Cisco CCNP Security (350-701 SCOR) Ports Sheet

High-yield ports and services for AAA, monitoring, VPN, secure management, and visibility workflows.

Best for	Focus	Use with
Fast port memorization	Port / protocol / service / use case	Use with commands sheet and quick summary

Port	Protocol	Name	Use case
22	TCP	SSH	Secure CLI management
49	TCP	TACACS+	Admin AAA for network devices
53	TCP/UDP	DNS	Resolution and policy dependency
67/68	UDP	DHCP	Addressing and onboarding
80	TCP	HTTP	Legacy web and proxy baseline
88	TCP/UDP	Kerberos	Authentication in AD-backed environments
123	UDP	NTP	Time sync for logs and auth
161/162	UDP	SNMP	Monitoring and traps
389	TCP/UDP	LDAP	Directory services
443	TCP	HTTPS	Secure web/API/management
445	TCP	SMB	File transfer / admin contexts
514	UDP	Syslog	Centralized log forwarding
636	TCP	LDAPS	Secure LDAP
830	TCP	NETCONF	Secure config management over SSH
1812/1813	UDP	RADIUS	Network access AAA
500	UDP	IKE	VPN negotiation
4500	UDP	IPsec NAT-T	IPsec through NAT
1194	UDP/TCP	OpenVPN	Common VPN reference point
3389	TCP	RDP	Remote desktop
5060/5061	UDP/TCP	SIP	Voice signaling

Exam traps

1812/1813 vs 49	RADIUS commonly supports access auth; TACACS+ is a classic device-admin protocol.
500 vs 4500	IKE negotiation differs from NAT-T data path handling in IPsec scenarios.
22 vs 443	SSH and HTTPS can both be management channels, but they solve different admin workflows.
514 UDP	Syslog is often UDP-based, so delivery assurance is different from session-based protocols.