Auth Shield
Multi Factor Authentication

An Authentication Security Organization

Whitepaper

Integration of AuthShield Multi-Factor Authentication with Virtual Private Network (VPN)

Contents

1. Introduction

The rapid growth of internet and digital communications has ensured that most of the organizations today have dispersed workforces across the world.

Employees opt for work from home policy or work remotely while connecting to centralized servers in the Data Center, thus having a regular flow of information between spread out end points and centralized servers. This convenience and pace of information sharing has been an important factor in the pace of growth of internet.

"Most organizations in the world today use a VPN to interconnect their different offices or provide employees functionality to work from home."

However, an infrastructure of this sort brings to fore its own set of problems. With tools like air crack, nighthawk gaining prominence even a school kid can hack into your Wifi network and gain access to data shared on your network. At the same time, organizations have no control over the security of end points leading to vulnerabilities or loopholes in their network.

To prevent this, organizations across the world are increasingly using VPN to connect to their internal networks. VPN or a Virtual Private Network has become one of the most critical components in a corporate network today. VPN provides an encrypted tunnel over the public network thereby encrypting the information flowing over the network

Not only this, but with more and more regularization of the internet by countries, VPN provides organizations with a method to bypass local firewalls and ISP restrictions.

"According to a survey carried out 70% of people reuse their passwords in multiple accounts. Less than 2% users have passwords that are complex enough and long enough to resist a combination of dictionary, rainbow and brute-force attacks"

While VPN ensures that the information flowing over the network is encrypted, it gives attackers a new target - end points connecting to the network. Since VPN work on a single factor of authentication (user name, password), installing a small keylogger on the end point can provide an attacker access to VPN credentials thereby compromising one of the most critical assets of the organization. Trojans such as Citadel have been specifically created to steal VPN credentials from public networks such as airports, open wi-fi networks etc.

In such a scenario, to protect themselves, more and more organizations are using a Two Factor Authentication system to protect VPN.

2. Threats to VPN Accounts

a. Social Engineering or Password Sharing

Most people end up sharing their passwords with their friends or colleagues. The act may be deliberate or accidental. But the fact remains that a user seldom even remembers the number of people the account details may have been shared with. At the same time, passwords are not changed at frequent interval, giving an outsider unlimited access to an account. Occasionally, users also fall prey to common social engineering techniques and end up revealing answers to their security questions thereby providing intruders a chance to gain unauthorized access to the account.

"VPNs provide easy access from the Internet into a corporate network and its internal resources. VPN security is only as strong as the methods used to authenticate the users (and the devices) at the remote end of the VPN connection."

b. Reuse Logins

A user on the net usually has more than one account. Most users end up using same or similar passwords in multiple accounts leading to a possibility where an inadvertent leak may lead to providing access to multiple accounts

c.Identity thefts – Phishing

"One Phishing attack at a Bank / Online Portal / store/ BPO etc can lead to a loss of thousands of accounts in one step

Acquire details such as credentials to SAP and other critical applications etc by masquerading as a trustworthy entity. Such an information breach by authorized personnel either intentionally or accidentally, can cause irreparable damage to an organization.

d. Virus, worms, Trojans

Keyloggers, remote sniffers, worms and other types of Trojans have been used since the evolution of the internet to steal user's identity. Most data is accessed from stolen computers and laptops or by hackers capturing data on unprotected networks.

3. Protecting VPN Accounts

When your organization banks on you, what do you bank on?

Prevention is always better than cure. It is truer today than ever before when the theft is conducted on the net with no physical threats and with less cost to the perpetrator of the crime. The only challenge that remains is to cover ones tracks and considering the massive flow of information on the net almost on a daily basis, it is not much difficult either.

Multi-Factor Authentication: why do you need it?

> ***"The best way to beat a thief is to think like one."***

Phishers try to obtain personal information such as your password or PIN-code by pretending to be a legitimate entity.

Using Phishing, static passwords can be easily hacked providing fraudsters easy access your personal accounts, files and confidential information.

AuthShield - Multi Factor Authentication maps the physical identity of the user to the server and increases the security of financial and other critical systems. Integrating Stronger User Authentication system not only helps prevent Online Credit Card fraud, Card Cloning, Identity theft but also helps in the capture of habitual cyber criminals.

AuthShield authenticates and verifies the user based on –

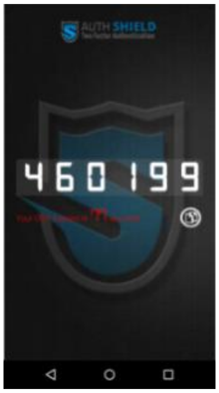
- ❖ something only the user has (mobile phone/ land line/ hard token)
- ❖ something only the user knows (user id and password)

- something the user is (Biometrics)

AuthShield technology uses a dual mode of identification where along with the user id and password, verification is done through a secure randomly generated through One-time password (OTP). This is provided to the user through:

Hard Token

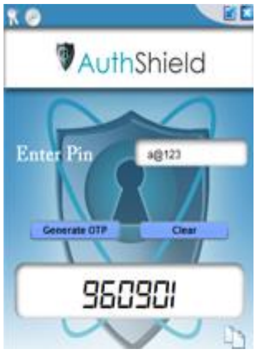
AuthShield’s Hard token is a security device given to authorized users who keep them in their possession. To verify a transaction using second factor of authentication, the device displays a changing number that is typed in as a password. The new number is based on a pre-defined unbreakable randomized algorithm. Thereby, the hard token enables the server to authenticate the digital identity of the sender using a hardware device apart from his user name and password.



Mobile Token

AuthShield's mobile token is an application installed on smart phones which generates an OTP for the user on the phone itself.

The architecture remains similar to a Hard Token except that the user only has to carry his mobile phone. Thereby, the device enables the server to authenticate the digital identity of the sender using a mobile phone apart from his user name and password.



Enter Pin a@123

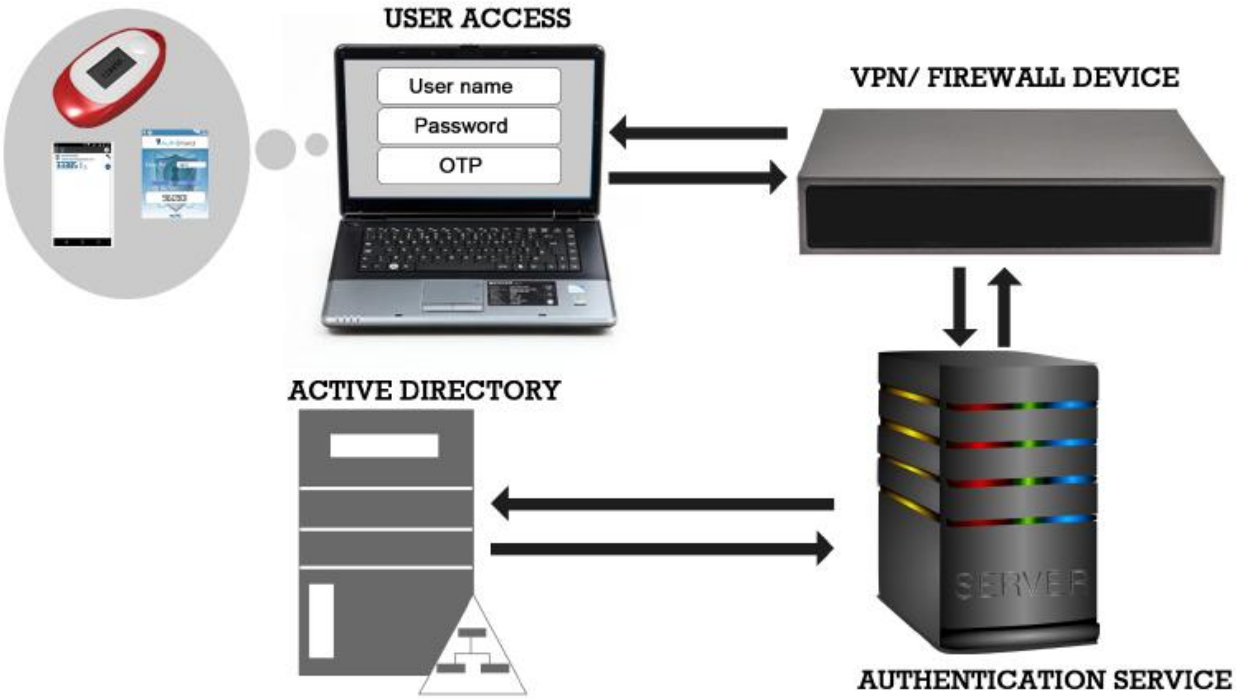
960901

Soft Token

AuthShield soft token is a convenient form factor installed on the laptop / desktop itself. The token generates a new password after fixed intervals of time. The user enters the password generated by the soft token as a secondary form of authentication.

Integration of AuthShield with VPN

Architecture



Process

- ❖ VPN Authentication is done via RADIUS Protocol
- ❖ Client logs into VPN by entering his User name, Password along with One Time Password (OTP).
- ❖ User name and Password are validated from Active Directory (AD) while User name and One time password are authenticated from the Authentication server.
- ❖ Once validated, the client will then log into the VPN.

4. Features

- OS Independent Authentication Mechanism
- Seamless Integration with the current business and security architecture
- Increases the log on security for Mails
- 99% security from Phishing attacks and identity thefts
- Unbreakable encryption on the lines of those used by US Government
- Logs are maintained to fix responsibility in case of an unlawful event.

5. Advantages of using AuthShield

For Users

Using AuthShield Multi-factor authentication can help in preventing-

- Online credit card fraud Phishing
- Card cloning
- Unauthorized access to data by employees.

For the organization

- OS Independent Authentication Mechanism
- Seamless Integration with the current business and security architecture
- Increases the log on security for critical applications.

6. About Us

The world today revolves around information. Information today is the energy that plays a critical role in our personal lives and drives our businesses. As we move further into this digital age, it has become imperative to not just protect our information from outsiders but to also draw intelligence from the vast amount information available to us.

Internet is the new playground for unwanted elements of society intent on committing terrorist or espionage activities, financial frauds or identity thefts. Keeping this in mind, it has become imperative to not only prevent these acts but also be in a position to intercept, monitor and block Internet communication to draw intelligence out of them.

AuthShield is an Authentication Security solution with a patented technology on implementing Multifactor Authentication at a protocol level. This makes it an application independent technology and needs no changes at the application. As an advantage of working at protocol rather than application level, an organization can use AuthShield to implement Multifactor Authentication in any and every technology such as **Downloading mails on phones / desktops,** SAP, Database queries, Internet of Things, or any other enterprise or cloud technology in a matter of minutes.

For more information visit - www.auth-shield.com