VPN Configuration & Management Cheat Sheet

A handy reference for VPN commands and configurations, covering various aspects of VPN setup, management, and troubleshooting across different platforms and tools. This cheat sheet provides quick access to essential commands and configurations for OpenVPN, WireGuard, IPsec, and common network utilities.

OpenVPN Management

Basic OpenVPN Commands

`openvpn --config client.conf`	Start OpenVPN client with a specific configuration file.
`openvpn --daemon --config server.conf`	Start OpenVPN server in daemon mode (background process).
`systemctl start openvpn@client`	Start OpenVPN client service (using systemd).
`systemctl stop openvpn@server`	Stop OpenVPN server service (using systemd).
`systemctl status openvpn@client`	Check the status of the OpenVPN client service.
`journalctl -u openvpn@server`	View OpenVPN server logs (using journalctl).

Configuration File Directives

`client`	Specifies that this is a client configuration.
`server 10.8.0.0 255.255.255.0`	Configures OpenVPN server with a specific subnet.
`remote myvpn.example.com 1194`	Specifies the remote VPN server address and port.
`dev tun`	Uses a TUN (Layer 3) virtual network device.
`dev tap`	Uses a TAP (Layer 2) virtual network device.
`proto udp`	Uses UDP protocol for the VPN connection.
`proto tcp`	Uses TCP protocol for the VPN connection.
`tls-client`	Enables TLS client mode.

Troubleshooting

Check OpenVPN logs for error messages. Common issues include certificate errors, firewall problems, and incorrect configuration settings.
Verify that the OpenVPN service is running using `systemctl status openvpn@client` or `systemctl status openvpn@server`.
Use `ping` and `traceroute` to test connectivity to the VPN server and other network resources.

WireGuard Essentials

Basic WireGuard Commands

`wg-quick up wg0`	Activate WireGuard interface `wg0`.
`wg-quick down wg0`	Deactivate WireGuard interface `wg0`.
`wg show`	Show current WireGuard status and configuration.
`wg show wg0`	Show configuration and status for interface `wg0`.
`wg genkey | tee privatekey`	Generate a private key and save it to `privatekey`.
`wg pubkey < privatekey | tee publickey`	Generate a public key from a private key and save it to `publickey`.

Configuration File Parameters

`[Interface]`	Section for interface-specific settings.
`PrivateKey = <private_key>`	Sets the private key for the interface.
`Address = 10.0.0.2/24`	Sets the IP address and subnet for the interface.
`ListenPort = 51820`	Sets the port WireGuard listens on.
`[Peer]`	Section for peer-specific settings.
`PublicKey = <public_key>`	Sets the peer's public key.
`AllowedIPs = 0.0.0.0/0`	Sets the allowed IPs for the peer. `0.0.0.0/0` allows all IPs.
`Endpoint = example.com:51820`	Sets the peer's endpoint (IP address and port).

Troubleshooting

Ensure that the WireGuard interface is active using `wg show wg0`. Check for any errors in the output.
Verify that the firewall allows UDP traffic on the specified port (default is 51820).
Use `tcpdump` or `wireshark` to capture and analyze network traffic to identify any connectivity issues.

IPsec VPN Configuration

StrongSwan Commands

`ipsec start`	Start the IPsec service.
`ipsec stop`	Stop the IPsec service.
`ipsec restart`	Restart the IPsec service.
`ipsec status`	Check the status of IPsec connections.
`ipsec up <connection_name>`	Initiate a specific IPsec connection.
`ipsec down <connection_name>`	Terminate a specific IPsec connection.

IPsec Configuration Files

`ipsec.conf`	Main configuration file for IPsec connections.
`ipsec.secrets`	File containing pre-shared keys or RSA private keys.
`left=%any`	Local IP address or identifier. `%any` means any address.
`right=192.168.1.1`	Remote IP address or identifier.
`auto=start`	Automatically start the connection when IPsec starts.
`keyexchange=ikev2`	Use IKEv2 key exchange protocol.
`ike=aes256-sha256-modp2048!`	IKE (Phase 1) encryption, hash, and DH group.
`esp=aes256-sha256!`	ESP (Phase 2) encryption and hash algorithm.

Troubleshooting

Check the IPsec logs for errors. These are typically located in `/var/log/auth.log` or `/var/log/syslog`.
Use `tcpdump` to capture packets and analyze the IKE and ESP exchanges.
Verify that the firewall rules allow UDP ports 500 and 4500 for IKE and NAT-T traffic, respectively.

Network Utility Commands

Basic Network Commands

`ping <host>`	Test network connectivity to a host.
`traceroute <host>`	Trace the route packets take to reach a host.
`ifconfig` or `ip addr`	Display network interface configuration.
`netstat -rn` or `ip route`	Display the routing table.
`nslookup <host>`	Query DNS to find the IP address of a host.
`tcpdump -i <interface> <filter>`	Capture network traffic on a specific interface with a filter.

VPN-Specific Network Checks

`ifconfig tun0` or `ip addr show tun0`	Check the configuration of the TUN interface (OpenVPN).
`ifconfig tap0` or `ip addr show tap0`	Check the configuration of the TAP interface (OpenVPN).
`wg show wg0`	Check the status of the WireGuard interface.
`ping -I tun0 <ip_address>`	Ping a host using the TUN interface.
`traceroute -i tun0 <ip_address>`	Trace the route via the TUN interface.

Firewall Commands (iptables)

`iptables -L` - List current iptables rules.
`iptables -A INPUT -i tun0 -j ACCEPT` - Allow traffic from the TUN interface.
`iptables -A FORWARD -i tun0 -j ACCEPT` - Forward traffic through the TUN interface.
`iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE` - Enable NAT for VPN traffic.
`iptables -P FORWARD DROP` - Set default forward policy to DROP.