

LU:s centrala brandvägg

Det finns en read-only-vy på <https://fw ldc.lu.se>. Dock måste man ha:

1. konto där
2. ange vilka IP-adresser som skall kunna komma åt sidan
3. Lucat-behörigheten "Brandväggsadministratör"

Brandväggsverktyget läser in sin information var 15:e minut

Man ändrar brandväggsreglerna via [servicedesken](#) (tjänster → Brandväggsregler).

Vid NetInfo 2024-11-20 meddelades att man strävar mot att integrera visningen av brandväggsregler i NetTools. Tidplan angavs dock inte.

Regelverk

LU:s [regler för brandväggar](#) står bl.a.:

- Brandvägg ska finnas och vara aktiverad för varje VLAN
- Följande generella regler gäller:
 - utgående trafik tillåts (och svar på denna tillåts in)
 - ingen datatrafik tillåts in, dock:
 - servernät tillåts ha nödvändiga portar öppna
 - tjänstenät tillåts endast ha de portar öppna som krävs för att tjänsterna skall fungera
 - Alla nät ska tillåta ping från hela LUNET
 - öppningar i brandväggen ska minimeras till minsta antal portar öppna mot minsta antalet datorer
 - tjänster som tillåter inloggning på klientdatorer (t.ex. RDP) ska inte vara öppna för hela Internet, utan kravet är att användaren alltid först ska behöva koppla upp sig med VPN

VLAN 666: externt nåbara maskiner

Rapport baserat på LU:s brandväggsverktyg

(<https://fw ldc.lu.se/index.php?key=XxXxXxX&vlan=666&lookup=yes>)

2025-05-16

Nedan finns alla enheter i VLAN 666 som har Src Addr = any:

Regel	CNAME	Port 22	Port 80	Port 443	Övriga portar	Kontaktperson
4636	bjornix		■	■	tcp_8000-8100	Björn R
5148	coursegit	■	■	■		
5305	dokuwiki		■	■		
4671	forsete		■	■		Jonas S
5760	git	■	■	■		
6803	jonassmini			■		Jonas S
6534	kojo		■	■	tcp_8080, tcp_8880	Björn R
5482	llb755		■	■	tcp_8880	
4717	login	■				
4663	logo		■	■		
4628	miao		■	■		Jakob N
5338	moodle		■	■		
4954	mystery		■	■		Christoph R
4708	perforce				tcp_1666	Lars B
6545	sam		■	■		
4658	vilde		■	■		
3939	web	■	■	■		

Gemensamma LTH-nät

LDC delar in nät i tre kategorier:

- **gröna nät**: publika nät
- **gula nät**: NAT (privat)
- **orange nät**: helt stängda för Internet (möjligt att öppna för LU)

Publika nät

Fysiska servrar

576-LTH-Green

130.235.93.64/26, 62 adresser

ID	Source	Destination	DNS CNAME	Service	Comments	Ärenden
----	--------	-------------	-----------	---------	----------	---------

ID	Source	Destination	DNS CNAME	Service	Comments	Ärenden
6917	ag_lunet	h_130.235.93.71	filemaker	tcp_80, tcp_443, tcp_5003		
7562	h_130.235.148.212	n_130.235.93.64/26		tcp_1500	tsm4	TICIT0143476
7569	ag_cs_it	h_130.235.93.71	filemaker	tcp_22, tcp_443, tcp_80		TICIT0143476

VM

404-LTH-Green

130.235.93.0/26, 62 adresser

ID	Source	Destination	DNS CNAME	Service	Comments	Ärenden
7528	ag_vpn	h_130.235.93.11	llb755	tcp_22		CHG0168018, CHG0189776, TICIT0143476
7530	all	h_130.235.93.11	llb755	tcp_443, tcp_80, tcp_8880		CHG0170473, CHG0199559, TICIT0143476
7531	all	h_130.235.93.12	moodle	tcp_443, tcp_80		CHG0159997, TICIT0143476
7533	ag_it_ldc-kah	h_130.235.93.13	git	tcp_2222.		TICIT0129149, TICIT0129150, TICIT0143476
7535	all	h_130.235.93.13	git	tcp_22, tcp_80_443	Git	TICIT0143476
7536	h_10.5.119.4 (runner)	h_130.235.93.13	git	tcp_22, tcp_443	Git	TICIT0143476
7537	all	h_130.235.93.14	sam	tcp_80, tcp_443		TICIT0084400, TICIT0143476
7538	ag_it_ldc-kah	h_130.235.93.15	coursegit	tcp_2222		TICIT0129149, TICIT0129150, TICIT0143476
7539	all	h_130.235.93.15	coursegit	tcp_22, tcp_443, tcp_80	coursegit	TICIT0143476
7540	h_10.5.119.4 (runner)	h_130.235.93.15	coursegit	tcp_22, tcp_443		CHG0198662, TICIT0005740, TICIT0143476
7570	ag_cs_it	h_130.235.93.15 h_130.235.93.11 h_130.235.93.12 h_130.235.93.13 h_130.235.93.14	coursegit llb755 moodle git sam	tcp_22, tcp_443, tcp_80, tcp_2222		TICIT0143476, TICIT0146185

NAT-nät

Fysiska servrar

538-LTH-Yellow
10.5.103.0/24, 256 adresser

ID	Source	Destination	DNS CNAME	Service	Comments	Ärenden
4902 5970	10.5.119.16 (lmon762)	h_10.5.103.13	almon2056.srv.lu.se / "monitor"	tcp_22	Innehåller även 130.235.16.20 (regel 5970; skall tas bort i höst)	TICIT0146993
7541	n_10.0.17.0/24 (651 - a190-cs-protected), n_10.5.113.0/24 (570- LTH-Orange, Physical), n_10.5.119.0/24 (584- LTH-Yellow, VM), n_10.5.127.0/24 (821- LTH-Orange, VM), n_130.235.11.64/26 (653 - a190-cs-iot), n_130.235.148.208/28 (652 - h001-srv-652; backup), n_130.235.16.0/23 (666 - a190-cs-lth-se), n_130.235.88.192/26 (686 - a190-exjob-cs- lth-se), n_130.235.93.0/26 (404-LTH-Green, VM), n_130.235.93.64/26 (576-LTH-Green, Physical)	h_10.5.103.11	logger	tcp_6514	Logger	TICIT0143476
7542	ag_lunet	h_10.5.103.12	lagring3	tcp_139, tcp_445	fildelning till lagring3	TICIT0143476
7543	h_130.235.148.212 (tsm4)	h_10.5.103.12	lagring3	tcp_22		CHG0193560, TICIT0143476
7544	ag_lunet	h_10.5.103.13	monitor	tcp_443	monitor	TICIT0143476
7545	ag_lunet	h_10.5.103.14	dokuwiki	tcp_80, tcp_443		CHG0157865, TICIT0143476
7546	ag_vpn	h_10.5.103.15	sde-algol	tcp_22		TICIT019640, TICIT0143476

ID	Source	Destination	DNS CNAME	Service	Comments	Ärenden
7547	ag_cs_it	h_10.5.103.16, h_10.5.103.17, h_10.5.103.18, h_10.5.103.19, h_10.5.103.20, h_10.5.103.21, h_10.5.103.22, h_10.5.103.23, h_10.5.103.24, h_10.5.103.25, h_10.5.103.26, h_10.5.103.27	semantica001, semantica002, semantica003, semantica004, semantica005, semantica007, semantica008, semantica009, semantica010, semantica012, semantica013, semantica014	tcp_22, tcp_443, tcp_80	semantica001-014	TICIT0143476
7560	h_130.235.148.212 (tsm4)	n_10.5.103.0/24	VLAN 538	tcp_1500	tsm4	TICIT0143476
7571	ag_cs_it	h_10.5.103.11 h_10.5.103.12 h_10.5.103.13 h_10.5.103.14 h_10.5.103.15	logger lagring3 monitor dokuwiki sde-algol	tcp_22, tcp_443, tcp_80		TICIT0143476

VM

584-LTH-Yellow

10.5.119.0/24, 256 adresser

ID	Source	Destination	DNS CNAME	Service	Comments	Ärenden
7548	n_10.0.16.0/24 (a190-cs-client), ag_vpn	h_10.5.119.11	moodle-test	tcp_443		CHG0167629, TICIT0057671, TICIT0143476
7549	n_10.0.16.0/24 (a190-cs-client)	h_10.5.119.12	git-test	tcp_80, tcp_443	git-test	TICIT0143476
7550	ag_it_ldc-kah	h_10.5.119.12 h_10.5.119.13	git-test coursegit-test	tcp_2222		TICIT0129149, TICIT0129150, TICIT0143476
7551	n_10.0.16.0/24 (a190-cs-client)	h_10.5.119.13	coursegit-test	tcp_22, tcp_443	coursegit-test	TICIT0143476
7554	ag_it_op5_servers	h_10.5.119.13	coursegit-test	icmp_ping, tcp_161, udp_161	OP5 övervakning	CHG0174359, TICIT0143476
7555	ag_vpn	h_10.5.119.14	sam-test	tcp_80_443	samtest	CHG0193929, TICIT0143476
7556	h_130.235.16.4 (llb755), h_130.235.93.11 (llb755, ny IP)	h_10.5.119.15	jobe2	tcp_80	jobe2	TICIT0143476, TICIT0145749
7557	ag_cs_it	h_10.5.119.16	monmon	tcp_22, tcp_443, tcp_80	monmon	TICIT0143476
7572	ag_cs_it	h_10.5.119.11 h_10.5.119.12 h_10.5.119.13 h_10.5.119.14 h_10.5.119.15	moodle-test git-test coursegit-test sam-test jobe2	tcp_22, tcp_443, tcp_80, tcp_2222		TICIT0143476, TICIT0146183

ID	Source	Destination	DNS CNAME	Service	Comments	Ärenden
????	130.235.16.5 (moodle)	h_10.5.119.11	moodle-test	tcp_22		TICIT0147338
????	130.235.10.164	10.5.119.16	monmon	tcp_22	För DNS-överföring	TIC

Skyddade nät

Fysiska servrar

570-LTH-Orange
10.5.113.0/24, 256 adresser

Skyddat LTH-nät

[Detta nät **kan inte** öppnas mot internet (varken inkommande eller utgående)]

ID	Source	Destination	DNS CNAME	Service	Comments	Ärenden
7558	ag_vpn, ag_cs_cs-jsk, ag_cs_it	h_10.5.113.11, h_10.5.113.12, h_10.5.113.13, h_10.5.113.14	power, power2, power8, power9	tcp_22	power	TICIT0143476
7561	h_130.235.148.212 (tsm4)	n_10.5.113.0/24	VLAN 570		tsm4	TICIT0143476
7573	ag_cs_it	h_10.5.113.11, h_10.5.113.12, h_10.5.113.13, h_10.5.113.14	power, power2, power8, power9	tcp_22, tcp_443, tcp_80		TICIT0143476

Skyddat LTH-nät, VM

821-LTH-Orange
10.5.127.0/24, 256 adresser

Skyddat LTH-nät

[Detta nät **kan inte** öppnas mot internet (varken inkommande eller utgående)]

Övriga VLAN

475 - IPMI

ID	Source	Destination	DNS CNAME	Service	Comments	Ärenden
7559	ag_cs_it	h_172.20.18.21	logger-bmc	tcp_80, tcp_443		TICIT0143476
7559	ag_cs_it	h_172.20.18.22	monitor-bmc	tcp_80, tcp_443		TICIT0143476

From:
<https://dokuwiki.cs.lth.se/> - **Datavetenskaps dokuwiki**

Permanent link:
https://dokuwiki.cs.lth.se/doku.php?id=lunds_universitet:natverk:firewall&rev=1761119254

Last update: **2025-10-22 07:47**

