10 reasons why IPsec VPN failed

During the discussion around IPsec VPN deployment issues, I heard an idea as follows: 'We have an IPsec VPN, and it is configured to use encryption algorithms. So it's absolutely safe, and you can

As an independent advisor, I am often asked to have a 'keen eye' when performing a network assessment. Sometimes including IPsec VPN survey.

During the discussion around IPsec VPN deployment issues, I heard an idea as follows: " *We have an IPsec VPN, and it is configured to use encryption algorithms. Therefore it It is absolutely safe, and you can spend more time with other members of the network than spend time surveying VPN* ". This is sometimes too complacent and believes in the surprising widespread popularity of IPsec VPNs, especially when using powerful encryption algorithms such as AES, is very secure without bothering to design. and configure correctly.

Until now, almost everyone knew that it was not a good idea to use weak 56-bit DES algorithms on IPsec VPN.

But there are still sometimes unexplainable things that even though an IPsec VPN uses relatively strong algorithms like AES, all the power and protection proposed by these algorithms can be weakened. by IPsec design VPN and bad configuration.

So, if you have an IPsec VPN and are unsure of its configuration, this might be a good idea to double check if you have used the correct algorithms or not and also consider Is VPN also designed and configured correctly?

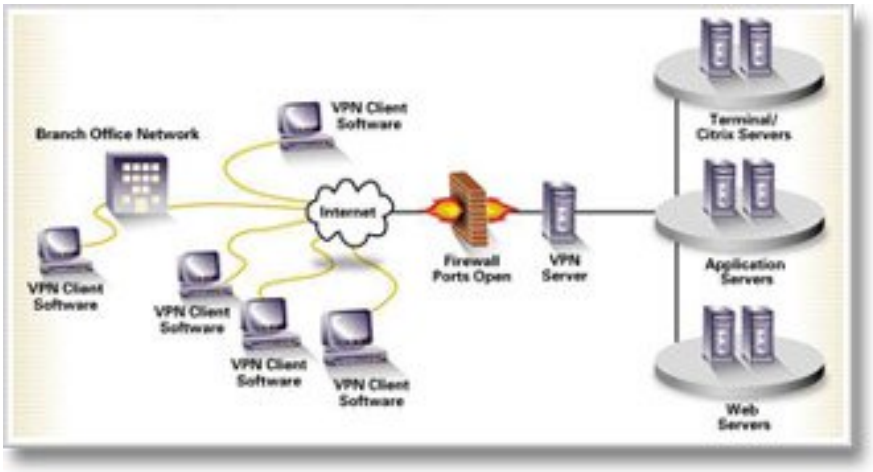
Here are ten weaknesses that need to be checked when accessing IPsec VPN :

1. Use weak shared keys.

2. Use of inappropriate IKE / ISAKMP attack method (weak shared key).

3. Appropriate authentication method (shared key when electronic signature [certificate] based on authentication may be more appropriate).

4. Use inappropriate groups of wildcards or wildcards (using more solutions will be better).



5. Use a shared shared key with multiple equivalent devices (similar # 4).

6. Inappropriate use of extended authentication (XAuth, vulnerable when used with shared keys and IKE / ISAKMP).

7. Vulnerability of NTP or CRLs / OCSP used by PKI for DOS attack (related when using electronic signature authentication).

8. Securing the weaknesses of storing primary keys CA.

9. Store IPsec VPN gateway configuration files containing shared key color letters.

10. Use encryption without authentication.

The ten weak points on the offer just started. Therefore, there is a need for good precautions until you have embraced every facility and are absolutely satisfied that the IPsec VPN is truly secure.

And if you need more information about the ten points I listed above, then Google is a good search engine. If Google does not do this, please refer to some books on Amazon.