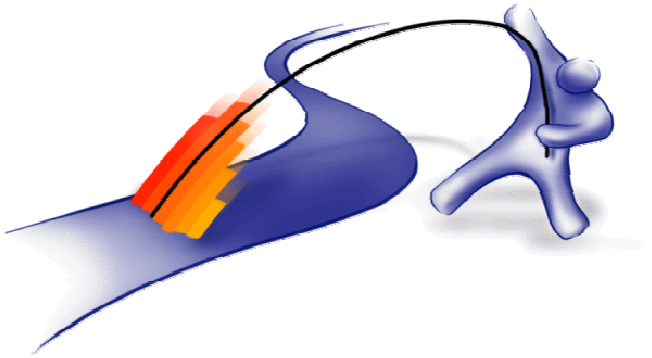
IsarFlow Überblick



IsarNet AG
Q3/2006

Wie profitiert man durch den Einsatz von IsarFlow ?

Fehlersuche

Planung

Security

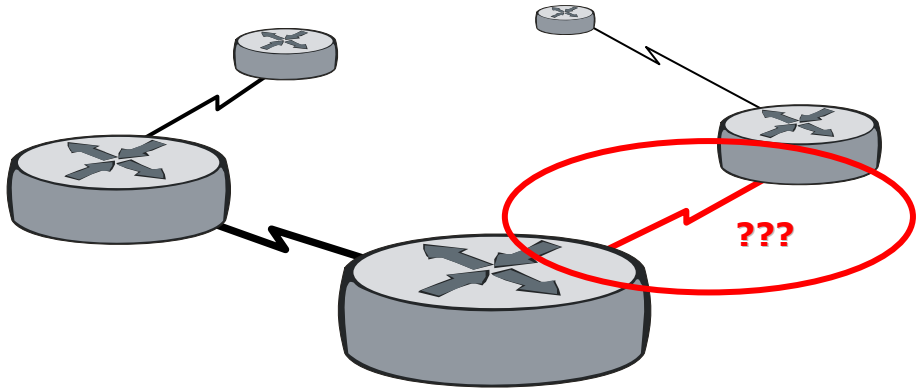
QoS Monitoring

Accounting

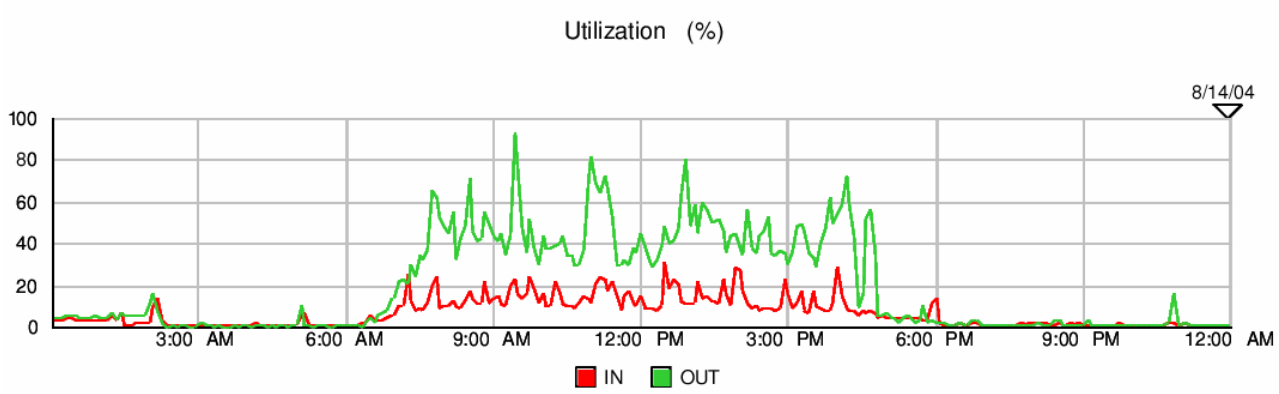
isarNet
Professional Networking

Link Transparenz : SNMP

Auf einer Leitung gibt es Probleme mit SAP :



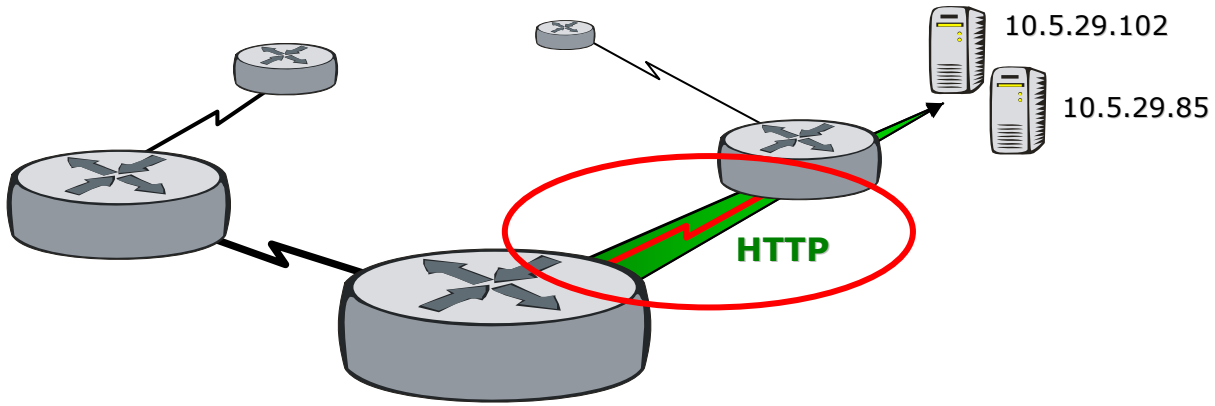
Welche Informationen liefert Ihr SNMP Netzwerk-Management ?
„Eine Hohe Last auf der Leitung“ – keine wirklich neue Information !



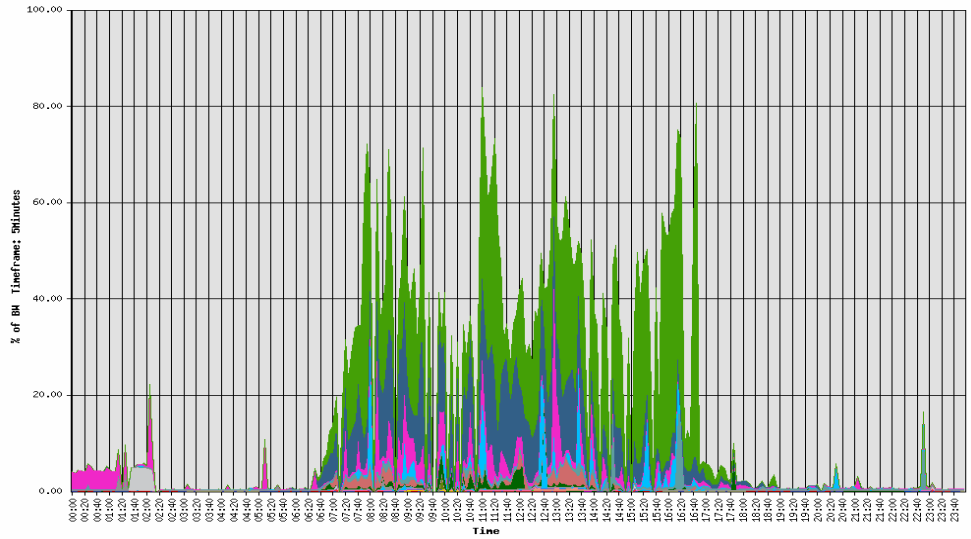
Link Transparenz : IsarFlow

Fehlersuche

Auf einer Leitung gibt es Probleme mit SAP :



Welche Informationen liefert Ihnen **IsarFlow** ?



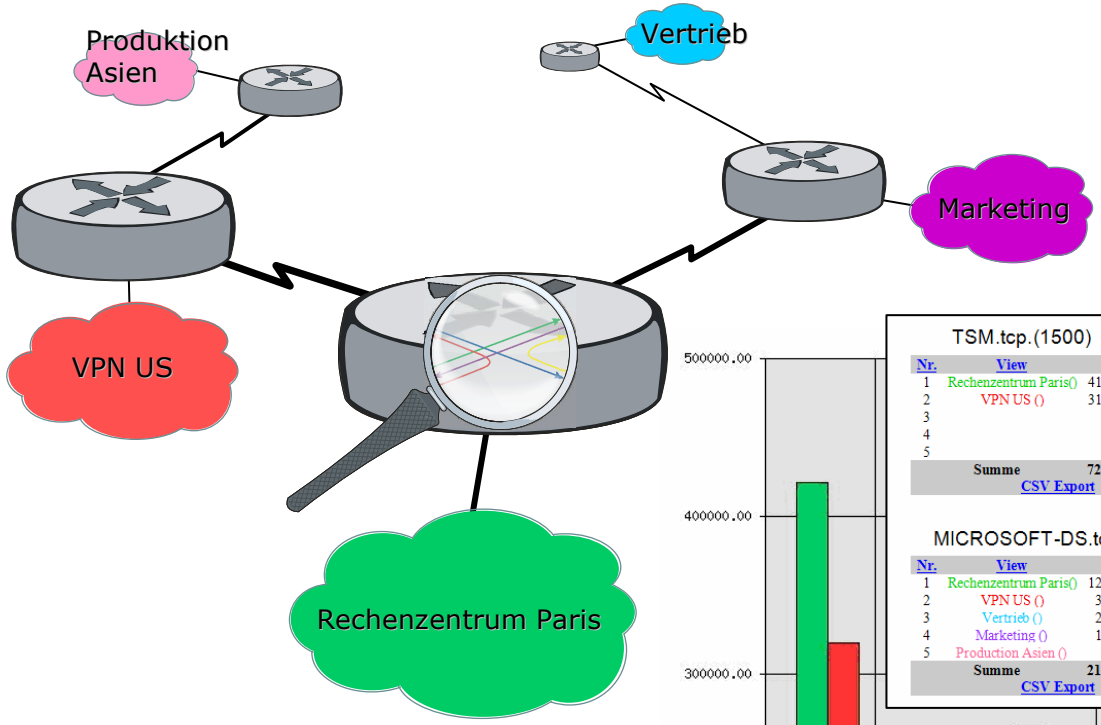
Protocol	Byte	%
WWW-HTTP	637.54 MB	35.10
NETBIOS-NS	378.62 MB	20.85
SAP	348.50 MB	19.19
GRE	134.20 MB	7.39
NCP	79.36 MB	4.37
RTP-AUDIO	66.53 MB	3.66
SOCKS	53.06 MB	2.92
HTTPS	30.62 MB	1.69
EPMAP	26.14 MB	1.44
SNMP	15.23 MB	0.84
...	...	...
...	...	...

Top Sessions
View: WAN link Shanghai
There were no filters selected
8/13/2004 00:55 - 23:55

No.	Source	Destination	Protocol	Byte	Percentage
1	193.27.112.2	10.5.29.102	WWW-HTTP	128.97 MB	7.18
2	64.236.34.196	10.5.29.85	WWW-HTTP	87.79 MB	4.89
3	10.5.65.164	10.120.97.164	SAP	73.62 MB	4.10
4	10.120.97.164	10.5.65.164	RTP-AUDIO	65.02 MB	3.62
5	10.5.254.25	10.120.254.3	GRE	64.52 MB	3.59
6	209.61.191.11	10.5.29.72	WWW-HTTP	56.02 MB	3.12
7	10.5.254.9	10.120.254.3	GRE	52.56 MB	2.93
8	10.120.97.164	10.5.29.34	SAP	47.49 MB	2.65
9	194.138.38.22	10.5.29.102	WWW-HTTP	32.05 MB	1.79
10	10.5.29.34	10.120.97.164	SAP	25.95 MB	1.45
11	10.120.106.250	10.5.67.36	SAP	24.81 MB	1.38
12	193.225.54.240	10.5.29.114	WWW-HTTP	24.60 MB	1.37
13	10.120.97.159	10.5.65.161	NCP	23.43 MB	1.30
14	10.5.65.161	10.120.97.159	NCP	21.88 MB	1.22
15	10.92.161.30	10.88.36.33	SAP	20.31 MB	1.13
16	10.5.65.110	10.120.104.242	SOCKS	16.78 MB	0.93
17	10.5.65.110	10.120.106.247	SOCKS	16.66 MB	0.93
18	10.92.161.25	10.5.67.167	SAP	15.04 MB	0.84
19	10.120.104.244	10.5.67.8	NETBIOS-SSN	13.34 MB	0.74
20	204.157.3.229	10.5.29.72	WWW-HTTP	13.26 MB	0.74
sum				824.10 MB	45.91
total traffic				1.75 GB	100%

Wer benutzt die Hauptanwendungen (bezogen auf die Volumina) ?

planning



IsarFlow erlaubt beliebige "View" Definitionen
-basierend auf physikalischen Interfaces oder IP Adressen bzw. Subnets

TSM.tcp.(1500)

Nr.	View	byte	%
1	Rechenzentrum Paris()	410.91 GB	56.82
2	VPN US ()	312.21 GB	43.17
3			0.00
4			0.00
5			0.00
	Summe	723.18 GB	99.99

CSV Export

HTTP-PROXY.tcp(8080)

Nr.	View	Byte	%
1	Rechenzentrum Paris()	258.12 GB	58.43
2	VPN US ()	79.62 GB	18.02
3	Vertrieb ()	34.27 GB	7.76
4	Marketing ()	16.95 GB	3.84
5	Production Asien ()	13.24 GB	3.00
	Summe	402.20 GB	91.05

CSV Export

LOTUSNOTES.tcp(1352)

Nr.	View	byte	%
1	Rechenzentrum Paris()	193.41 GB	50.75
2	VPN US ()	57.77 GB	15.16
3	Vertrieb ()	30.56 GB	8.02
4	Marketing ()	27.89 GB	7.32
5	Production Asien ()	27.46 GB	7.21
	Summe	337.09 GB	88.46

CSV Export

MICROSOFT-DS.tcp(445)

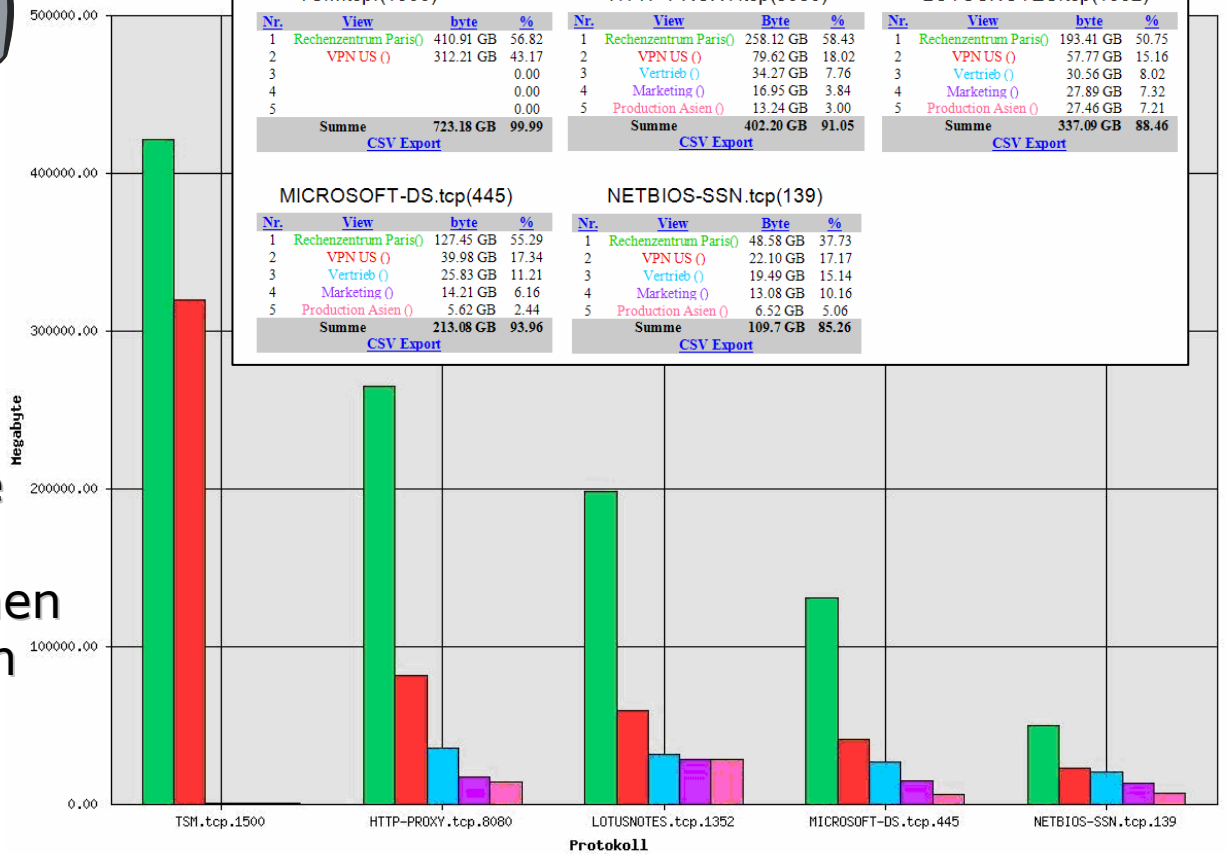
Nr.	View	byte	%
1	Rechenzentrum Paris()	127.45 GB	55.29
2	VPN US ()	39.98 GB	17.34
3	Vertrieb ()	25.83 GB	11.21
4	Marketing ()	14.21 GB	6.16
5	Production Asien ()	5.62 GB	2.44
	Summe	213.08 GB	93.96

CSV Export

NETBIOS-SSN.tcp(139)

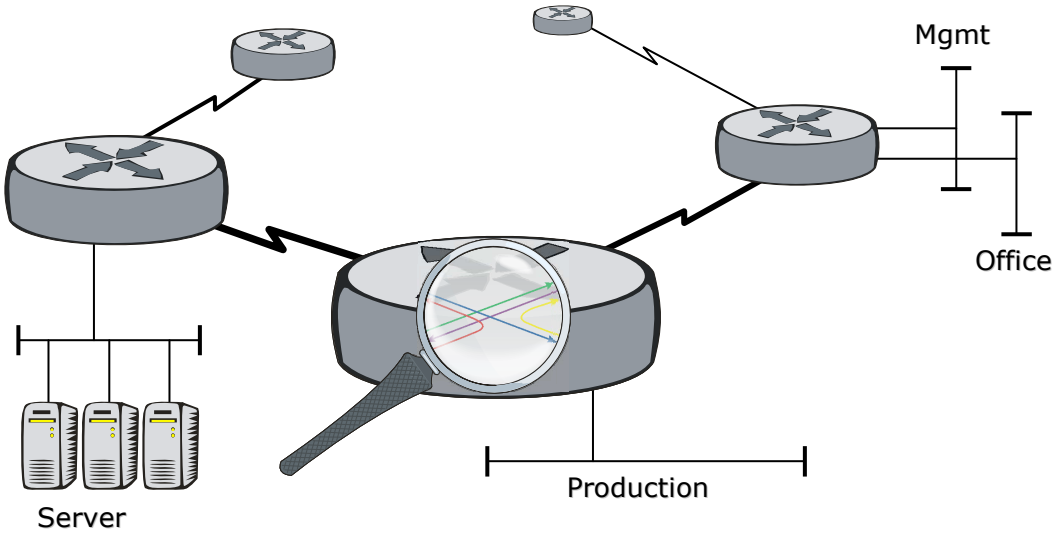
Nr.	View	Byte	%
1	Rechenzentrum Paris()	48.58 GB	37.73
2	VPN US ()	22.10 GB	17.17
3	Vertrieb ()	19.49 GB	15.14
4	Marketing ()	13.08 GB	10.16
5	Production Asien ()	6.52 GB	5.06
	Summe	109.7 GB	85.26

CSV Export



Kommunikations Matrix

planning



Passt die aktuelle InfrastruKtur zu den Datenströmen ?
Macht eine Server-Zentralisierung Sinn ?

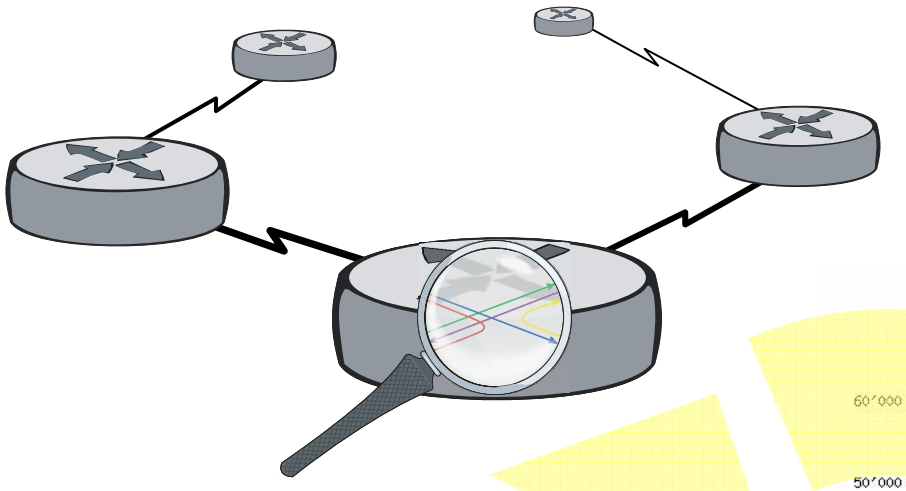
...

Sender / Empfänger	Prod	Server	Mgmt	Office	IsarNet-office	Restverkehr
Prod	0.00 B	20.71 MB	0.00 B	190.90 MB	0.00 B	2.73 MB
Server	6.75 KB	0.00 B	0.00 B	248.00 B	0.00 B	36.50 MB
Mgmt	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B
Office	65.43 MB	277.74 KB	0.00 B	9.87 KB	0.00 B	56.25 MB
IsarNet-office	0.00 B	499.03 KB	0.00 B	0.00 B	0.00 B	4.19 MB
Restverkehr	308.65 KB	2.84 MB	0.00 B	257.13 MB	18.39 KB	0.00 B
Summe der Bytes:	637.76 MB					

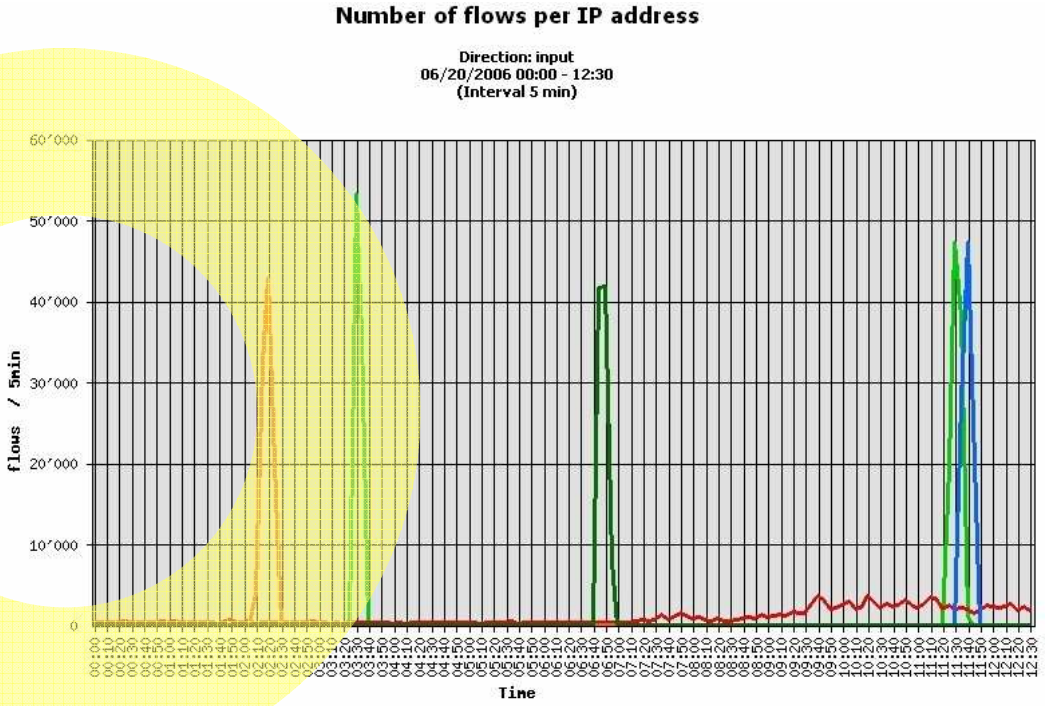
Anteil an dargestellter Bytesumme

< 10%
10% - 20%
20% - 30%
30% - 40%
40% - 50%
50% - 60%
60% - 70%
70% - 80%
80% - 90%
90% - 100%

Security



IsarFlow untersucht alle IP Adressen im Netz einmal pro 5 Minuten-Intervall und schickt Reports bei auffälligem Verhalten



Security Alarm report

IP Tracking analysis

IP-2-IP: 62.159.42.157 - any
View: default group - input
06/20/2006

No.	Time	Source	Destination	Protocol	Bytes	Percentage
1	11:30:00	62.159.42.157	192.212.57.21	EPMAP.tcp.135	48.00 B	0.00
2	11:30:00	62.159.42.157	192.212.57.22	EPMAP.tcp.135	48.00 B	0.00
3	11:30:00	62.159.42.157	192.212.57.23	EPMAP.tcp.135	48.00 B	0.00
4	11:30:00	62.159.42.157	192.212.57.24	EPMAP.tcp.135	48.00 B	0.00
5	11:30:00	62.159.42.157	192.212.57.25	EPMAP.tcp.135	48.00 B	0.00
6	11:30:00	62.159.42.157	192.212.57.26	EPMAP.tcp.135	48.00 B	0.00
7	11:30:00	62.159.42.157	192.212.57.41	EPMAP.tcp.135	48.00 B	0.00
8	11:30:00	62.159.42.157	192.212.57.42	EPMAP.tcp.135	48.00 B	0.00
9	11:30:00	62.159.42.157	192.212.57.43	EPMAP.tcp.135	48.00 B	0.00
10	11:30:00	62.159.42.157	192.212.57.44	EPMAP.tcp.135	48.00 B	0.00
11	11:30:00	62.159.42.157	192.212.57.45	EPMAP.tcp.135	48.00 B	0.00
12	11:30:00	62.159.42.157	192.212.57.46	EPMAP.tcp.135	48.00 B	0.00
13	11:30:00	62.159.42.157	192.212.57.47	EPMAP.tcp.135	48.00 B	0.00
14	11:30:00	62.159.42.157	192.212.57.48	EPMAP.tcp.135	48.00 B	0.00
15	11:30:00	62.159.42.157	192.212.57.49	EPMAP.tcp.135	48.00 B	0.00

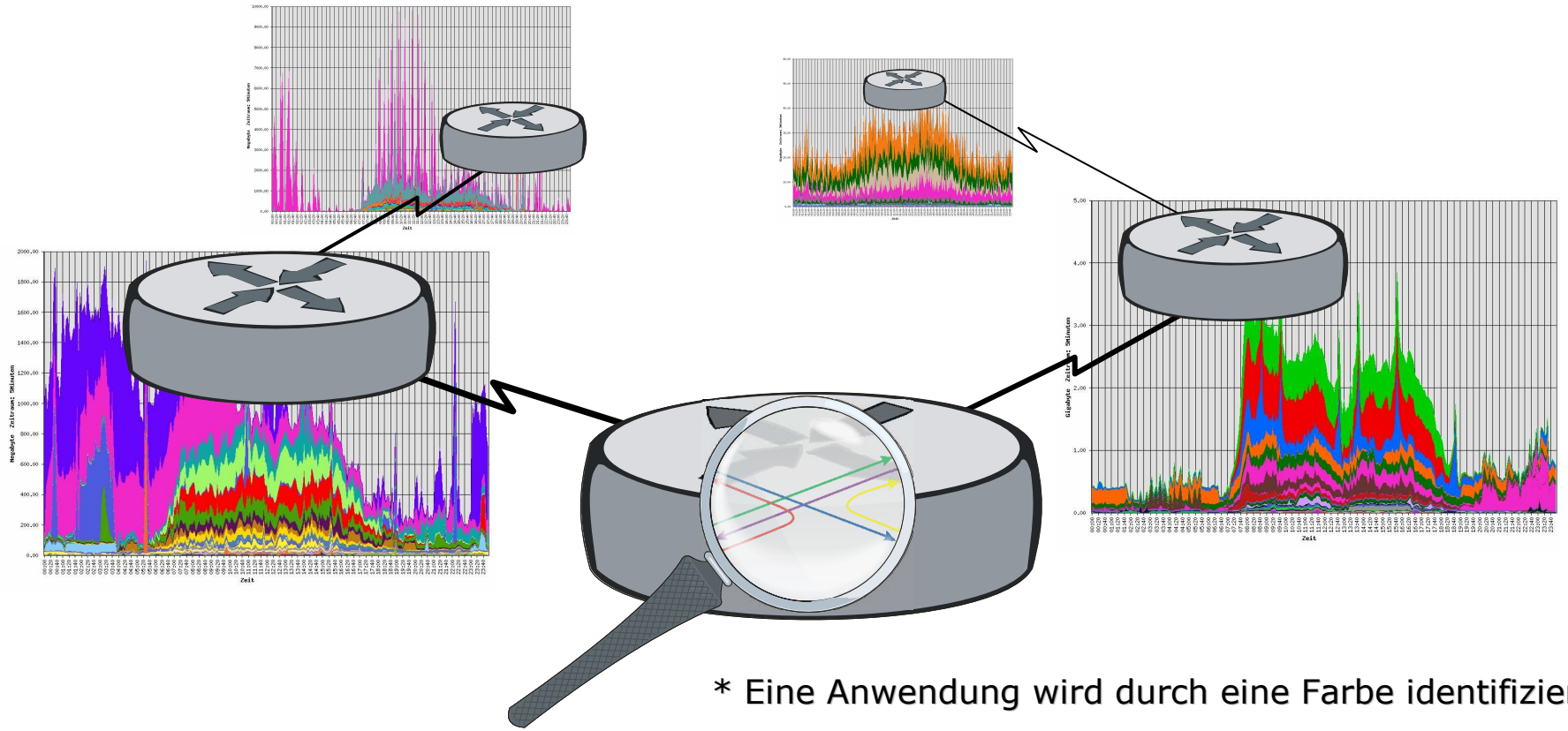
Nr.	IP	name	flows	byte	Percent (flows)
1	62.159.42.157	vzadmin.rdsmaster52.keyvirtual.de	194'255	73.46 MB	31.58
2	192.67.198.79	av2.RZ.FH-Augsburg.DE	131'183	219.08 MB	21.33
3	192.67.198.2	Host Unknown	100'075	55.52 MB	16.27
4	192.67.198.62	x1-6-00-40-c7-81-f1-d4.k248.webspeed.dk	98'694	17.31 MB	16.04
5	149.239.166.78	31-114-60-69.serverpronto.com	90'902	13.52 MB	14.78

Hilfe bei der Einführung von QoS

Stellen Sie QoS-Konzepte mit Daten aus Ihrem Netz zusammen :

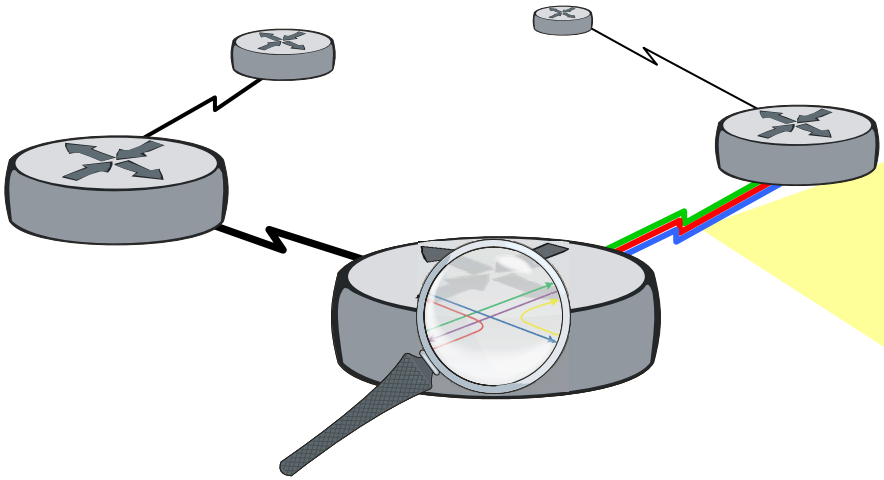
- Welche Volumina pro Anwendung gibt es ?
- Gibt es Lokations-typischen Verkehr ?
- In welchen Bereichen wird VoIP verwendet ?

=> Design der QoS policies !



* Eine Anwendung wird durch eine Farbe identifiziert

QoS : Kontrolle des Verkehrs pro Klasse



Arbeitet QoS wie geplant ?

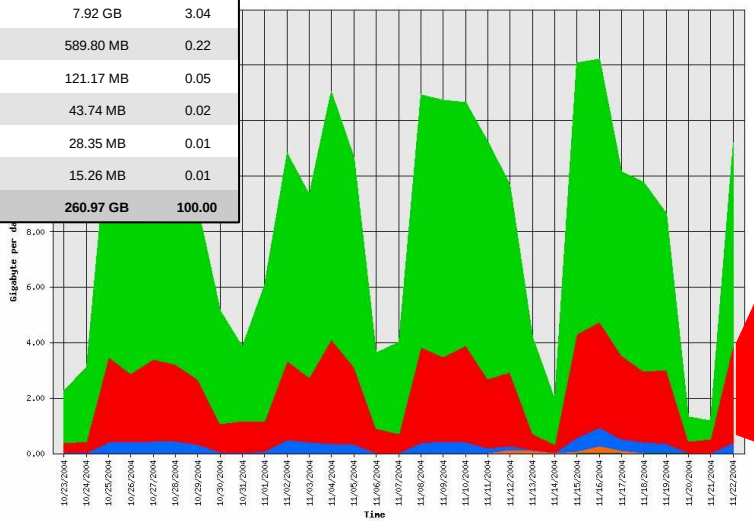
Welche Anwendungen werden in einer bestimmten Klasse transportiert ?

TOS	byte	%
(PREC 0)	185.12 GB	70.94
IP Precedence 5 (PREC 5)	67.15 GB	25.73
IP Precedence 6 (PREC 6)	7.92 GB	3.04
(PREC 4)	589.80 MB	0.22
IP Precedence 2 (PREC 2)	121.17 MB	0.05
(PREC 3)	43.74 MB	0.02
(PREC 1)	28.35 MB	0.01
(PREC 7)	15.26 MB	0.01
Summe	**260.97 GB**	**100.00**

Trend QoS Analyse

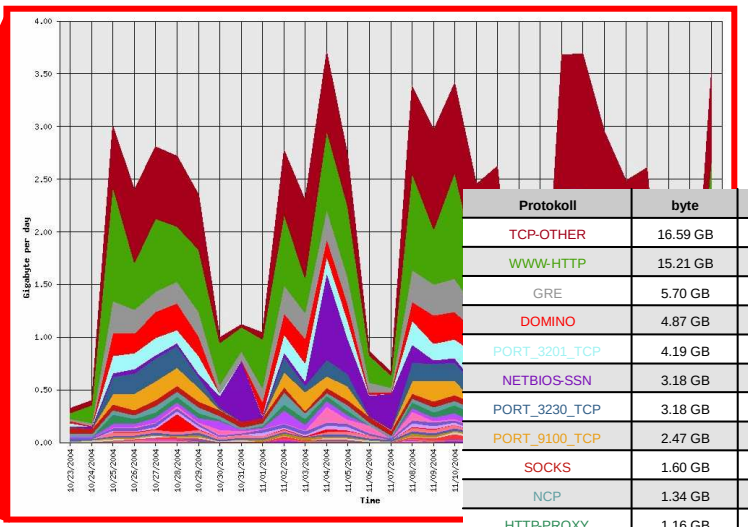
Es wurden keine Filter ausgewählt

23.10.2004- 22.11.2004
(Intervall 1 Tag)



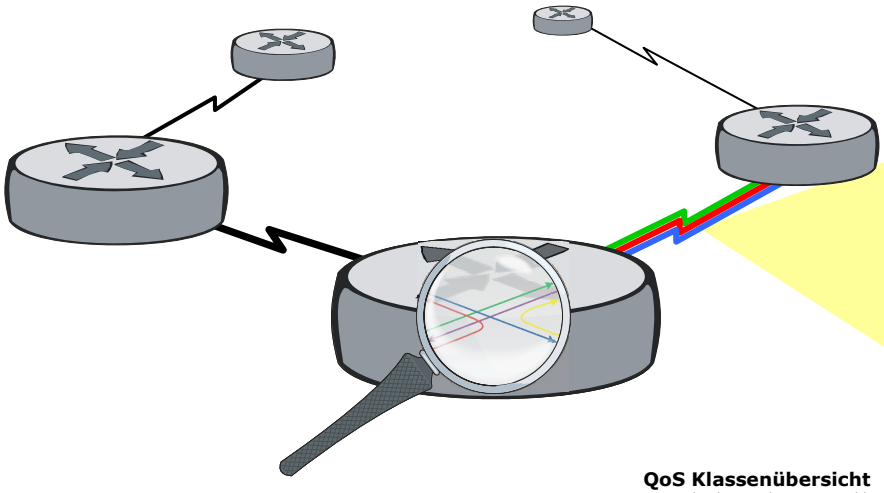
Trend Analyse

TOS: Precedence 5
23.10.2004- 22.11.2004
(Intervall 1 Tag)

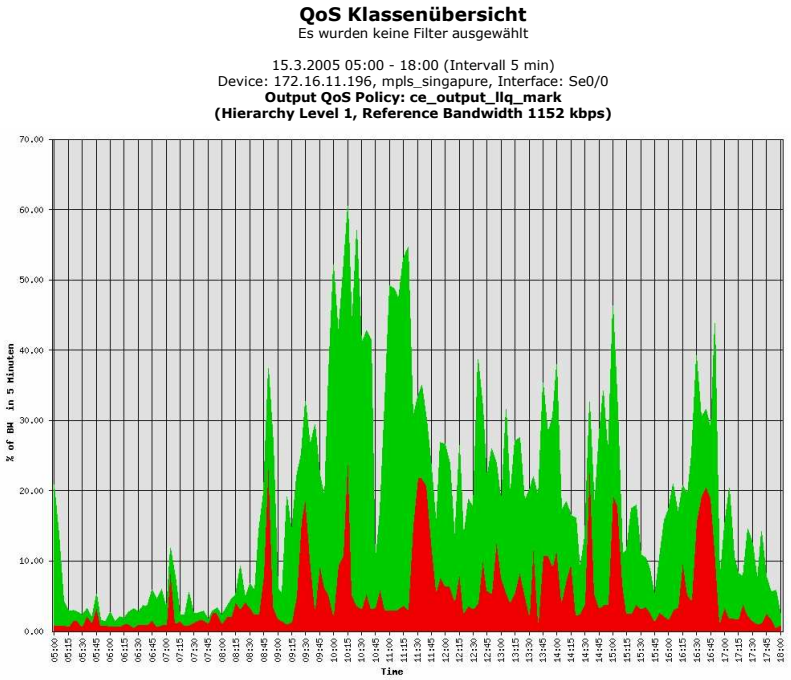


Protokoll	byte	%
TCP-OTHER	16.59 GB	25.03
WWW-HTTP	15.21 GB	22.94
GRE	5.70 GB	8.59
DOMINO	4.87 GB	7.35
PORT_3201_TCP	4.19 GB	6.32
NETBIOS-SSN	3.18 GB	4.80
PORT_3230_TCP	3.18 GB	4.79
PORT_9100_TCP	2.47 GB	3.73
SOCKS	1.60 GB	2.42
NCP	1.34 GB	2.02
HTTP-PROXY	1.16 GB	1.75
PRINTER	1.09 GB	1.65

QoS : Alarm für verworfene Pakete



Werden an irgendeinem Interface, in irgendeiner Klasse Pakete verworfen ?

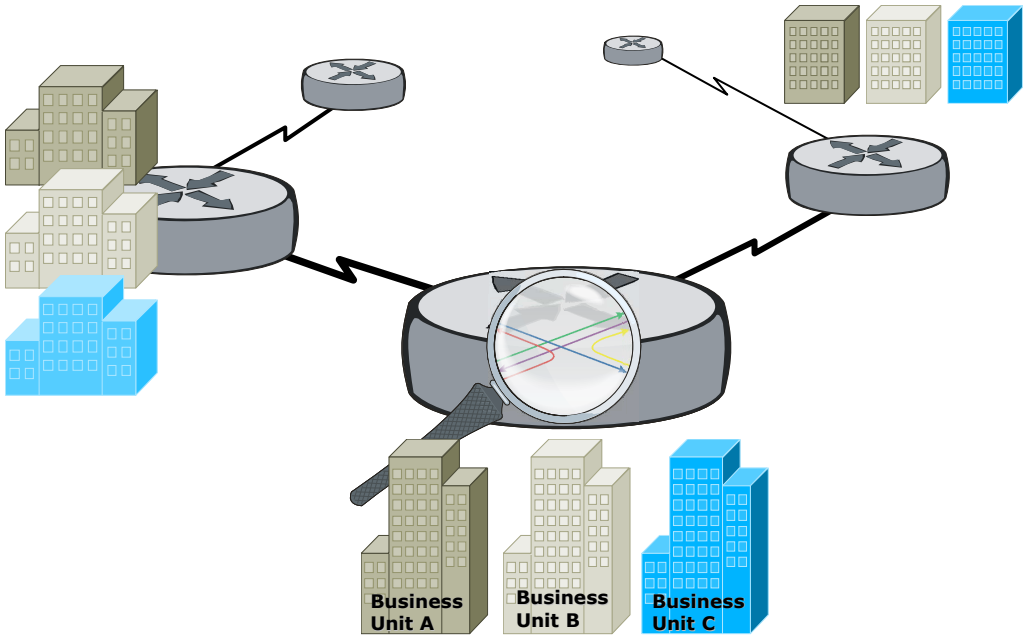


Service-Policy 'ce_output_llq_mark'

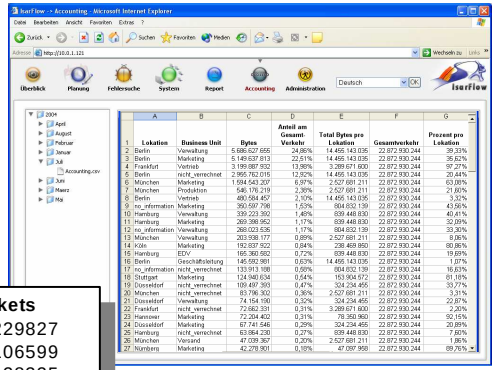
Klassenname	bytes	dropped bytes	%
class-default	876.67 MB	170.05 KB	71.77
ce_class_output	344.26 MB	0.00 B	28.18
ce-management-output	393.60 KB	0.00 B	0.03
Summe	**1.19 GB**	**170.05 KB**	**100%**

IsarFlow kann konfiguriert werden, Alarme zu schicken, wenn Schwellwerte über-schritten werden.

Accounting



Verschiedene Unternehmens-Bereiche nutzen weltweit an allen Lokationen das gleiche Netzwerk und müssen einzeln abgerechnet werden. **IsarFlow** bietet beliebig definierbare Abrechnungs-Modelle !



Department	Server	Bytes	Packets
OFFICE	File-Server	1004824231	1613270
VPN	File-Server	990160195	1421661
OFFICE	CENTRAL_SERVER	11683486	163493
LAB-Netz	File-Server	1444655	14326
LAB-Netz	GSX	1091862	10400
VPN	CENTRAL_SERVER	72492	1340
LAB-Netz	CENTRAL_SER	41039	302

Subnet 1	Subnet 2	Bytes	Packets
10.0.0.0/24	10.0.0.0/24	19831610	229827
217.233.0.0/16	217.233.0.0/16	30121694	106599
10.0.1.0/24	10.0.1.0/24	3058186	28325
10.0.0.0/24	10.0.1.0/24	2004413	25993
217.172.0.0/16	217.233.0.0/16	67038	58
	217.172.0.		

Subnet	VPN	Bytes	Packets
10.0.0.0/24	VPN-A	994,779,209	7,877,820
10.0.0.0/24	VPN-B	827,942,465	5,861,859
10.0.1.0/24	VPN-A	247,337,971	1,194,709
10.0.1.0/24	VPN-B	227,521,032	1,124,320
10.0.0.0/24	VPN-C	12,156,078	82,217

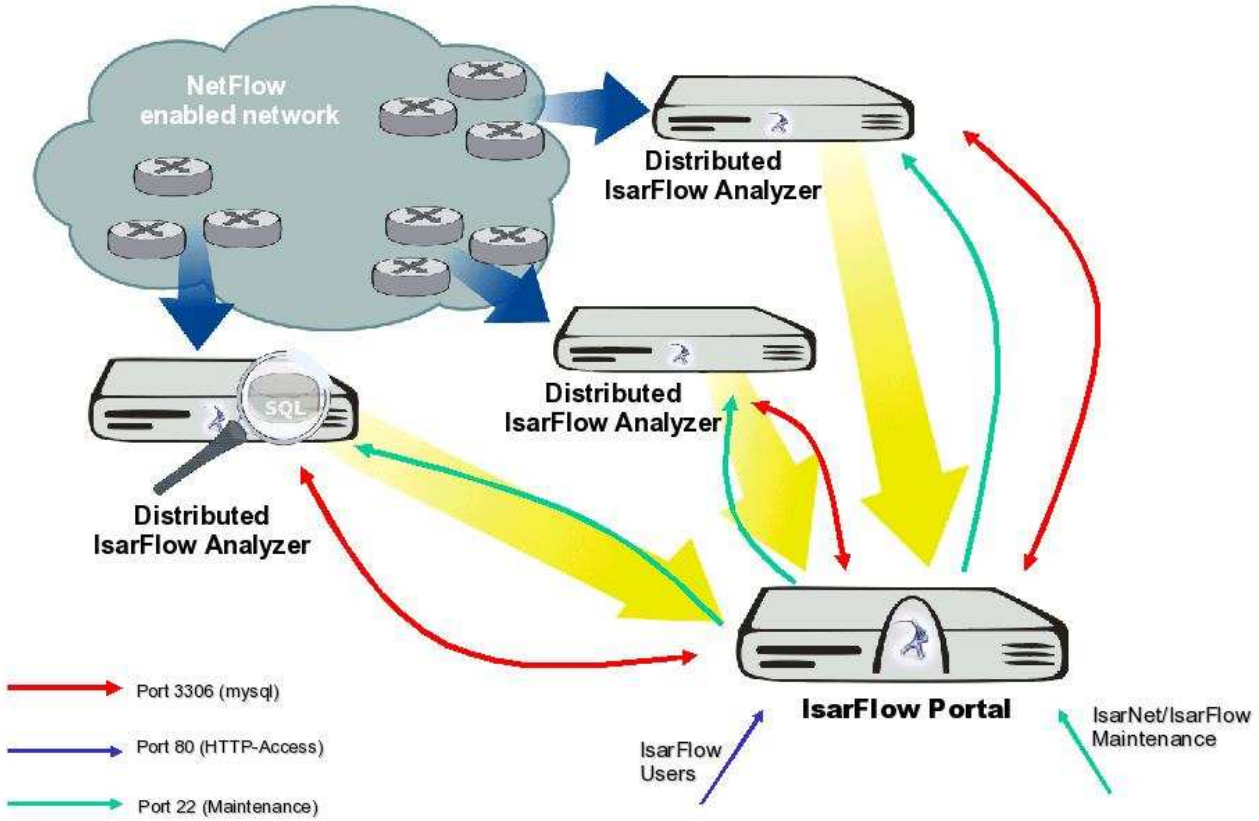
Subnet	TOS	Bytes	Packets
10.0.0.0/24	Class 1	248,516,917	4,080,459
10.0.0.0/24	Best Effort	676,835,942	3,560,342
172.20.0.0/16	Best Effort	603,613,403	2,399,300
10.0.1.0/24	Best Effort	290,322,449	1,384,079
172.20.0.0/16	Class 1	93,166,403	700,725
10.0.0.0/24	Class 2	113,686,488	477,787
172.20.0.0/16	Class 2	106,774,196	357,470
10.0.1.0/24	Class 1	16,859,674	287,261
10.0.1.0/24	Class 2	1,358,909	17,632

Was sind die Stärken von IsarFlow gegenüber anderen Netflow Tools ?

isarNet
Professional Networking

Skalierbarkeit

- Beliebige Skalierbarkeit durch ein dezentrales Datenbank-Modell
- Ein zentrales Portal für einfache Konfiguration & Analysen
- Hochverfügbarkeit für die IsarFlow Analyzer
- Referenz-Installation für 10 Milliarden flows/Tag



Vielfältige Anwendungsbereiche

IsarFlow

- **Accounting**
  (sehr flexible Konfiguration & viel Erfahrung mit großen Kunden)
- **QoS Monitoring**
  (Netflow & SNMP basiert)
- Fehlersuche
- Kapazitätsplanung
- Security

Support

IsarFlow

- Cisco Developer Partner Status
- Erfahrung mit Netzwerken großer Konzerne
- Kontinuierliche Entwicklung & Support (vs. open source)
- Partner in Deutschland, England, Österreich, USA und Singapur

Kontakt

IsarNet AG
Terminalstrasse Mitte 18
85356 München

Tel: +49 89 97007 401
Fax: +49 89 97007 200

info@isarnet.de

http://www.isarnet.de
http://www.isarflow.de

CISCO SYSTEMS

Technology
Developer
Partner