**Enterprise-Class Security Considerations**

Develop virtual private network (VPN) usage and security policies to the exact scale and scope of the network.

Ensure that only approved individuals and authorized third-parties access and use the VPN service by performing the following:

* Establish strong authentication mechanisms. For example, token devices, private keys, or passphrases.
* Establish VPN usage restrictions, like who may use it and how it may be used.
* Force VPN traffic through the VPN tunnel and drop all other traffic.
* Enforce strong password selections and idle user logon timeouts.
* Enforce strict VPN client usage and maintain updates on mandatory security software (that is, antivirus.)

Remember to notify remote users that they are subject to the company’s network rules and regulations. Develop a roadmap to check, recheck, configure, update, and service VPN components as per the schedule. VPN policies cover everything from security practices to maintenance routines.

**Define Users, Groups, and Access Rights**

Ask important questions about who can use the VPN, how they can use it, and what to track and record when they use it. Your VPN policy should generally address every foreseeable usage scenario, user behavior, and unauthorized activity. Start with highpoints and drill down into the specifics. Define acceptable behavior and develop procedures and processes for enforcing compliance and handling violations. Some considerations are:

* The types of users and groups who may remotely access the network:
	+ Employees who work from home and need to access the company intranet.
	+ Server administrators who often need to update and make changes on their server machines remotely.
	+ Branch office workers who need a secure connection to the main office intranet.
	+ Off-site contractors working on a project with company personnel.
* Servers, services, and systems that remote workers should be able to access:
	+ VPN servers must be authorized by the network administrator.
	+ Administrators must restrict access to internal resources for VPN users; for example, contractors have access only to specific project folders.
* Permissible and impermissible user and group behaviors
	+ Policy should state that non-company related use of computers with VPN clients is prohibited; the VPN user is responsible for all activities that originate from his or her computer or logon account.
	+ VPN users are responsible for the physical security of their computers.
	+ VPN users are responsible for keeping anti-malware software on their computers up to date.
	+ VPN users must follow all rules established for company network access.
	+ VPN users must report any security incidents to the company security department within a specific time period of detection.
	+ VPN users must create strong passwords and change them every 90 days, when prompted.
	+ All VPN usage will be monitored and logged. Policy violations by VPN users will be handled on a case-by-case basis. Repeat violations may result in the suspension of access.
* Time-of-day restrictions or enforcement of idle user timeouts:
	+ Limit VPN usage to a specific range of hours, such as between 8 a.m. and 5 p.m.
	+ Configure the VPN server to disconnect connections that have been idle for a period of time; such as 30 minutes, 1 hour, and so on.

**Policies, Standards, and Guidelines**

Policies outline specific requirements that cover high-level points, such as acceptable use policies that cover rules and regulations for using systems and networks.

Standards comprise system-specific or procedural requirements all users must practice when using the systems, services, and networks.

Guidelines specify systematic or procedural suggestions that are not strict requirements but instead best practices. Effective policies are built on standards and guidelines applicable to the organization.

Federal regulations and industry practices often factor into the standards and guidelines upon which policies are built. Governmental laws regulate how sensitive data is processed, stored, and transmitted. Laws may mandate certain levels of security and assurances that appropriate measures are taken to safely handle sensitive information. Industry practices are built on experience and best practices that are applicable to a particular process or procedure.

**Usability Concerns and Usage Models**

VPN clients and servers must use compatible protocols and software for connectivity. Network administrators must also establish minimum and maximum thresholds for user tunnel connections so that all users can access the VPN without consuming all available bandwidth.

User reservation model (per concurrent user per tunnel): Specific tunnel speeds (e.g., 56K, 128K, 256K, and 384K), increments of concurrent users (i.e., 10 concurrent users at 1,000 concurrent maximum), same size tunnels within a given domain.

Bandwidth reservation model (per user): Reserve bandwidth among multiple users, 1Mbps increments up to a maximum 45Mbps per port, maximum 1,000 concurrent sessions per instance, and maximum tunnel size with Transmission Control Protocol (TCP) control flow rates as new users connect (tunnel balancing).