should also be pointed out that some threats are incorporated in the system within the network whether it is the case of a malicious intrusion of an individual employee or an unintentional entry into forbidden areas. However, regardless the doer, this intrusion can come from the most powerful appliance or a simple personal computer. There is no clear pattern in this, and since all devices are networked together it is logical that the security tools must be integrated within the mere network. Such an intelligently incorporated security system within the network also has a positive effect on productivity. These direct advantages of a healthy and secure network include the following:

- Reduction of costs – such an incorporated security network infrastructure creates added value on investment
- Increased efficiency and functionality – the changes in the security procedures are directed from a single place and are rapidly and globally dispatched throughout the network, thus creating an instantaneous, quick and automated protection within the entire system
- Automatism – automatically set procedures as defined by the administrators result in an overall system protection

Increased productivity can also be achieved by providing a secure connection to be used by your clients. Each individual client must be sure that the data stored on his or her PC will not be endangered while using your network when accessing the Internet. This cooperation strengthens partnership relations and trust. Furthermore, if a company wishes to do so, it may decide upon which data can be made available to its users. It is also necessary to point out that an unobstructed interconnection between internal groups, supply chains and internal business function increases profit due to increased efficiency of business processes.

Through a multicriterial approach, we have tried to determine the optimal solution i.e. the one that most fully meets present security standards considering the financial and security criteria as well as the possibility of upgrading the system and providing a more practical access for users [2].

3 REMOTE ACCESS TECHNOLOGIES

When giving access the data within our corporate network to either our own employee or an outside partner it is hard to determine which technology offers maximum efficiency and service and minimal security risk for possible abuse of data or reading of forbidden data. Furthermore, we must take into account the possibility that someone from the outside has already obtained the information about user's name and password.

This paper analyses access to corporate data by finding the optimal balance between price, security, functionality and stability.

In terms of **security** , the objective is to implement access technologies that would resistant, as much as possible, to the growing number of network attacks such as:

- Eavesdropping
- Identity Spoofing
- Sniffer Attack
- Fishing
- Denial of Service
- MITM Attack
- Scanning for Security Flaws
- Identity Theft

Users accessing the corporate network should have access only to those contents necessary for their business activity. Their computers should meet the security policy set by the company they are accessing to. (All tested security patches have to be uploaded and antivirus and antispam bases updated). Computers without Service Pack should be denied access regardless the valid authentication of the user [3].

These accesses have been analyzed based on three different aspects:

- Financial aspect – finding the optimal balance between offered options and price because each investment, and thus the investment into information security, has to have a return on investment, especially in Croatia where financial resources are quite limited
- Serviceability aspect – enabling simple access to desired resources and applications
- Stability aspect – providing continuous service, reliability and functionality of browsers

The four basic remote access technologies analyzed within this paper include the following:

1. RDC (Terminal services)
2. Remote access VPN
3. INTELIGENT APLICATION GATEWAY-A 2007 (Network access control)

4. Access to company web applications, publishing internal applications for direct access via SSL

3.1 Terminal services or remote desktop connection

The advantage of this technology is quick and simple distribution of applications. The uploading of the application is done on a single computer and by implementing group policy it is possible to restrict access at user level. In addition, it also enables access to the terminal server by a single user or user groups by using the existing Active Directory and optimal use of bandwidth due to the fact that there is no transmission of data i.e. it is processed locally on the server itself.

In addition users themselves can redirect resources, for example a user on a remote terminal session can print and read data found on his or her local computer. If viewed from the security aspect, there is a possibility of logging on by using the Smart card. However, even though this option offers a very high security level in view of authentication, the costs for implementing it are quite costly and thus not an optimal option. The communication process is secured by 128 - bit rc4 encryption if supported by Vista, XP, but it is also possible to connect with older clients using a lower encryption unless otherwise specified by the system e.g. system policy allows access to high encryption clients only. Terminal services within the operating system Windows 2003 also support the FIPS 140-2 (Standard for Personal Identity Verification of Federal Employees and Contractors) encryption level. This is a case of a very high security standard that supports PKI technology, biometric authentication etc. [8].
The disadvantage of such an access is the licenses that have to be bought by the company for each individual user in order for them to be able to have access via terminal services. Another disadvantage is that in order to have an increased number of simultaneous users online we either need a system with high processing power and a large amount of RAM or more servers have to be clustered. As a result, the implementation of this access is rather impractical in cases when different users have to access more application servers [1].

3.2 Remote Access VPN

The VPN technology has three available implementations. However, due to the issues dealt with within this analysis, our interest is oriented towards the Remote Access over the Internet.

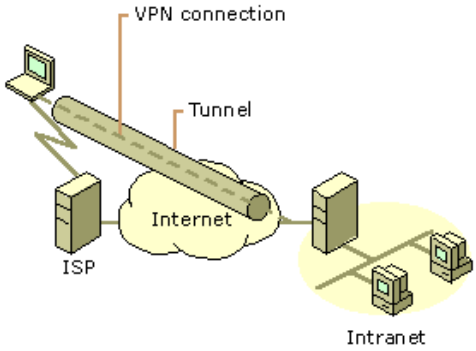

Figure 1. VPN Remote Access

VPN enables the client to access the corporate network over a dial-up connection or over public internetwork such as the Internet. The dial-up connection will not be considered since its costs are quite high and the bandwidth is too low.

Connection over the Internet enables a secure entrance into the corporate network since it encrypts public internetwork connection traffic. We can choose between two industrial standards available when implementing Microsoft technologies: Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol with Internet Protocol Security encryption method (L2TP/IPSec). The PPTP uses the MPPE stream cipher based on Rivest-Shamir-Aldeman (RSA) RC-4 encryption algorithm which uses 40, 56, or a 128-bit encryption keys. On the other hand, the L2TP/IPSec connection uses Data Encryption Standard (DES) which is based on a block cipher using a 56-bit key. The PPTP requires just the user level authentication whereas the L2TP/IPSEC requires both the user level authentication and computer level authentication through certificates. Furthermore, the PPTP encrypts only data traffic while L2TP/IPSec encrypts the authentication as well. The L2TP/IPSec also requires a public key infrastructure and cannot be placed behind NAT [8].
Even though these two standards have equal functionality, they have different security level and thus different costs of implementation. Depending on the company's needs, existing infrastructure and available financial resources, the best choice between these two VPN industrial standards will be made. Regardless the choice of technology, the best implementation restricting user access upon his connection to the local network is assigning each user an IP address on an isolated network segment (quarantine) and then selectively allowing connection to the computers of your choice with ports opened only to that particular connection. However, such an implementation requires a lot of administrative work and not just in its initial phase i.e. implementation but also later on when modifications are needed [1].

3.3 Network Access Control

The majority of the biggest world brands in network equipment production have developed a Network Access Control product in optimizing security and functionality remote network access. We have analyzed three such devices: Citrix's Access Gateway Enterprise Edition, Microsoft's Intelligent Application Gateway 2007 and Cisco's Cisco Clean ACCESS. All products, including these three, have been developed on the Firewall platform and have been upgraded with special software for user access control [5]. The prices range from 20.000 $ upwards depending on the products features in terms of possibilities, security and performance as well as the number of licenses and different features that have to be acquired additionally. We can say that this type of products have managed to incorporate all the best functions offered by access technologies and have further upgraded these products with numerous additional features. Apart from incorporating the top security standards of other access technologies such as simultaneous user and computer authentication, it enables access control over strictly defined resources and applications, detection if computers accessing the network have updated security patches as well as antivirus and spyware databases and finally the possibility of placing these users into a *quarantine* until they solve the problem [4]. As we can see from the above mentioned, these products have high efficiency and highest security standards and are primarily developed for the needs of the most demanding users, especially in terms of security, such as government bodies and financial institutions and therefore the return on investment is quite acceptable.

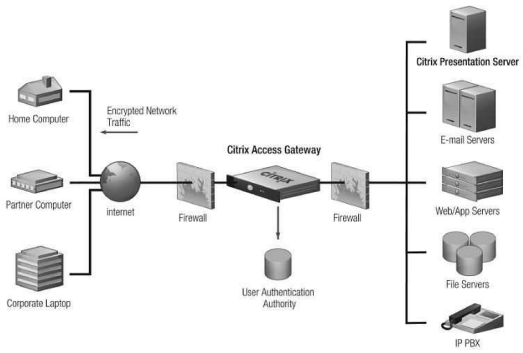

Figure 2. Citrix Access Gateway Secure Remote Access Solutions from Anywhere

However, the disadvantage of this product is its interoperability with a large number of operative systems, network devices and applications and thus rendering possibility for security flaws.

3.4 Access to company resources through web applications

For this type of access the content that the user wants to access must be completely coded by a certain technology which enables access via an Internet browser. Even though this is in accordance with the latest application development trends, the question is whether the IT staff is capable of following the developments in security standards needed for publishing web applications for public Internet usage. In this process 80 % of security requirement is based on the application's own program code and 20 % on the Firewall protection.[9] The application must be coded in such a way that it allows data access based on user authentication. The system must be resistant to intentional overload (DOS attack). The users should not have directly access to real databases but are given access to virtual databases which filter the transactions to real databases. Moreover, the system has to be resistant to various types of attacks such as SQL Injection [6]. Such a project requires more testing procedures and more investment resources then a more or less similar application developed to work on the Intranet [7].

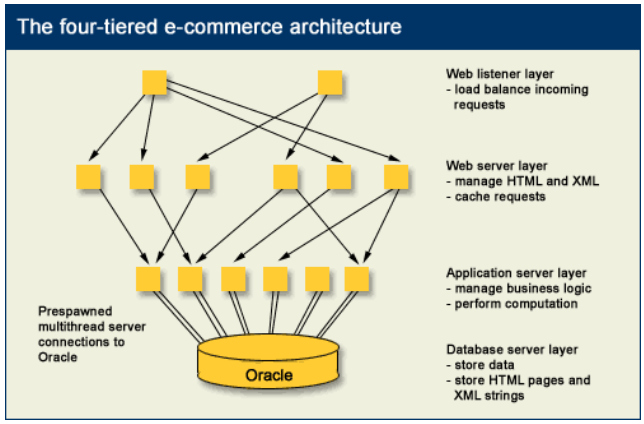

Figure 3. The four-tiered e-commerce architecture

4 CHOICE PHASE - Analytical Hierarchy Process (AHP)

Author of AHP methodology is T.L.Saaty, and it's developed for US Arms Control and Disarmament Agency during leadership for investigations projects. Method is developed as a reaction for impossibility to find simple methodology which can be very simply used during decision making process, and in the same time be simply understandable. AHP is a method of multicriterial deciding and it provides analysis of a very complex problem
in the hierarchic structure in which is easily seen connection between goal, criterions, sub criteria and possible alternatives. Advantage of the AHP method

is that we can include in analysis uncertainty and other factors and take them into consideration. AHP is also very practical because it can compare two different types of data- those of quantitative and qualitative nature i.e. it allows incorporation of subjective and objective consideration in decision making process unlike other multicriterial methods. Humans take easier relative then absolute decision and in that sense AHP gives us new possibilities and allows us comparison of qualitative factors by words, and in hat way we can derive ratio scale of priority and in that way they can be combined with quantitative factors. We can simply tell that this method is one of closely related to way of human thinking and thus is very simple for acquired during process of solving diverse kind of problems. We can say that AHP is compensatory deciding methodology, because some of alternatives can compensate deficiency of one criteria with advantages of others, what is good because we as a final result get alternative which is in relation to all criteria most acceptable as a solution. AHP is composed of different concepts and techniques. This method is based on the pair wise comparison defined before pursuit itself so the goal can be defined, criteria which are important in some problem, and alternatives which are offered as a solution. Basic AHP structure is shown in Figure 4.

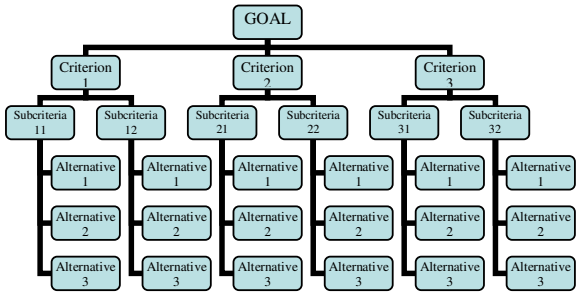

Figure 4.- Basic Structure of the AHP

4.1 Saaty's Scale [10]

Whence we made a hierarchy form of the problem, it's important to identify weights for every single criteria. The weights of determined criteria are assigned according to so called scale of Saaty which defines intensities of priorities accordingly to table 1.

Table 1. The Fundamental Scale

Intensity of importance	Definition	Explanation
1	Equal importance	Two activities contribute equally to the objective
2	Weak	
3	Moderate importance	Expirience and judgement slightly favor one activity over another
4	Moderate plus	
5	Strong importance	Expirience and judgement trongly favor one activity over another
6	Strong plus	
7	Very strong or demonstrated importance	AnActivity is favored very strongly over another
8	Very, very strong	
9	Extreme importance	The evidence favoring one activity over another is of the highest possible order of affirmation

If we want to give briefly interpretation of the methodology we can say that it works in the way of compering alternative's criterion in pairs. AHP method compairs every two criterion between themselves, i.e. it makes pair wise comparision in relation to their assigned weights.That relative inportance of elements is implemented through every level of the hierarchy starting from the top to the bottom. With help of mathematical induction it is not hard to describe pairwise comparision supposing that we have n criterion (alternatives)with their weights given with w_i, and determined by estimated values $a_{ij} = w_i / w_j$. With the help of those ratios is formed

matrix A, and if is $a_{ij} = a_{ik} \cdot a_{kj}$ (measure of consistency) than $Aw = nw$. Matrix A has rank 1, i.e. all rows are proportional with first row, all elements are positive and $a_{ij} = 1/a_{ji}$. From all eigenvalues only one differs from zero and obtain value n. If matrix A contains inconsistent estimations, then we can get weight vector from the equation $A - \lambda_{\max} Iw = 0$ with respect of that $\sum w_i = 1$, where $\lambda_{\max}$ represents the maximal eingenvalue of matrix A. Value $\lambda_{\max} - n$ represents measure of estimations consistency since $\lambda_{\max} \geq n$. Using consistency $CI = \frac{\lambda_{\max} - n}{n-1}$ it can be calculated measure of consistency $CR = \frac{CI}{RI}$ (where RI represents random index i.e. index of consistency of matrix of order n, randomly generated pair wise comparison) If for a given matrix A we have $CR \leq 0.10$, then the estimations of relative importance and obtained alternative ranking are considered acceptable, while in vice-versa has to be reexamined why is measure of consistency unacceptably high.

4.2 Selection of the best solution

Previously we described few technologies of remote access. With the help of analysis and by multicriterial approach we'll try to choose the optimal one. Criteria that we use in the analysis are presented in the table below (Table 2)

Table 2. Input data

Accesses / Criteria		RDC	VPN (PPTP)	VPN (L2TP)	NAC	Publishing	RDC + VPN PPTP	RDC+ L2TP	Publishing SSL
FIPS Compliant		YES	YES	YES	YES	YES	YES	YES	YES
User Authentication		YES	YES	YES	YES	YES	YES	YES	YES
Computer Authentication		NO	NO	YES	YES	NO	NO	YES	YES
Data Encryption		YES	YES	YES	YES	NO	YES	YES	YES
Data Compression		YES	YES	YES	YES	NO	YES	YES	NO
Encrypted Authentication		NO	NO	YES	NO	NO	NO	YES	YES
Advanced authentication	SMART CARD	YES	YES	YES	YES	YES	YES	YES	YES
	Biometrics	YES	NO	NO	YES	YES	YES	YES	YES
	Token	NO	YES	YES	NO	YES	NO	NO	YES
Network Access Quarantine Control		NO	YES	YES	YES	NO	YES	YES	NO
Access Restrictions		YES	YES	YES	YES	YES	YES	YES	YES
Management Simplicity		YES	NO	NO	YES	YES	YES	YES	YES
Simplicity of configuration		YES	NO	NO	YES	YES	YES	YES	YES
Implementation Period	Short	YES	YES	YES	YES	NO	YES	YES	NO
	Middle	NO	NO	NO	NO	NO	NO	NO	NO
	Long	NO	NO	NO	NO	YES	NO	NO	YES
Implementation Costs		NO	NO	YES	YES	YES	NO	YES	YES

Preliminary we have described few technologies of remote access. We'll try to select the optimal one with the help of analysis and multicriterial approach across all selected criteria (see Table 2.). Weights of certain criteria and sub criteria are assigned according to questionnaire results and information from the literature. The results we have got are given below.

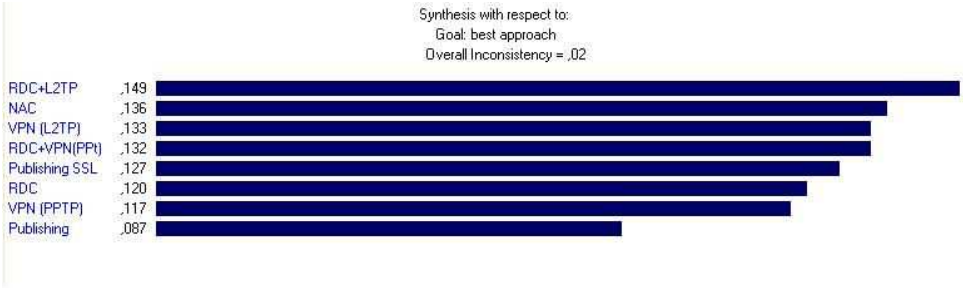

Figure 5. Results of the Analysis

5. Conclusion

The results we obtain have confirmed expectations of the authors. Center of gravity in this analysis was on different aspects of security of remote access approaches. Network Access Control and Remote Desktop Connection in the combination of L2TP/IPSEC represents definitely the safest access technologies. Informatical market supply with security plug inns such are USB keys or support of biometrical readers for every access technology is day by day more ample. Use of such implements enlarges security level of authentication, but unfortunately the price of implementation grows according to it. Selecting the optimal technology of remote access from financial aspect must be determined with real financial loss if the oversight happens. Technology of remote access which appeared as the best compromise-solution for the companies with moderate budget is the RDC+ VPN PPTP. It should be pointed that absolutely safe technology does not exist, so on the end when we take resume, we may say that weakest link in the chain is always human. Therefore, besides implementation of technology itself there exist a need for improvement of knowledge and skills of customers and IT staff.

References

[1] Joseph Davies**, TCP/IP Fundamentals for Microsoft Windows**,Microsoft Corporation,USA,2006

[2] Ronald L. Krutz and Russell Dean Vines**, The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking**, Wiley,USA,2007

[3] Neil R. Wyler,Bruce Potter,Chris Hurley, **Aggressive Network Self-Defense**, Syngress,USA, 2005

[4] Cisco Site,**Cisco NAC Appliance (Clean Access),**Aviable at *http://www.cisco.com/en/US/products/ps6128/tsd_products_support_general_information.html*, Accessed 10th May 2008

[5] Citrix Site, **Citrix Access Gateway Secure Remote Access Solutions from Anywhere**, available at *http://www.citrix.com/English/ps2/products/product.asp?contentID=15005&ntref=hp_nav_US* ,Accessed 12th July 2008

[6] Donald Burleson, **Managing Web Development with Oracle**, Available at *http://www.dba-oracle.com/art_web_devl.htm*, Accessed 10th May.2008

[7] Donald Burleson, **Trends in Oracle web security management**, , Available at http://www.dba-oracle.com/t_oracle_web_security_trends.htm, Accessed 12th February 2008.

[8] Microsoft TechNet**, Deploying Dial-up and VPN Remote Access Servers**, available at *http://technet2.microsoft.com/windowsserver/en/library/8ff3534e-0f08-45bc-8487-3b618bc8ad621033.mspx?mfr=true*,Accessed 17th February 2008

[9] Roger A. Grimes**, Is your Web site FIPS compliant?** Available at *http://www.infoworld.com/article/08/02/15/07OP-secadvise-fip-compliant_1.html* Accessed 17th February 2008

[10] Saaty T.L.,: **Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process,** RWS Publications, Pittsburgh, SAD, 2006