abc_new

checkpoint-demo

checkpoint-demo

Number	Name	Source	Destination	Services	Action	Track	Disabled	UID	Comment
1 DEBUG: 5000		Cactus-extern@ vpn-sources-IsoAAAA	gateway.local (10.222.0.19/32) IsoAAADray.local (10.222.0.15/32)	http (80/TCP) domain-udp (53/UDP) ntp-udp (123/UDP) rdp (3389/TCP) CIFS	client encrypt	Log		IsoAAAA__uid__4D877153-65A8-48A9-9D11-B30CA56946EF	
2 DEBUG: 6000		IsoAAAG-g@ vpn-sources-IsoAAAA	scratchy.local (10.222.0.16/32)	RAdmin-custom (60000/TCP)	client encrypt	Log		IsoAAAA__uid__AC6B21DA-86AF-4EB3-B294-3387F815E66E	
3 DEBUG: 7000		IsoAAAG-g@ vpn-sources-IsoAAAA	Any (0.0.0.0/0)	HBCI (3000/TCP) T-online-classic (866/TCP)	client encrypt	Log		IsoAAAA__uid__5289C1E3-9679-4537-AFD3-AA8663CA5F39	
4 DEBUG: 8000		Cactus-extern@ vpn-sources-IsoAAAA	mg.IsoAAAA-es.com (10.222.0.11/32) spike.local (10.222.0.50/32)	imaps (993/TCP) imap (143/TCP) squid (3128/TCP)	client encrypt	Log		IsoAAAA__uid__73F2144F-4C58-4361-94B5-459B469A6541	
5 DEBUG: 9000		Cactus-extern@ vpn-sources-IsoAAAA	itchy (10.222.0.10/32)	smtp (25/TCP)	client encrypt	Log		IsoAAAA__uid__6ADC5431-5B24-47FC-A9A6-F8DC912B0515	
6 DEBUG: 10000		Cactus-extern@ vpn-sources-IsoAAAA	wasp (10.222.0.9/32)	ntp-udp (123/UDP)	client encrypt	Log		IsoAAAA__uid__09847FA8-6AD8-4196-A6BA-C2E5A4380CAF	
7 DEBUG: 11000		Cactus-extern@ vpn-sources-IsoAAAA	sol8 (10.222.0.55/32) hpux (10.222.0.41/32) wasp (10.222.0.9/32)	ftp (21/TCP) ssh (22/TCP) telnet (23/TCP)	client encrypt	Log		IsoAAAA__uid__67784DF8-6440-4F4A-891C-C7062E0F32B0	

8 DEBUG: 12000		Cactus-extern@ vpn-sources-IsoAAAA	IsoAAAA-100 (10.222.0.35/32)	icmp-requests	client encrypt	Log		IsoAAAA__uid__C6951C02-A10A-4757-A85F-5C197D6B95EB	
9 DEBUG: 15000		SonicLAN (10.222.0.67/32)	IsoAAAA-100 (10.222.0.35/32)	Any	encrypt	Log		IsoAAAA__uid__1B421F3A-CCFB-4816-B5D0-2D69F5D98DC3	
10 DEBUG: 16000		IsoAAAA-100 (10.222.0.35/32)	Sonic1 (10.222.0.59/32) SonicLAN (10.222.0.67/32)	Any	encrypt	Log		IsoAAAA__uid__7F7BEC1D-4972-4E6B-9F74-2808D5D82A44	
11 DEBUG: 18000		IsoAAAA-100 (10.222.0.35/32) IsoAAAA_home_tim (10.222.0.38/32) mg.IsoAAAA-es.com (10.222.0.11/32)	IsoAAAD (10.222.0.63/32)	https (443/TCP) ssh (22/TCP)	accept	Log		IsoAAAA__uid__EACACDFF-02E7-4014-9DA7-1A5487AB8481	
12 DEBUG: 19000		IsoAAAA-100 (10.222.0.35/32) IsoAAAA_home_tim (10.222.0.38/32)	daba (10.222.0.36/32)	mysql (3306/TCP) ssh (22/TCP)	accept	Log		IsoAAAA__uid__C5F973E3-CBB2-4C15-A735-52B51AC9DAE7	
13 DEBUG: 20000		IsoAAAD (10.222.0.63/32)	mg.IsoAAAA-es.com (10.222.0.11/32) wasp (10.222.0.9/32)	ntp-udp (123/UDP)	accept	None		IsoAAAA__uid__0D4D75A0-8203-453F-9C3E-F68E1995DE88	
14 DEBUG: 21000		IsoAAAD (10.222.0.63/32)	IsoAAADray.local (10.222.0.15/32)	domain-udp (53/UDP)	accept	None		IsoAAAA__uid__A1ACBE88-9F38-4947-B497-B34A2F3878B3	
15 DEBUG: 22000		IsoAAAD (10.222.0.63/32)	mg.IsoAAAA-es.com (10.222.0.11/32) spike.local (10.222.0.50/32)	smtp (25/TCP) domain-udp (53/UDP) ssh_version_2 (22/TCP) syslog (514/UDP)	accept	Log		IsoAAAA__uid__321D1155-8DB8-48D3-8F89-789456335EA5	
16 DEBUG: 24000		IsoAAAA-100 (10.222.0.35/32)	ras.IsoAAAA-es.com (10.222.0.57/32) mg.IsoAAAA-es.com (10.222.0.11/32) spike.local (10.222.0.50/32)	SpikeServices	accept	Log		IsoAAAA__uid__F18D892E-EED1-488B-A0D9-832B742CE27B	
17 DEBUG: 26000		IsoAAAA-100 (10.222.0.35/32)	Cactus-DMZ4 (10.222.0.65/32) Cactus-DMZ2 (10.222.0.43/32) Cactus-DMZ1 (10.222.0.22/32)	sshv2-24 (24/TCP) ssh_version_2 (22/TCP)	accept	Log		IsoAAAA__uid__00477CC9-4940-4C79-B2E6-A137781B1C25	
18 DEBUG: 27000		IsoAAAA-100 (10.222.0.35/32)	Cactus10.222.0.1 (10.222.0.1/32)	VNC (5900/TCP)	accept	Log		IsoAAAA__uid__2CDC82FD-6292-45D7-A4B8-6794C378A47B	

19 DEBUG: 28000		IsoAAAA-100 (10.222.0.35/32)	itchy (10.222.0.10/32)	CIFS domain-udp (53/UDP)	accept	Log	IsoAAAA__uid__8EDEBE48-F02B-4AEA-8337-FBE1E2079BE0	
20 DEBUG: 29000		IsoAAAA-100 (10.222.0.35/32)	MailServer	smtp (25/TCP)	accept	Log	IsoAAAA__uid__0F6D252E-7562-457F-81A3-60192F3EC815	
21 DEBUG: 30000		IsoAAAA-100 (10.222.0.35/32)	mg.IsoAAAA-es.com (10.222.0.11/32) wasp (10.222.0.9/32)	ntp-udp (123/UDP)	accept	None	IsoAAAA__uid__A3B9D85B-AD6D-4991-8A9D-960939C491C2	
22 DEBUG: 32000		IsoAAAA-100 (10.222.0.35/32)	Any (0.0.0.0/0)	HBCI (3000/TCP) T-online-classic (866/TCP)	accept	Log	IsoAAAA__uid__E6AB0ADC-7E23-4B1D-B568-E47FF7B3D4F5	
23 DEBUG: 33000		Cactus-extern@ IsoAAAA-100 (10.222.0.35/32)	Any (0.0.0.0/0)	TeamSpeak (8767/UDP) ssh_version_2 (22/TCP)	client auth	Log	IsoAAAA__uid__F2D50B88-90A6-4BF1-A0F9-724F4FF20600	
24 DEBUG: 34000		IsoAAAA-100 (10.222.0.35/32)	t-onlineUpdate	https (443/TCP) http (80/TCP)	accept	Log	IsoAAAA__uid__1F4E5C97-C290-48AF-84A5-C1A13178FDB7	
25 DEBUG: 35000		IsoAAAA-100 (10.222.0.35/32)	LSYI-pptp (10.222.0.49/32) auth1.lhsystems.com (10.222.0.48/32)	PPTP FW1_clntauth_telnet (259/TCP)	accept	Log	IsoAAAA__uid__8D43F752-841E-4B9E-B610-635F7C17D4D9	
26 DEBUG: 36000		speedy2 (10.222.0.44/32)	mail.light-life.net (10.222.0.62/32) mail.light-life.netOld (10.222.0.61/32)	pop-3 (110/TCP) smtp (25/TCP)	accept	Log	IsoAAAA__uid__167BC623-43EB-405D-BC29-442298C96DC9	
27 DEBUG: 38000		mg.IsoAAAA-es.com (10.222.0.11/32)	gateway.local (10.222.0.19/32) IsoAAADray.local (10.222.0.15/32)	UPS-Monitor (7000/TCP) CIFS http (80/TCP) rdp (3389/TCP)	accept	Log	IsoAAAA__uid__A8A57015-68D5-4341-ADD1-895EC21419DB	
28 DEBUG: 39000		mg.IsoAAAA-es.com (10.222.0.11/32)	scratchy.local (10.222.0.16/32)	RAdmin-custom (60000/TCP)	accept	Log	IsoAAAA__uid__5DEBDFAA-F691-4041-8E3A-EAF002F8B690	
29 DEBUG: 40000		mg.IsoAAAA-es.com (10.222.0.11/32)	daba (10.222.0.36/32)	ssh_version_2 (22/TCP) mysql (3306/TCP)	accept	Log	IsoAAAA__uid__DC9D47B1-CEB2-43AB-B32E-5BFACD49181F	

30 DEBUG: 41000		mg.IsoAAAA-es.com (10.222.0.11/32)	hpux (10.222.0.41/32)	telnet (23/TCP)	accept	Log		IsoAAAA__uid__B706F7FA-C0AA-41E6-9BE1-99FAA2073339	
31 DEBUG: 42000		mg.IsoAAAA-es.com (10.222.0.11/32) ITSecOrg-dev (10.222.0.66/32)	SecOVID_Authserver (10.222.0.60/32)	NEW-RADIUS (1812/UDP)	accept	Log		IsoAAAA__uid__FFAB5EA6-1C92-49CA-B971-6739815B346B	
32 DEBUG: 43000		Cactus10.222.0.1 (10.222.0.1/32)	IsoAAADray.local (10.222.0.15/32)	http (80/TCP)	accept	Log		IsoAAAA__uid__2B48CB5C-959B-4212-83BA-D0C31C9E81FD	SUS-Access 4 Stichling
33 DEBUG: 44000		wlan-router (10.222.0.17/32)	IsoAAADray.local (10.222.0.15/32)	domain-udp (53/UDP)	accept	Log		IsoAAAA__uid__A4D7B2E7-4461-41FD-BBFB-F7A4738CE081	WLAN-DNS
34 DEBUG: 46000		Any (0.0.0.0/0)	Any (0.0.0.0/0)	ICMPgute	accept	Log		IsoAAAA__uid__E079D5BF-271E-4004-B4C5-8372C37B4661	
35 DEBUG: 47000		IsoAAAD (10.222.0.63/32)	Any (0.0.0.0/0)	redirect	accept	Log		IsoAAAA__uid__89F7C56B-1A5F-4C4A-BC98-F777664BBEC9	
36 DEBUG: 48000		IsoAAAA-100 (10.222.0.35/32)	Any (0.0.0.0/0)	Drop_nologServices	reject	None		IsoAAAA__uid__F134ED1C-8FC1-4ED1-9751-39EE88C79BAA	
37 DEBUG: 49000		IsoAAAA-100 (10.222.0.35/32)	Drop_nologDest	Any	reject	None		IsoAAAA__uid__7067EE72-61D1-4555-9832-8E9279772BCA	
38 DEBUG: 50000		CactusDA	Any (0.0.0.0/0)	Any	reject	Log		IsoAAAA__uid__A6F53BCD-748C-4585-B8FB-1DF23129F085	
39 DEBUG: 51000		Any (0.0.0.0/0)	Any (0.0.0.0/0)	Any	drop	Log		IsoAAAA__uid__9CD8CE05-32DB-483A-A44A-0C9131CCA022	

fortigate-test

fortigate-test

Number	Name	Source	Destination	Services	Action	Track	Disabled	UID	Comment
1 DEBUG: 0		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99001	

#	Name	Source	Destination	Service	Action	Log		ID	Comment
2 DEBUG: 1000	vpn_Cactus-DA_remote	Cactus-DA_remote	Cactus-DA_local	PING	accept	all		52	2020-11-01 14:45:01.094135
3 DEBUG: 2000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99002	
4 DEBUG: 3000	guest2inet	all (0.0.0.0/0)	all (0.0.0.0/0)	ALL	accept	none		72	guest2internet
5 DEBUG: 4000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99003	
6 DEBUG: 5000	gameserver ubuntu updates	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	extras.ubuntu.com (0.0.0.0/0) de.archive.ubuntu.com (0.0.0.0/0) security.ubuntu.com (0.0.0.0/0)	HTTPS (443/TCP) HTTP (80/TCP) PING	accept	none		20	ubuntu updates
7 DEBUG: 6000	temp steam update	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	all (0.0.0.0/0)	steam-tcp-27015-27020 (27015/TCP) valve_ports steam-udp-27000-27050 (27000/UDP) PING HTTPS (443/TCP) HTTP (80/TCP)	accept	none		42	temp rule 2nd line 3rd line +4th line
8 DEBUG: 7000	ARK - temp test 2017-02-17	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	all (0.0.0.0/0)	ARK-7777-7778-udp (7777/UDP) ARK-7777-7778-tcp (7777/TCP) udp-high-ports (1024/UDP)	accept	none		75	Clone of temp steam update
9 DEBUG: 10000	game-server to dns-inet	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	G-google-dns-srv fritzbox_10.0.0.24_global (10.0.0.24/32)	DNS	accept	none		21	dns
10 DEBUG: 11000	gameserver ntp	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	all (0.0.0.0/0)	NTP	accept	none		83	Clone of game-server to dns-inet
11 DEBUG: 12000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99004	
12									VPN: Cactus-DA (Created by VPN

#	Name	Source	Destination	Service	Action	Log		Count	Comment
12 DEBUG: 13000	vpn_Cactus-DA_local	Cactus-DA_local	Cactus-DA_remote	ALL	accept	none		50	VPN: Cactus-DA (Created by VPN wizard)
13 DEBUG: 14000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99005	
14 DEBUG: 15000	game server access	internal-10.0.0.35_24 (10.0.0.35/32) wlan_pi_10.0.0.53_24 (10.0.0.53/32)	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	ark-udp-32768-65535 (32768/UDP) steam-udp-27000-27050 (27000/UDP) PING SSH (22/TCP) minecraft-25565 (25565/TCP) ARK-7777-7778-udp (7777/UDP)	accept	all		4	internal to gameserver
15 DEBUG: 16000	udp high ports to ark	wlan_pi_10.0.0.53_24 (10.0.0.53/32) internal-10.0.0.35_24 (10.0.0.35/32)	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	udp-high-ports (1024/UDP)	accept	all		48	fucking ark server using dynamic ports for user sessions
16 DEBUG: 17000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99006	
17 DEBUG: 18000	internal to knappe	wlan_pi_10.0.0.53_24 (10.0.0.53/32) internal-10.0.0.35_24 (10.0.0.35/32) wlan_10.0.0.36_24 (10.0.0.36/32)	knappe_10.0.0.15 (10.0.0.15/32)	HTTP (80/TCP) SSH (22/TCP) SQUID (3128/TCP) tcp_8081_phpfreechat (8081/TCP) PING afp_548_tcp (548/TCP) SMB (445/TCP) HTTPS (443/TCP)	accept	all		5	knappe standard access
18 DEBUG: 19000	silently drop 139/tcp	internal-10.0.0.35_24 (10.0.0.35/32)	knappe_10.0.0.15 (10.0.0.15/32)	SAMBA (139/TCP)	deny	none		65	Clone of internal to knappe
19 DEBUG: 20000	internal to printer	internal-10.0.0.35_24 (10.0.0.35/32) wlan_pi_10.0.0.53_24 (10.0.0.53/32) wlan_10.0.0.36_24 (10.0.0.36/32)	drucker-10.0.0.38 (10.0.0.38/32)	ALL	accept	all		19	printing
20 DEBUG: 21000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99007	

21 DEBUG: 22000	quiet mail gware	all (0.0.0.0/0)	gware.cactus.de_10.0.0.43 (10.0.0.43/32)	IMAPS (993/TCP) HTTPS (443/TCP) SMTPS (465/TCP) PING	accept	none		33	silent mail@cactus
22 DEBUG: 23000		all (0.0.0.0/0)	klaut.cactus.de (0.0.0.0/0)	HTTPS (443/TCP) PING	accept	none		37	silent klaut.cactus.de
23 DEBUG: 24000	internal 2 dns	all (0.0.0.0/0)	opendns_10.0.0.48 (10.0.0.48/32) fritzbox_inet_10.0.0.24 (10.0.0.24/32)	PING DNS	accept	none		32	silent dns
24 DEBUG: 28000	LG Fernseher to LG	LG Fernseher 10.0.0.44 (10.0.0.44/32)	LG Server 10.0.0.45_24 (10.0.0.45/32)	HTTP (80/TCP)	accept	all		40	
25 DEBUG: 29000	LG Fernseher to Mediatheken	LG Fernseher 10.0.0.44 (10.0.0.44/32)	all (0.0.0.0/0)	NTP PING HTTPS (443/TCP) HTTP (80/TCP)	accept	all		41	
26 DEBUG: 30000	WLAN to Internet	wlan_pi_10.0.0.53_24 (10.0.0.53/32) fritzbox_oben_nat_10.0.0.18 (10.0.0.18/32) fb7240_10.0.0.55 (10.0.0.55/32)	all (0.0.0.0/0)	ALL	accept	all		39	Standard Access from wlan to internet
27 DEBUG: 31000	drop kids without fritzbox	internal-10.0.0.35_24 (10.0.0.35/32)	all (0.0.0.0/0)	ALL	deny	all		38	drop all traffic not passing fritzbox checks
28 DEBUG: 34000		fritzbox_oben_nat_10.0.0.18 (10.0.0.18/32)	www.avm.de (0.0.0.0/0)	tcp-8011-to-avm (8011/TCP)	accept	none		25	8011 to avm, nolog
29 DEBUG: 35000		all (0.0.0.0/0)	all (0.0.0.0/0)	tcp_40000_up (40000/TCP)	deny	all		35	block suspicious ports
30 DEBUG: 36000	block traffic to russia and india	all (0.0.0.0/0)	geo-russia (0.0.0.0/0)	ALL	deny	all		34	block suspicious geo dest

DEBUG: 36000		all (0.0.0.0/0)	geo-china (0.0.0.0/0)	ALL					
31 DEBUG: 38000	test ipv6 policy1	all (::/0)	all (::/0)	test_service_multi-port PING HTTPS (443/TCP) HTTP (80/TCP)	accept	all		ipv6.1	v6 comment
32 DEBUG: 40000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99008	
33 DEBUG: 41000	eltern-keller-2-knappe	eltern-keller-10.0.0.66_24 (10.0.0.66/32)	knappe_10.0.0.15 (10.0.0.15/32)	HTTP (80/TCP) SSH (22/TCP) SQUID (3128/TCP) tcp_8081_phpfreechat (8081/TCP) PING afp_548_tcp (548/TCP) SMB (445/TCP) HTTPS (443/TCP)	accept	all		80	Clone of internal to knappe
34 DEBUG: 42000	keller-printing	eltern-keller-10.0.0.66_24 (10.0.0.66/32)	drucker-10.0.0.38 (10.0.0.38/32)	ALL	accept	all		81	Clone of internal to printer
35 DEBUG: 43000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99009	
36 DEBUG: 44000	eltern keller to inet1	all (0.0.0.0/0)	gware.cactus.de_10.0.0.43 (10.0.0.43/32)	IMAPS (993/TCP) HTTPS (443/TCP) SMTPS (465/TCP) PING	accept	none		76	Clone of quiet mail gware
37 DEBUG: 45000	keller2inet-main	eltern-keller-10.0.0.66_24 (10.0.0.66/32)	all (0.0.0.0/0)	ALL	accept	all		78	Clone of WLAN to Internet
38 DEBUG: 46000	eltern2klautquiet	all (0.0.0.0/0)	klaut.cactus.de (0.0.0.0/0)	HTTPS (443/TCP) PING	accept	none		77	Clone of 37
39 DEBUG: 47000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99010	

40 DEBUG: 48000	wlan-kids auth	233.141.201.179 (233.141.201.179/32) 29.116.180.54 (29.116.180.54/32) 182.53.124.243 (182.53.124.243/32) 58.26.140.137 (58.26.140.137/32) 251.105.57.113 (251.105.57.113/32) 222.142.170.245 (222.142.170.245/32) 137.232.145.98 (137.232.145.98/32) 30.66.136.5 (30.66.136.5/32)	wifi-kids-wlan-router-ip (10.0.0.5/32)	fortinet-captive-portal-auth (1003/TCP)	accept	none		60	auth kids
41 DEBUG: 49000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99011	
42 DEBUG: 50000	wifikids2knappe	wlan-kids (10.0.0.62/32)	knappe_10.0.0.15 (10.0.0.15/32)	SMB (445/TCP) PING	accept	none		57	
43 DEBUG: 51000	wlankids2printer	wlan-kids (10.0.0.62/32)	drucker-10.0.0.38 (10.0.0.38/32)	ALL	accept	none		58	Clone of wifikids2serverlan
44 DEBUG: 52000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99012	
45 DEBUG: 53000	kids2internet	all (0.0.0.0/0)	all (0.0.0.0/0)	ALL	accept	none		56	
46 DEBUG: 54000	wlan-kids 2 dns	all (0.0.0.0/0)	fritzbox_inet_10.0.0.24 (10.0.0.24/32)	DNS	accept	none		59	
47 DEBUG: 55000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99013	
48 DEBUG: 56000	ping-back-connect-keller	drucker-10.0.0.38 (10.0.0.38/32)	eltern-keller-10.0.0.66_24 (10.0.0.66/32)	tcp_5357_samsung_printer (5357/TCP) PING	accept	none		79	Clone of samsung to print clients
49 DEBUG: 57000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99014	

50 DEBUG: 58000		drucker-10.0.0.38 (10.0.0.38/32) knappe_10.0.0.15 (10.0.0.15/32)	fritzbox_inet_10.0.0.24 (10.0.0.24/32)	DNS PING	accept	none		13	dns
51 DEBUG: 59000		drucker-10.0.0.38 (10.0.0.38/32) knappe_10.0.0.15 (10.0.0.15/32)	all (0.0.0.0/0)	NTP PING	accept	none		22	get time
52 DEBUG: 60000		knappe_10.0.0.15 (10.0.0.15/32)	qnap-update-akamai-10.0.0.42_24 (10.0.0.42/32) qnap_update_net_10.0.0.39/32 (10.0.0.39/32)	HTTP (80/TCP) PING	accept	none		23	qnap update
53 DEBUG: 61000	drop strange printer traffic	drucker-10.0.0.38 (10.0.0.38/32)	net_10.0.0.64_24 (10.0.0.64/32)	ALL	deny	none		43	strange printer requests
54 DEBUG: 62000	drop printer2google https	drucker-10.0.0.38 (10.0.0.38/32)	all (0.0.0.0/0)	HTTPS (443/TCP)	deny	none		68	2. drop strange printer traffic
55 DEBUG: 63000	qnap apps download	knappe_10.0.0.15 (10.0.0.15/32)	all (0.0.0.0/0)	PING HTTPS (443/TCP) HTTP (80/TCP)	accept	none		49	
56 DEBUG: 64000	knappe2gware	knappe_10.0.0.15 (10.0.0.15/32)	gware.cactus.de_10.0.0.43 (10.0.0.43/32)	SMTPS (465/TCP)	accept	none		67	Clone of qnap apps download
57 DEBUG: 65000		knappe_10.0.0.15 (10.0.0.15/32)	all (0.0.0.0/0)	bittorrent (6881/UDP)	deny	none		24	silently drop bittorent
58 DEBUG: 66000	test-v6-nw-obj:1	ipv6-testgroup	test-ipv6addr (::/0)	PING	accept	none		ipv6.2	comment33
59 DEBUG: 67000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99015	
60 DEBUG: 68000	samsung to print clients	drucker-10.0.0.38 (10.0.0.38/32)	fwf60-wlan-client-net (10.0.0.61/32)	tcp_5357_samsung_printer (5357/TCP) PING	accept	none		64	
61 DEBUG: 69000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99016	

62 DEBUG: 70000	access to gameserver via ssl	SSl-VPN-10.0.0.40_24 (10.0.0.40/32)	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	SSH (22/TCP) PING HTTPS (443/TCP)	accept	none		71	Clone of admin FG and FB via ssl-VPN
63 DEBUG: 71000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99017	
64 DEBUG: 72000	admin FG and FB via ssl-VPN	SSl-VPN-10.0.0.40_24 (10.0.0.40/32)	pi_10.0.0.52 (10.0.0.52/32) fg_internal_10.0.0.7 (10.0.0.7/32)	SSH (22/TCP) PING HTTPS (443/TCP)	accept	none		36	fw admin via ssl vpn
65 DEBUG: 73000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99018	
66 DEBUG: 75000	SSL VPN access to knappe	SSl-VPN-10.0.0.40_24 (10.0.0.40/32)	knappe_10.0.0.15 (10.0.0.15/32)	SSH (22/TCP) tcp_8081_phpfreechat (8081/TCP) PING afp_548_tcp (548/TCP) SMB (445/TCP) HTTPS (443/TCP) SAMBA (139/TCP)	accept	none		26	knappe vpn access
67 DEBUG: 76000	silently drop broadcasts	all (0.0.0.0/0)	broadcast (255.255.255.255/32)	ALL	deny	none		45	
68 DEBUG: 77000	silently drop http	all (0.0.0.0/0)	all (0.0.0.0/0)	HTTP (80/TCP)	deny	none		69	silently drop http
69 DEBUG: 78000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99019	
70 DEBUG: 79000	admin fb internet via vpn	SSl-VPN-10.0.0.40_24 (10.0.0.40/32)	fritzbox_inet_10.0.0.24 (10.0.0.24/32)	HTTP (80/TCP) PING HTTPS (443/TCP)	accept	none		44	Clone of admin FG and FB via ssl-VPN
71 DEBUG: 80000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99020	
				ark-udp-32768-65535 (32768/UDP)					

#	Name	Source	Destination	Service	Action	Log		Count	Comment
72 DEBUG: 81000	internet to gameserver	all (0.0.0.0/0)	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	(32768/UDP) steam-udp-27000-27050 (27000/UDP) PING minecraft-25565 (25565/TCP) ARK-7777-7778-udp (7777/UDP)	accept	all		3	internet to gameserver
73 DEBUG: 82000	fb drop scans	fritzbox_inet_10.0.0.24 (10.0.0.24/32)	ubuntu-gameserver-10.0.0.51 (10.0.0.51/32)	tcp14013-fb (14013/TCP) HTTP (80/TCP)	deny	none		70	silent drop fb2internal
74 DEBUG: 83000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99021	
75 DEBUG: 84000	silent drop fb2internal	fritzbox_inet_10.0.0.24 (10.0.0.24/32)	internal-10.0.0.35_24 (10.0.0.35/32)	tcp14013-fb (14013/TCP) HTTP (80/TCP)	deny	none		61	Clone of drop fritzbox http scan
76 DEBUG: 85000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99022	
77 DEBUG: 86000	drop fb probes to keller	fritzbox_inet_10.0.0.24 (10.0.0.24/32)	eltern-keller-10.0.0.66_24 (10.0.0.66/32)	tcp14013-fb (14013/TCP) HTTP (80/TCP)	deny	none		82	Clone of silent drop fb2internal
78 DEBUG: 87000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99023	
79 DEBUG: 88000	drop fritzbox 2 nfm	fritzbox_inet_10.0.0.24 (10.0.0.24/32)	wlan-kids (10.0.0.62/32)	tcp14013-fb (14013/TCP) HTTP (80/TCP)	deny	none		28	fritzbox autodiscover and parental filter stuff
80 DEBUG: 89000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99024	
81 DEBUG: 90000	drop fb http scan	fritzbox_inet_10.0.0.24 (10.0.0.24/32)	drucker-10.0.0.38 (10.0.0.38/32) knappe_10.0.0.15 (10.0.0.15/32)	tcp14013-fb (14013/TCP) HTTP (80/TCP)	deny	none		27	fritzbox http autodiscover
82 DEBUG: 91000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99025	
83 DEBUG: 92000	ipsec-vpn-cactus	vpn-gw-cactus-ffm (10.0.0.65/32)	FG_10.0.0.1 (10.0.0.1/32)	ALL	accept	all		74	allow ipsec vpn cactus

84 DEBUG: 93000	stealth-rule	all (0.0.0.0/0)	FG_10.0.0.1 (10.0.0.1/32)	ALL	deny	all		73	Clone of silent drop fb2internal
85 DEBUG: 94000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99026	
86 DEBUG: 95000	silent drop fb 2 wch60e	fritzbox_inet_10.0.0.24 (10.0.0.24/32)	fwf60-wlan-client-net (10.0.0.61/32)	tcp14013-fb (14013/TCP) HTTP (80/TCP)	deny	none		62	Clone of silent drop fb2wlan
87 DEBUG: 96000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99027	
88 DEBUG: 97000	drop internal cross-nw traffic	fwf60-wlan-client-net (10.0.0.61/32)	all (0.0.0.0/0)	ALL	deny	none		63	silent ignore
89 DEBUG: 98000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99028	
90 DEBUG: 99000	wlan2serverlan	fwf60-wlan-client-net (10.0.0.61/32)	knappe_10.0.0.15 (10.0.0.15/32)	HTTP (80/TCP) SSH (22/TCP) SQUID (3128/TCP) tcp_8081_phpfreechat (8081/TCP) PING afp_548_tcp (548/TCP) SMB (445/TCP) HTTPS (443/TCP)	accept	all		54	Clone of internal to knappe
91 DEBUG: 100000	drop 139/tcp from wch60e2knappe	fwf60-wlan-client-net (10.0.0.61/32)	knappe_10.0.0.15 (10.0.0.15/32)	SAMBA (139/TCP)	deny	none		66	Clone of silently drop 139/tcp
92 DEBUG: 101000	wlan2printer	fwf60-wlan-client-net (10.0.0.61/32)	drucker-10.0.0.38 (10.0.0.38/32)	ALL	accept	all		55	wlan to printer
93 DEBUG: 102000		all (0.0.0.0/0)	all (0.0.0.0/0)		deny	none		99029	
94 DEBUG: 103000	fwf-wlan-to-internet	fwf60-wlan-client-net (10.0.0.61/32)	all (0.0.0.0/0)	ALL	accept	none		53	test

huhu

huhu