International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Secure Connection in VPN using AES

Mrs. Swapna[1], G .Sri Naga Sri[2], G. Nikila Santha Kumari[3], N. Sravani Devi[4]

[1]*Asst. Professor, Dept. of CSE & IT engineering, GPCEW, A.P, India*
[2]*Student, Dept. of IT engineering, GPCEW, A.P, India*
[3]*Student, Dept. of IT engineering, GPCEW, A.P, India*
[4]*Student, Dept. of IT engineering, GPCEW, A.P, India*

Abstract - Virtual Private network (VPN) provides one of the most promising services for network providers.Using a VPN when connected to the internet will hide your personal IP address and assign you one based on the server you are connected to. Once you connect to a VPN, you are essentially creating a tunnel between your device and the VPN server you have chosen, encrypting any data sent or received. Virtual private networks (VPNs) use advanced encryption techniques like AES(advanced encryption standard) and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks such as the Internet rather than using separate Leased lines. The advantage with the VPN technology is, using existing Internet connection we can communicate between two remote systems using built-in Windows VPN.

Keywords **-** tunneling, cipher text, plain text, hash function, encryption, authentication.

1. INTRODUCTION

Generally VPN is very expensive to use, it requires a VPN provider to establish that network through using leased lines or to our routers. However we don't need such requirement always if connection is between two individuals or more. We can build more easily by using built in VPN provided in Android, Windows etc through internet. Virtual Private Network which has proved itself to be lot reliable in transferring data between remote places via a secured network thus paving way for data security. The ideas of implementing a VPN connection featuring the setting up a server and client on individual system who want to communicate. The data will be transferred using AES encryption mechanism with HMAC (Hash based Message Authentication Code) which checks same message received on receiver end.

2. IMPLEMENTATION

VPN is established using built in vpn of windows between communicated systems.VPN has two types, site-to-site and remote access. We are setting up site-to-site vpn using PPTP.

Site-to-Site Intranet-based VPN: The connection established in or between a LAN Networks. It links headquarters, remote offices, and branch offices to an internal network over a shared infrastructure using dedicated connections.

PPTP (Point-to-Point Tunnelling Protocol) – It is one of the protocols VPN uses for establishing tunnelling. It allows you to implement your own VPN very quickly, and is compatible with most mobile devices. This protocol encrypts data and puts it into packets by creating a tunnel that provides secured communication over LAN or WAN. Because of the encapsulation of that data, encryption and required authentication, it is safe to transmit that data even over public networks like internet.

PPTP is based on authentication, encryption and PPP negotiation

It supports 40-bit and 128-bit encryption and will use any authentication scheme supported by PPP.

This protocol encrypts data and puts it into packets by creating a tunnel that provides secured communication over LAN or WAN. Because of the encapsulation of that data, encryption and required authentication, it is safe to transmit that data even over public networks like internet

The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products

The PPTP tunnel is instantiated by communication to the peer on TCP port

The data transmitted between VPN network systems implements AES for encryption and decryption, HMAC for authentication. By using 'Java Crypto Package', code is implemented for AES and HMAC.

2.1 AES (Advanced Encryption Standard) algorithm:

AES algorithm is called as Rijndael algorithm.

This algorithm is a block cipher intended to replace DES for commercial application

It has 10 rounds for 128-bit keys,12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

It does not use Fiestel Cipher structure. It uses Transformation function like substitution bytes, shift rows, mix columns and add round keys.
It is used to overcome the drawbacks of DES and triple DES algorithm.
It is based on design principle known as substitution and permutation network.
The sub keys are generated in the form of words.

The pseudo code for AES Encryption

```
public byte[] encrypt(String plainText, SecretKeySpec key)
{
        // since we are not using the built in padding, we must pad plaintext to a multiple of 16
if(plainText.length()%KEY_LENGTH != 0)
 plainText = padString(plainText);
       // start encrypting:
Cipher cipher = Cipher.getInstance("AES/CBC/NoPadding", "SunJCE");

cipher.init(Cipher.ENCRYPT_MODE, key, _IV);
byte[] cipherText = cipher.doFinal(plainText.getBytes("UTF-8"));
System.out.println(cipherText);
return cipherText;
}
```

2.2 HMAC (Hash Based Message Authentication Code) SHA (Secure Hash Algorithm)-1:

It is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. It may be used to simultaneously verify both the *data integrity* and the *authentication* of a message, as with any MAC. Any cryptographic hash function, such as SHA-1 used in the calculation of a HMAC.SHA-1 is based on the hash function MD4 and also specified in RFC-3174.
The hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function. SHA-1 operates on 512-bit blocks. The size of the output of HMAC is the same as that of the underlying hash function (128 or 160 bits in the case of SHA-1).
HMAC does not encrypt the message. Instead, the message must be sent unencrypted alongside the HMAC hash. Parties with the secret key will hash the message again themselves, and if it is authentic, the received and computed hashes will match.
MAC=**H** (key || **H** (key || message))
H -cryptographic hash function,
|| - denotes concatenation
The pseudo code for HMAC

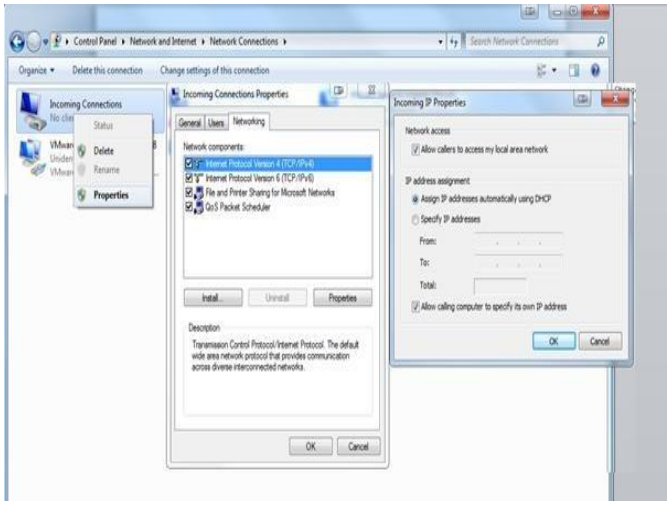
```
function hmac (key, message) {
  if (length(key) > blocksize) {
    key = hash(key) // keys longer than blocksize are shortened
  }
  if (length(key) < blocksize) {
    // keys shorter than blocksize are zero-padded (where || is concatenation)
    key = key || [0x00 * (blocksize - length(key))] // Where * is repetition.
  }
  o_key_pad = [0x5c * blocksize] ⊕ key // Where blocksize is that of the underlying hash function
  i_key_pad = [0x36 * blocksize] ⊕ key // Where ⊕ is exclusive or (XOR)

  return hash(o_key_pad || hash(i_key_pad || message)) // Where || is concatenation
}
```

3. EXPERIMENT AND RESULT

Setting up VPN server on server system
1. Go to “Control Panel\Network and Internet\Network Connections”
2. Press key combination [ALT] + F {you will see the file menu popup}
3. Select “New incoming connection”
4. Select the user you want to allow to connect remotely.
5. Yes we want to allow the PC to be connected over the internet.
6. Select the protocol you want to use. Mostly IPV4

Fig Setting IP address



7. OPTIONAL: If you wish to specify clients IP range you can do it here. Otherwise server will automatically provide IP via DCHP server.
8. Check the box “allow calling computer to specify its own IP address” or We can manually enter our wished IP in client pc’s.
9. Save everything and close it.

Setting up VPN client in client system
1. Go to control panel \network and internet\Network sharing centre
2. Click "Set up a new connection or network"
3. Click "Connect to a workplace "VPN"
4. Select "use my internet connection (VPN)
5. Fill the settings
a. **Internet address**: It asks for the remote server address, you can type the IP of the server.
b. **Destination Name:** The VPN connection name {leave as it is}
c. **Use smart card:** smart cards for the connection {leave empty if u don't have one}
d. **Allow other people to use this connection….. :** {This is internet sharing, we don't want to share internet so we leave this empty}
6. Give user name and password {not your computer username and password. It asks for the server pc username and its password to connect to the server pc.

After setting up VPN connection on both client and server systems by using built in VPN.

Fig 3.1 VPN connected to server on client system

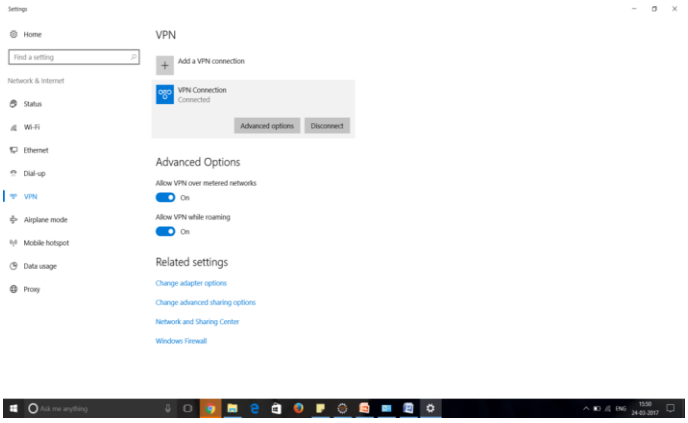
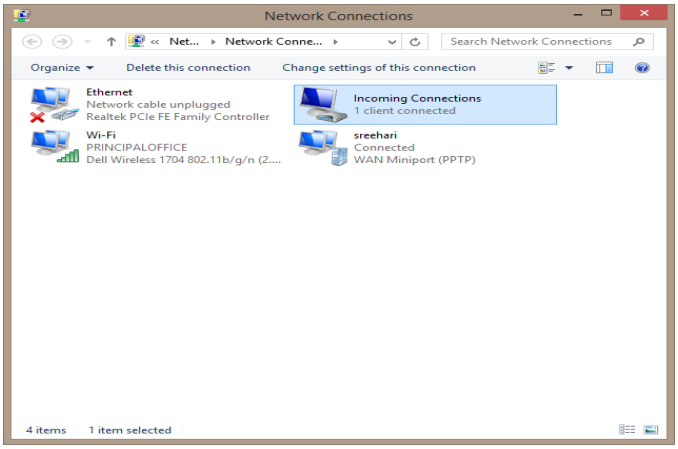


Fig 3.2 VPN server system connected to client



After the two systems come into VPN network, we can communicate data between them using java.
Now run the java code on both systems, it will ask for shared key (symmetric key). Give the same on client and server.

Fig 3.3 Prompt window on server

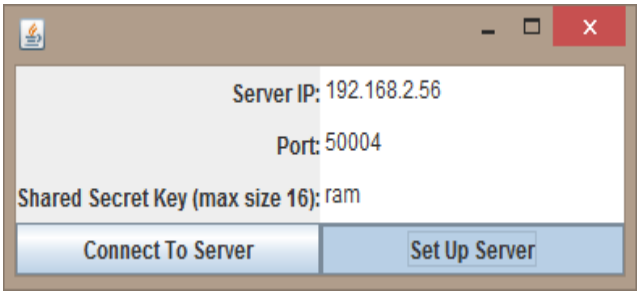
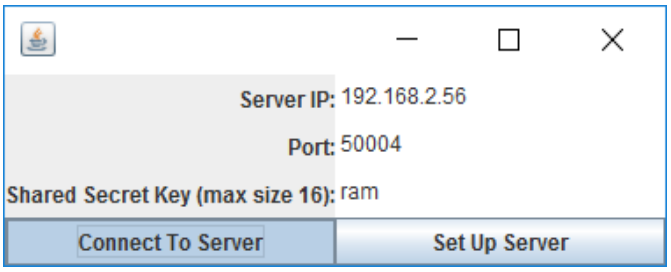


Fig 3.4 Prompt window on client



After connecting they both communicate in interface box provided by using java swings.

Fig 3.5 Message interface in client

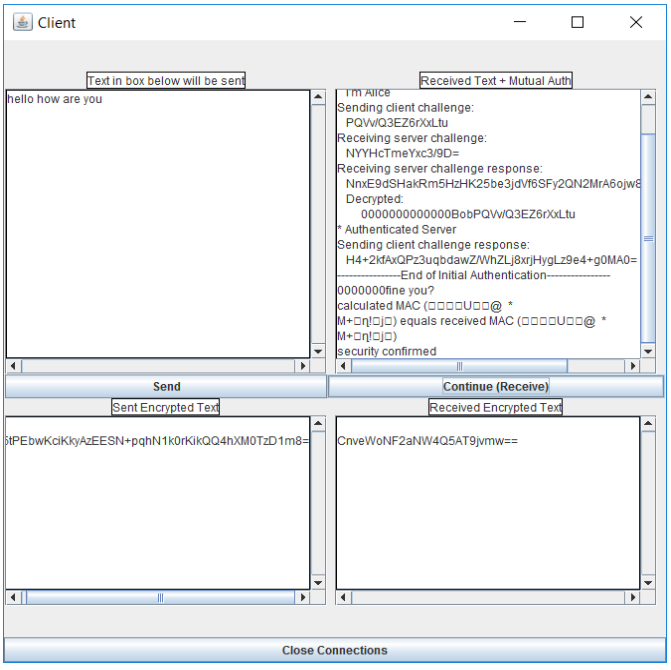
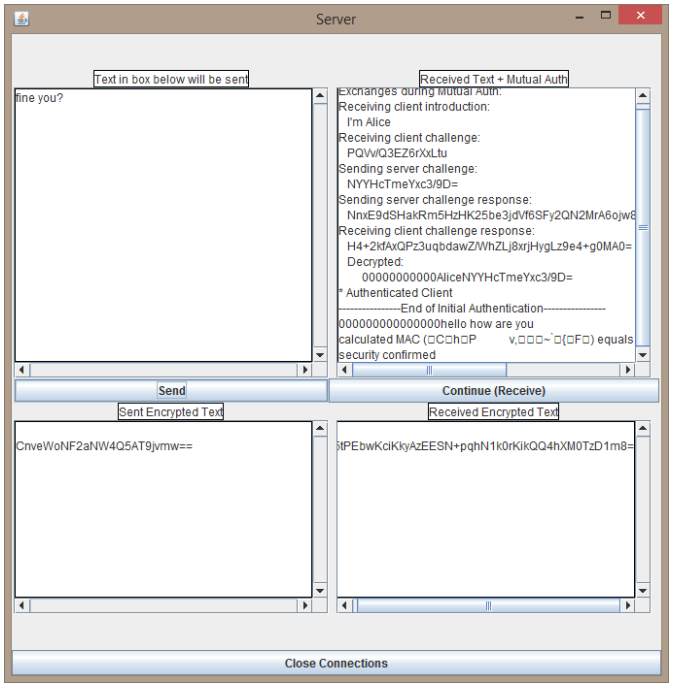


Fig 3.6 Message Interface in server



In both the interface we can see encrypted text, mutual authentication of both sender and receiver.

4. CONCLUSION

Our main objective is to establish a VPN network without putting so much cost and effort. This can be benefited for two or more individuals who want a private network to protect their data along with network from snooping. In this paper we explain how to establish a VPN network and showcased what mechanisms are used for data transmission (which we are represented using java crypto and swing package). While Firewall implementation help to prevent data from leaving and entering an enterprise by unauthorized users, they do little to protect against threat within the Internet. Sensitive data such as user names, passwords, account numbers, financial and personal medical information, server addresses, etc. is visible to hackers and to potential e-criminals over the Internet. This is where the benefits of VPN are seen. A VPN, at its core, is a fairly simple concept—the ability to use the shared, public Internet in a secure manner as if it were a private network. With a VPN, users encrypt their data and their identities to prevent unauthorized people or computers from looking at the data or from tampering with the data.

ACKNOWLEDGMENT

We would like to give our sincere gratitude to our guide Mrs. Swapna who guided us to pursue and helped us to complete this topic. We would also like to thank her for providing us remarkable suggestions and constant encouragement. I deem it my privilege to have carried out my research work under her guidance.

REFERENCES

[1] Weili Huang and Fanzheng Kong. The research of VPN over WLAN.
[2] Stallings W., Cryptography and Network Security, Third Edition, Pearson Education, 2003.
[3] Xinmiao Zhang and Keshab K. Parhi,"Implementation approaches for the advanced encryption standard algorithm", IEEE Transactions 1531-636X/12©2002IEEE.
[4] Prentice.Hall.Cryptography.And.Network.Security.5th.Edition.Jan.2010.ISBN.0136097049.
[5] "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, November 26, 2001.
[6] How to set-up simple VPN connection between two remote computers. Step by Step using with pictures (https://xkrishx.wordpress.com/tag/how-to-set-up-simple-vpn-connection-between-two-remote-computers-step-by-step-using-with-pictures/)
[7] CISCO VPN and VPN technologies (www.ciscopress.com/articles/article.asp?p=24)