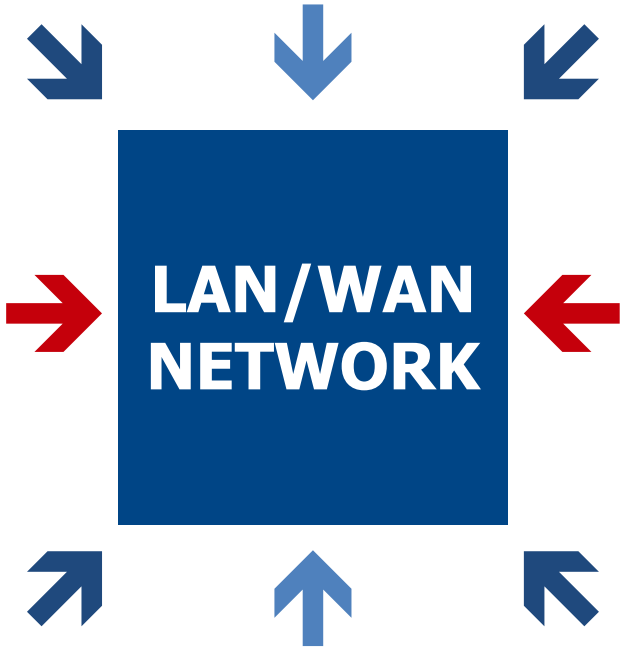
Synapse Networks - Magic Distributed Monitoring & Analysis (SYN-MA)

Fehler-Analyse / Troubelshooting

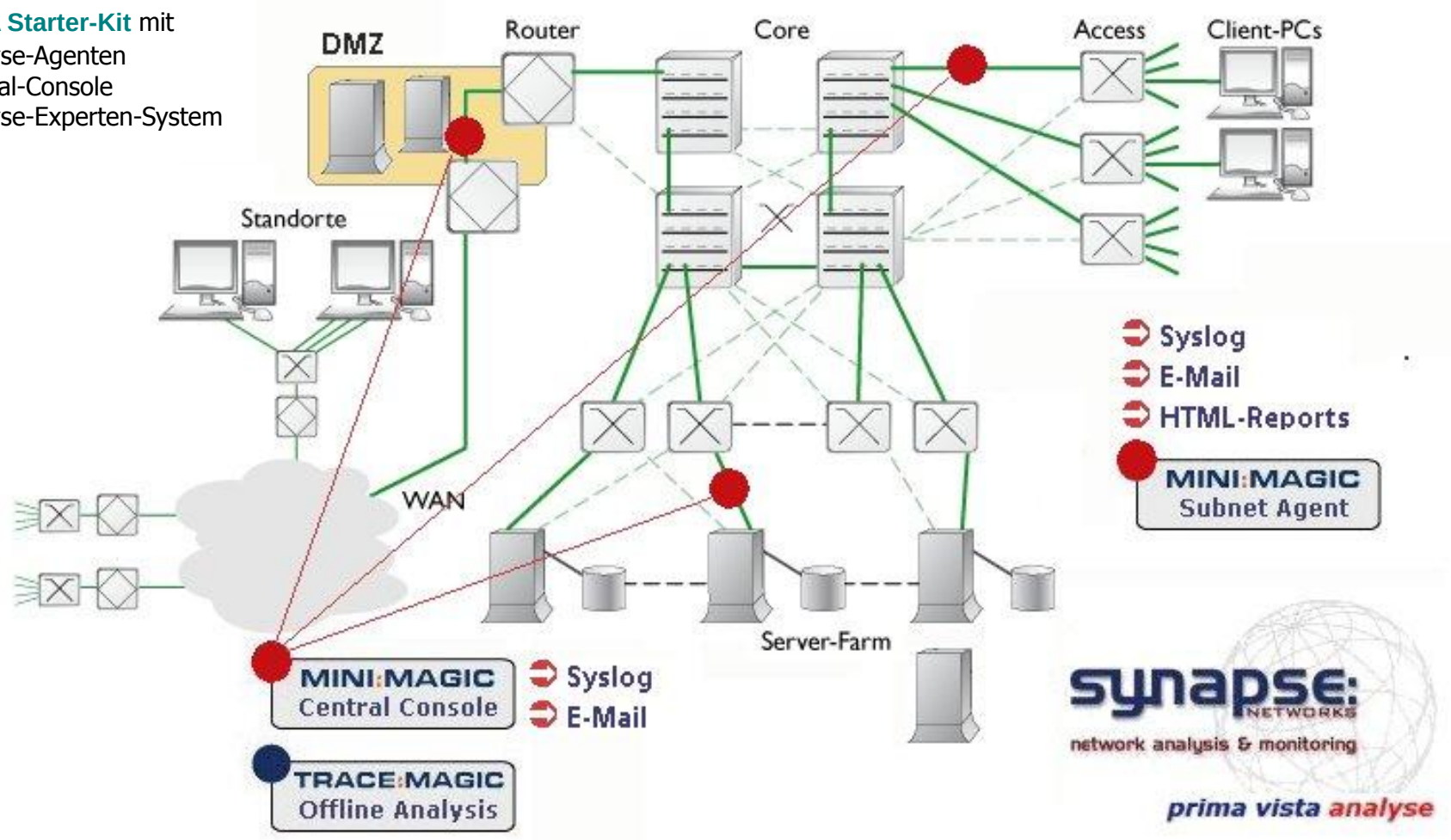
Verbindungs-Abbrüche, DNS-Fehler, lange Logon-Zeiten, Applikations-Probleme, Routing-Fehler, Schwierigkeiten bei AD-Integration/Migration, ...



Erkennung von Sicherheits-Gefahren

DMZ-Lücken, ungesicherte Namensdienste, gefährliche Web-Applikationen, interne Sicherheits-Minderungen durch Migrations-Unschärfen, zweideutige Adressen, ...

SYN-MA Starter-Kit mit
- 3 Analyse-Agenten
- 1 Zentral-Console
- 1 Analyse-Experten-System



Synapse Networks - Magic Distributed Monitoring & Analysis (SYN-MA)

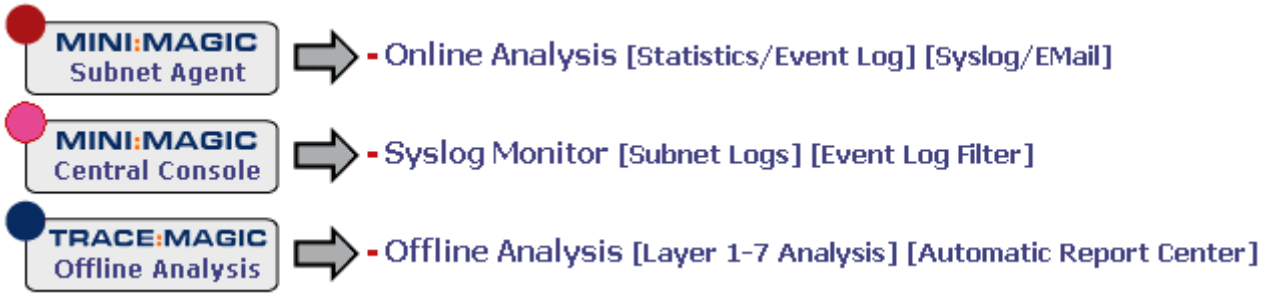
Ein typischer, erster Aufbau der **SYN-MA** beginnt mit folgender Einrüstung von Messtechnik:

- Analyse-Agenten in …

  - ➔ DMZ (Internet)
  - ➔ RZ / Domain Server (DHCP,DNS,AD)
  - ➔ Subnet / zunächst beginnend mit einer ersten, repräsentativen Client-Workgroup
  - ➔ Außenstellen / verteilte Standorte (weltweit)

  Diese Analyse-Agenten sind Standard-PCs (Windows-XP, 2 GB RAM, 1-2 TB USB-Festplatte).

- Zentrale Überwachungs-Konsole zum Emfang der Syslog-Meldungen der Analyse-Agenten
- Zentrales Experten-System zur Offline-Analyse binärer Messdaten bei speziellem Klärungsbedarf



Synapse Networks - Magic Distributed Monitoring & Analysis (SYN-MA)

Häufige Schwachstellen in LAN+DMZ

Viele Fehler und Gefahren werden nicht erkannt, weil die Standard-Ausrüstung Beschränkungen aufweist.

Firewalls schützen zwar, können aber komplexe Szenarien nicht erkennen und nicht dokumentieren.

Intruder Detection Systems (IDS) sind ebenfalls auf eher eindimensionale Ereignisse ausgerichtet.

Proxy-Server können Applikations-Auffälligkeiten nur begrenzt erkennen und blocken.

Analyse-Hardware-Appliances liefern zu viel Statistik und zu wenig Erkenntnis und sind zu teuer.

Anwender-Klagen über mangelnde Geschwindigkeit (**„Das Netzwerk ist langsam"**) bzw. Ursachen von Performance-Problemen können mit diesen Mitteln kaum aufgeklärt werden.

Synapse Experten-Analyse in LAN+DMZ

Der **Datenverkehr** wird an den entscheidenden Punkten des Netzwerkes vollständig aufgezeichnet (24/7).

Ring Buffer: Die Aufzeichnungen erzeugen ein **Daten-Archiv** mit einem über Tage oder Wochen mitwandernden Zeitfenster. Im Schadensfall ist dadurch volle **Beweisfähigkeit** gegeben.

Online-Analyse: Bereits während der Aufzeichnung hochwertige Analyse der aufgezeichneten Daten (Layer 1-7) und **Online-Warnungen** per **Syslog** und **E-Mail** durch die verschiedenen Subnetz-Agenten; ausgedehnte Tabellen und Ereignis-Protokolle.

Online-Monitoring: Eine zentrale Syslog-Console empfängt die Meldungen der Subnetz-Agenten (Filterung, Speicherung, Benachrichtigung).

Offline-Analyse: Bei Bedarf weitere Verarbeitung der Messdaten durch marktführendes **Experten-System**. Automatische Reports.

Synapse Networks - Magic Distributed Monitoring & Analysis (SYN-MA)

Fernwartung durch Synapse

SYN-MA ist für den Kunden am sinnvollsten, wenn ausgebildetes Analyse-Personal die Überwachung und Pflege übernimmt.

Synapse Networks GmbH bietet ein **SYN-MA Starter-Kit** mit

- Analyse-Agenten für 3 Subnetze bzw. 3 Messpunkte (z.B. DMZ, Domain-Server, Client-Workgroup)
- Zentral-Konsole (Syslog-Empfänger)
- TraceMagic Analyse Experten-System

samt Remote-Überwachung und Beratung ab **1.500 EUR** im Monat (12 Monate Laufzeit, Software wird leihweise überlassen, PC-Hardware stellt der Kunde).

Selbstverständlich können die Software-Lizenzen auch erworben werden, wenn der Kunde die Betreuung selbst leisten kann.

Erfahrung + Referenz

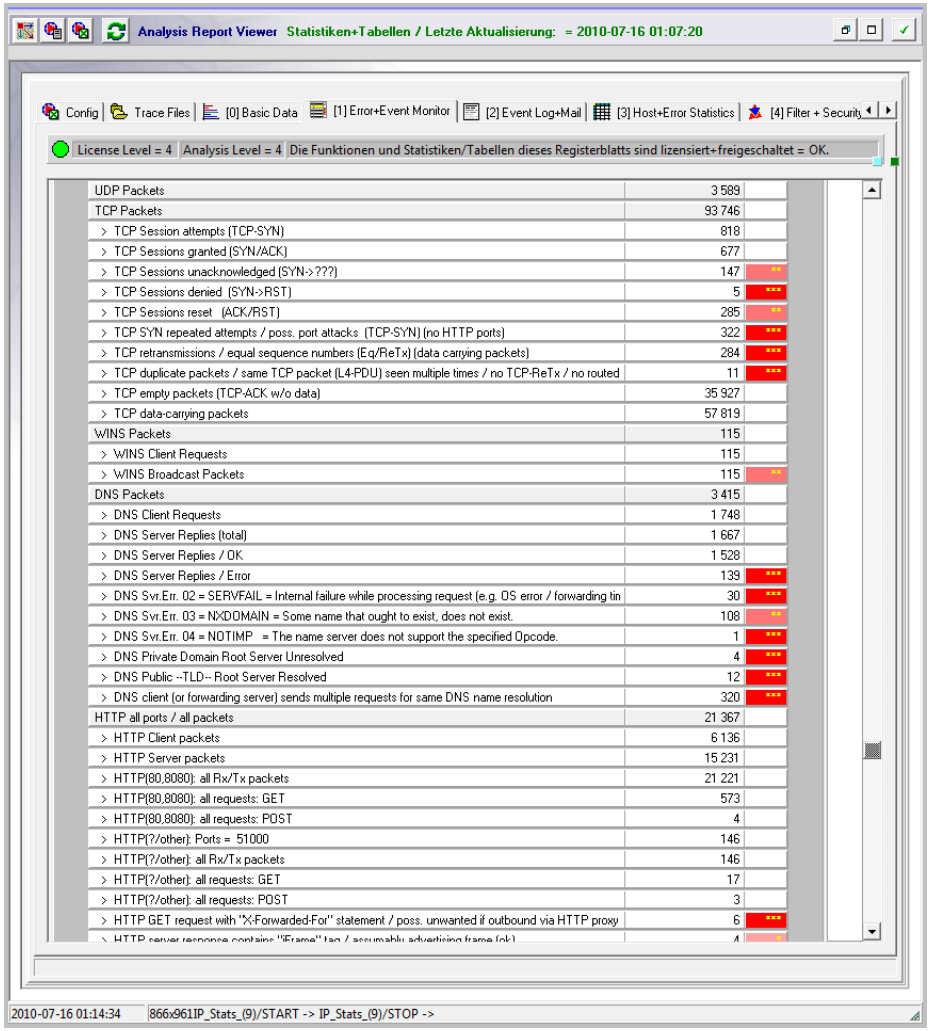
Synapse Networks GmbH betreut u.a. Institutionen

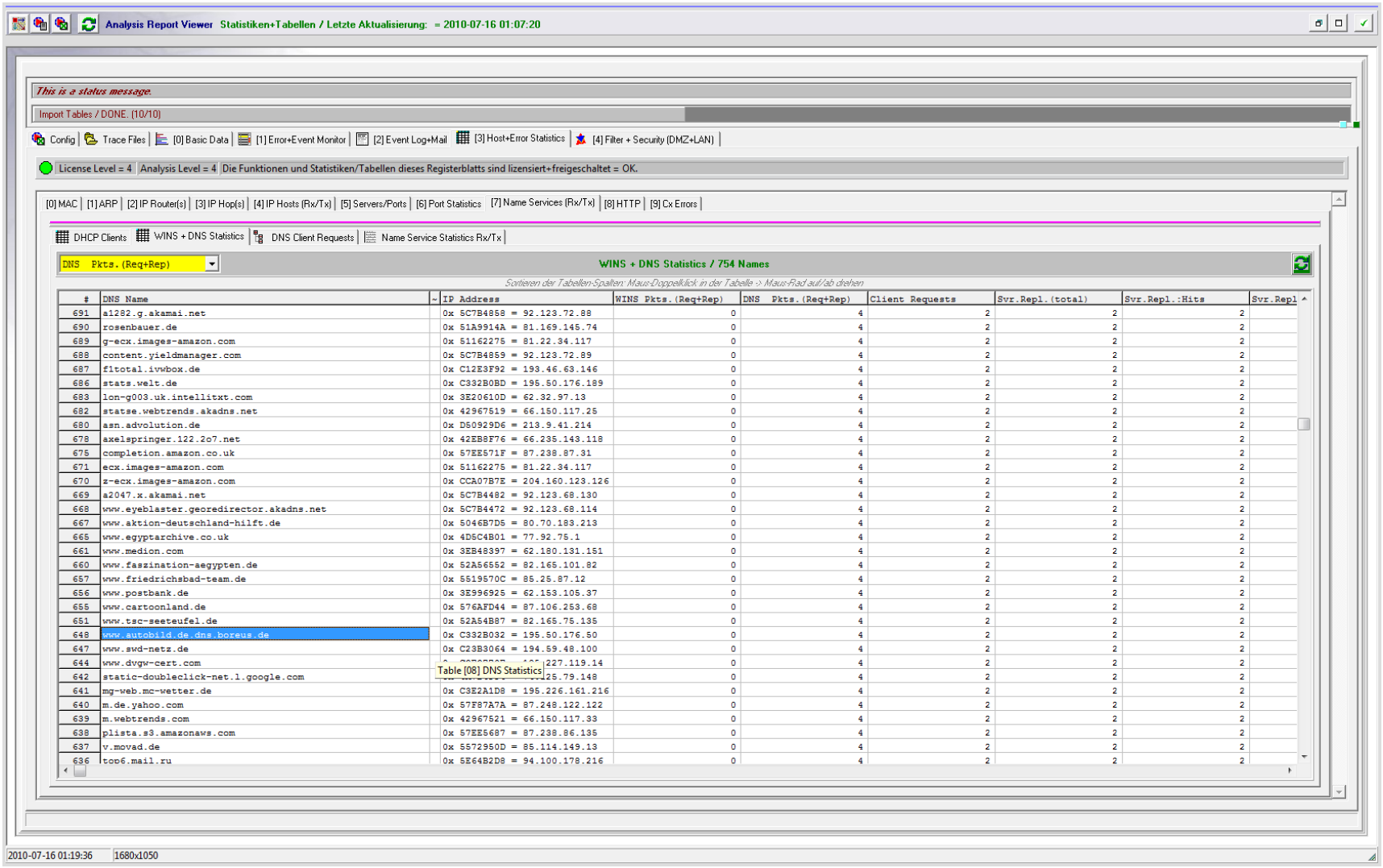
- der öffentlichen Hand (Bund+Land)
- der Finanzwelt
- der verarbeitenden Industrie

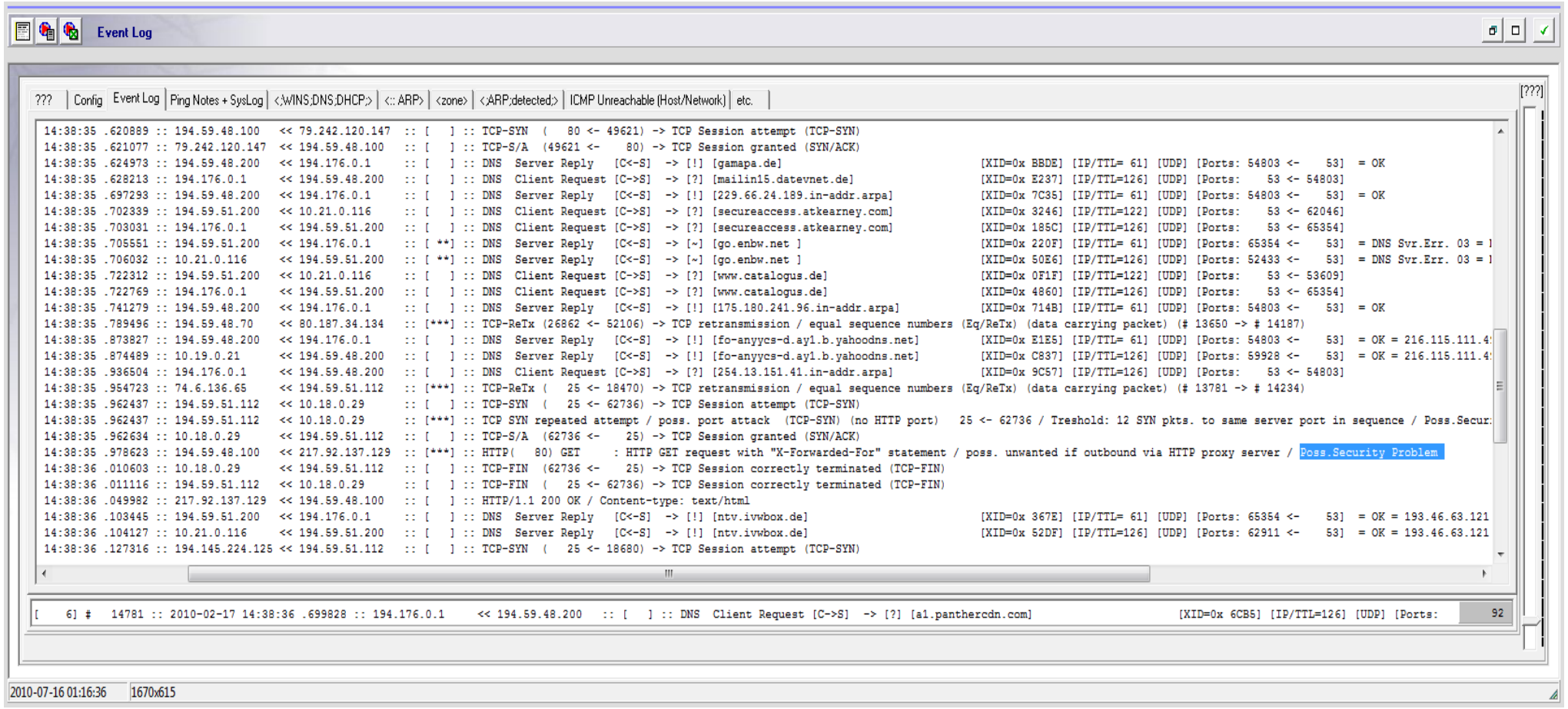
Sowohl **re**-aktive Störfall-Analyse wie auch **pro**-aktive System- und Struktur-Analyse werden hierdurch mit einem Höchstmaß an Automation und Präzision möglich.

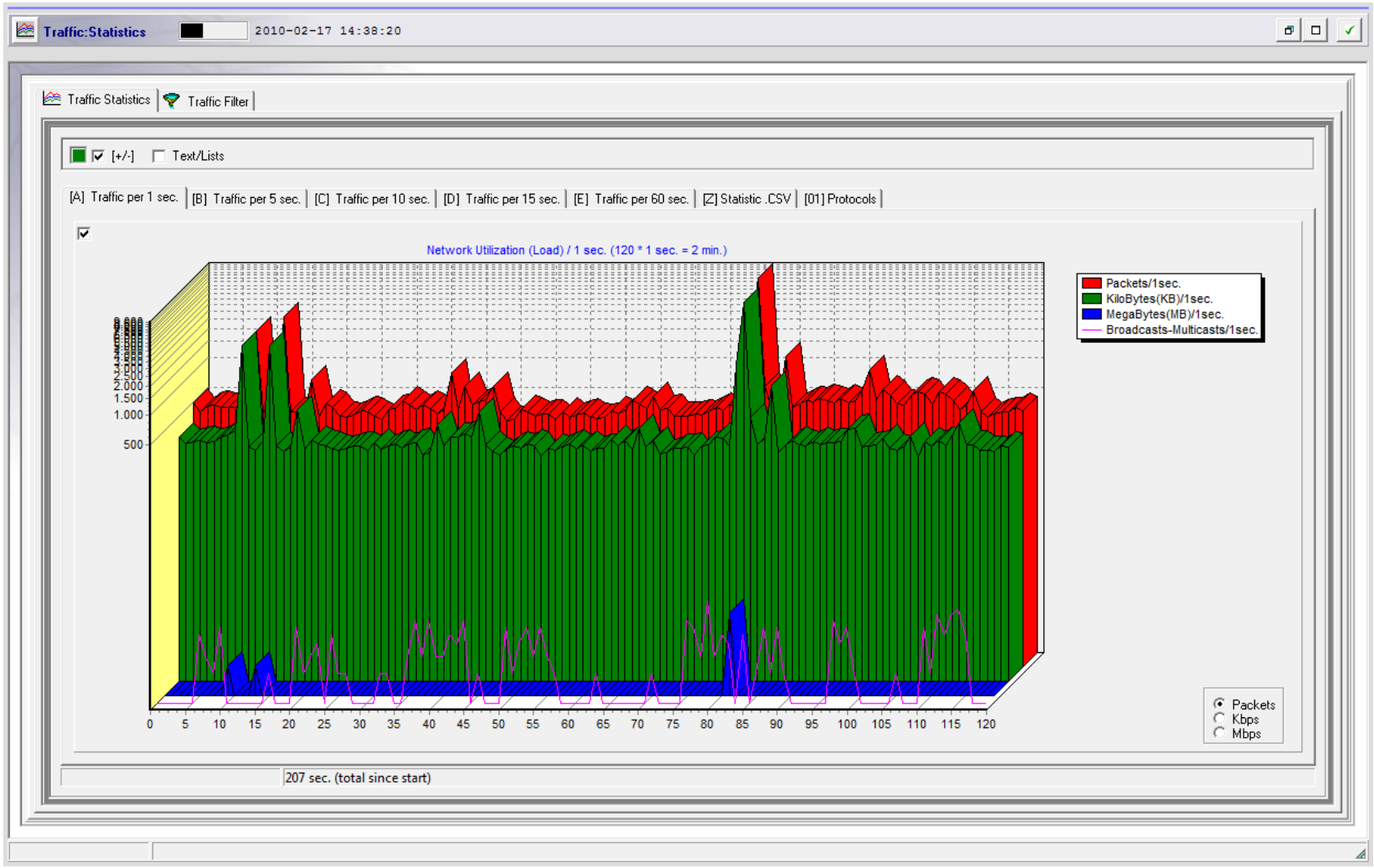
Sprechen Sie uns an!

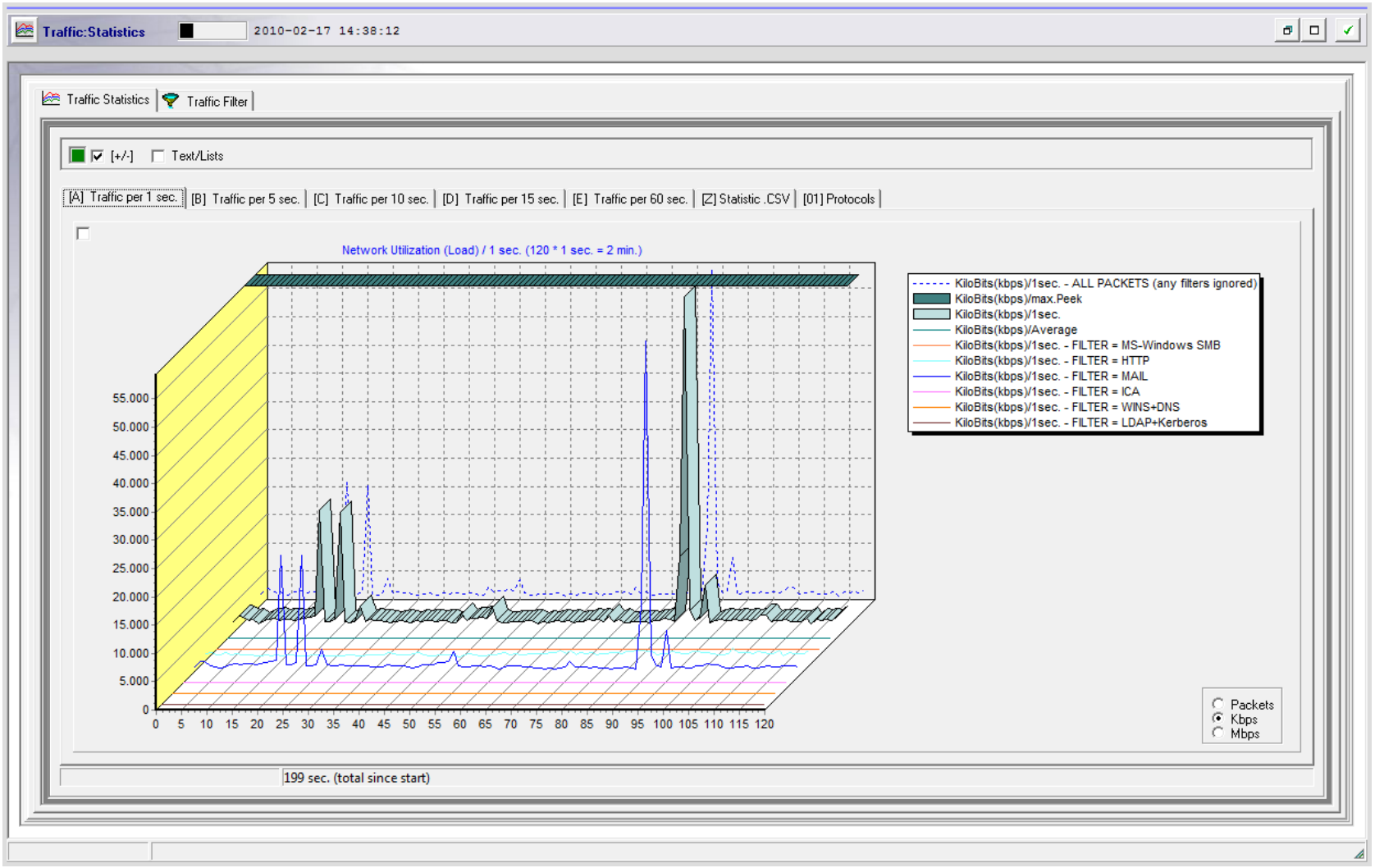
Ihr Synapse Team


Analysis Report Viewer Statistiken+Tabellen / Letzte Aktualisierung: = 2010-07-16 01:07:20
Config
Trace Files
[0] Basic Data
[1] Error+Event Monitor
[2] Event Log+Mail
[3] Host+Error Statistics
[4] Filter + Security
License Level = 4
Analysis Level = 4
Die Funktionen und Statistiken/Tabellen dieses Registerblatts sind lizensiert+freigeschaltet = OK.
UDP Packets 3 589
TCP Packets 93 746
> TCP Session attempts (TCP-SYN) 818
> TCP Sessions granted (SYN/ACK) 677
> TCP Sessions unacknowledged (SYN-> ???) 147
> TCP Sessions denied (SYN->RST) 5
> TCP Sessions reset (ACK/RST) 285
> TCP SYN repeated attempts / poss. port attacks (TCP-SYN) (no HTTP ports) 322
> TCP retransmissions / equal sequence numbers (Eq/ReTx) (data carrying packets) 284
> TCP duplicate packets / same TCP packet (L4-PDU) seen multiple times / no TCP-ReTx / no routed 11
> TCP empty packets (TCP-ACK w/o data) 35 927
> TCP data-carrying packets 57 819
WINS Packets 115
> WINS Client Requests 115
> WINS Broadcast Packets 115
DNS Packets 3 415
> DNS Client Requests 1 748
> DNS Server Replies (total) 1 667
> DNS Server Replies / OK 1 528
> DNS Server Replies / Error 139
> DNS Svr.Err. 02 = SERVFAIL = Internal failure while processing request (e.g. OS error / forwarding tin 30
> DNS Svr.Err. 03 = NXDOMAIN = Some name that ought to exist, does not exist. 108
> DNS Svr.Err. 04 = NOTIMP = The name server does not support the specified Opcode. 1
> DNS Private Domain Root Server Unresolved 4
> DNS Public --TLD-- Root Server Resolved 12
> DNS client (or forwarding server) sends multiple requests for same DNS name resolution 320
HTTP all ports / all packets 21 367
> HTTP Client packets 6 136
> HTTP Server packets 15 231
> HTTP(80,8080): all Rx/Tx packets 21 221
> HTTP(80,8080): all requests: GET 573
> HTTP(80,8080): all requests: POST 4
> HTTP(?/other): Ports = 51000 146
> HTTP(?/other): all Rx/Tx packets 146
> HTTP(?/other): all requests: GET 17
> HTTP(?/other): all requests: POST 3
> HTTP GET request with "X-Forwarded-For" statement / poss. unwanted if outbound via HTTP proxy 6
2010-07-16 01:14:34
866x961IP_Stats_(9)/START -> IP_Stats_(9)/STOP ->
Analysis Report Viewer Statistiken+Tabellen / Letzte Aktualisierung: = 2010-07-16 01:07:20
Config
Trace Files
[0] Basic Data
[1] Error+Event Monitor
[2] Event Log+Mail
[3] Host+Error Statistics
[4] Filter + Security
License Level = 4
Analysis Level = 4
Die Funktionen und Statistiken/Tabellen dieses Registerblatts sind lizensiert+freigeschaltet = OK.
> TCP data-carrying packets 57 819
WINS Packets 115
> WINS Client Requests 115
> WINS Broadcast Packets 115
DNS Packets 3 415
> DNS Client Requests 1 748
> DNS Server Replies (total) 1 667
> DNS Server Replies / OK 1 528
> DNS Server Replies / Error 139
> DNS Svr.Err. 02 = SERVFAIL = Internal failure while processing request (e.g. OS error / forwarding tin 30
> DNS Svr.Err. 03 = NXDOMAIN = Some name that ought to exist, does not exist. 108
> DNS Svr.Err. 04 = NOTIMP = The name server does not support the specified Opcode. 1
> DNS Private Domain Root Server Unresolved 4
> DNS Public --TLD-- Root Server Resolved 12
> DNS client (or forwarding server) sends multiple requests for same DNS name resolution 320
HTTP all ports / all packets 21 367
> HTTP Client packets 6 136
> HTTP Server packets 15 231
> HTTP(80,8080): all Rx/Tx packets 21 221
> HTTP(80,8080): all requests: GET 573
> HTTP(80,8080): all requests: POST 4
> HTTP(?/other): Ports = 51000 146
> HTTP(?/other): all Rx/Tx packets 146
> HTTP(?/other): all requests: GET 17
> HTTP(?/other): all requests: POST 3
> HTTP GET request with "X-Forwarded-For" statement / poss. unwanted if outbound via HTTP proxy 6
> HTTP server response contains "iFrame" tag / assumably advertising frame (ok) 4
SSL all packets 541
> SSL Client packets 259
> SSL Server packets 282
SECURITY: Poss.Security Problem(s)
> TCP SYN repeated attempts / poss. port attacks (TCP-SYN) (no HTTP ports) 322
> DNS Svr.Err. 02 = SERVFAIL = Internal failure while processing request (e.g. OS error / forwarding tin 30
> DNS Private Domain Root Server Unresolved 4
> DNS Public --TLD-- Root Server Resolved 12
> HTTP GET request with "X-Forwarded-For" statement / poss. unwanted if outbound via HTTP proxy 6
> HTTP server response contains "iFrame" tag / assumably advertising frame (ok) 4
2010-07-16 01:14:45
866x961IP_Stats_(9)/START -> IP_Stats_(9)/STOP ->


Analysis Report Viewer Statistiken+Tabellen / Letzte Aktualisierung: = 2010-07-16 01:07:20
This is a status message.
Import Tables / DONE. (10/10)
Config | Trace Files | [0] Basic Data | [1] Error+Event Monitor | [2] Event Log+Mail | [3] Host+Error Statistics | [4] Filter + Security (DMZ+LAN)
License Level = 4 | Analysis Level = 4 | Die Funktionen und Statistiken/Tabellen dieses Registerblatts sind lizensiert+freigeschaltet = OK.
[0] MAC | [1] ARP | [2] IP Router(s) | [3] IP Hop(s) | [4] IP Hosts (Rx/Tx) | [5] Servers/Ports | [6] Port Statistics | [7] Name Services (Rx/Tx) | [8] HTTP | [9] Cx Errors
DHCP Clients | WINS + DNS Statistics | DNS Client Requests | Name Service Statistics Rx/Tx
DNS Pkts. (Req+Rep)
WINS + DNS Statistics / 754 Names
Sortieren der Tabellen-Spalten: Maus-Doppelklick in der Tabelle -> Maus-Rad auf/ab drehen
| DNS Name | IP Address | WINS Pkts. (Req+Rep) | DNS Pkts. (Req+Rep) | Client Requests | Svr.Repl. (total) | Svr.Repl.:Hits | Svr.Repl
691 | a1282.g.akamai.net | 0x 5C7B4858 = 92.123.72.88 | 0 | 4 | 2 | 2 | 2
690 | rosenbauer.de | 0x 51A9914A = 81.169.145.74 | 0 | 4 | 2 | 2 | 2
689 | g-ecx.images-amazon.com | 0x 51162275 = 81.22.34.117 | 0 | 4 | 2 | 2 | 2
688 | content.yieldmanager.com | 0x 5C7B4859 = 92.123.72.89 | 0 | 4 | 2 | 2 | 2
687 | f1total.ivwbox.de | 0x C12E3F92 = 193.46.63.146 | 0 | 4 | 2 | 2 | 2
686 | stats.welt.de | 0x C332B0BD = 195.50.176.189 | 0 | 4 | 2 | 2 | 2
683 | lon-g003.uk.intellitxt.com | 0x 3E20610D = 62.32.97.13 | 0 | 4 | 2 | 2 | 2
682 | statse.webtrends.akadns.net | 0x 42967519 = 66.150.117.25 | 0 | 4 | 2 | 2 | 2
680 | asn.advolution.de | 0x D50929D6 = 213.9.41.214 | 0 | 4 | 2 | 2 | 2
678 | axelspringer.122.2o7.net | 0x 42EB8F76 = 66.235.143.118 | 0 | 4 | 2 | 2 | 2
675 | completion.amazon.co.uk | 0x 57EE571F = 87.238.87.31 | 0 | 4 | 2 | 2 | 2
671 | ecx.images-amazon.com | 0x 51162275 = 81.22.34.117 | 0 | 4 | 2 | 2 | 2
670 | z-ecx.images-amazon.com | 0x CCA07B7E = 204.160.123.126 | 0 | 4 | 2 | 2 | 2
669 | a2047.x.akamai.net | 0x 5C7B4482 = 92.123.68.130 | 0 | 4 | 2 | 2 | 2
668 | www.eyeblaster.georedirector.akadns.net | 0x 5C7B4472 = 92.123.68.114 | 0 | 4 | 2 | 2 | 2
667 | www.aktion-deutschland-hilft.de | 0x 5046B7D5 = 80.70.183.213 | 0 | 4 | 2 | 2 | 2
665 | www.egyptarchive.co.uk | 0x 4D5C4B01 = 77.92.75.1 | 0 | 4 | 2 | 2 | 2
661 | www.medion.com | 0x 3EB48397 = 62.180.131.151 | 0 | 4 | 2 | 2 | 2
660 | www.faszination-aegypten.de | 0x 52A56552 = 82.165.101.82 | 0 | 4 | 2 | 2 | 2
657 | www.friedrichsbad-team.de | 0x 5519570C = 85.25.87.12 | 0 | 4 | 2 | 2 | 2
656 | www.postbank.de | 0x 3E996925 = 62.153.105.37 | 0 | 4 | 2 | 2 | 2
655 | www.cartoonland.de | 0x 576AFD44 = 87.106.253.68 | 0 | 4 | 2 | 2 | 2
651 | www.tsc-seeteufel.de | 0x 52A54B87 = 82.165.75.135 | 0 | 4 | 2 | 2 | 2
648 | www.autobild.de.dns.boreus.de | 0x C332B032 = 195.50.176.50 | 0 | 4 | 2 | 2 | 2
647 | www.swd-netz.de | 0x C23B3064 = 194.59.48.100 | 0 | 4 | 2 | 2 | 2
644 | www.dvgw-cert.com | 227.119.14 | 0 | 4 | 2 | 2 | 2
642 | static-doubleclick-net.l.google.com | 25.79.148 | 0 | 4 | 2 | 2 | 2
641 | mg-web.mc-wetter.de | 0x C3E2A1D8 = 195.226.161.216 | 0 | 4 | 2 | 2 | 2
640 | m.de.yahoo.com | 0x 57F87A7A = 87.248.122.122 | 0 | 4 | 2 | 2 | 2
639 | m.webtrends.com | 0x 42967521 = 66.150.117.33 | 0 | 4 | 2 | 2 | 2
638 | plista.s3.amazonaws.com | 0x 57EE5687 = 87.238.86.135 | 0 | 4 | 2 | 2 | 2
637 | v.movad.de | 0x 5572950D = 85.114.149.13 | 0 | 4 | 2 | 2 | 2
636 | top6.mail.ru | 0x 5E64B2D8 = 94.100.178.216 | 0 | 4 | 2 | 2 | 2
Table [08] DNS Statistics
2010-07-16 01:19:36
1680x1050


Event Log
??? | Config | Event Log | Ping Notes + SysLog | <;WINS;DNS;DHCP;> | <:: ARP> | <zone> | <;ARP;detected;> | ICMP Unreachable (Host/Network) | etc.
[???]
14:38:35 .620889 :: 194.59.48.100 << 79.242.120.147 :: [ ] :: TCP-SYN (80 <- 49621) -> TCP Session attempt (TCP-SYN)
14:38:35 .621077 :: 79.242.120.147 << 194.59.48.100 :: [ ] :: TCP-S/A (49621 <- 80) -> TCP Session granted (SYN/ACK)
14:38:35 .624973 :: 194.59.48.200 << 194.176.0.1 :: [ ] :: DNS Server Reply [C<-S] -> [!] [gamapa.de] [XID=0x BBDE] [IP/TTL= 61] [UDP] [Ports: 54803 <- 53] = OK
14:38:35 .628213 :: 194.176.0.1 << 194.59.48.200 :: [ ] :: DNS Client Request [C->S] -> [?] [mailin15.datevnet.de] [XID=0x E237] [IP/TTL=126] [UDP] [Ports: 53 <- 54803]
14:38:35 .697293 :: 194.59.48.200 << 194.176.0.1 :: [ ] :: DNS Server Reply [C<-S] -> [!] [229.66.24.189.in-addr.arpa] [XID=0x 7C35] [IP/TTL= 61] [UDP] [Ports: 54803 <- 53] = OK
14:38:35 .702339 :: 194.59.51.200 << 10.21.0.116 :: [ ] :: DNS Client Request [C->S] -> [?] [secureaccess.atkearney.com] [XID=0x 3246] [IP/TTL=122] [UDP] [Ports: 53 <- 62046]
14:38:35 .703031 :: 194.176.0.1 << 194.59.51.200 :: [ ] :: DNS Client Request [C->S] -> [?] [secureaccess.atkearney.com] [XID=0x 185C] [IP/TTL=126] [UDP] [Ports: 53 <- 65354]
14:38:35 .705551 :: 194.59.51.200 << 194.176.0.1 :: [**] :: DNS Server Reply [C<-S] -> [~] [go.enbw.net] [XID=0x 220F] [IP/TTL= 61] [UDP] [Ports: 65354 <- 53] = DNS Svr.Err. 03 = I
14:38:35 .706032 :: 10.21.0.116 << 194.59.51.200 :: [**] :: DNS Server Reply [C<-S] -> [~] [go.enbw.net] [XID=0x 50E6] [IP/TTL=126] [UDP] [Ports: 52433 <- 53] = DNS Svr.Err. 03 = I
14:38:35 .722312 :: 194.59.51.200 << 10.21.0.116 :: [ ] :: DNS Client Request [C->S] -> [?] [www.catalogus.de] [XID=0x 0F1F] [IP/TTL=122] [UDP] [Ports: 53 <- 53609]
14:38:35 .722769 :: 194.176.0.1 << 194.59.51.200 :: [ ] :: DNS Client Request [C->S] -> [?] [www.catalogus.de] [XID=0x 4860] [IP/TTL=126] [UDP] [Ports: 53 <- 65354]
14:38:35 .741279 :: 194.59.48.200 << 194.176.0.1 :: [ ] :: DNS Server Reply [C<-S] -> [!] [175.180.241.96.in-addr.arpa] [XID=0x 714B] [IP/TTL= 61] [UDP] [Ports: 54803 <- 53] = OK
14:38:35 .789496 :: 194.59.48.70 << 80.187.34.134 :: [***] :: TCP-ReTx (26862 <- 52106) -> TCP retransmission / equal sequence numbers (Eq/ReTx) (data carrying packet) (# 13650 -> # 14187)
14:38:35 .873827 :: 194.59.48.200 << 194.176.0.1 :: [ ] :: DNS Server Reply [C<-S] -> [!] [fo-anyycs-d.ay1.b.yahoodns.net] [XID=0x E1E5] [IP/TTL= 61] [UDP] [Ports: 54803 <- 53] = OK = 216.115.111.4
14:38:35 .874489 :: 10.19.0.21 << 194.59.48.200 :: [ ] :: DNS Server Reply [C<-S] -> [!] [fo-anyycs-d.ay1.b.yahoodns.net] [XID=0x C837] [IP/TTL=126] [UDP] [Ports: 59928 <- 53] = OK = 216.115.111.4
14:38:35 .936504 :: 194.176.0.1 << 194.59.48.200 :: [ ] :: DNS Client Request [C->S] -> [?] [254.13.151.41.in-addr.arpa] [XID=0x 9C57] [IP/TTL=126] [UDP] [Ports: 53 <- 54803]
14:38:35 .954723 :: 74.6.136.65 << 194.59.51.112 :: [***] :: TCP-ReTx (25 <- 18470) -> TCP retransmission / equal sequence numbers (Eq/ReTx) (data carrying packet) (# 13781 -> # 14234)
14:38:35 .962437 :: 194.59.51.112 << 10.18.0.29 :: [ ] :: TCP-SYN (25 <- 62736) -> TCP Session attempt (TCP-SYN)
14:38:35 .962437 :: 194.59.51.112 << 10.18.0.29 :: [***] :: TCP SYN repeated attempt / poss. port attack (TCP-SYN) (no HTTP port) 25 <- 62736 / Treshold: 12 SYN pkts. to same server port in sequence / Poss.Secur
14:38:35 .962634 :: 10.18.0.29 << 194.59.51.112 :: [ ] :: TCP-S/A (62736 <- 25) -> TCP Session granted (SYN/ACK)
14:38:35 .978623 :: 194.59.48.100 << 217.92.137.129 :: [***] :: HTTP(80) GET : HTTP GET request with "X-Forwarded-For" statement / poss. unwanted if outbound via HTTP proxy server / Poss.Security Problem
14:38:36 .010603 :: 10.18.0.29 << 194.59.51.112 :: [ ] :: TCP-FIN (62736 <- 25) -> TCP Session correctly terminated (TCP-FIN)
14:38:36 .011116 :: 194.59.51.112 << 10.18.0.29 :: [ ] :: TCP-FIN (25 <- 62736) -> TCP Session correctly terminated (TCP-FIN)
14:38:36 .049982 :: 217.92.137.129 << 194.59.48.100 :: [ ] :: HTTP/1.1 200 OK / Content-type: text/html
14:38:36 .103445 :: 194.59.51.200 << 194.176.0.1 :: [ ] :: DNS Server Reply [C<-S] -> [!] [ntv.ivwbox.de] [XID=0x 367E] [IP/TTL= 61] [UDP] [Ports: 65354 <- 53] = OK = 193.46.63.121
14:38:36 .104127 :: 10.21.0.116 << 194.59.51.200 :: [ ] :: DNS Server Reply [C<-S] -> [!] [ntv.ivwbox.de] [XID=0x 52DF] [IP/TTL=126] [UDP] [Ports: 62911 <- 53] = OK = 193.46.63.121
14:38:36 .127316 :: 194.145.224.125 << 194.59.51.112 :: [ ] :: TCP-SYN (25 <- 18680) -> TCP Session attempt (TCP-SYN)
[6] # 14781 :: 2010-02-17 14:38:36 .699828 :: 194.176.0.1 << 194.59.48.200 :: [ ] :: DNS Client Request [C->S] -> [?] [a1.panthercdn.com] [XID=0x 6CB5] [IP/TTL=126] [UDP] [Ports: 92
2010-07-16 01:16:36
1670x615


Traffic:Statistics
2010-02-17 14:38:20
Traffic Statistics
Traffic Filter
[+/-]
Text/Lists
[A] Traffic per 1 sec.
[B] Traffic per 5 sec.
[C] Traffic per 10 sec.
[D] Traffic per 15 sec.
[E] Traffic per 60 sec.
[Z] Statistic .CSV
[01] Protocols
Network Utilization (Load) / 1 sec. (120 * 1 sec. = 2 min.)
Packets/1sec.
KiloBytes(KB)/1sec.
MegaBytes(MB)/1sec.
Broadcasts-Multicasts/1sec.
2.500
2.000
1.500
1.000
500
0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95 100 105 110 115 120
Packets
Kbps
Mbps
207 sec. (total since start)


Traffic:Statistics
2010-02-17 14:38:12
Traffic Statistics
Traffic Filter
[+/-]
Text/Lists
[A] Traffic per 1 sec.
[B] Traffic per 5 sec.
[C] Traffic per 10 sec.
[D] Traffic per 15 sec.
[E] Traffic per 60 sec.
[Z] Statistic .CSV
[01] Protocols
Network Utilization (Load) / 1 sec. (120 * 1 sec. = 2 min.)
KiloBits(kbps)/1sec. - ALL PACKETS (any filters ignored)
KiloBits(kbps)/max.Peek
KiloBits(kbps)/1sec.
KiloBits(kbps)/Average
KiloBits(kbps)/1sec. - FILTER = MS-Windows SMB
KiloBits(kbps)/1sec. - FILTER = HTTP
KiloBits(kbps)/1sec. - FILTER = MAIL
KiloBits(kbps)/1sec. - FILTER = ICA
KiloBits(kbps)/1sec. - FILTER = WINS+DNS
KiloBits(kbps)/1sec. - FILTER = LDAP+Kerberos
55.000
50.000
45.000
40.000
35.000
30.000
25.000
20.000
15.000
10.000
5.000
0
0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95 100 105 110 115 120
Packets
Kbps
Mbps
199 sec. (total since start)