

Portsperrern

Basierend auf dem Sicherheitskonzept von [BelWü](#) wurde Ende 2001 eine Liste von Services zusammengestellt, die ein Sicherheitsrisiko darstellen und daher auf der Firewall gesperrt wurden. Es handelt sich um Services, die darüber hinaus entweder

1. nicht über die Grenzen einer Organisation angeboten werden sollten, oder
2. durch sicherere Services ersetzt werden können, oder
3. durch Modifikation (z.B. Tunneling) weiter verwendet werden können.

Überblick über die **zwischen dem TUNET und dem Internet** gesperrten Ports:

Transport	Port	Protokoll	Beschreibung	Richtung
ICMP	-	ping	Echo request	von außen
IP protocol 41	-	IP in IP Tunneling	IPv6-Tunnelverfahren wie 6to4 und ISATAP	beide
UDP,TCP	7	echo	Echo Service	von außen
UDP,TCP	9	discard	Discard Service	von außen
TCP	25	SMTP	Simple Mail Transfer Protocol - E-Mail-Transport	von außen *)
UDP,TCP	53	DNS	Domain Name System - Nameservice	von außen
UDP	67	BOOTPS	Boot Strap Protocol Server, DHCP	beide
UDP	68	BOOTPC	Boot Strap Protocol Client, DHCP	beide
UDP	69	TFTP	Trivial Filetransfer Protocol (ohne Passwort)	von außen
UDP,TCP	111	ONC RPC	(Sun RPC) Portmapper (u.a. für NFS)	beide
UDP	123	NTP	Network Time Protocol - Time Services	von außen
UDP,TCP	135	msrpc	Microsoft Remote Procedure Call	beide
UDP,TCP	136	Profile Name Service	keine legitime Anwendung mehr	beide
UDP,TCP	137-139	NETBIOS via TCP	SMB (Server Message Block) - Datei- und Druckerservice	beide
UDP,TCP	161-162	SNMP	Netz-Management	beide
UDP,TCP	177	XDMCP	X Display Manager Control Protocol	beide
UDP,TCP	445	Microsoft-DS	Microsoft Directory Service (SMB over IP, CIFS) - Datei- und Druckerservice	beide
TCP	512	rexec	R-Kommandos (Remote Exec)	von außen
TCP	513	rlogin	R-Kommando (Remote Login)	von außen
				von

UDP	514	syslog	System Logging Service	außen
TCP	514	rsh, rcp, rdump, rrestore, rdist	R-Kommandos (Remote Shell, Copy, Dump, Distribution)	von außen
TCP	515	lpd	Line Printer Daemon - Druckerservice	von außen
TCP	540	UUCP	Unix to Unix Copy Protocol - u.a. E-Mail-Transport	von außen
TCP	1080	SOCKS	Anwendungsproxy	von außen
UDP	1434	SSRS	SQL Server Resolution Service	beide
UDP,TCP	1900	SSDP	Simple Service Discovery Protocol	von außen
UDP,TCP	2049	NFS	Network Filesystem (andere Ports möglich) - Dateiservice	beide
TCP	3128	Squid	Web-Proxy	von außen
UDP	3544	Teredo	Kapselung von IPv6-Datenpaketen in IPv4-UDP-Datenpaketen	beide
UDP,TCP	4045	lockd	NFS Lock Manager - Dateiservice	beide
UDP,TCP	5000	UPnP	Universal Plug and Play Service	von außen
TCP	6000-6063	X11	X Window Display Server (X-Terminal)	beide
UDP,TCP	9100	PDL	Page Description Language - Druckerservice wie z.B. JetDirect	beide

*) Einkommende Mails werden über den [Mailbastionsrechner](#) geleitet.
([Fremddomains mit TU Wien Mailserver](#) können eben so durch die Mailbastion behandelt werden)

Behandlung von externen Zugängen zum TUNET (TU-ADSL, xDSL@student, VPN, Hörsäle, WLAN):

- Abgehender Verkehr wie in der obenstehenden Tabelle.
- Aus dem Internet kommender Verkehr ist gesperrt. Ausgenommen ist - wegen interuniversitär eingerichteter Studien - SSH von den Studentenarbeitsplätzen der Universität Wien.