

VPN

&

Remote Networking

Topics To Cover:

Mirox
Reinforce Your Security
Selutorce Your Security

- ☐ VPN Policies
- ☐ VPN Registrations And Passwords
- □ Common VPN Flaws

■ VPN Policies



- Periodically scans computers connected to the network.
- All computers connected to internal networks via the VPN, must use the most up-to-date anti-virus software and operating system patches.
- Individual users are responsible for selecting an Internet Service Provider (ISP), coordinating installation, and installing any required software necessary for Internet service.

- Devices identified as a potential security threat may be blocked from the network until further action is taken by the user.
- VPN users will be automatically disconnected from the network after thirty minutes of inactivity. The user must then logon again to reconnect to the network.

■ The VPN does not allow dual (split) tunneling; only one network connection is allowed.



- It is the responsibility of users with VPN privileges to ensure that unauthorized persons are not allowed access to internal networks.
- Jailbroken or rooted tablet devices (i.e. devices which have had security settings disabled) will be denied access to the service for security reasons.
- All client devices are checked for security compliance every 15 minutes.
 Devices that fail compliance will have their session disconnected and must meet policy again in order to successfully connect.

• Users accessing sensitive systems and data must additionally request and authenticate to the VPN with strong or two factor authentication, which will be provided to them as part of the VPN solution.

■ Each user is responsible for ensuring that any software accessed while connected to the VPN is appropriately licensed.



■ All sessions have a maximum lifetime of 10 hours after which users should reauthenticate to create a new remote session.

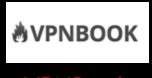
☐ VPN Registrations And Passwords











VPNBook









CyberGhost



 Virtual Private Network is most economical and secure method of connecting private networks over Internet.



- VPN helps mobile users to connect to their corporate network from Internet.
- Password must be made up of a minimum of eight alphanumeric characters, containing at least one letter and one numeral.
- Password must be changed at least every 90 days.
- Password must be locked out at a maximum of six failed attempts.



> Ewilter

F Follow



Home

VPN Service	VPN Solution	Community	Downloads		Search	0
Registr	ation					
⊕ Requ	ired field ation is required in orde	r to get access to the Op	oenVPN Access Server	Support Center and Softw	are	
First N	ame:	•				
Last Na	ame:	•				
Email:		•				
Passwe	ord:	•				
Verify	Password:	•				
Securi	ty Code: pc 97	16				
Enter Security Code:		•				
Make su	ıre you can receive e-mail	from OpenVPN.net to acti	vate your account. Activa	ation takes just a few minutes	S.	
	er and create a FREE acco	unt				
⊌ Requ	ired field					

□ Common VPN Flaws

Mirox Reinforce Your Security

> HACKING ATTACKS:

- An intruder could exploit bugs or misconfiguration in a client machine, or use other types of hacking tools to launch an attack.
- VPN hijacking is the unauthorized take over of an established VPN connection from a remote client, and impersonating that client on the connecting network.

> USER AUTHENTICATION:

- By default VPN does not provide / enforce strong user authentication.
- If the authentication is not strong enough to restrict unauthorized access, an unauthorized party could access the connected network and its resources

> CLIENT SIDE RISKS:

A client machine may also be shared with other parties who are not fully aware of the security implications.



- In addition, a laptop used by a mobile user may be connected to the Internet, a wireless LAN at a hotel, airport or on other foreign networks.
- If the VPN client machine is compromised, either before or during the connection, this poses a risk to the connecting network

> VIRUS / MALWARE INFECTIONS:

- A connecting network can be compromised if the client side is infected with a virus.
- If a virus or spyware infects a client machine, there is chance that the password for the VPN connection might be leaked to an attacker.

➤ INCORRECT NETWORK ACCESS RIGHTS:

Some client and/or connecting networks may have been granted more access rights than is actually needed.



> INTEROPERABILITY:

• Interoperability is also a concern. For example, IPsec compliant software from two different vendors may not always be able to work together.



THANK YOU !!!