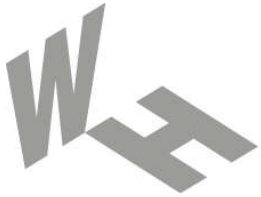


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Gefahr erkannt, Gefahr gebannt
→ Kommunikationslagebild

Prof. Dr. (TU NN)
Norbert Pohlmann

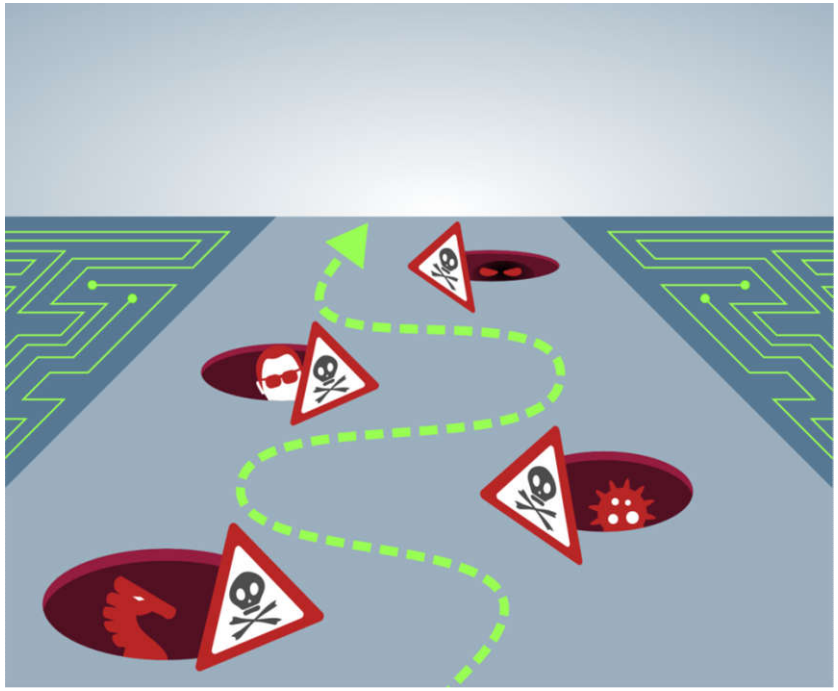
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Kommunikationslagebild
→ Gefahr erkannt, Gefahr gebannt

- Die **größte Gefahr** besteht immer dann,
  wenn Gefahren **falsch eingeschätzt** werden.

- Wer dagegen die **Gefahren kennt**,
  kann sich **besser schützen**.



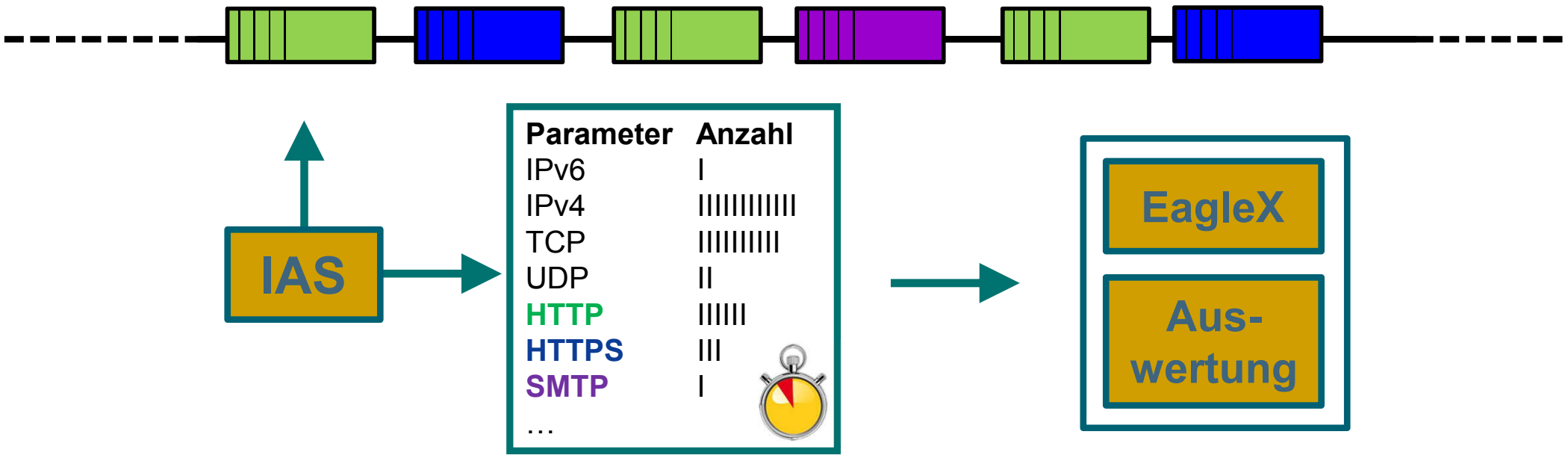
- Das **Internet-Analyse-System** erstellt ein **Kommunikationslagebild**

→ Angriffe und Schwachstellen erkennen

→ Gefahr bewerten

→ Risiko reduzieren

Internet-Analyse-System (IAS)
→ Generierung der Kommunikationslage



- Mehr als **3.000.000 potentielle Kommunikationsmerkmale** helfen, die Kommunikationslage zu **ermitteln**, **darzustellen** und **bewerten** zu können.
  - **Verschiedene Informationen in den Kommunikationsmerkmalen** (**Angriffe** *(Ports, SYN-ACK, …)*, **Technologien** *(User-Agent, Versionen, …)*, **Nutzung/Verteilung** *(alle)*, …)
  - Methode ist Datenschutzkonform (**Datenschutz by Design**)

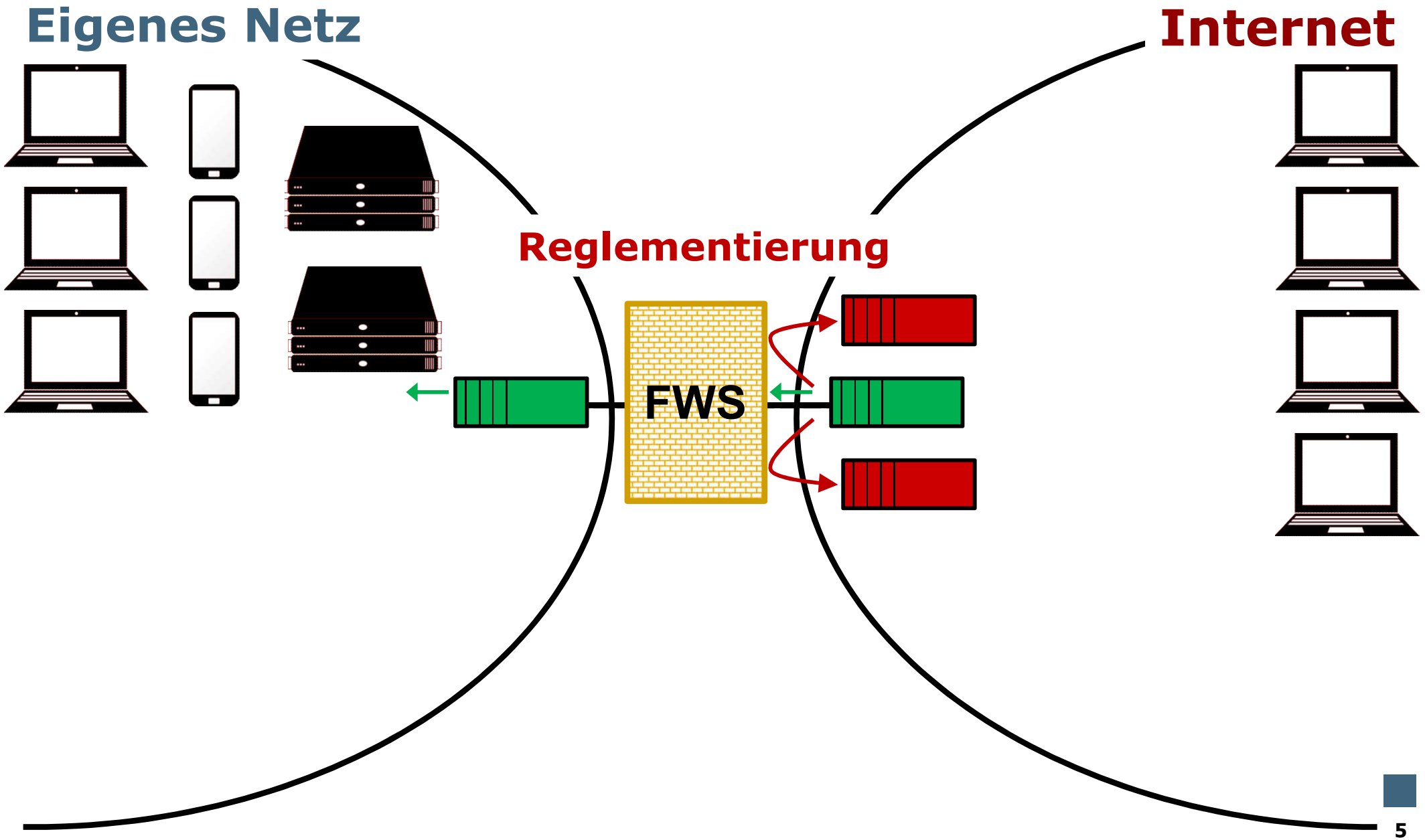
Internet-Analyse-System (IAS)
→ Ziele

- **Erkennen von Angriffssituationen**

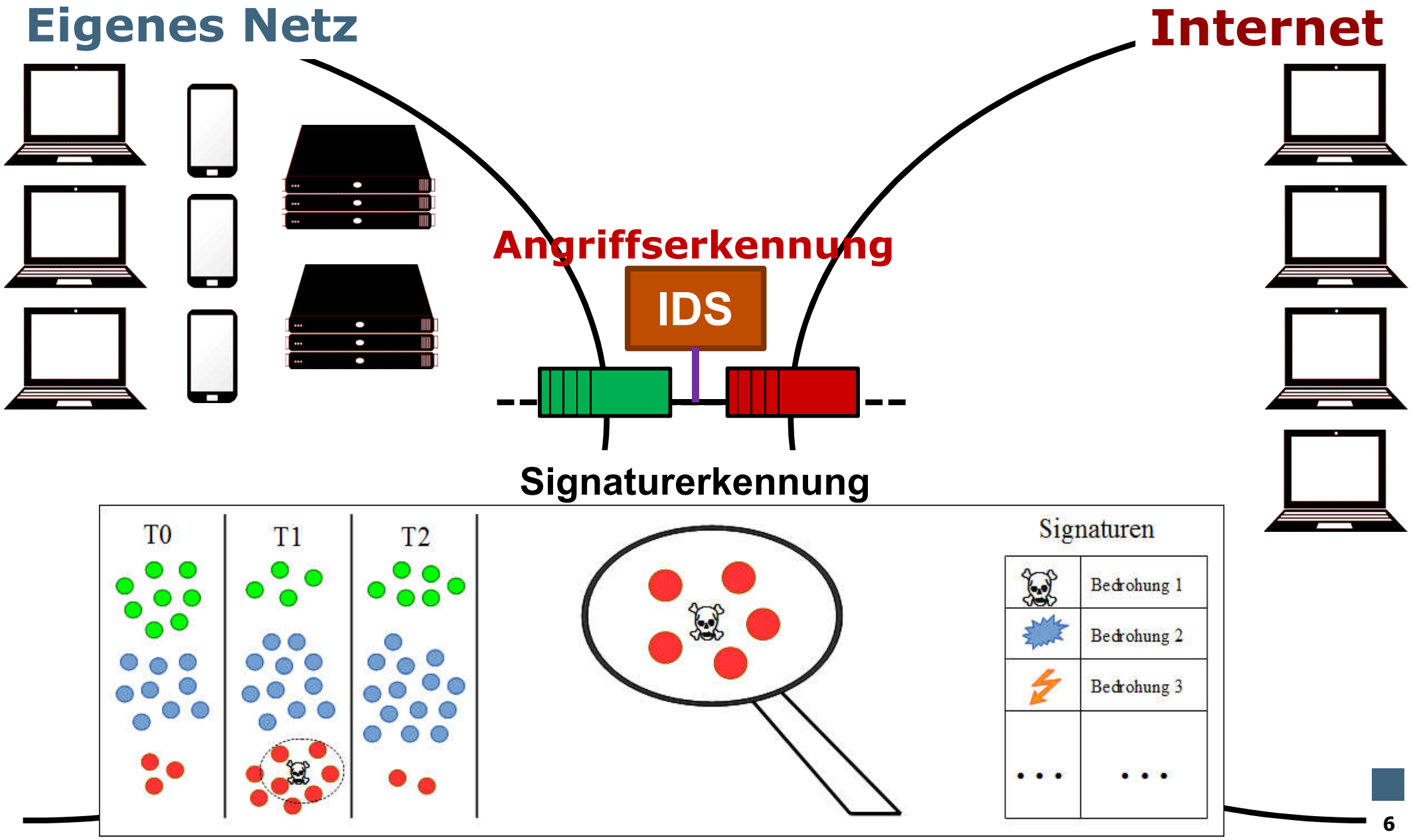
- **Experten-System für die Kommunikationssicherheit**
  - Umfängliche Darstellungen von Situationen
  - Favoriten-System für detaillierte Analysen (Angriffe, Probleme, …)
  - Wissensdatenbank, um Situationen bewerten zu können
  - …

- **Übersicht über das aktuelle Kommunikationslagebild (Report)**
  - Nutzungsverhalten der Kommunikationsprotokolle
  - Reale Verwendung von aktuellen und legacy Technologien (Betriebssystem, Browser, Sicherheitstools, …)
  - Anwendung von Verschlüsselung (HTTPS, IMAPS, POP3S, SMTPS, IPSec, …)
  - Verwendung von kryptographischen Profilen (SSL/TLS, …)
  - …

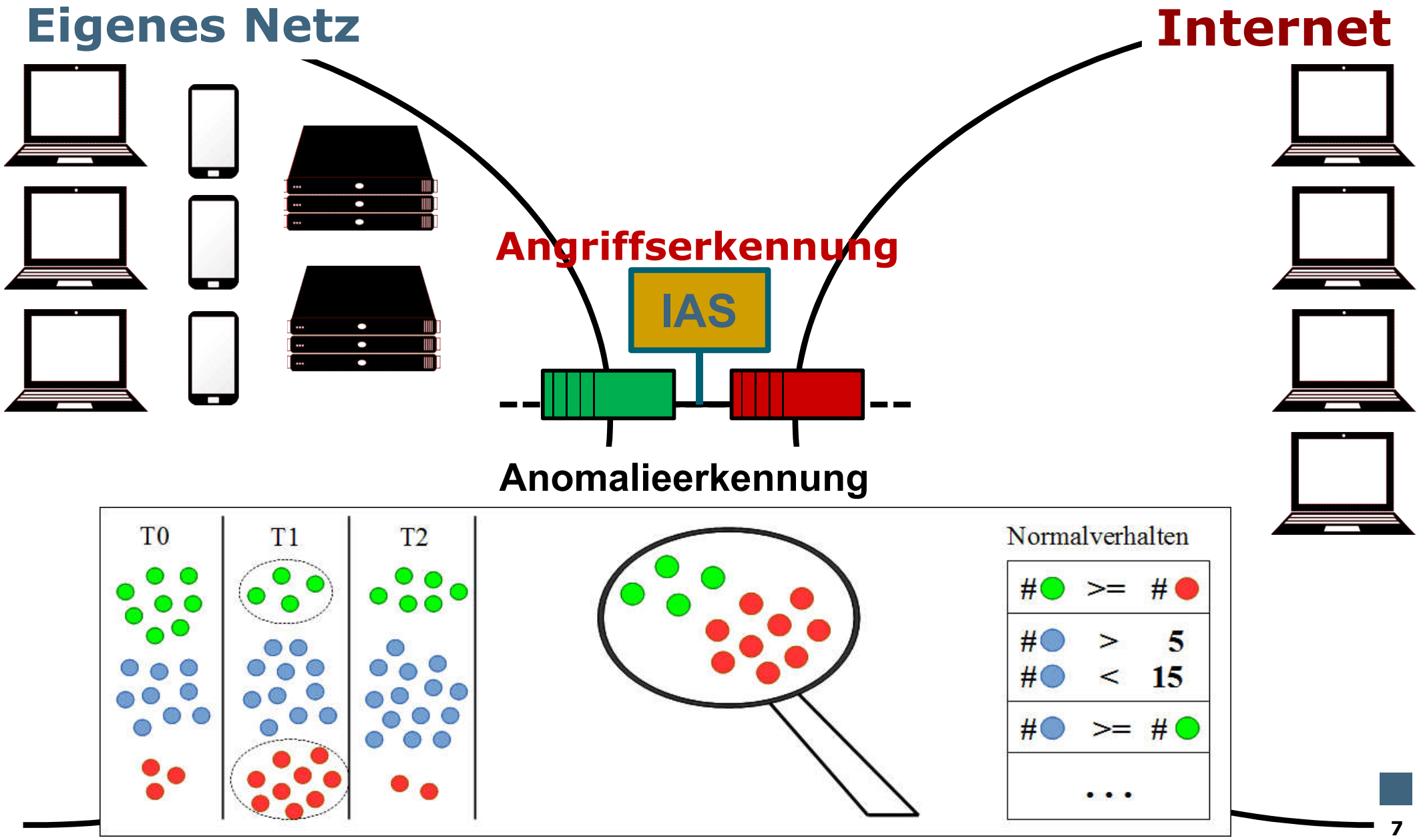
Kommunikationssicherheit
→ Firewall-Systems (FWS)



Kommunikationssicherheit
→ Intrusion Detection System (IDS)

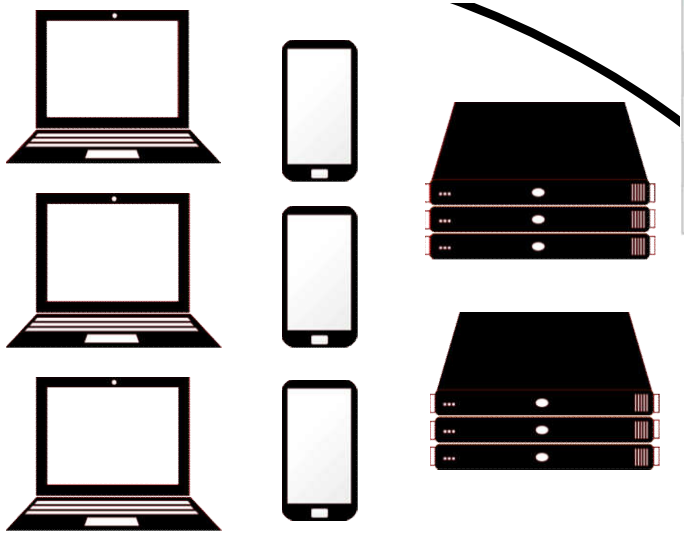


Kommunikationssicherheit
→ Internet-Analyse-System (IAS)



IAS: Nutzung, Verteilung, Verlauf, …
→ Kommunikationsprotokoll

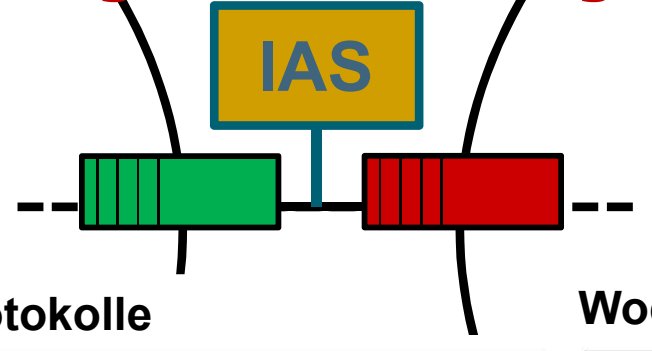
Eigenes Netz



Traffic Art

	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Src >= 1024 and Dst >= 1024 ("P2P") - client-to-client	49.922.825	10,66	23.096	0,31	6,44
Src < 1024 and Dst < 1024 ("B2B") - server-to-server	326.388	0,07	22	<0,01	<0,01
Src >= 1024 and Dst < 1024 ("P2B") - client-to-server	152.183.466	32,49	22.752	0,30	6,35
Src < 1024 and Dst >= 1024 ("B2P") - server-to-client	266.037.102	56,79	312.589	4,13	87,20
Gesamt	**468.469.781**	**100,00**	**358.458**	**4,74**	**100,00**

Angriffserkennung



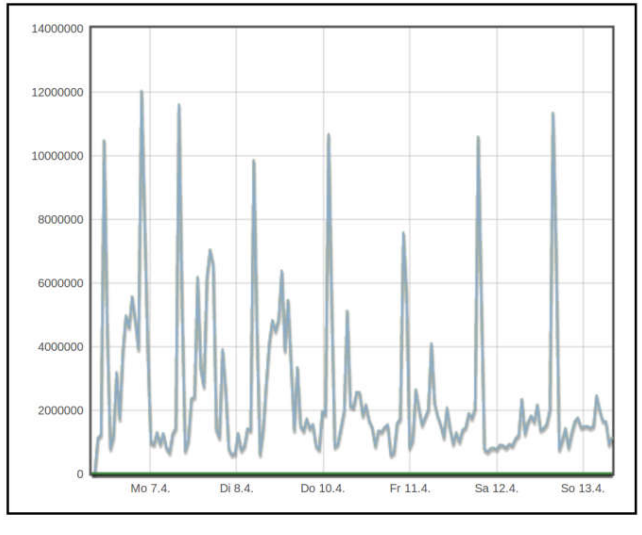
Traffic

	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Gesamt	725.009.432	100,00	413.780,64	5,47	100,00
VLAN	724.973.419	>99,99	413.776,38	5,47	>99,99
IPv4	724.970.615	>99,99	413.776,38	5,47	>99,99
IPv6	36.013	<0,01	4,25	<0,01	<0,01
Teredo	36.013	<0,01	4,25	<0,01	<0,01
ARP	2.804	<0,01	<0,01	<0,01	<0,01

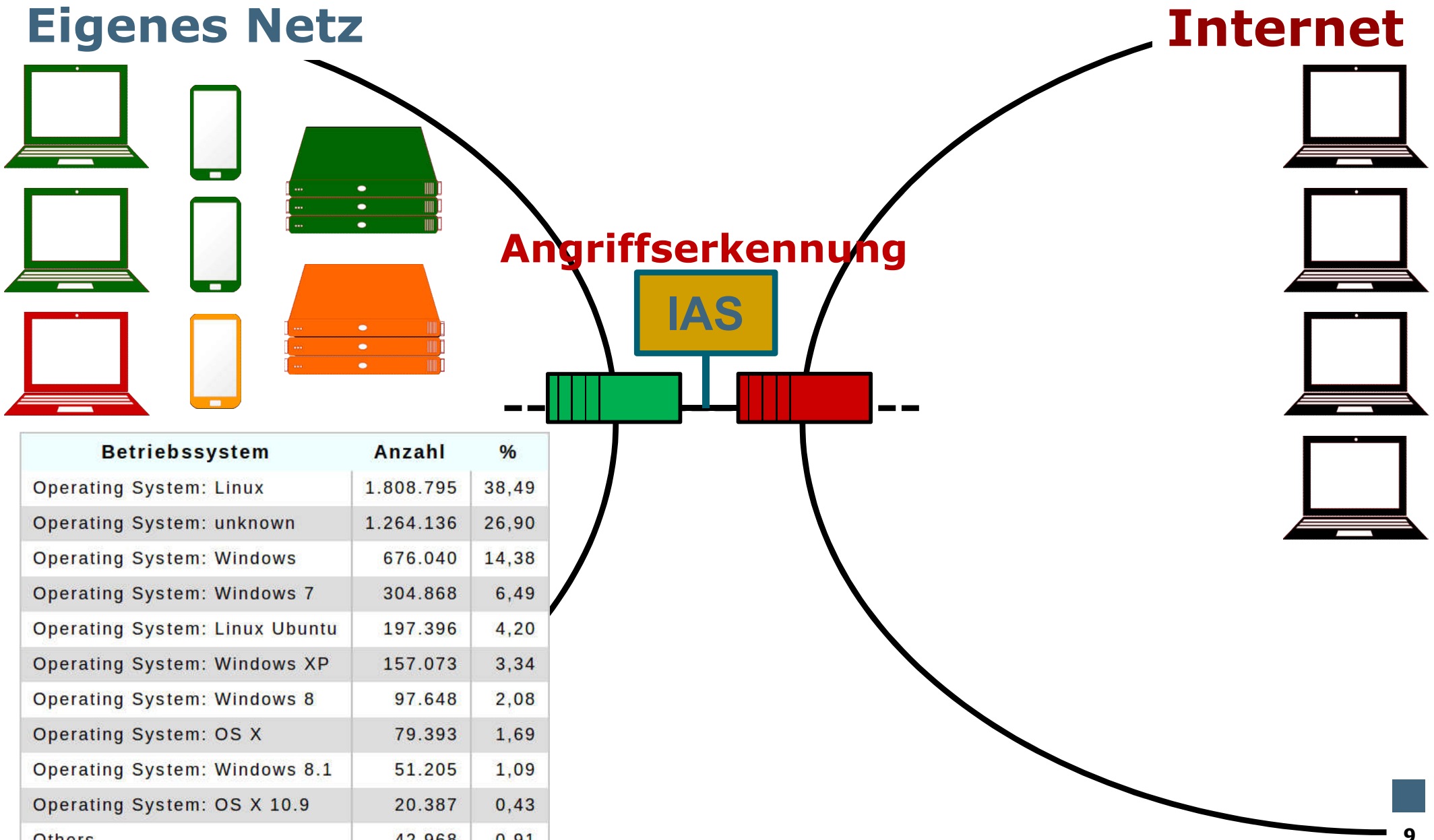
TOP Kommunikationsprotokolle

Port		Pakete		Traffic	Bandbreite	
	Richtung	Anzahl	%	MB	Mbps	%
80 (HTTP)	DST	64.684.674	15,53	6.247	<0,01	1,87
	SRC	119.764.297	28,76	152.480	2,02	45,53
	Alle	**184.448.971**	**44,29**	**158.726**	**2,10**	**47,39**
22 (SSH)	DST	36.189.875	8,69	6.821	<0,01	2,04
	SRC	73.040.334	17,54	98.176	1,30	29,31
	Alle	**109.230.209**	**26,23**	**104.997**	**1,39**	**31,35**
443 (HTTPS)	DST	30.334.171	7,28	5.568	<0,01	1,66
	SRC	47.446.836	11,39	49.740	<0,01	14,85
	Alle	**77.781.007**	**18,68**	**55.308**	**<0,01**	**16,51**

Wochenverlauf

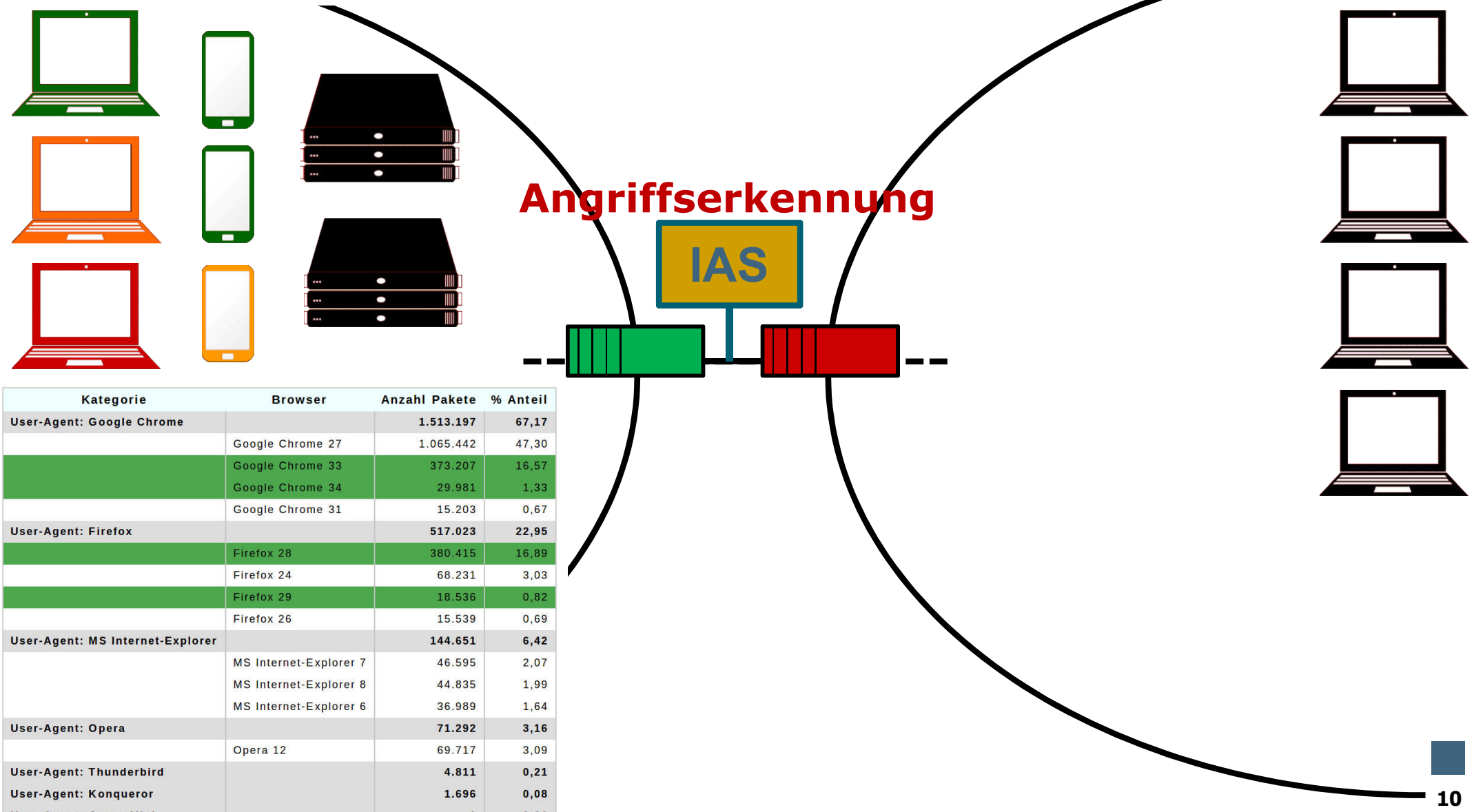


IAS: Schwachstellen
→ Betriebssystemnutzung



Betriebssystem	Anzahl	%
Operating System: Linux	1.808.795	38,49
Operating System: unknown	1.264.136	26,90
Operating System: Windows	676.040	14,38
Operating System: Windows 7	304.868	6,49
Operating System: Linux Ubuntu	197.396	4,20
Operating System: Windows XP	157.073	3,34
Operating System: Windows 8	97.648	2,08
Operating System: OS X	79.393	1,69
Operating System: Windows 8.1	51.205	1,09
Operating System: OS X 10.9	20.387	0,43
Others	42.968	0,91

IAS: Schwachstellen
→ Browsernutzung

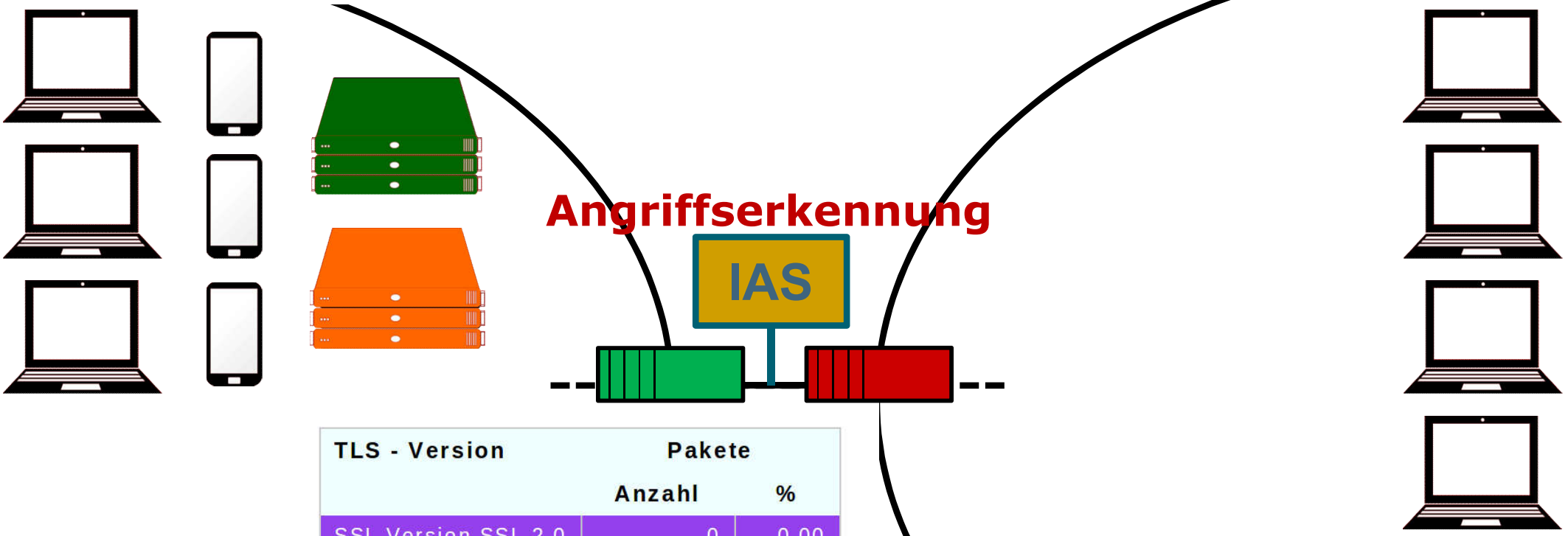


Kategorie	Browser	Anzahl Pakete	% Anteil
User-Agent: Google Chrome		**1.513.197**	**67,17**
	Google Chrome 27	1.065.442	47,30
	Google Chrome 33	373.207	16,57
	Google Chrome 34	29.981	1,33
	Google Chrome 31	15.203	0,67
User-Agent: Firefox		**517.023**	**22,95**
	Firefox 28	380.415	16,89
	Firefox 24	68.231	3,03
	Firefox 29	18.536	0,82
	Firefox 26	15.539	0,69
User-Agent: MS Internet-Explorer		**144.651**	**6,42**
	MS Internet-Explorer 7	46.595	2,07
	MS Internet-Explorer 8	44.835	1,99
	MS Internet-Explorer 6	36.989	1,64
User-Agent: Opera		**71.292**	**3,16**
	Opera 12	69.717	3,09
User-Agent: Thunderbird		**4.811**	**0,21**
User-Agent: Konqueror		**1.696**	**0,08**
User-Agent: Opera Mini		**1**	**<0,01**

IAS: Schwachstellen
→ TLS/SSL-Nutzung

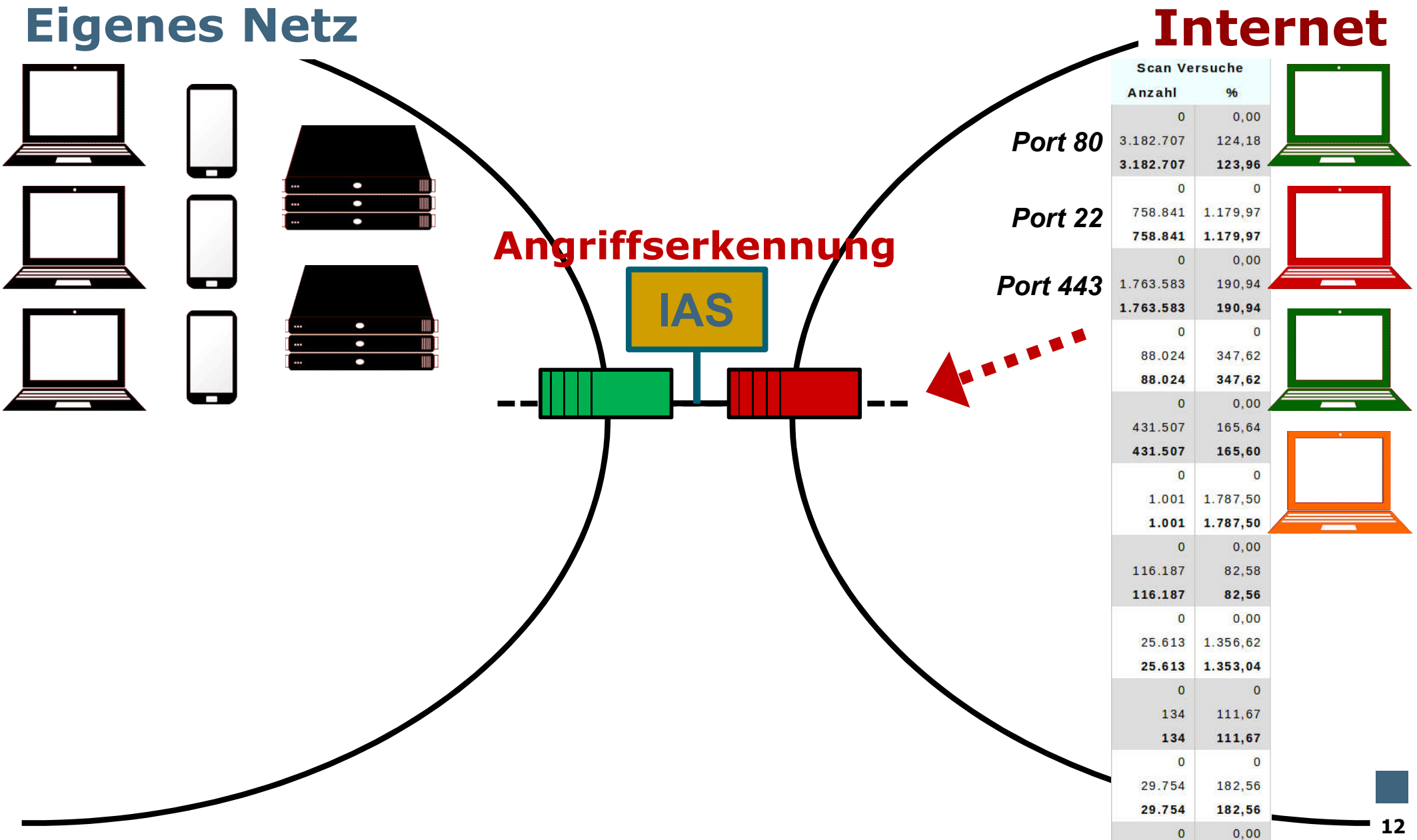
Eigenes Netz

Internet



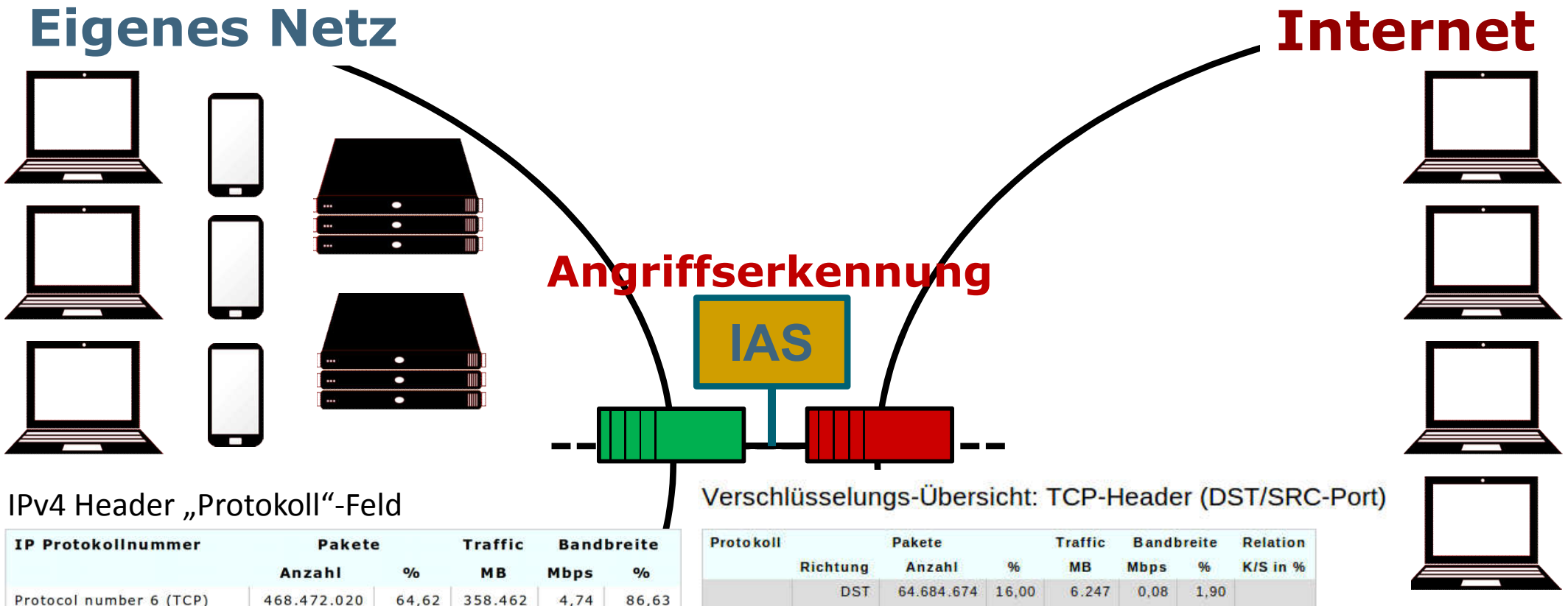
TLS - Version	Pakete	
	Anzahl	%
SSL Version SSL 2.0	0	0,00
SSL Version SSL 3.0	25.989	0,12
SSL Version TLS 1.0	10.154.344	48,42
SSL Version TLS 1.1	608.026	2,90
SSL Version TLS 1.2	10.182.293	48,55
SSL Version Other	0	0,00
Gesamt	**20.970.652**	**100,00**

IAS: Angriffspotential
→ Port-Scan-Potential



Scan Versuche	
Anzahl	%
0	0,00
3.182.707	124,18
3.182.707	**123,96**
0	0
758.841	1.179,97
758.841	**1.179,97**
0	0,00
1.763.583	190,94
1.763.583	**190,94**
0	0
88.024	347,62
88.024	**347,62**
0	0,00
431.507	165,64
431.507	**165,60**
0	0
1.001	1.787,50
1.001	**1.787,50**
0	0,00
116.187	82,58
116.187	**82,56**
0	0,00
25.613	1.356,62
25.613	**1.353,04**
0	0
134	111,67
134	**111,67**
0	0
29.754	182,56
29.754	**182,56**
0	0,00

IAS: Nutzung, Verteilung, Verlauf, …
→ Anwendung von Verschlüsselung



IPv4 Header „Protokoll“-Feld

IP Protokollnummer	Pakete		Traffic	Bandbreite	
	Anzahl	%	MB	Mbps	%
Protocol number 6 (TCP)	468.472.020	64,62	358.462	4,74	86,63
Protocol number 17 (UDP)	237.139.295	32,71	53.729	0,71	12,99
Protocol number 1 (ICMP)	18.914.729	2,61	1.582	0,02	0,38
Protocol number 50 (ESP)	5.799.799	0,8	<1	<0,01	<0,01
Protocol number 2 (IGMP)	4.431	<0,01	2	<0,01	<0,01
Protocol number 132 (SCTP)	12	<0,01	<1	<0,01	<0,01
Protocol number 46 (RSVP)	1	<0,01	<1	<0,01	<0,01
Rest	0	0,00	0	0,00	0,00
Gesamt	**724.974.918**	**100,00**	**413.776**	**5,47**	**100,00**

Jedes 125. Paket
ist IPSec verschlüsselt

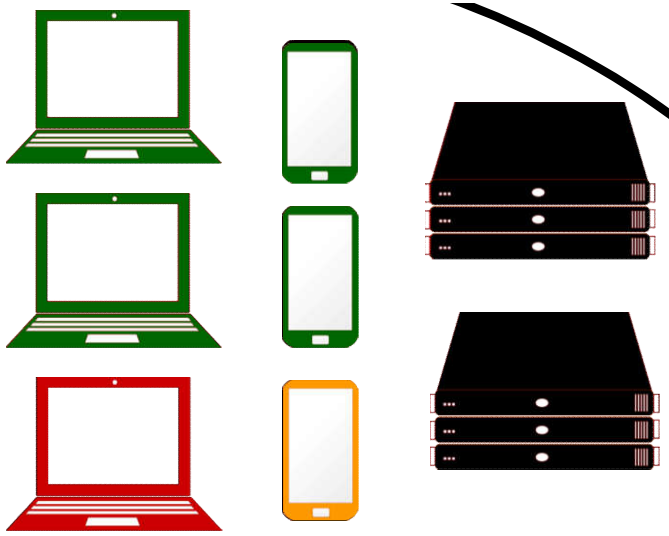
Verschlüsselungs-Übersicht: TCP-Header (DST/SRC-Port)

Protokoll		Pakete		Traffic	Bandbreite		Relation
	Richtung	Anzahl	%	MB	Mbps	%	K/S in %
HTTP	DST	64.684.674	16,00	6.247	0,08	1,90	
	SRC	119.764.297	29,00	152.480	2,02	46,00	74,16
	Alle	**184.448.971**	**45,00**	**158.726**	**2,10**	**47,90**	
HTTPS	DST	30.334.171	7,30	5.568	0,07	1,70	
	SRC	47.446.836	11,00	49.740	0,66	15,00	25,84
	Alle	**77.781.007**	**18,30**	**55.308**	**0,73**	**16,70**	
SMTP	DST	3.681.795	0,89	2.341	0,03	0,70	
	SRC	2.759.396	0,66	260	<0,01	0,08	95,94
	Alle	**6.441.191**	**1,55**	**2.602**	**0,03**	**0,78**	
SMTPS	DST	180.931	0,04	105	<0,01	0,03	
	SRC	61.817	0,02	5	<0,01	<0,01	4,06
	Alle	**242.748**	**0,06**	**110**	**<0,01**	**0,03**	
POP3	DST	104.942	0,02	10	<0,01	<0,01	
	SRC	105.330	0,02	46	<0,01	0,01	61,13
	Alle	**210.272**	**0,05**	**56**	**<0,01**	**0,02**	

Jedes 7. Paket
ist SSL
verschlüsselt

IAS: Schwachstellen
→ Crypto Profile

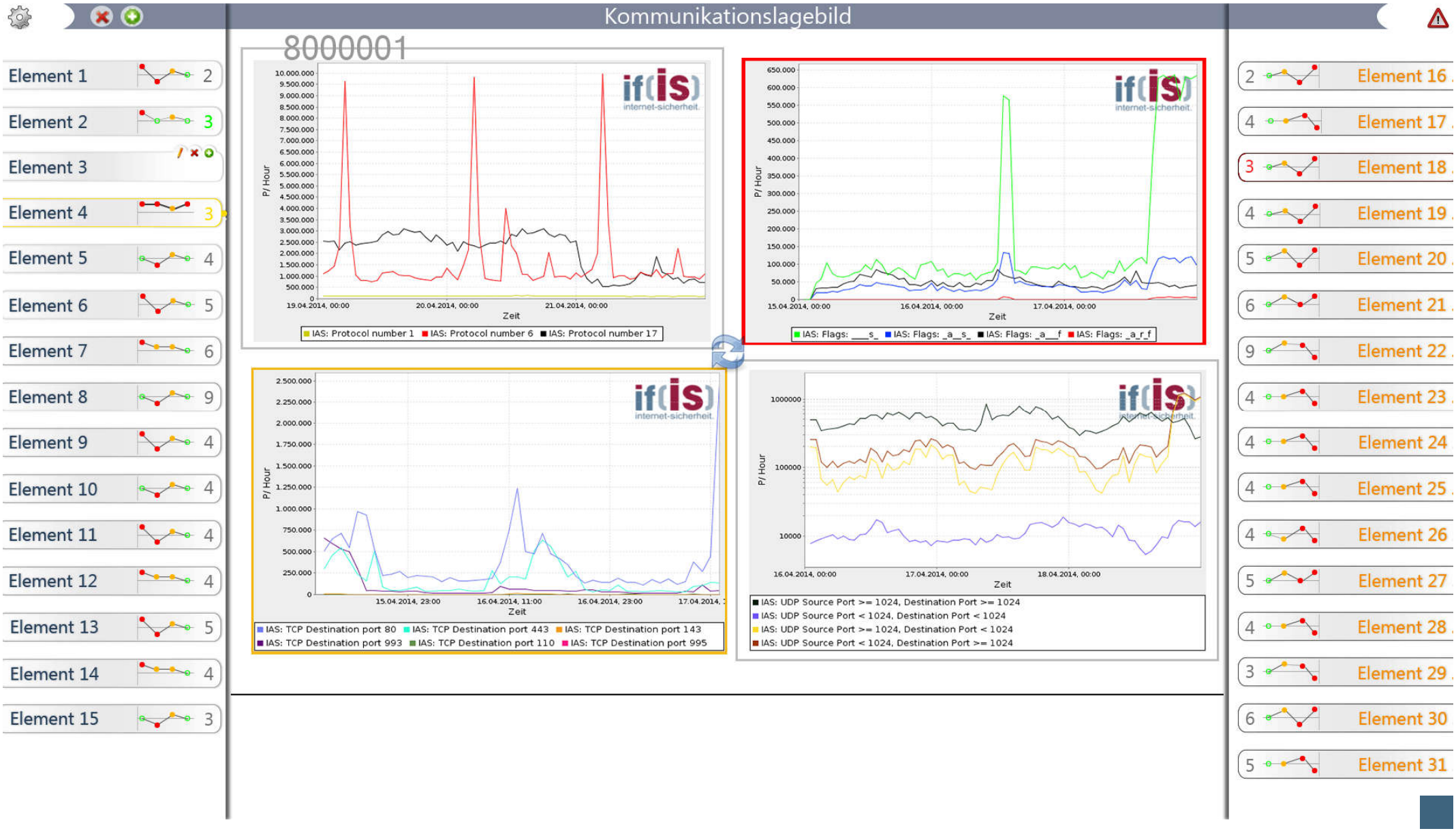
Eigenes Netz



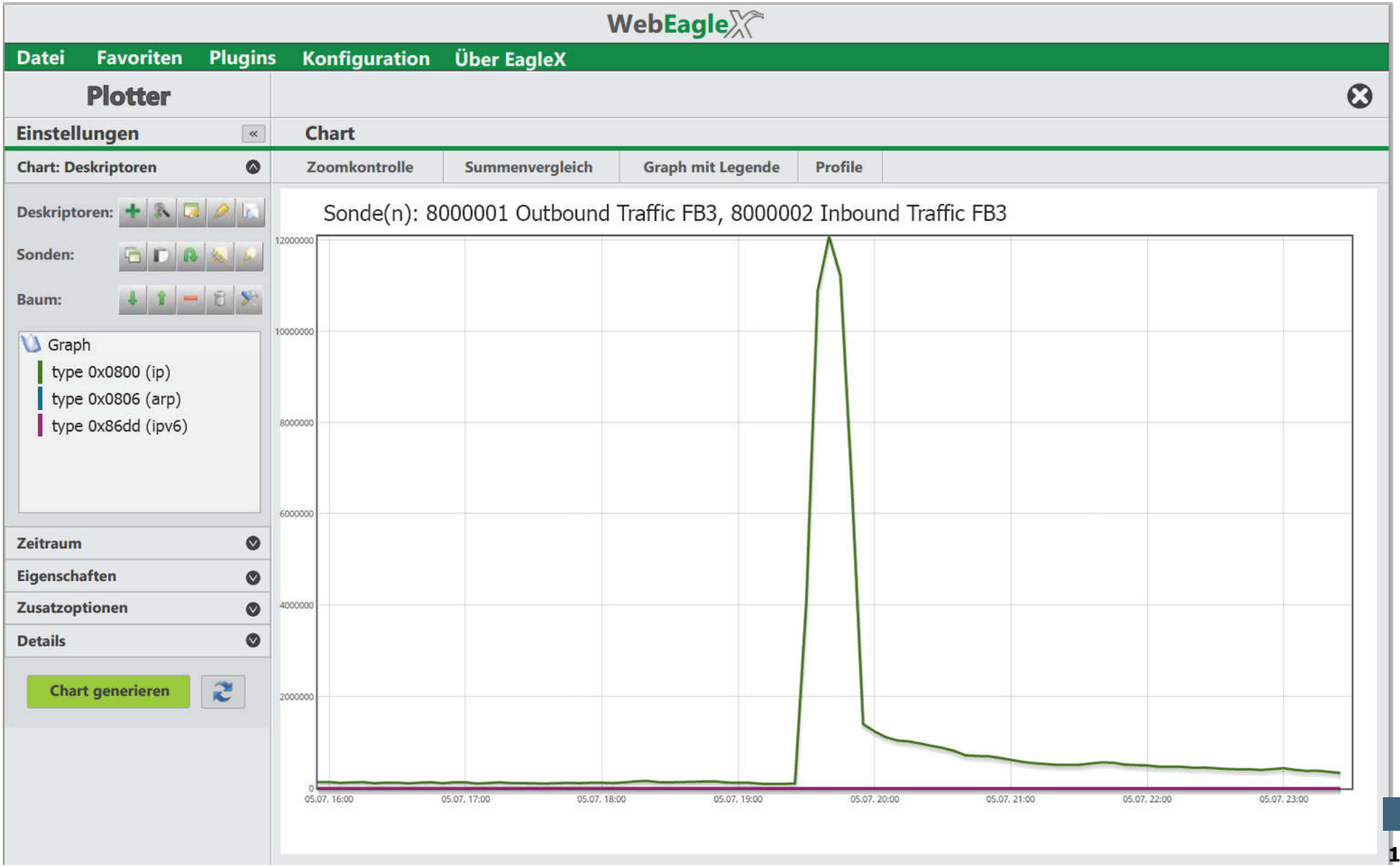
Verschlüsselungsart	Pakete	
	Anzahl	%
TLS_RSA_WITH_AES_256_CBC_SHA	175.682	20,29
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	149.562	17,28
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	567	0,07
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	1.409	0,16
TLS_RSA_WITH_AES_256_CBC_SHA256	1.839	0,21
TLS_RSA_WITH_AES_256_GCM_SHA384	43	<0,01
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	3.269	0,38
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	23.178	2,68
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	15	<0,01
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	114	0,01
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	255	0,03
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	22	<0,01
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	23.594	2,73
TLS_RSA_PSK_WITH_AES_256_CBC_SHA	39	<0,01
TLS_PSK_WITH_AES_256_CBC_SHA384	2	<0,01
TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384	1	<0,01
TLS_RSA_WITH_AES_128_CBC_SHA256	14.027	1,62
TLS_RSA_WITH_AES_128_GCM_SHA256	85.313	9,85
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	9	<0,01
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	5.626	0,65
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	180	0,02
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	102.224	11,81
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	37.434	4,32
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	1.324	0,15
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	2	<0,01
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	11.789	1,36
TLS_RSA_WITH_AES_128_CBC_SHA	39.527	4,57
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	14.659	1,69
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	4	<0,01
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	1.507	0,17
TLS_ECDHE_RSA_WITH_RC4_128_SHA	37.733	4,36
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	5	<0,01
TLS_RSA_WITH_RC4_128_MD5	13.660	1,58
TLS_RSA_WITH_RC4_128_SHA	116.392	13,44
TLS_RSA_WITH_3DES_EDE_CBC_SHA	3.578	0,41
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	32	<0,01
SSL_TRIPLE_DES_SHA_US	1	<0,01
Cipher Suite Used Unassigned	550	0,06
Cipher Suite Used Other	550	0,06
SSL_TRIPLE_DES_SHA_US	1	<0,01

Internet

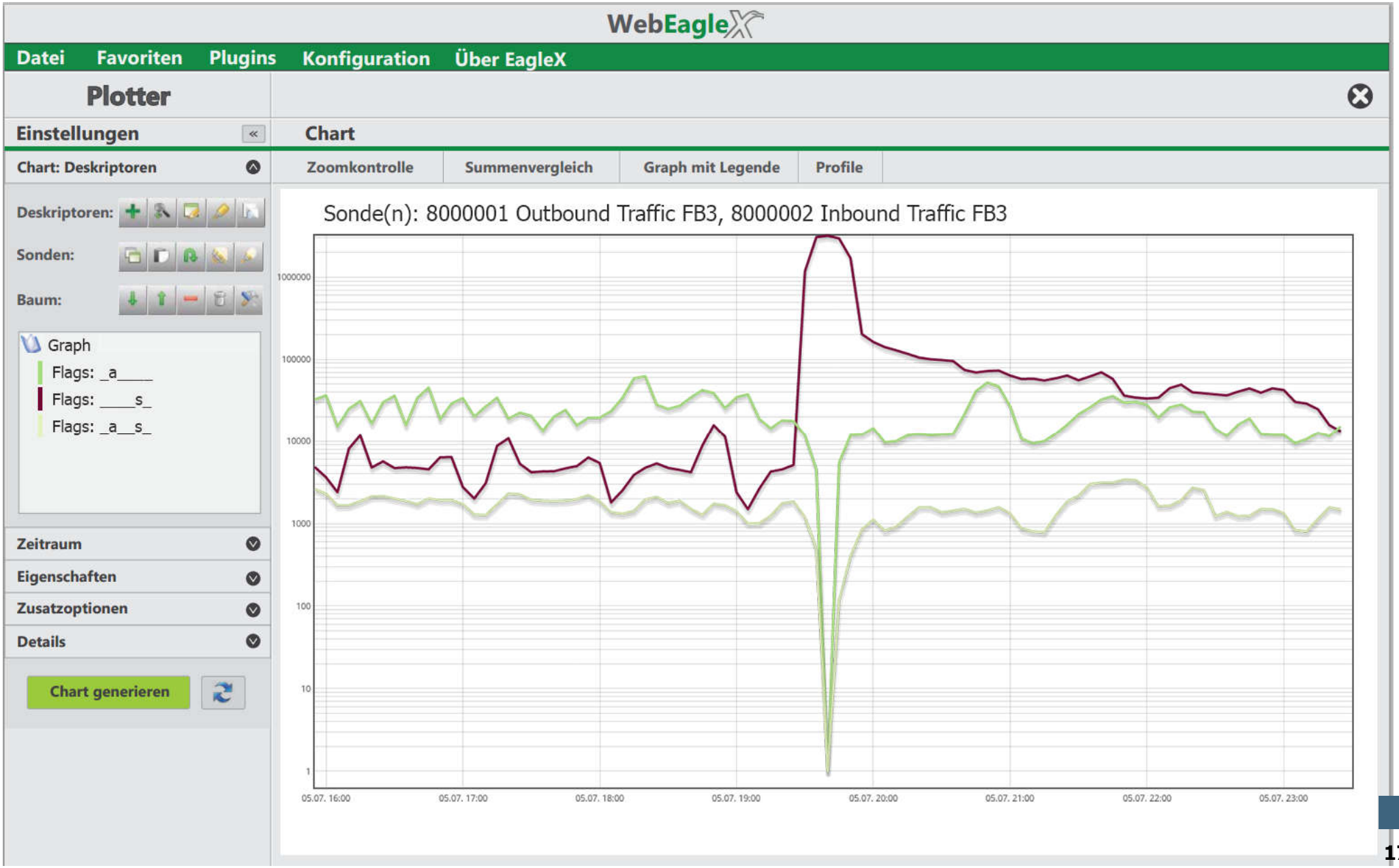
Wichtige Kommunikationsparameter
→ auf einen Blick (Live-Übersicht)



Experten-System
→ Detaillierte Betrachtung (1/2)



Experten-System
→ Detaillierte Betrachtung (2/2)



Internet-Analyse-System (IAS)
→ Vorteile

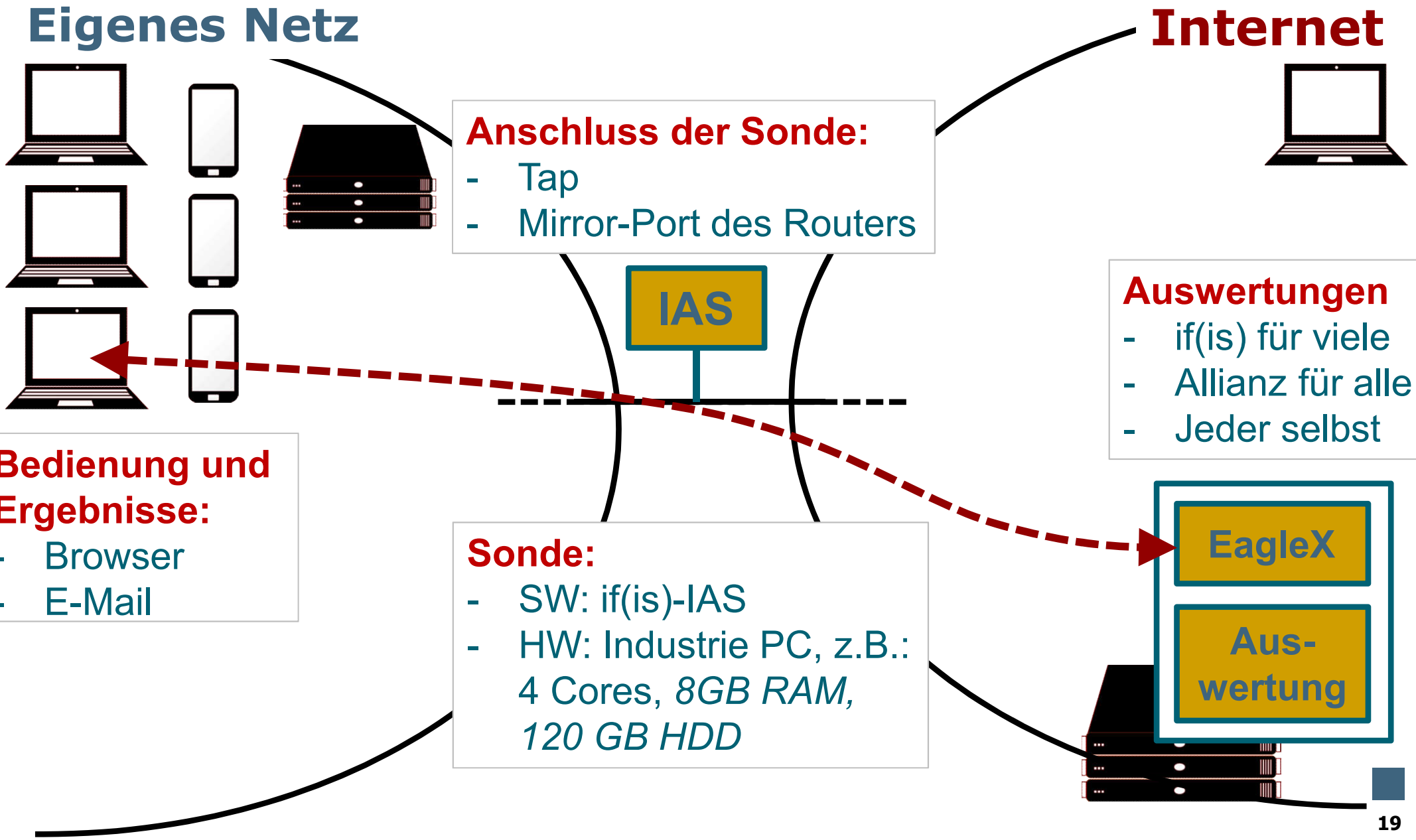
- **Erfüllt die Datenschutzauflagen**
  - Datenschutz by Design
  - Keine Mitarbeiterüberwachung möglich

- **IT Security made in Germany**
  - Einhaltung des Qualitätszeichens von TeleTrusT (Entwicklung in DE, keine Backdoors, …)
  - Common Criteria Profil, Code ist OpenSource
  - BSI nutzt das Internet-Analyse-System im Regierungsnetz

- **Automatisierte, intelligente Berichte für das Kommunikationslagebild**

- **Nutzung eines Experten-Systems für die Kommunikationssicherheit**

Einfache Umsetzung
→ Die ersten Schritte mit dem IAS



Weitere Schritte
→ Ideen

- **Viele Organisationen nutzen das IAS, um Erfahrungen zu sammeln**
  (Gleiche Methoden zur Messung → Ergebnisse können verglichen werden)
  - Kosten kein Geld (nur eigene Hardware für Sonde)
  - „Bezahlen“ mit Feedback

- **Berechnung von globalen Kommunikationsrisiken**
  (Zusammenarbeit, weniger Risiko, geringere Kosten für jeden)
  - Anonymer Vergleich von hilfreichen Werten (Nutzungen, Bedrohungen, …)
  - Hilfestellung bei den richtigen Maßnahmen
  - Höhere gemeinsame IT-Sicherheit

- **Weitere Entwicklungen des IAS**
  - Botnetz-Erkennung, Anwendungserkennung, …
  - Feedback soll Richtung positiv beeinflussen,
    dadurch höherer Mehrwert für alle

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Gefahr erkannt, Gefahr gebannt
→ Kommunikationslagebild

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.