

What kind of policies and procedures need to be developed for VPN?

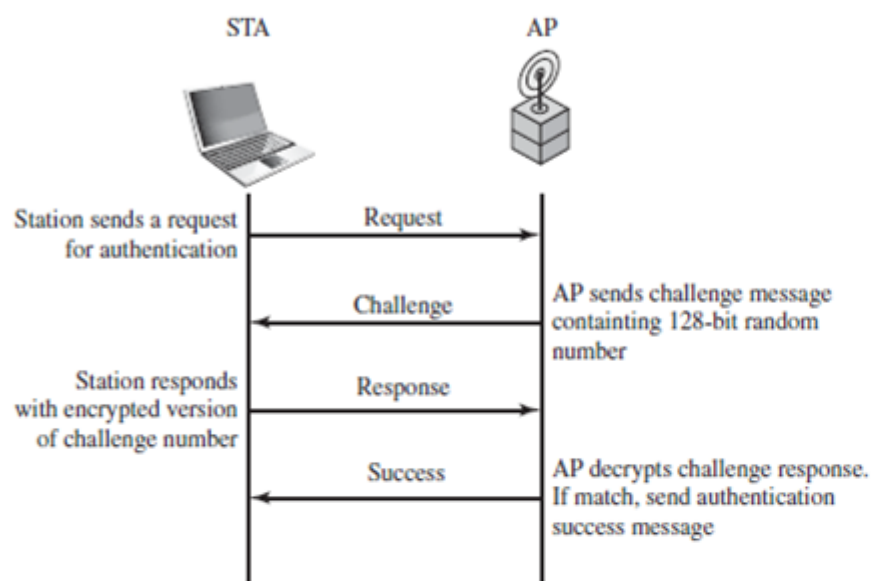
Your Answer:

One key policy/procedure that users need to have when using a VPN is having good management skills. Users within an organization must be able to properly manage other employees and their computer systems, preventing confusion.

The user needs to follow the correct procedure to download the proper VPN software and version for their computer system, as an older version or improper one may not be beneficial and out of date, which in turn could actually be detrimental. Organizations follow the same procedure to ensure that all computers have the correct VPN configurations. They also may have to follow different procedures if an employee uses their own VPN. There may be heightened security tensions when this happens which is why they require special attention and configurations.

We cannot forget the upmost security protection needed for a computer that anyone can use, which is an anti-virus. Having a good, reliable anti-virus that schedules periodic scans throughout the computer for malicious malware can provide substantial security for the computer's information along with the VPN.

Prior to the introduction of IEEE 802.11i, the security scheme for IEEE 802.11 was Wired Equivalent Privacy (WEP). WEP assumed all devices in the network share a secret key. The purpose of the authentication scenario is for the STA to prove that it possesses the secret key. Authentication proceeds as shown in the figure below. The STA sends a message to the AP requesting authentication. The AP issues a challenge, which is a sequence of 128 random bytes sent as plaintext. The STA encrypts the challenge with the shared key and returns it to the AP. The AP decrypts the incoming value and compares it to the challenge that it sent. If there is a match, the AP confirms that authentication has succeeded.



- What are the benefits of this authentication scheme?
- This authentication scheme is incomplete. What is missing and why is this important? Hint: The addition of one or two messages would fix the problem.
- What is a cryptographic weakness of this scheme?

Your Answer:

- It is a quicker method of authentication since it carries simpler encryption practices. There is basic access control since only stations with the proper shared secret key can authenticate. There are also random challenges making infiltration for an attacker harder since it is completely randomized.
- It is missing both challenge protection and mutual authentication. An attacker could easily intercept the challenge since it is plaintext. They could also recover the secret key since they can capture both this and the encrypted response. One sided authentication from the client to the AP opens vulnerabilities.
- The encryption is rather weak due to its simplicity. The visibility the hacker has on the encryption process opens the vulnerabilities that exist with the scheme. They can see between the plaintext challenge and the encrypted response and the key could easily be cracked since there is also weak key management.