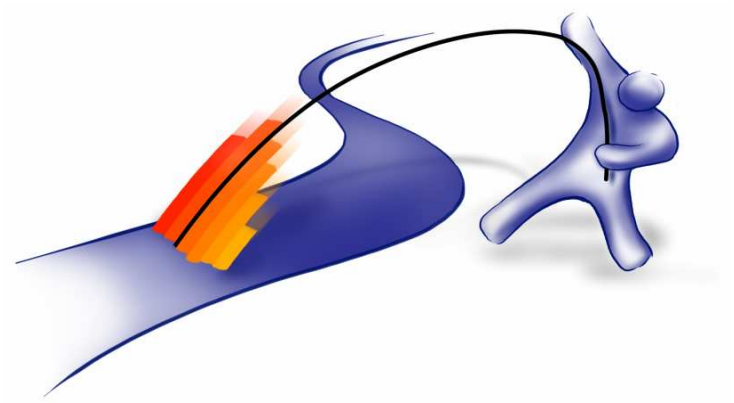


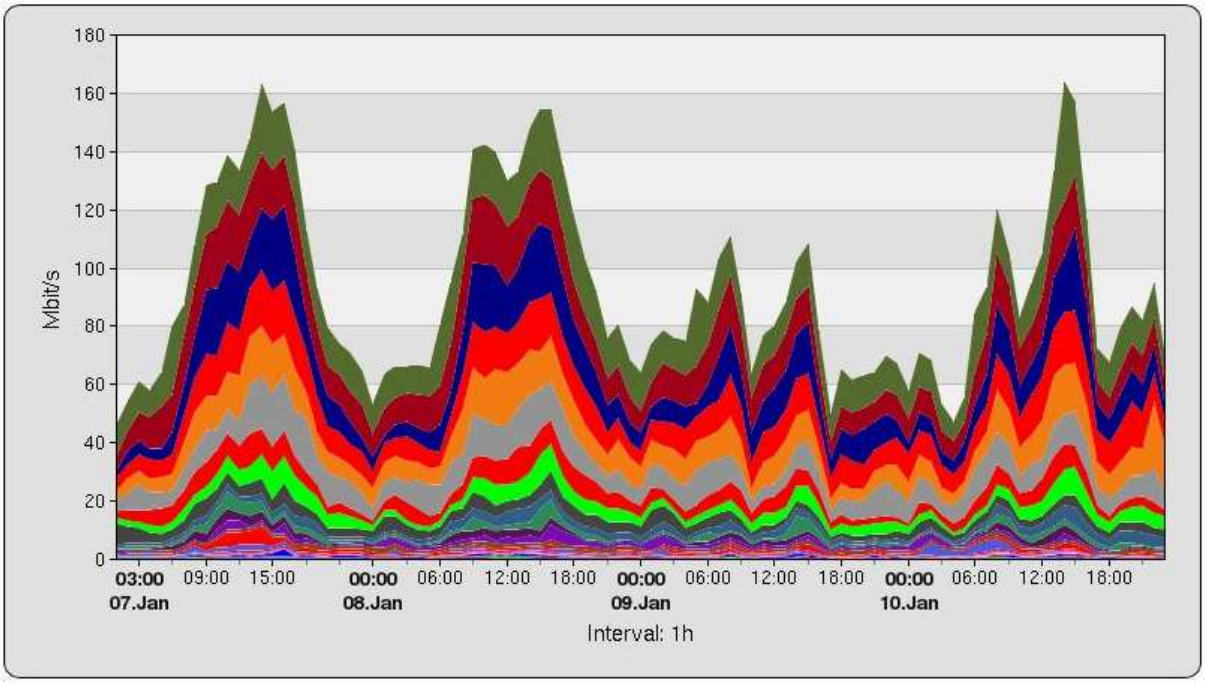
IsarFlow
Whitepaper

Bandbreite und Anzahl Sessions pro Anwendung

Bei den folgenden 2 Auswertungen handelt es sich um den gleichen Standort und den gleichen Zeitraum. Der Standort ist über zwei Router angebunden. In der ersten Darstellung wurden die übertragenen Protokoll-Volumina dargestellt, in der zweiten die Anzahl Sessions (Flows) pro Protokoll. Bei den Volumina erhält man ein vertrautes Bild : das Ansteigen und Abfallen der übertragenen Datenmengen im Tagesverlauf. Bei der Abbildung der Sessions tauchen überraschende Aspekte auf :

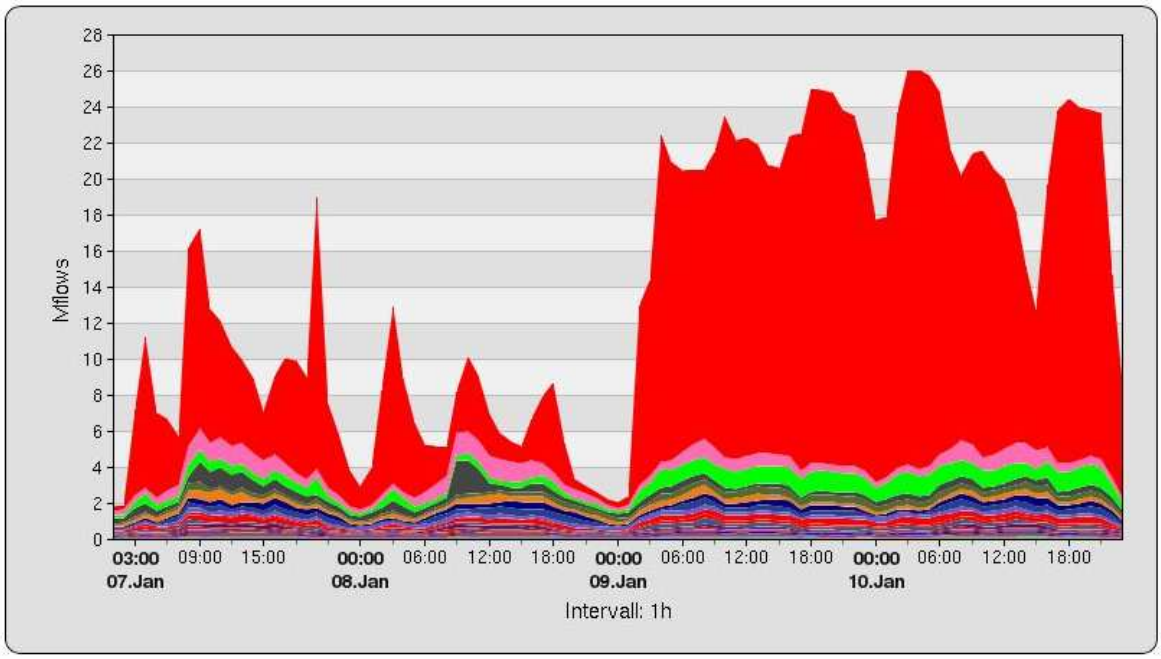
- Die Anzahl der Sessions ändert sich nicht periodisch mit dem Tagesverlauf
- Die Protokolle die bei den Volumina dominieren sind nicht die gleichen die bei der Anzahl Sessions dominieren :
    - Ein einziger Protokoll-Bereich (TCP-Other) dominiert die Anzahl Sessions sehr stark
    - http und http die zusammen rund 28% des Volumens erzeugen, repräsentieren nur 3,3% der Sessions
    - ICMP, das nur 0,4% des Volumens ausmacht, erzeugt 4,3% aller Sessions

Applikationen --> Details --> Applikationen und Interfaces
InterfaceView: München (router-mch01,Gi0/1 router-mch02,Gi0/1)
01/07/2008 01:00 - 01/10/2008 23:59
(Interval 60 minutes)



Nr.	Protokoll	Byte	min	avg	max	%
1	HTTP (tcp: 80)	579.43 GB	6.39 Mbps	14.55 Mbps	41.25 Mbps	15.28
2	SMTP (tcp: 25)	506.46 GB	5.13 Mbps	12.72 Mbps	23.59 Mbps	13.35
3	HTTPS (tcp: 443)	471.28 GB	2.34 Mbps	11.84 Mbps	28.01 Mbps	12.43
4	TCP-Other	429.43 GB	4.54 Mbps	10.79 Mbps	19.42 Mbps	11.32
5	MICROSOFT-DS (tcp: 445)	391.36 GB	3.19 Mbps	9.83 Mbps	22.41 Mbps	10.32
6	ESP	367.28 GB	3.99 Mbps	9.22 Mbps	19.04 Mbps	9.68
7	HTTP Proxy (tcp: 81)	207.28 GB	1.12 Mbps	5.21 Mbps	11.67 Mbps	5.47
8	SAP (tcp: 3200-3500)	169.91 GB	1.25 Mbps	4.27 Mbps	10.19 Mbps	4.48
9	LDAP (tcp: 389)	146.14 GB	1.33 Mbps	3.67 Mbps	7.17 Mbps	3.85
10	NETBIOS-SSN (tcp: 139)	94.79 GB	775.70 Kbps	2.38 Mbps	6.65 Mbps	2.50
11	HTTP-PROXY (tcp: 8080)	64.46 GB	155.33 Kbps	1.62 Mbps	7.61 Mbps	1.70
12	MIT-ML-DEV (tcp: 83,85)	55.77 GB	232.93 Kbps	1.40 Mbps	3.83 Mbps	1.47
13	SSH (tcp: 22)	52.58 GB	125.42 Kbps	1.32 Mbps	4.81 Mbps	1.39
14	MSEXCH-ROUTING (tcp: 691)	45.08 GB	423.06 Kbps	1.13 Mbps	1.84 Mbps	1.19
15	LOTUS NOTES (tcp: 1352)	34.68 GB	24.11 Kbps	871.04 Kbps	6.17 Mbps	0.91
16	FTP-DATA (tcp: 20)	28.36 GB	2.23 Kbps	712.43 Kbps	4.04 Mbps	0.75
17	HTTP-PROXY-SQUID (tcp: 3128)	16.41 GB	7.44 Kbps	412.18 Kbps	885.15 Kbps	0.43
18	ICMP	14.97 GB	137.02 Kbps	376.11 Kbps	723.94 Kbps	0.39
19	DOMAIN (udp) (udp: 53)	10.65 GB	127.25 Kbps	267.59 Kbps	416.38 Kbps	0.28
20	UDP-Other	8.99 GB	22.58 Kbps	225.83 Kbps	2.38 Mbps	0.24
21	DOMAIN (tcp: 53)	8.12 GB	50.52 Kbps	203.84 Kbps	391.81 Kbps	0.21
22	KERBEROS (tcp: 88)	8.11 GB	96.59 Kbps	203.72 Kbps	433.49 Kbps	0.21
23	MFCOBOL (tcp: 86)	7.23 GB	25.30 Kbps	181.58 Kbps	693.22 Kbps	0.19
24	NEW_PORT_7777 (tcp: 7777)	5.83 GB	214.39 bps	146.32 Kbps	922.67 Kbps	0.15
25	MS-SQL (tcp: 1433)	4.49 GB	15.79 Kbps	112.87 Kbps	333.26 Kbps	0.12
Summe		**3.64 TB**				**98.33**
Gesamter Verkehr		**3.70 TB**				**100.00**
CSV Export						

Applikationen --> Details --> Applikationen und Interfaces
InterfaceView: München (router-mch01,Gi0/1 router-mch02,Gi0/1)
07.01.2008 01:00 - 10.01.2008 23:59
(Intervall 60 Minuten)



Nr.	Protokoll	Flows	min	avg	max	%
1	TCP-Other	960'810'554	223.74 Kflows	10.11 Mflows	22.18 Mflows	66.07
2	ICMP	61'824'197	207.22 Kflows	650.78 Kflows	1.23 Mflows	4.25
3	SAP (tcp: 3200-3500)	60'731'463	135.65 Kflows	639.28 Kflows	1.14 Mflows	4.18
4	LDAP (tcp: 389)	37'440'394	164.10 Kflows	394.11 Kflows	1.90 Mflows	2.57
5	HTTP (tcp: 80)	24'870'830	77.01 Kflows	261.80 Kflows	482.64 Kflows	1.71
6	MICROSOFT-DS (tcp: 445)	24'527'834	145.31 Kflows	258.19 Kflows	557.37 Kflows	1.69
7	HTTPS (tcp: 443)	22'444'017	41.90 Kflows	236.25 Kflows	464.70 Kflows	1.54
8	SNMP (udp) (udp: 161)	21'905'790	29.63 Kflows	230.59 Kflows	436.87 Kflows	1.51
9	DOMAIN (udp) (udp: 53)	18'183'461	118.09 Kflows	191.40 Kflows	253.45 Kflows	1.25
10	BITTORRENT_DATA (tcp: 6881-6999)	16'999'925	551.00 flows	178.95 Kflows	401.44 Kflows	1.17
11	HTTP Proxy (tcp: 81)	16'005'791	64.25 Kflows	168.48 Kflows	360.85 Kflows	1.10
12	NETBIOS-SSN (tcp: 139)	14'171'294	62.70 Kflows	149.17 Kflows	264.56 Kflows	0.97
13	MIT-ML-DEV (tcp: 83,85)	8'626'868	14.84 Kflows	90.81 Kflows	248.88 Kflows	0.59
14	EPMAP (tcp: 135)	7'340'892	35.65 Kflows	77.27 Kflows	186.52 Kflows	0.50
15	LDAP (udp) (udp: 389)	6'266'997	31.18 Kflows	65.97 Kflows	107.73 Kflows	0.43
16	UDP-Other	5'807'387	12.98 Kflows	61.13 Kflows	120.24 Kflows	0.40
17	KERBEROS (tcp: 88)	5'480'154	33.48 Kflows	57.69 Kflows	100.95 Kflows	0.38
18	SMTP (tcp: 25)	4'354'078	20.32 Kflows	45.83 Kflows	70.56 Kflows	0.30
19	HTTP-PROXY (tcp: 8080)	4'249'415	8.76 Kflows	44.73 Kflows	109.63 Kflows	0.29
20	DOMAIN (tcp: 53)	4'179'589	22.83 Kflows	44.00 Kflows	80.06 Kflows	0.29
21	NETBIOS-NS (udp) (udp: 137)	2'568'133	14.39 Kflows	27.03 Kflows	44.98 Kflows	0.18
22	SUNRPC (udp) (udp: 111)	2'368'547	12.33 Kflows	24.93 Kflows	30.13 Kflows	0.16
23	RTP (udp) (udp: 16384-32768)	2'281'123	698.00 flows	24.01 Kflows	53.29 Kflows	0.16
24	PRINTER (tcp: 515)	2'094'033	12.46 Kflows	22.04 Kflows	26.22 Kflows	0.14
25	NETBIOS-DGM (udp) (udp: 138)	1'840'024	11.89 Kflows	19.37 Kflows	25.12 Kflows	0.13
Summe		**1'337'372'790**				**91.97**
Gesamter Verkehr		**1'454'140'984**				**100.00**
CSV Export						

Über Drill Down erhält man weitere Informationen, die helfen den Verkehr zu bestimmen der für die vielen Sessions verantwortlich ist : Zum Einen die Top Talker und zum Anderen die Kommunikationsbeziehungen der Adressen die unter den Top Talkern aufgeführt sind.

Endgeräte --> Übersicht --> Top talker
InterfaceView: München (router-mch01,Gi0/1 router-mch02,Gi0/1)
10.01.2008 18:00 - 18:30
(Intervall 1 Minute)

Nr.	Source	Protokoll	TX Flows	RX Flows	Flows gesamt
1	10.25.231.134	TCP-Other	1'617'462	2'908'586	4'526'048
2	10.25.231.135	TCP-Other	1'519'920	2'811'114	4'331'034
3	10.25.231.133	TCP-Other	344'475	535'513	879'988
4	10.25.231.136	TCP-Other	151'057	292'678	443'735
5	10.25.231.134	SAP (tcp: 3200-3500)	75'619	136'078	211'697
6	10.25.231.135	SAP (tcp: 3200-3500)	70'708	130'732	201'440
7	10.25.231.137	TCP-Other	111'018	19'980	130'998
8	10.25.231.134	BITTORRENT_DATA (tcp: 6881-6999)	30'432	53'929	84'361
9	10.25.231.135	BITTORRENT_DATA (tcp: 6881-6999)	27'659	51'104	78'763
10	10.29.27.238	SNMP (udp) (udp: 161)	31'643	46'078	77'721
dargestellte Elemente			**3'979'993**	**6'985'792**	**10'965'785**
CSV Export					

Ein Klick auf eine IP-Adresse liefert die genauen Kommunikationsbeziehungen innerhalb der ausgewählten Zeit :

Hosts --> IP-Tracking --> Sessions
IP-2-IP: 10.25.231.134 - any

Location : Munich (router-mch01,Gi0/1 router-mch02,Gi0/1)
Protocol shown: TCP-Other
01/10/2008 18:00 - 18:30
(Interval 1 minute)

Nr.	Time	Source	Destination	protocol	byte	Percentage of the whole traffic
1	18:00:00	10.25.231.134	172.73.17.59	TCP-Other	215 B	0.00
2	18:00:00	10.25.231.134	172.73.22.94	TCP-Other	21.75 KB	0.01
3	18:00:00	10.25.231.134	172.73.22.151	TCP-Other	5.99 KB	0.00
4	18:00:00	10.25.231.134	172.73.23.57	TCP-Other	144 B	0.00
5	18:00:00	10.25.231.134	172.73.24.223	TCP-Other	144 B	0.00
6	18:00:00	10.25.231.134	172.73.25.139	TCP-Other	11.13 KB	0.01
7	18:00:00	10.25.231.134	172.73.27.194	TCP-Other	48 B	0.00
8	18:00:00	10.25.231.134	172.73.38.92	TCP-Other	23.09 KB	0.01
9	18:00:00	10.25.231.134	172.73.38.213	TCP-Other	2.50 KB	0.00
10	18:00:00	10.25.231.134	172.73.38.227	TCP-Other	48 B	0.00
11	18:00:00	10.25.231.134	172.73.44.43	TCP-Other	48 B	0.00
12	18:00:00	10.25.231.134	172.73.44.79	TCP-Other	48 B	0.00
13	18:00:00	10.25.231.134	172.73.44.88	TCP-Other	48 B	0.00
14	18:00:00	10.25.231.134	172.73.44.89	TCP-Other	48 B	0.00
15	18:00:00	10.25.231.134	172.73.45.128	TCP-Other	144 B	0.00
16	18:00:00	10.25.231.134	172.73.47.240	TCP-Other	48 B	0.00
17	18:00:00	10.25.231.134	172.73.52.6	TCP-Other	48 B	0.00
18	18:00:00	10.25.231.134	172.73.52.42	TCP-Other	48 B	0.00
19	18:00:00	10.25.231.134	172.73.56.93	TCP-Other	48 B	0.00
20	18:00:00	10.25.231.134	172.73.58.213	TCP-Other	240 B	0.00
21	18:00:00	10.25.231.134	172.73.59.234	TCP-Other	35.99 KB	0.02
22	18:00:00	10.25.231.134	172.73.60.248	TCP-Other	21.76 KB	0.01
21	18:00:00	10.25.231.134	172.73.66.6	TCP-Other	55.57 KB	0.03
22	18:00:00	10.25.231.134	172.73.67.33	TCP-Other	3.73 KB	0.00
23	18:00:00	10.25.231.134	172.73.74.251	TCP-Other	24.11 KB	0.01
24	18:00:00	10.25.231.134	172.73.75.168	TCP-Other	51.38 KB	0.02
25	18:00:00	10.25.231.134	172.73.83.53	TCP-Other	480 B	0.00
26	18:00:00	10.25.231.134	172.73.84.37	TCP-Other	48 B	0.00
27	18:00:00	10.25.231.134	172.73.84.88	TCP-Other	50.51 KB	0.02

IsarNet
Software Solutions GmbH
Terminalstrasse Mitte 18
85356 München
Germany

Tel. 07000 ISARNET
Fax. 089 97007 200
e-mail: isarflow@isarnet.de
http://www.isarnet.de
http://www.isarflow.de