ARBOR NETWORKS

Arbor Networks DDoS Solutions

Alex Lopez
alopez@arbor.net
+34 676995439

Agenda

The Problem

The Business Risk

Smart.
Secure.
Available.

The Arbor Solution

Company Overview

Agenda

The Problem

- What is a DDoS attack?
- How does DDoS work?
- Who and why launches DDoS?
- What types of attacks exist?
- Am I already protected?

The Business Risk

Smart.
Secure.
Available.

The Arbor Solution

Company Overview

ARBOR NETWORKS

DDoS?

VIRUS | Incidencia a nivel mundial

El mayor ciberataque de la historia disminuye la velocidad de Internet

Portaltic/EP | Madrid
Actualizado miércoles 27/03/2013 **18:58 horas**

Comentarios 20

El mayor ciberataque registrado hasta el momento en Internet ha provocado que la velocidad en la Red en todo el mundo se vea alterada. Causada por una disputa entre la organización Spamhaus y la compañía de almacenamiento Cyberbunker, está **afectando a especialmente a servicios tan populares como Netflix**.

El conflicto se ha iniciado después de que **Spamhaus**, con sede en Londres y Ginebra, haya señalado a **Cyberbunker** como plataforma utilizada para la difusión de spam. Spanhaus lucha contra el correo no deseado y tiene una serie de listas en las que detalla páginas y servicios que lo promueven.

En este listado, Cyberbunker aparece **calificada como plataforma de spam**. Algo que ha despertado la ira de sus trabajadores y que, según Spamhaus, les ha llevado a atacar sus sistemas como represalia.

Según expertos de seguridad citados por la **BBC**, el ataque contra Spamhaus es **el mayor en la historia de Internet**.

300 GB de información por segundo

Al parecer se han utilizado ataques DDoS que han intentado bloquear los sistemas de Spanhaus, aunque no han tenido éxito. Se ha llegado a enviar 300 GB de información por segundo contra los sistemas de la

Un ataque DDoS a un servidor visualizado al estilo videojuego

EL 41% DE LOS RESPONSABLES DE TI RECONOCE SENTIRSE 'MUY PREOCUPADO' ANTE UN POSIBLE ATAQUE DDOS

ESCRITO POR MARCELO_LOZANO EL 23/04/2013. POSTEADO EN ANÁLISIS, SEGURIDAD

Un ataque informático tumba la web del Congreso horas antes de su "asedio"

Mt Gox sufre un ataque DDoS "peor de lo normal" y el valor del Bitcoin se hunde

12 de abril de 2013 | 10:07 CET

Reddit fue víctima de un ataque DDoS

Detenido en Barcelona el autor del mayor ataque DDoS de la historia

ARBOR NETWORKS

What techniques are used to attack?

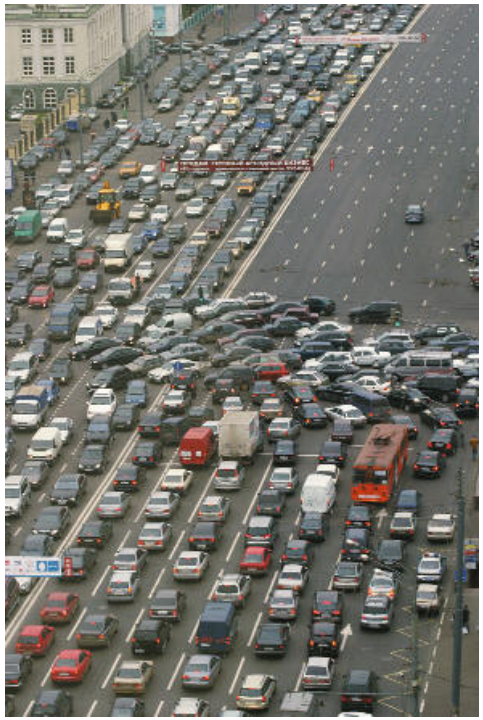
Apr 2	Izz ad-din al-Qassam Cyber Fighters	BB&T	And here we are again: in name of Operation Ababil, the Izz ad-din al-Qassam Cyber Fighters take down the website of BB&T.[8]	DDoS	Industry: Finance	Hacktivism
Apr 3	?	Scribd.	The world's largest document sharing site Scribd says it was hacked and believes up to 1% of its **100 million** users' passwords were compromised due to being stored with an outdated hashing algorithm.[9]	Unknown	Internet Services	Cyber Crime
Apr 3	?	MTGOX	Mtogox (mtgox.com), a Bitcoin Exchange Service is the target of a DDoS attack that disrupts the service for two days.[10]	DDoS	Bitcoin Exchange	Cyber Crime
Apr 3	?	bitinstant	BitInstant is the latest Bitcoin exchange website to fall victim to hackers. The company is forced to shuts down its website after attackers manage to steal $12,480 (€9,500) in BTC.[11]	DNS Hijacking	Bitcoin Exchange	Cyber Crime
Apr 3		MUSEUM WITH NO FRONTIERS	Unknown hackers under the Anonymous Umbrella hack the Museum With No Frontiers website (museumwnf.org) and dump a 5.6 mb archive containing personal data.[12]	Unknown	Organization: Non-Profit	Hacktivism
Apr 3	Izz ad-din al-Qassam Cyber Fighters	Bank of America, REGIONS	Another round of the Operation Ababil, this time the victims are:[13] • Bank Of America; • Regions Bank.	DDoS	Finance	Hacktivism
Apr 4	?	instawallet	Yet another Bitcoin Service Exchange, targeted by hackers, this time with severe consequences. Instawallet suspends the service indefinitely after the company's systems have been hacked.[14]	Unknown	Bitcoin Exchange	Cyber Crime
Apr 4		STANDARD Digital	@LulzSecWiki hacks the website of a well known publisher (standardmedia.co.ke) and dumps a mix of server, administrator, user and claimed client logins.[15]	SQLi	Industry: News	Hacktivism
Apr 4	Izz ad-din al-Qassam Cyber Fighters	WELLS FARGO, BB&T	Other Banks targeted by the Operation Ababil DDoS attacks:[16] • Wells Fargo • BB&T (again)	DDoS	Finance	Hacktivism
Apr 5	?	ING, iDEAL	DDoS attacks land in the Netherlands. The iDEAL payment system and the ING Bank are both hit by DDoS.[17]	DDoS	Finance	Cyber Crime
Apr 5	?	HARMONIX	The sites of Rock Band and Dance Central are down while the publisher, Harmonix looks into an attack that may have compromised some user information. Fortunately, that information does not include any financial details or social security numbers.[18]	Unknown	Industry: Games	Cyber Crime
Apr 7			Again a breach by the @LulzSecWiki. Unfortunately the target is HPTH (hpth.org.uk), a small charity and a voluntary patient support organization for a rare medical condition called hypoparathyroidism (HPTH).[22]	SQLi	Organization: charity	Hacktivism
Apr 8			Anonymous discloses the alleged damage report of OpIsrael. It includes:[23] • 100k+ websites • 40k Facebook pages • 5k twitter accounts • 30k Israeli bank accts • Israeli prime minister's wife number • 3k+ websites of companies in israeli cyber space deleted • Secret Israel Documents of Military leaked • Several Gov websites hacked Other Breached websites include: • Avg.co.il (security Company): 2686 accounts.[24] • Alon.co.il (Oil Company): 682 accounts[25] • Idinfo.co.il (Israel Army): 679 accounts[26] The hacktivists claim to have caused **$3-plus** billion damage. However Israeli official reply that there is not real damage.[27]	N/A	Several Targets	Hacktivism
Apr 8	?	Kirkwood	The Kirkwood Community College in Cedar Rapids announces that hackers gained access to an online database containing personal information of **125,000** people who applied to take credit classes during the last eight years.[28]	Targeted Attack	Education	Cyber Crime
Apr 8			Hackers of Anonymous Belgium breach the official website of the Bree fire department (brandweerbree.be) after learning that two of its volunteers have been accused of molesting a 13-year-old girl.[29]	Unknown	Law Enforcement	Hacktivism
Apr 9	Izz ad-din al-Qassam Cyber Fighters	CHASE, Bank of America, Capital One, BB&T, WELLS FARGO	Again a new of Cyber Attacks against the U.S. Banks in name of the Operation Ababil. The targets of this wave include:[30] • Chase, • Bank of America, • Capital One, • American Express, • BB&T, • Wells Fargo.	DDoS	Finance	Hacktivism
Apr 10	Izz ad-din al-Qassam Cyber	CHASE, PNC	Yet another wave of Cyber Attacks against the U.S. Banks in name of the Operation Ababil. Targets include:[31] • Chase, • PNC,	DDoS	Finance	Hacktivism

www.hackmageddon.com

ARBOR NETWORKS

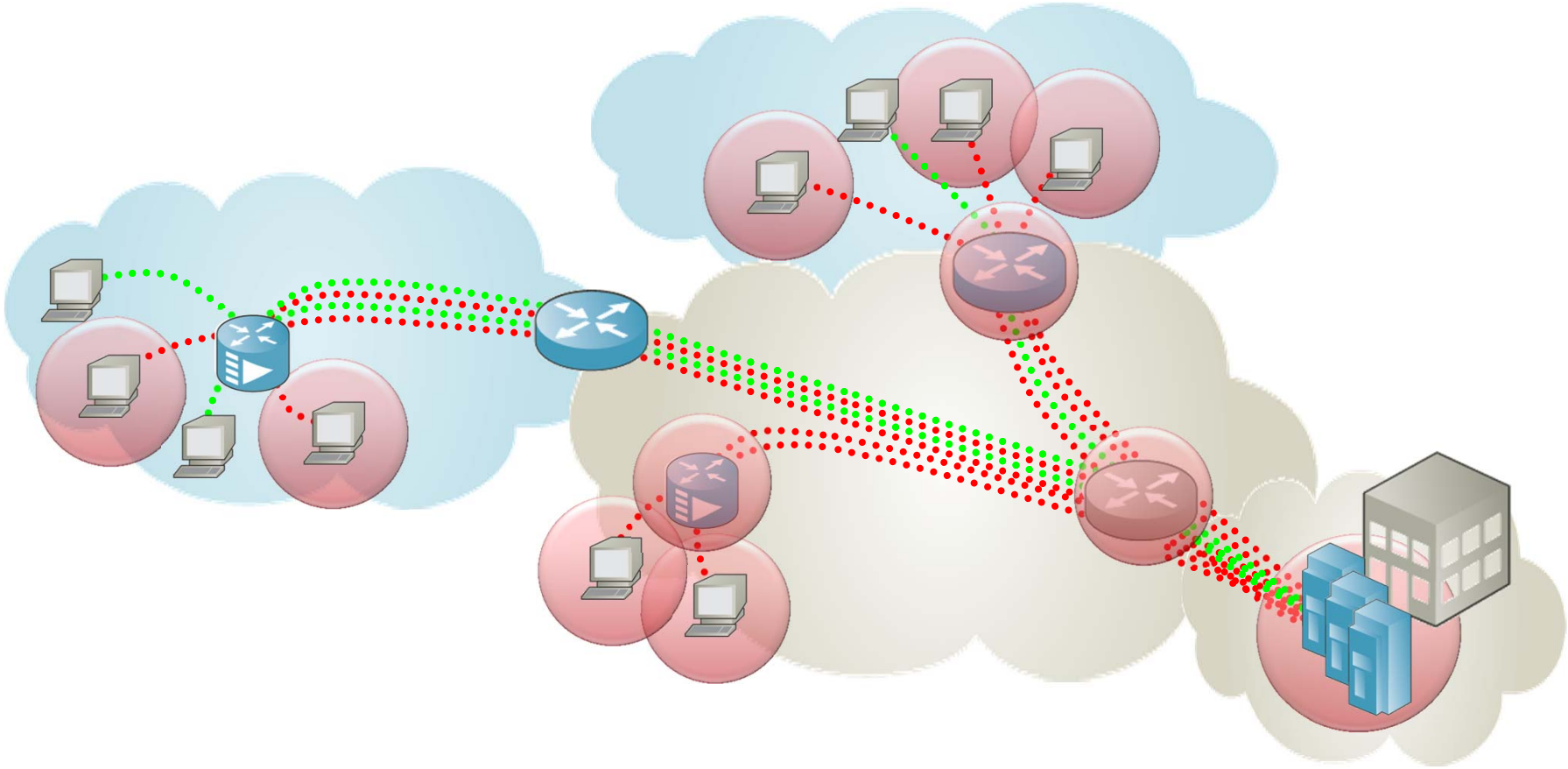
What is DoS and DDoS?

- In computing, a **denial-of-service attack** (DoS attack) is an attempt to make a **machine or network** resource **unavailable to** its intended **users**. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely **interrupt or suspend services** of a host connected to the Internet
- A **distributed denial of service attack** (DDoS) occurs when **multiple systems** flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods.



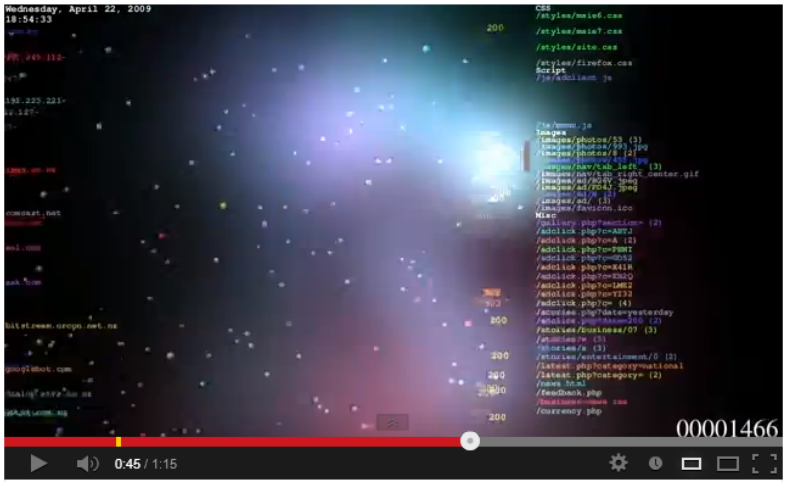
ARBOR NETWORKS

How does a DDoS attack work?

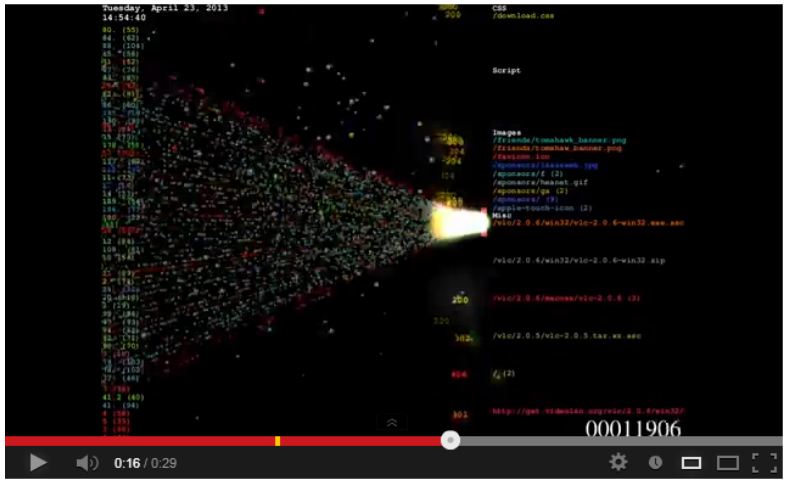


During a **Distributed Denial of Service (DDoS) attack**, compromised hosts or **bots** coming from distributed sources overwhelm the target with illegitimate traffic so that the servers can not respond to legitimate clients.

The “art” of DDoS: Logstalgia



http://www.youtube.com/watch?v=HeWfkPeDQbY

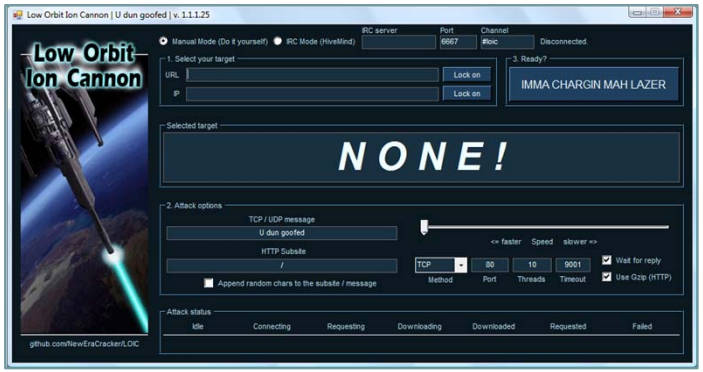


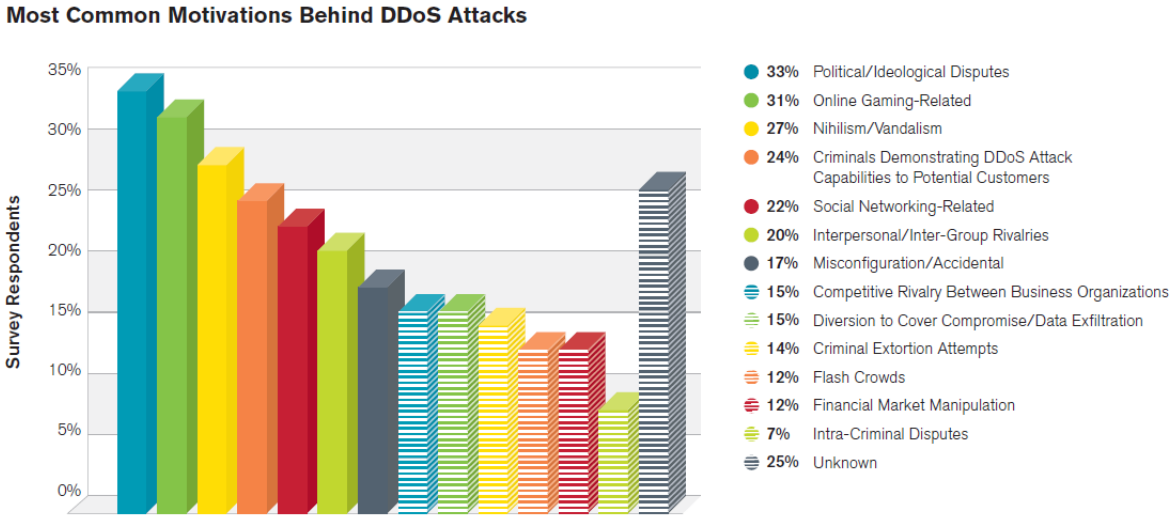
http://www.youtube.com/watch?v=hNjdBSoIa8k

ARBOR NETWORKS

Why are these attacks happening?

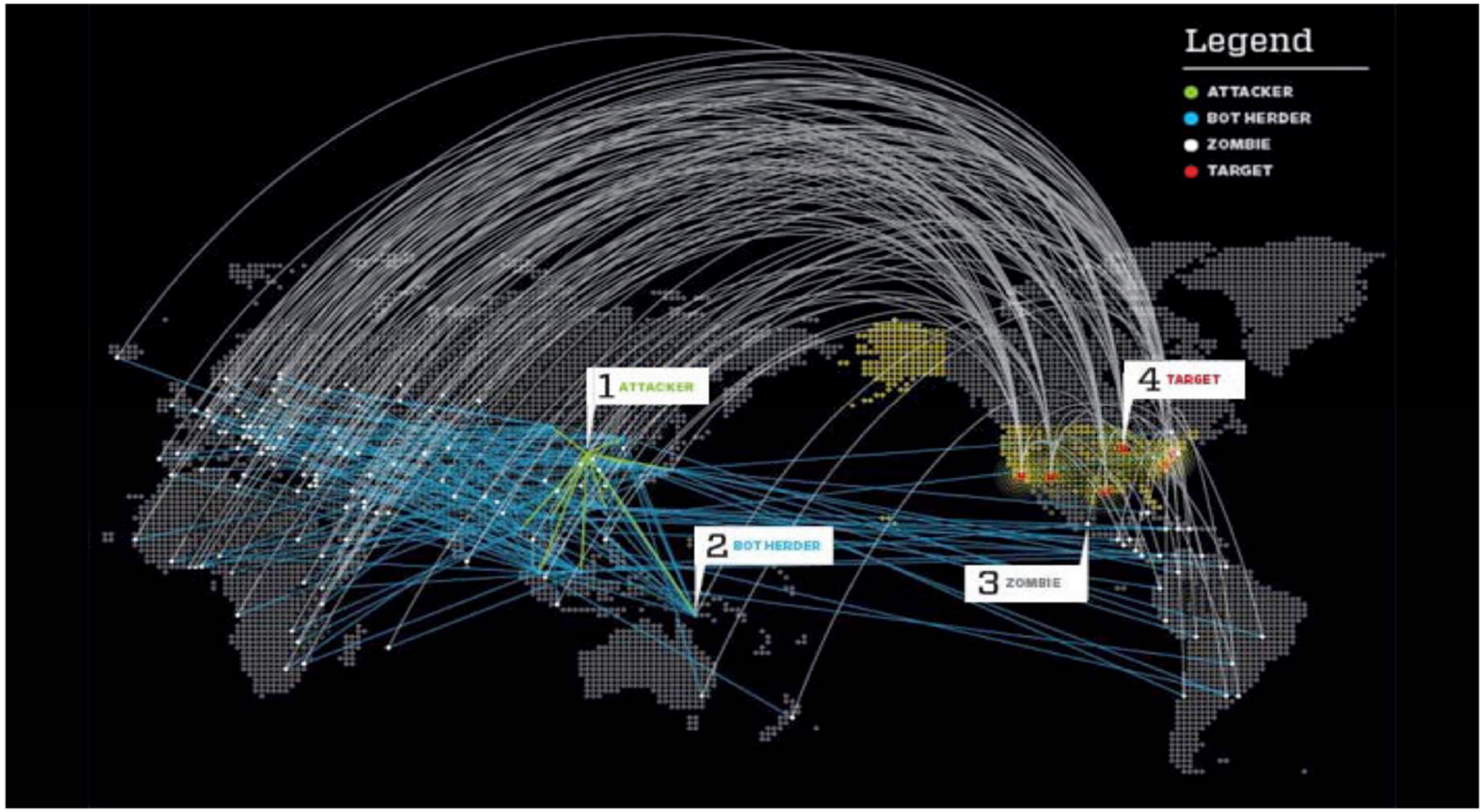
- Hacktivism: Volunteer botnets (LOIC)
- Extorsion: “comercial” botnets
- Online demonstrations
- Ciberwar
- Vandalism/nihilism





ARBOR NETWORKS

How does a botnet work?



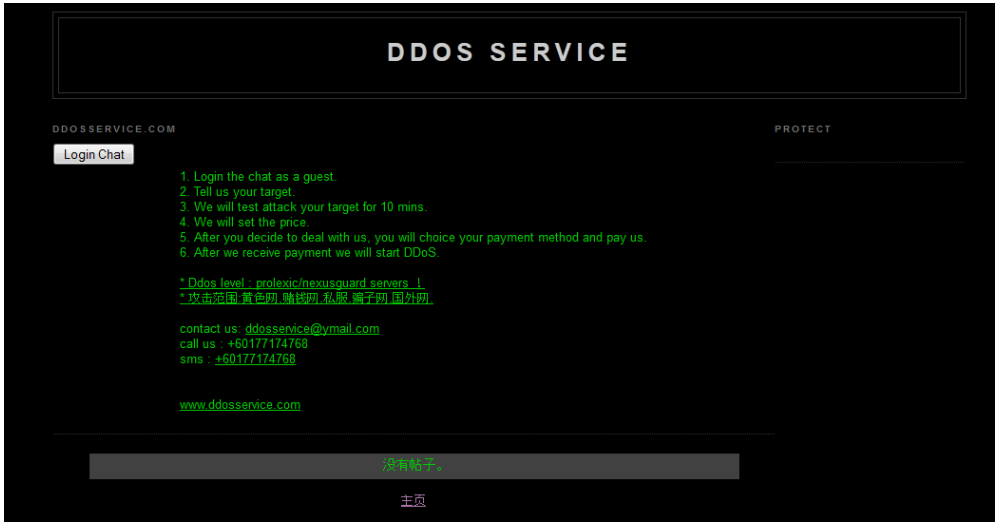
There are botnets reported of up to… 30 million computers!! (BredoLab)

In Spain, Mariposa, created by DDP, managed to have as many as.. 12 million infected computers!!

A single residential computer can easily launch 1000 sessions per second

ARBOR NETWORKS

Is it difficult/expensive to launch an attack?



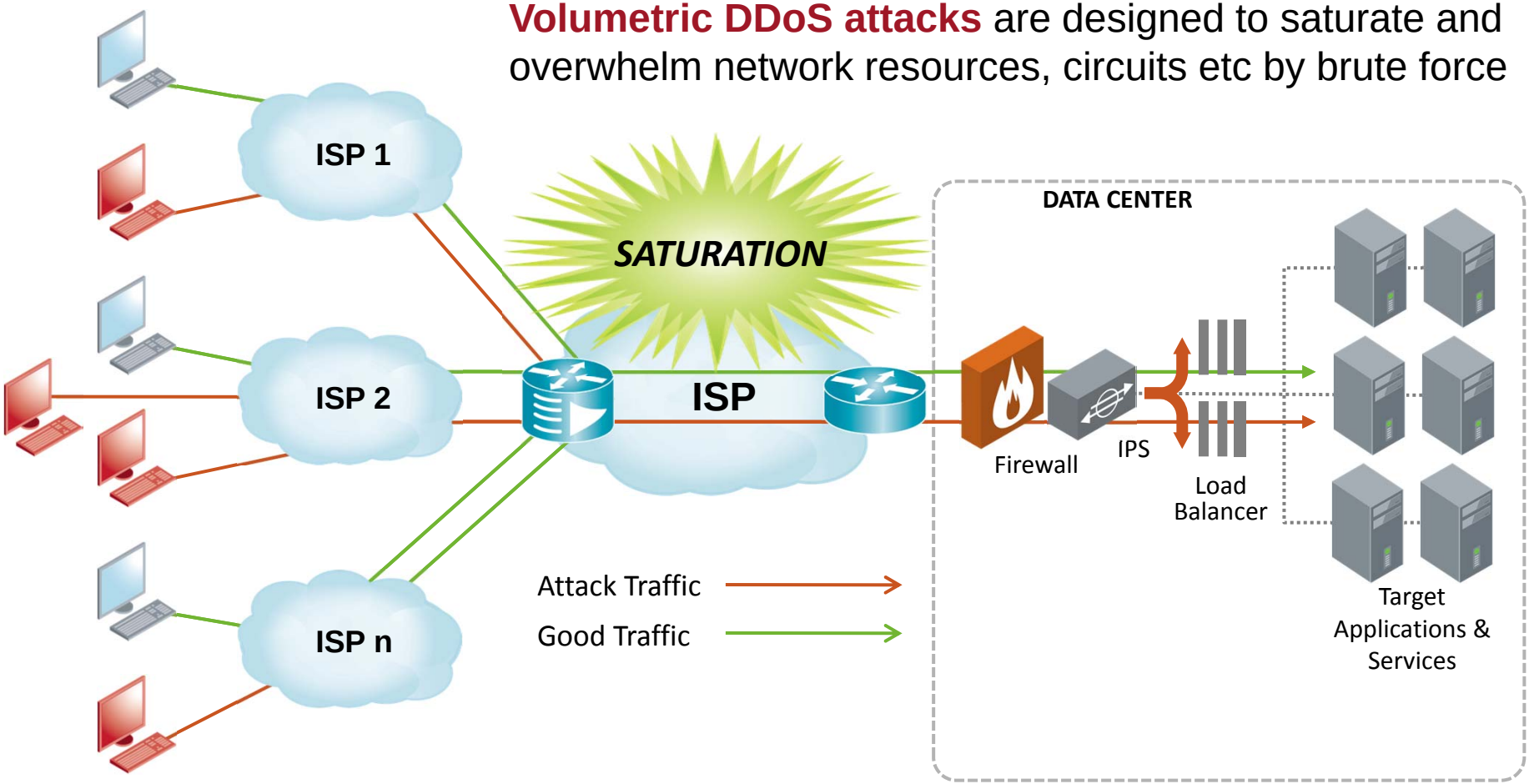
www.ddosservice.com

http://www.youtube.com/watch?v=c9MuuW0HfSA

ARBOR NETWORKS

DDoS Attack Types: Volumetric

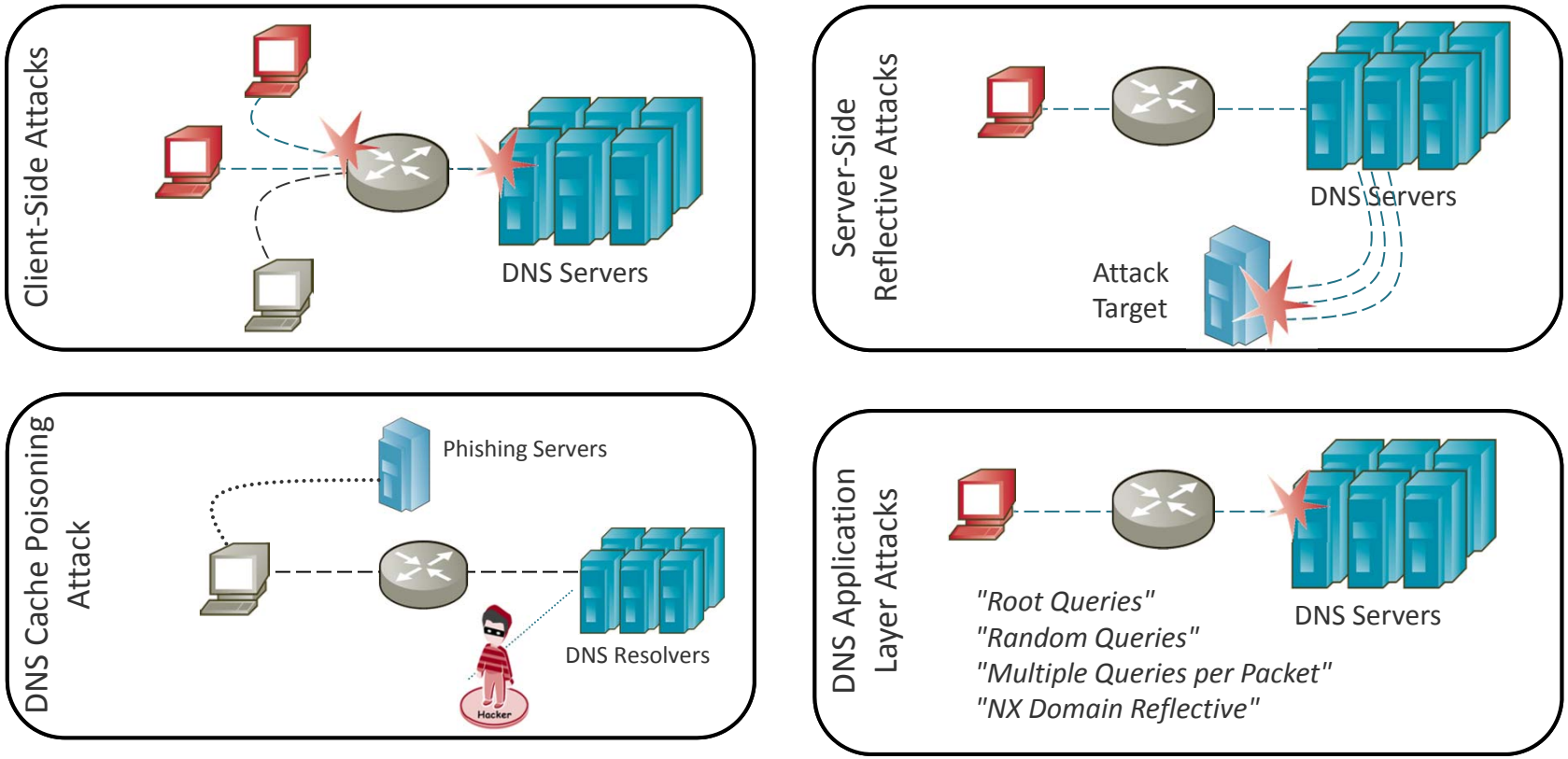
Volumetric DDoS attacks are designed to saturate and overwhelm network resources, circuits etc by brute force



Common attacks: TCP Flood, UDP Flood, Packet Flood, DNS Reflection, DNSSec Amplification…

ARBOR NETWORKS

DNS Threats

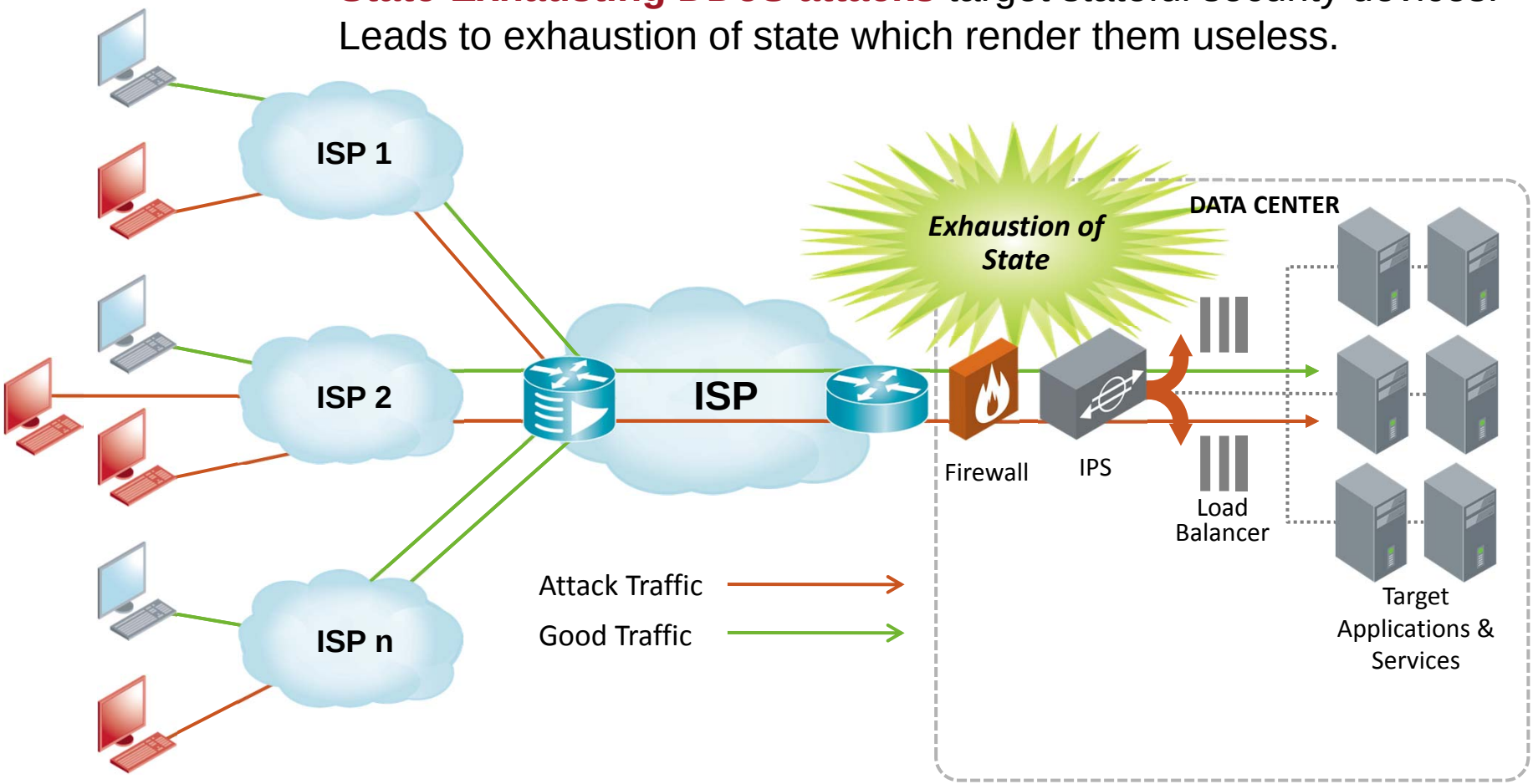


- Multiple threat vectors against DNS whose impacts include loss of service availability, reduced customer satisfaction, and hurt profitability

ARBOR NETWORKS

DDoS Attack Types: State-Exhausting

State-Exhausting DDoS attacks target stateful security devices. Leads to exhaustion of state which render them useless.



Common attacks: SYN Flood, RST Flood, FIN Flood, SockStress…

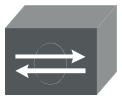
ARBOR NETWORKS

Does my FW/IDS/WAF protect me from DDoS?

Existing perimeter security devices focus on integrity and confidentiality but not on ***availability***

Information Security Triangle


Firewall


IPS

Firewalls including **WAFs** help enforce ***confidentiality*** or that information and functions can be accessed only by properly authorized parties

Intrusion Prevention Systems (IPS) help enforce ***integrity*** or that information can be added, altered, or removed only by authorized persons

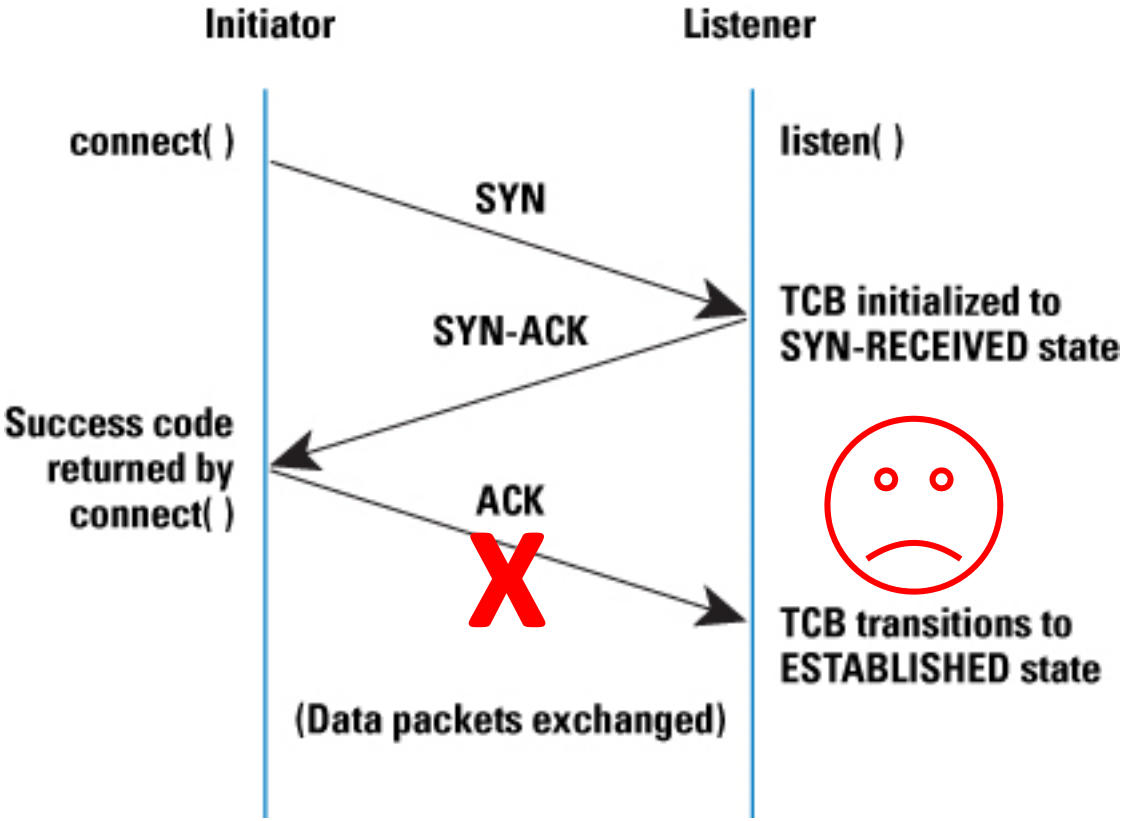
All firewalls and IPS are ***stateful*** devices which are targeted by state-based DoS attacks from botnets!

Connections per second	1,800	1,800	2,200	2,800	8,500	27,000	35,000
Maximum concurrent sessions DRAM options	16 K / 32 K[1] 512 MB3 / 1 GB DRAM	32 K[1] 1 GB DRAM	32 K / 64 K[1] 512 MB / 1 GB DRAM	96 K 1 GB DRAM	64 K / 128 K[1] 512 MB / 1 GB DRAM	375 K[2] 2 GB DRAM	512 K[2] 2 GB DRAM

Concurrent Connections	10,000; 25,000*	50,000; 130,000*	280,000	400,000	650,000
New Connections/Second	4000	9000	12,000	25,000	33,000

ARBOR NETWORKS

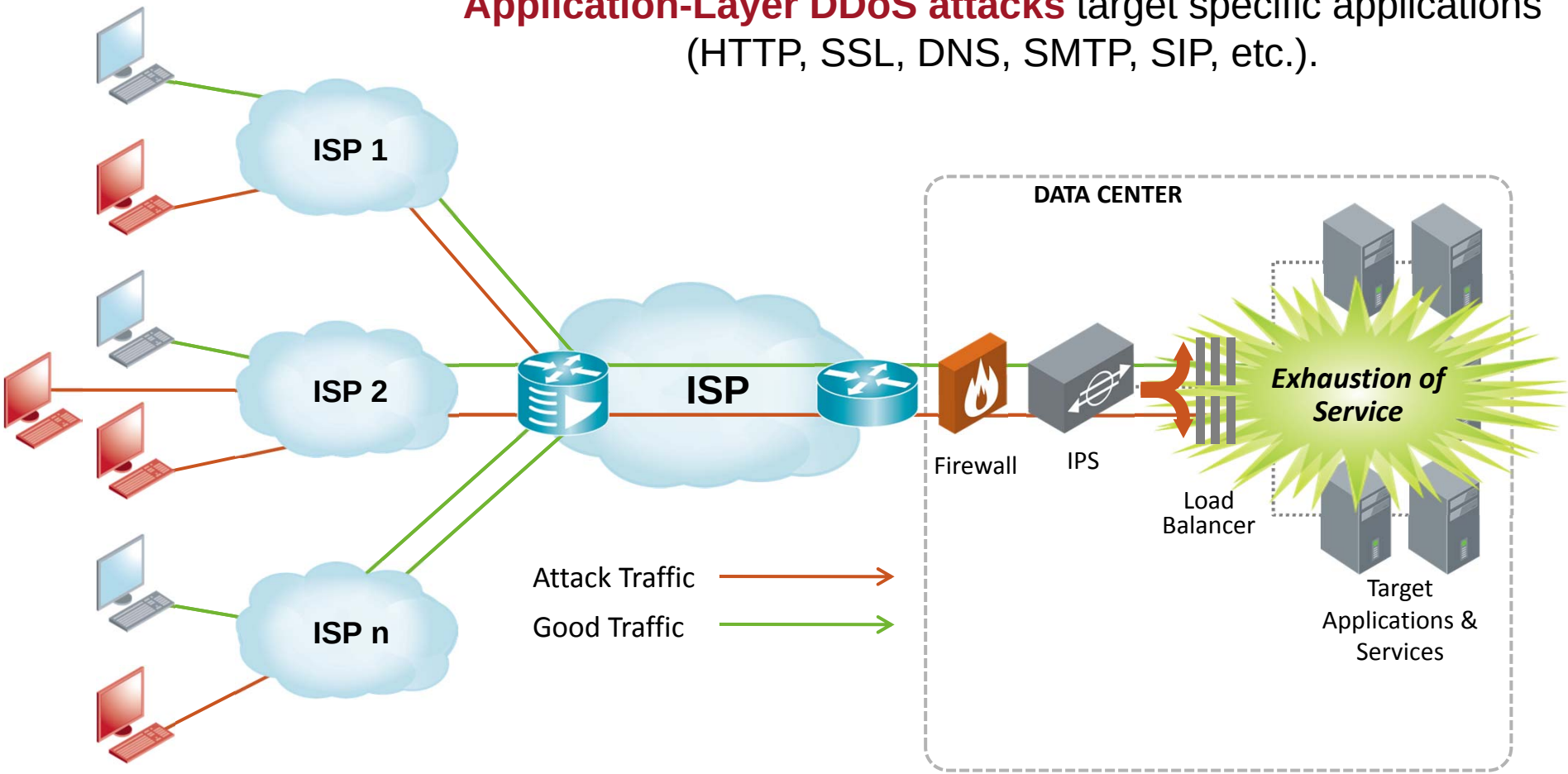
TCP Stack Attack – Syn Attack



ARBOR NETWORKS

DDoS Attack Types: Application Layer

Application-Layer DDoS attacks target specific applications (HTTP, SSL, DNS, SMTP, SIP, etc.).



Common attacks: URL Floods, R U Dead Yet (RUDY), Slowloris, Pyloris, LOIC, HOIC, DNS dictionary attacks…

ARBOR NETWORKS

Exhaustion of Memory Attacks: ApacheKiller

HEAD / HTTP/1.1

Host: 208.109.47.175

Range:bytes=0-,5-0,5-1,5-2,5-3,5-4,5-5,5-6,5-7,5-8,5-9,5-10,5-11,5-12,5-13,5-14,5-15,5-25,5-26,5-27,5-28,5-29,5-30,5-31,5-32,5-33,5-34,5-35,5-36,5-37,5-38,5-39,5-40,5-41,5-42,5-43,5-44,5-45,5-46,5-47,5-48,5-49,5-50,5-51,5-63,5-64,5-65,5-66,5-67,5-68,5-69,5-70,5-71,5-72,5-73,5-74,5-75,5-76,5-77,5-78,5-79,5-80,5-81,5-82,5-83,5-84,5-85,5-86,5-87,5-100,5-101,5-102,5-103,5-104,5-105,5-106,5-107,5-108,5-109,5-110,5-111,5-112,5-113,5-114,5-115,5-116,5-117,5-118,5-119,5-131,5-132,5-133,5-134,5-135,5-136,5-137,5-138,5-139,5-140,5-141,5-142,5-143,5-144,5-145,5-146,5-147,5-148,5-149,5-162,5-163,5-164,5-165,5-166,5-167,5-168,5-169,5-170,5-171,5-172,5-173,5-174,5-175,5-176,5-177,5-178,5-179,5-192,5-193,5-194,5-195,5-196,5-197,5-198,5-199,5-200,5-201,5-202,5-203,5-204,5-205,5-206,5-207,5-208,5-209,5-222,5-223,5-224,5-225,5-226,5-227,5-228,5-229,5-230,5-231,5-232,5-233,5-234,5-235,5-236,5-237,5-238,5-239,5-240,5-252,5-253,5-254,5-255,5-256,5-257,5-258,5-259,5-260,5-261,5-262,5-263,5-264,5-265,5-266,5-267,5-268,5-269,5-270,5-271,5-282,5-283,5-284,5-285,5-286,5-287,5-288,5-289,5-290,5-291,5-292,5-293,5-294,5-295,5-296,5-297,5-298,5-299,5-300,5-301,5-302,5-312,5-313,5-314,5-315,5-316,5-317,5-318,5-319,5-320,5-321,5-322,5-323,5-324,5-325,5-326,5-327,5-328,5-329,5-330,5-331,5-332,5-333,5-342,5-343,5-344,5-345,5-346,5-347,5-348,5-349,5-350,5-351,5-352,5-353,5-354,5-355,5-356,5-357,5-358,5-359,5-360,5-361,5-362,5-363,5-364,5-372,5-373,5-374,5-375,5-376,5-377,5-378,5-379,5-380,5-381,5-382,5-383,5-384,5-385,5-386,5-387,5-388,5-389,5-390,5-391,5-392,5-393,5-394,5-395,5-402,5-403,5-404,5-405,5-406,5-407,5-408,5-409,5-410,5-411,5-412,5-413,5-414,5-415,5-416,5-417,5-418,5-419,5-420,5-421,5-422,5-423,5-424,5-425,5-426,5-432,5-433,5-434,5-435,5-436,5-437,5-438,5-439,5-440,5-441,5-442,5-443,5-444,5-445,5-446,5-447,5-448,5-449,5-450,5-451,5-452,5-453,5-454,5-455,5-456,5-457,5-462,5-463,5-464,5-465,5-466,5-467,5-468,5-469,5-470,5-471,5-472,5-473,5-474,5-475,5-476,5-477,5-478,5-479,5-480,5-481,5-482,5-483,5-484,5-485,5-486,5-487,5-488,5-492,5-493,5-494,5-495,5-496,5-497,5-498,5-499,5-500,5-501,5-502,5-503,5-504,5-505,5-506,5-507,5-508,5-509,5-510,5-511,5-512,5-513,5-514,5-515,5-516,5-517,5-518,5-519,5-522,5-523,5-524,5-525,5-526,5-527,5-528,5-529,5-530,5-531,5-532,5-533,5-534,5-535,5-536,5-537,5-538,5-539,5-540,5-541,5-542,5-543,5-544,5-545,5-546,5-547,5-548,5-549,5-550,5-551,5-552,5-553,5-554,5-555,5-556,5-557,5-558,5-559,5-560,5-561,5-562,5-563,5-564,5-565,5-566,5-567,5-568,5-569,5-570,5-571,5-572,5-573,5-574,5-575,5-576,5-577,5-578,5-579,5-580,5-581,5-582,5-583,5-584,5-585,5-586,5-587,5-588,5-589,5-590,5-591,5-592,5-593,5-594,5-595,5-596,5-597,5-598,5-599,5-600,5-601,5-602,5-603,5-604,5-605,5-606,5-607,5-608,5-609,5-610,5-611,5-612,5-613,5-614,5-615,5-616,5-617,5-618,5-619,5-620,5-621,5-622,5-623,5-624,5-625,5-626,5-627,5-628,5-629,5-630,5-631,5-632,5-633,5-634,5-635,5-636,5-637,5-638,5-639,5-640,5-641,5-642,5-643,5-644,5-645,5-646,5-647,5-648,5-649,5-650,5-651,5-652,5-653,5-654,5-655,5-656,5-657,5-658,5-659,5-660,5-661,5-662,5-663,5-664,5-665,5-666,5-667,5-668,5-669,5-670,5-671,5-672,5-673,5-674,5-675,5-676,5-677,5-678,5-679,5-680,5-681,5-682,5-683,5-684,5-685,5-686,5-687,5-688,5-689,5-690,5-691,5-692,5-693,5-694,5-695,5-696,5-697,5-698,5-699,5-700,5-701,5-702,5-703,5-704,5-705,5-706,5-707,5-708,5-709,5-710,5-711,5-712,5-713,5-714,5-715,5-716,5-717,5-718,5-719,5-720,5-721,5-722,5-723,5-724,5-725,5-726,5-727,5-728,5-729,5-730,5-731,5-732,5-733,5-734,5-735,5-736,5-737,5-738,5-739,5-740,5-741,5-742,5-743,5-744,5-745,5-746,5-747,5-748,5-749,5-750,5-751,5-752,5-753,5-754,5-755,5-756,5-757,5-758,5-759,5-760,5-761,5-762,5-763,5-764,5-765,5-766,5-767,5-768,5-769,5-770,5-771,5-772,5-773,5-774,5-775,5-776,5-777,5-778,5-779,5-780,5-781,5-782,5-783,5-784,5-785,5-786,5-787,5-788,5-789,5-790,5-791,5-792,5-793,5-794,5-795,5-796,5-797,5-798,5-799,5-800,5-801,5-802,5-803,5-804,5-805,5-806,5-807,5-808,5-809,5-810,5-811,5-812,5-813,5-814,5-815,5-816,5-817,5-818,5-819,5-820,5-821,5-822,5-823,5-824,5-825,5-826,5-827,5-828,5-829,5-830,5-831,5-832,5-833,5-834,5-835,5-836,5-837,5-838,5-839,5-840,5-841,5-842,5-843,5-844,5-845,5-846,5-847,5-848,5-849,5-850,5-851,5-852,5-853,5-854,5-855,5-856,5-857,5-858,5-859,5-860,5-861,5-862,5-863,5-864,5-865,5-866,5-867,5-868,5-869,5-870,5-871,5-872,5-873,5-874,5-875,5-876,5-877,5-878,5-879,5-880,5-881,5-882,5-883,5-884,5-885,5-886,5-887,5-888,5-889,5-890,5-891,5-892,5-893,5-894,5-895,5-896,5-897,5-898,5-899,5-900,5-901,5-902,5-903,5-904,5-905,5-906,5-907,5-908,5-909,5-910,5-911,5-912,5-913,5-914,5-915,5-916,5-917,5-918,5-919,5-920,5-921,5-922,5-923,5-924,5-925,5-926,5-927,5-928,5-929,5-930,5-931,5-932,5-933,5-934,5-935,5-936,5-937,5-938,5-939,5-940,5-941,5-942,5-943,5-944,5-945,5-946,5-947,5-948,5-949,5-950,5-951,5-952,5-953,5-954,5-955,5-956,5-957,5-958,5-959,5-960,5-961,5-962,5-963,5-964,5-965,5-966,5-967,5-968,5-969,5-970,5-971,5-972,5-973,5-974,5-975,5-976,5-977,5-978,5-979,5-980,5-981,5-982,5-983,5-984,5-985,5-986,5-987,5-988,5-989,5-990,5-991,5-992,5-993,5-994,5-995,5-996,5-997,5-998,5-999,5-1000,5-1001,5-1002,5-1003,5-1004,5-1005,5-1006,5-1007,5-1008,5-1009,5-1010,5-1011,5-1012,5-1013,5-1014,5-1015,5-1016,5-1017,5-1018,5-1019,5-1020,5-1021,5-1022,5-1023,5-1024,5-1025,5-1026,5-1027,5-1028,5-1029,5-1030,5-1031,5-1032,5-1033,5-1034,5-1035,5-1036,5-1037,5-1038,5-1039,5-1040,5-1041,5-1042,5-1043,5-1044,5-1045,5-1046,5-1047,5-1048,5-1049,5-1050,5-1051,5-1052,5-1053,5-1054,5-1055,5-1056,5-1057,5-1058,5-1059,5-1060,5-1061,5-1062,5-1063,5-1064,5-1065,5-1066,5-1067,5-1068,5-1069,5-1070,5-1071,5-1072,5-1073,5-1074,5-1075,5-1076,5-1077,5-1078,5-1079,5-1080,5-1081,5-1082,5-1083,5-1084,5-1085,5-1086,5-1087,5-1088,5-1089,5-1090,5-1091,5-1092,5-1093,5-1094,5-1095,5-1096,5-1097,5-1098,5-1099,5-1100,5-1101,5-1102,5-1103,5-1104,5-1105,5-1106,5-1107,5-1108,5-1109,5-1110,5-1111,5-1112,5-1113,5-1114,5-1115,5-1116,5-1117,5-1118,5-1119,5-1120,5-1121,5-1122,5-1123,5-1124,5-1125,5-1126,5-1127,5-1128,5-1129,5-1130,5-1131,5-1132,5-1133,5-1134,5-1135,5-1136,5-1137,5-1138,5-1139,5-1140,5-1141,5-1142,5-1143,5-1144,5-1145,5-1146,5-1147,5-1148,5-1149,5-1150,5-1151,5-1152,5-1153,5-1154,5-1155,5-1156,5-1157,5-1158,5-1159,5-1160,5-1161,5-1162,5-1163,5-1164,5-1165,5-1166,5-1167,5-1168,5-1169,5-1170,5-1171,5-1172,5-1173,5-1174,5-1175,5-1176,5-1177,5-1178,5-1179,5-1180,5-1181,5-1182,5-1183,5-1184,5-1185,5-1186,5-1187,5-1188,5-1189,5-1190,5-1191,5-1192,5-1193,5-1194,5-1195,5-1196,5-1197,5-1198,5-1199,5-1200,5-1201,5-1202,5-1203,5-1204,5-1205,5-1206,5-1207,5-1208,5-1209,5-1210,5-1211,5-1212,5-1213,5-1214,5-1215,5-1216,5-1217,5-1218,5-1219,5-1220,5-1221,5-1222,5-1223,5-1224,5-1225,5-1226,5-1227,5-1228,5-1229,5-1230,5-1231,5-1232,5-1233,5-1234,5-1235,5-1236,5-1237,5-1238,5-1239,5-1240,5-1241,5-1242,5-1243,5-1244,5-1245,5-1246,5-1247,5-1248,5-1249,5-1250,5-1251,5-1252,5-1253,5-1254,5-1255,5-1256,5-1257,5-1258,5-1259,5-1260,5-1261,5-1262,5-1263,5-1264,5-1265,5-1266,5-1267,5-1268,5-1269,5-1270,5-1271,5-1272,5-1273,5-1274,5-1275,5-1276,5-1277,5-1278,5-1279,5-1280,5-1281,5-1282,5-1283,5-1284,5-1285,5-1286,5-1287,5-1288,5-1289,5-1290,5-1291,5-1292,5-1293,5-1294,5-1295,5-1296,5-1297,5-1298,5-1299

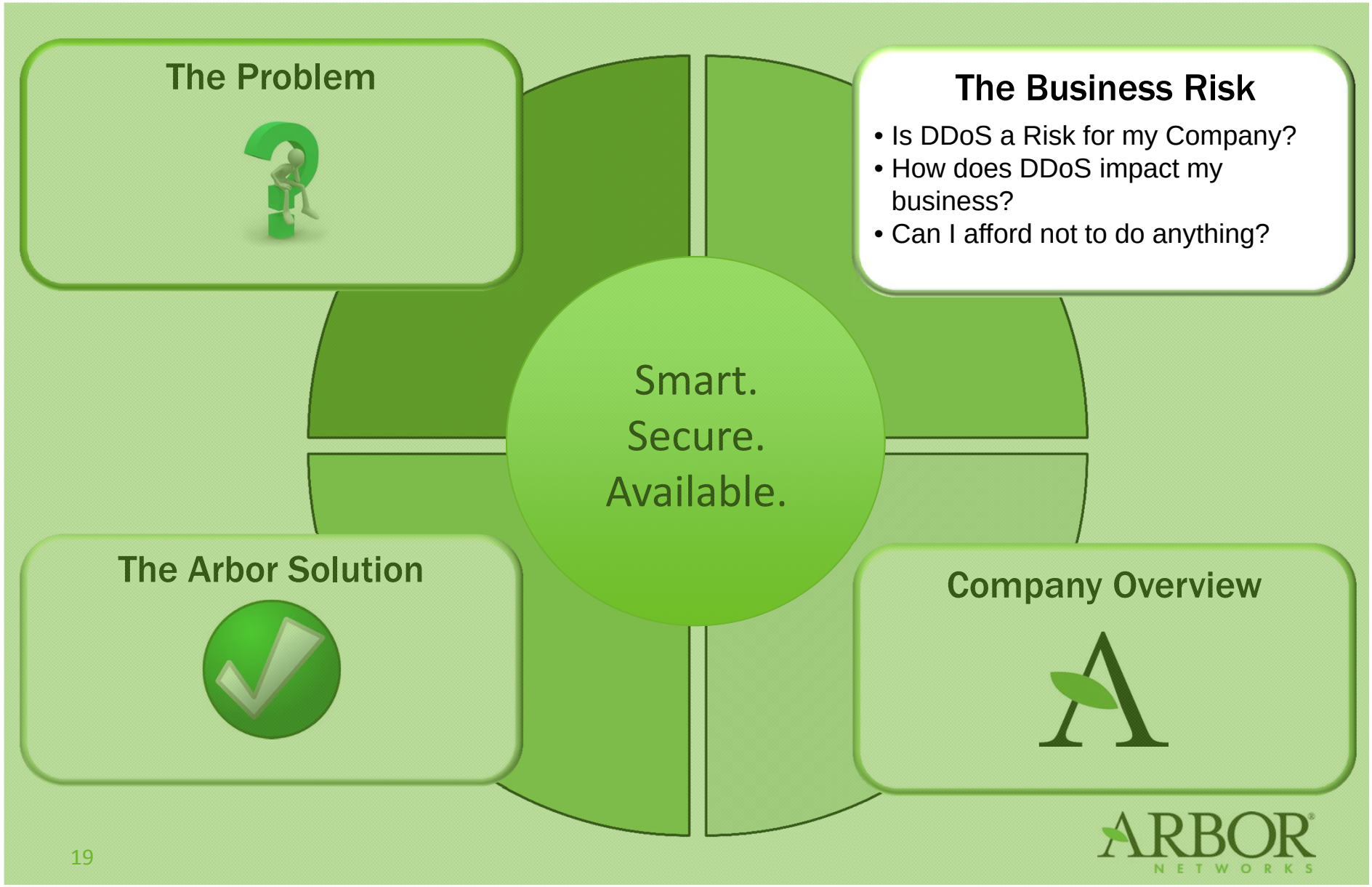
Accept-Encoding: gzip

Connection: close

Server needs to load big files into memory to allow resumes and die.

ARBOR NETWORKS

Agenda


The Problem
The Business Risk
• Is DDoS a Risk for my Company?
• How does DDoS impact my business?
• Can I afford not to do anything?
Smart.
Secure.
Available.
The Arbor Solution
Company Overview
ARBOR
NETWORKS

The Increases in DDoS Attacks

Increased Attack Tools

More and more tools available to perform the attacks (LOIC, HOIC; Slowloris, SlowPost…)

Increased Complexity

Over quarter of attacks are now *application-based DDoS mostly targeting HTTP, DNS, SMTP*

Increased Frequency

More than 50% of data center operators are seeing more than 10 attacks per month

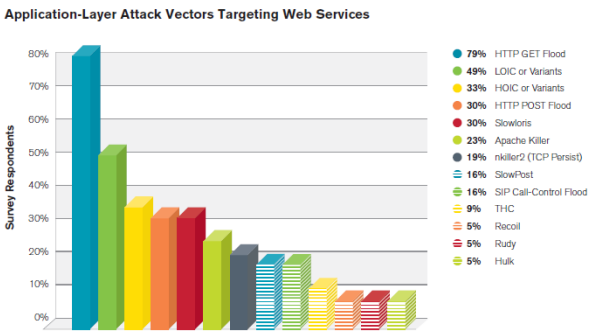


Figure 25 Source: Arbor Networks, Inc.

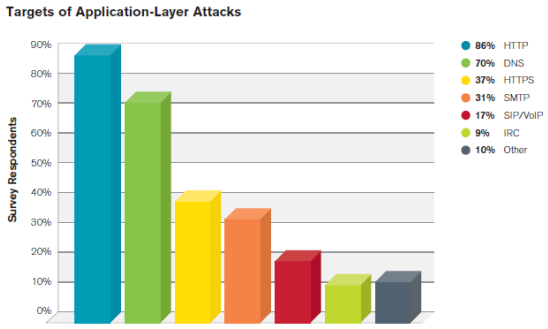


Figure 24 Source: Arbor Networks, Inc.

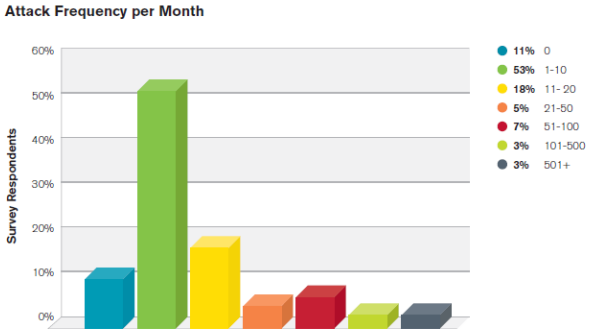


Figure 27 Source: Arbor Networks, Inc.

The Increased Complexity and Frequency is Driving Demand in Midsize Enterprises

Attacks Size historic report & Duration

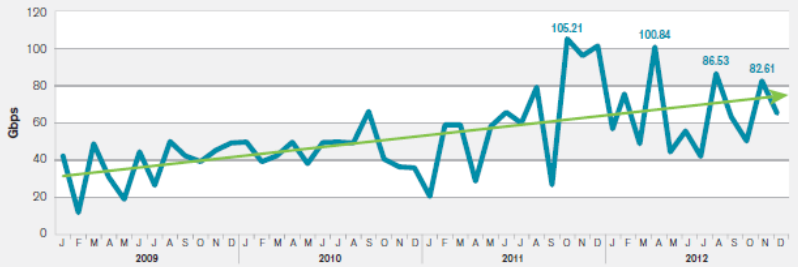


Figure 17 Source: Arbor Networks, Inc.

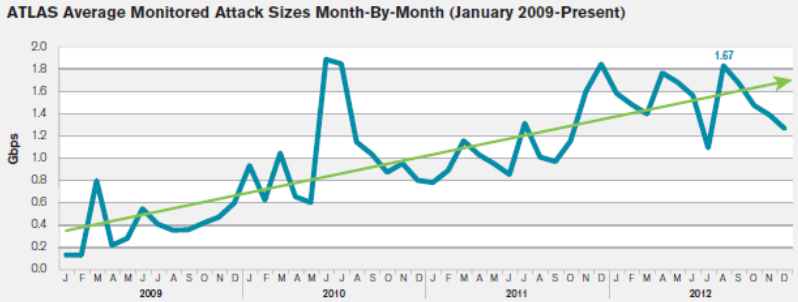


Figure 18 Source: Arbor Networks, Inc.

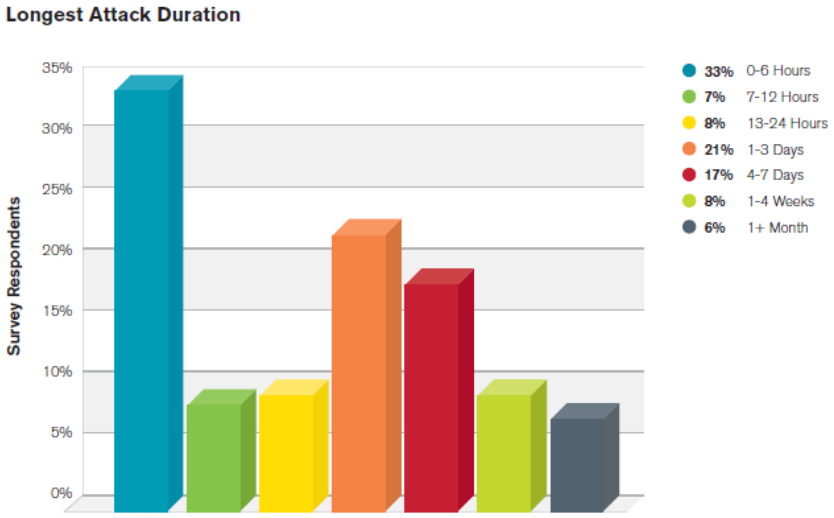


Figure 28 Source: Arbor Networks, Inc.

ARBOR NETWORKS

What impact has DDoS in my business?

Table 1: Cost elements

Operation	How many IT personnel will be tied up addressing the attack?
Help Desk	How many more help desk calls will be received, and at what cost per call?
Recovery	How much manual work will need to be done to re-enter transactions?
Lost Worker Output	How much employee output will be lost?
Lost Business	How much business will we lose during the outage?
Lost Customers	How many existing customers will defect to competitors? What is the lifetime value of these customers?
Penalties	How much will have to be paid in service level agreement (SLA) credits or other penalties?
Lost Future Business	How much will the ability to attract new customers be affected? What is the full value of that lost business?
Brand and Reputation Damage	What is the cost to the company brand and reputation?

Source: Gartner Report Making the case for DDoS protection

ARBOR NETWORKS

Reputation impact due to DDoS

Chile: Sitios de HidroAysén y Endesa son derribados por Anonymous

MEDIOS Y REDES

Wikileaks está caído por un ataque de negación de servicio

- El polémico portal de filtraciones lleva cinco días inaccesible y ha pedido donaciones para contratar más ancho de banda por los problemas que le está causando el grupo «AntiLeaks»

El secretario de Defensa de EE UU avisa del riesgo de un ataque cibernético

- Leon Panetta asegura que existe una amenaza real de que Estados Unidos sufra un ataque cibernético por el aumento de la vulnerabilidad de sus infraestructuras

El 64% de los bancos sufrieron ataques DDoS en 2012

europa press Europa Press – mié, 30 ene 2013

Anonymous convoca un ataque DDoS contra Telefónica y Movistar este domingo

el 22-06-2011 18:16

CASO WIKILEAKS | Problemas en el 'site' del Ministerio de Justicia

Anonymous 'tumba' webs del Gobierno británico en apoyo de Julian Assange

- Los 'hackers' apoyan al recluido en la embajada de Ecuado
- Bloquean varias páginas de instituciones públicas británicas

ELMUNDO.es sufre de madrugada un ataque de denegación de servicio (DDoS)

- Se realizó a través de las técnicas 'SYN Flood' e 'IP address spoofing'
- También estuvieron 'caídas' Marca.com y Expansion.com, entre otras
- Entre las 5.30 y las 8.30 hubo peticiones de acceso masivas a las páginas
- A partir de las 8.00 se controló el ataque y se recuperó la normalidad

ARBOR NETWORKS

DDoS *is* Availability Risk Planning

DDoS is the #1 threat to the availability of services – but it is not part of the risk analysis

When measuring the risk to the availability or resiliency of services, where does **the risk of DDoS attacks** fall on the list?

ARBOR NETWORKS

Spanish Law for Critical Infraestructures Securization

BOLETÍN OFICIAL DEL ESTADO

Núm. 102 Viernes 29 de abril de 2011 Sec. I. Pág. 43370

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

7630 *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.*

En consecuencia, y dada la complejidad de la materia, su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la **Directiva 2008/114/CE,** se hace preciso elaborar una norma cuyo objeto es, por un lado, regular la **protección de las infraestructuras críticas** contra **ataques** deliberados de todo tipo (tanto de carácter físico como **cibernético**) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas. Como pieza básica de este sistema**, la Ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas** como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema.

GUÍA DE BUENAS PRÁCTICAS

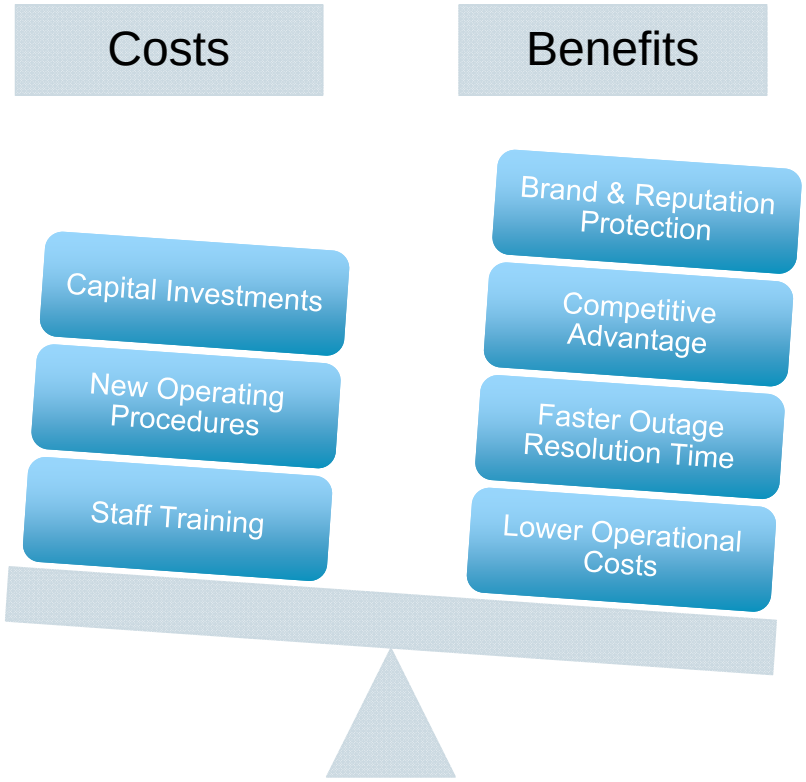
CNPIC

ARBOR NETWORKS

All Firms Must Have DDoS Risk Mitigation Plan

All enterprises must ***take control*** of their DDoS risk mitigation strategy – don't be an ostrich!

A simple cost-benefit analysis reveals the benefits of a proactive strategy – can any enterprise simply afford to not control their response to a DDoS attack?



ARBOR NETWORKS

Agenda

The Problem

The Business Risk

Smart.
Secure.
Available.

The Arbor Solution

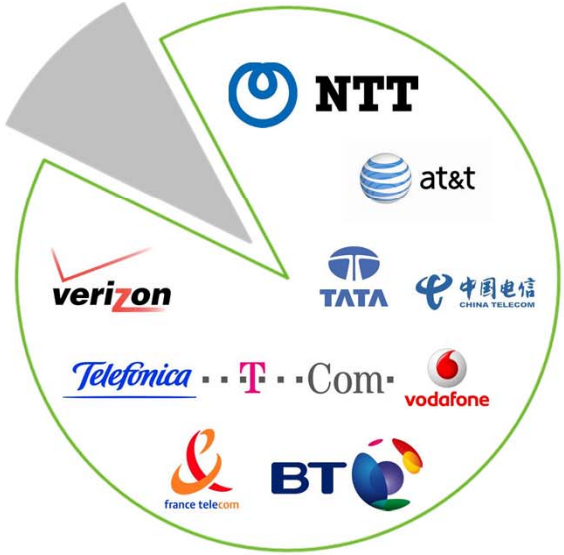
Arbor Overview

- Arbor History
- What people say about Arbor
- Market Shares

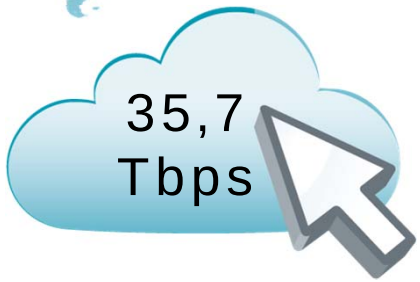
ARBOR NETWORKS

Arbor - a Trusted & Proven Vendor Securing the World's Largest and Most Demanding Networks

90% Percentage of world's Tier 1 service providers who are Arbor customers



115 Number of countries with Arbor products deployed



Amount of global traffic monitored by the ATLAS security intelligence initiative right now – **25% of global Internet traffic!**

13 Number of years Arbor has been delivering innovative security and network visibility technologies & products

Arbor market position in Carrier, Enterprise and Mobile DDoS equipment market segments – **61% of total market**
[Infonetics Research Dec 2012]

$16B 2011 GAAP revenues [USD] of Danaher – Arbor's parent company providing deep financial backing

ARBOR NETWORKS

Agenda

The Problem

The Business Risk

Smart.
Secure.
Available.

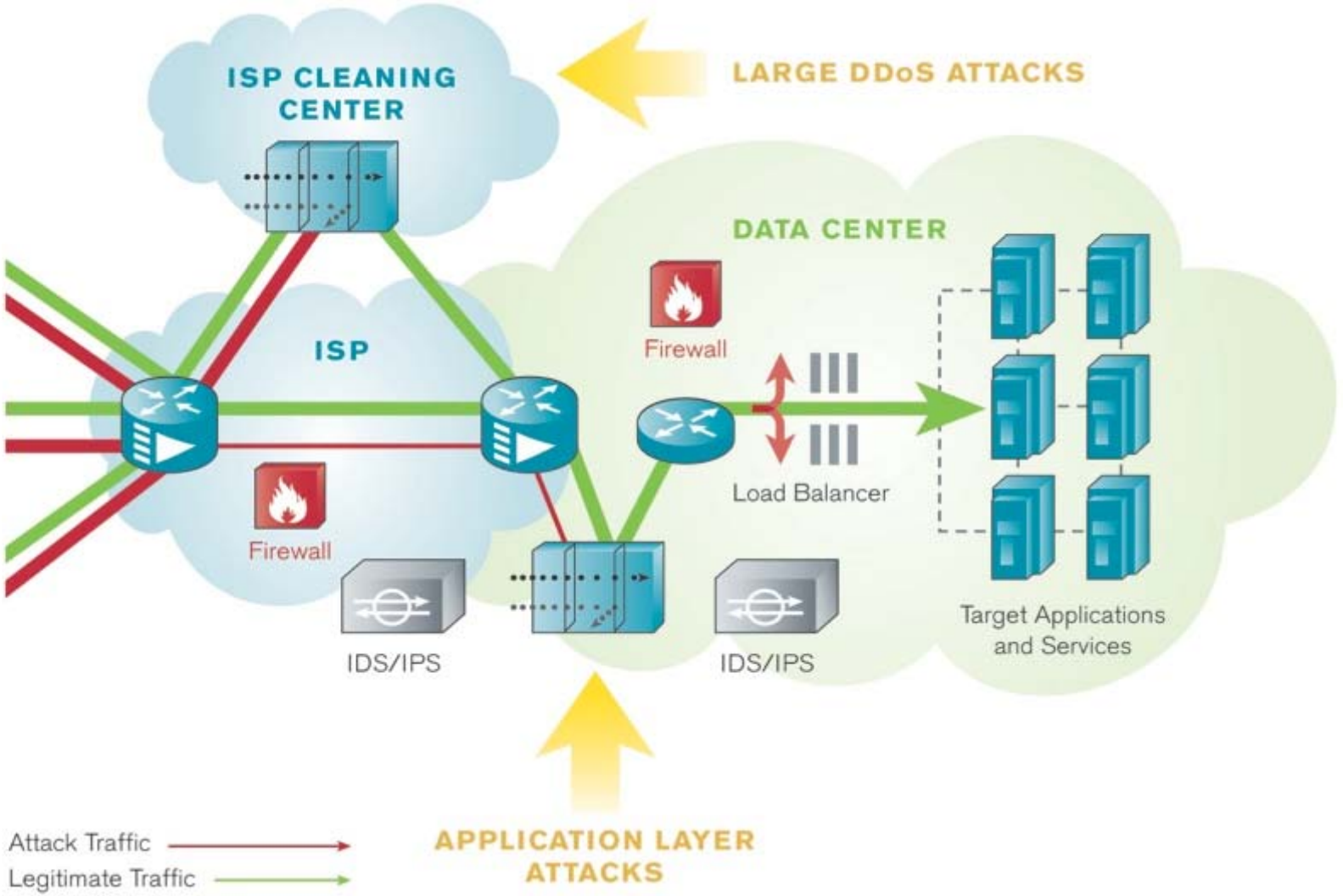
Arbor's Solution

- Arbor Solution Positioning
- Products for SP & Enterprise
- Services for SP & Enterprise
- Cloud Signalling

Company Overview

ARBOR NETWORKS

Stopping Attacks in the Right Place



ARBOR NETWORKS

Arbor's Key Technologies

Visibility

Arbor's products are the premier analyzers of **full network flow** data providing holistic traffic & security visibility

Arbor's products offer **deep insight** into applications and services as more services move to standard ports

Arbor's products leverage the **real-time Internet-wide visibility** of the ATLAS initiative to detect and stop active threats

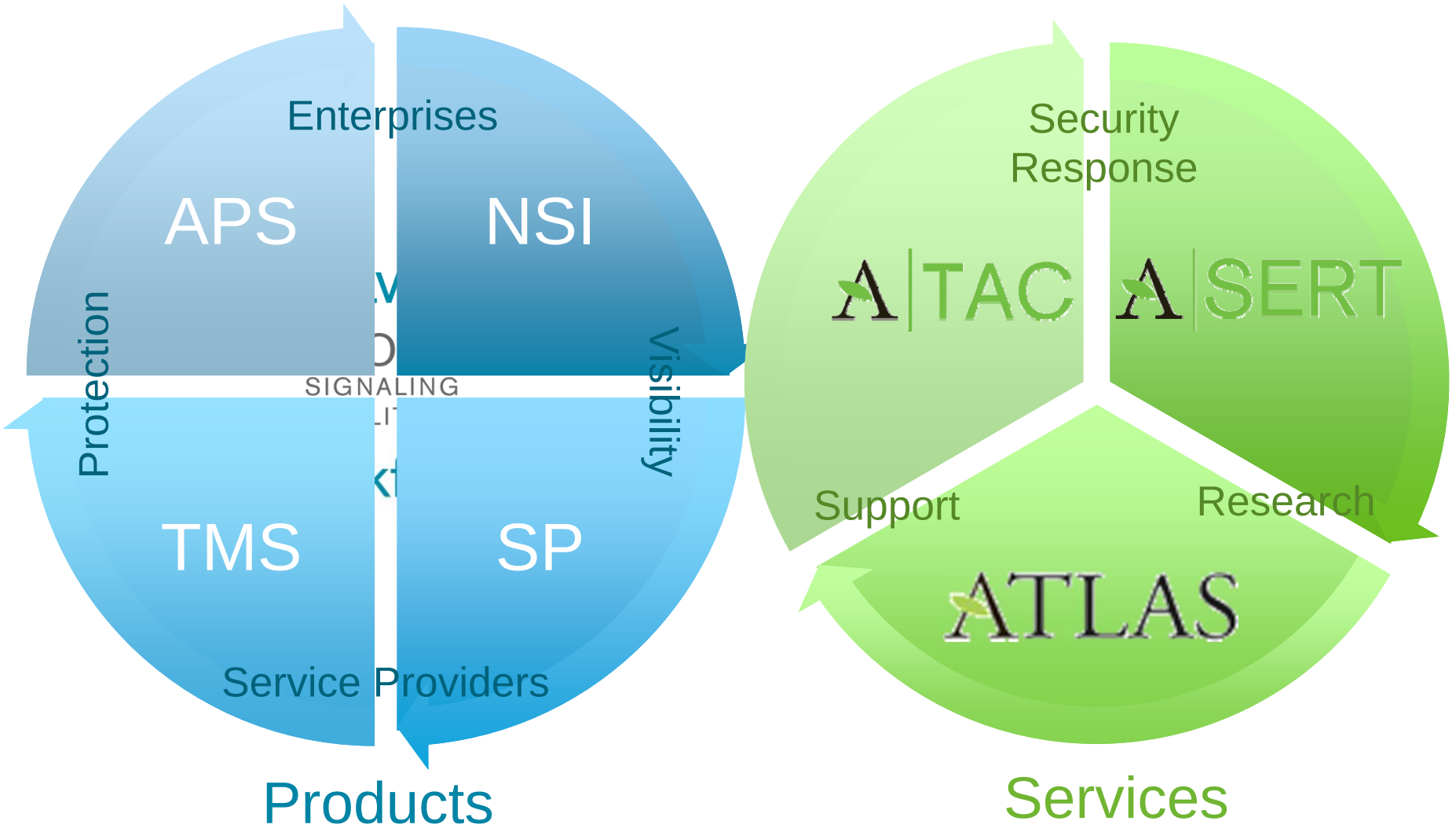
Protection

Arbor's core packet analysis & blocking engine can **stop** and is also **immune** to all threats against availability.

Arbor's Security & Emergency Response Team (ASERT) conducts **unique research** into botnets and malware.

Arbor's proprietary protocol enables signaling from the enterprise edge to the cloud for **complete protection**

Arbor Products & Services



Peakflow Products

Peakflow®

Visibility

Peakflow SP

Models: CP-5500, PI-5500, BI-5500, FS-5500

The **Peakflow Service Provider (SP)** solution collects and analyzes Flow, BGP, and SNMP data; conducts network ***anomaly detection*** for security visibility; provides user interface for managed services; and ***massive scale*** to meet the needs of the world's largest service providers and cloud operators.

Protection

Peakflow TMS

Models: TMS-1200, TMS-2500, TMS-3000 Series, TMS-4000 Series

The **Peakflow Threat Management System (TMS)** is built for high-performance, carrier-class networks and used for ***surgical*** mitigation of DDoS attack traffic ***with no additional latency*** for legitimate traffic; and serves as protection platform for in-cloud managed security services.

ARBOR® NETWORKS

Pravail Products

Pravail

Visibility

Pravail NSI

Models: Collectors 5003, 5004, 5005, 5006, 5007; Controllers 5110, 5120, 5130, 5220, 5230

The **Pravail Network Security Intelligence (NSI)** solution (*formally known as Peakflow X*) collects and analyzes Flow and raw packet data; performs behavioral anomaly detection; and provides application-level and pervasive ***security intelligence*** across the enterprise network.

Protection

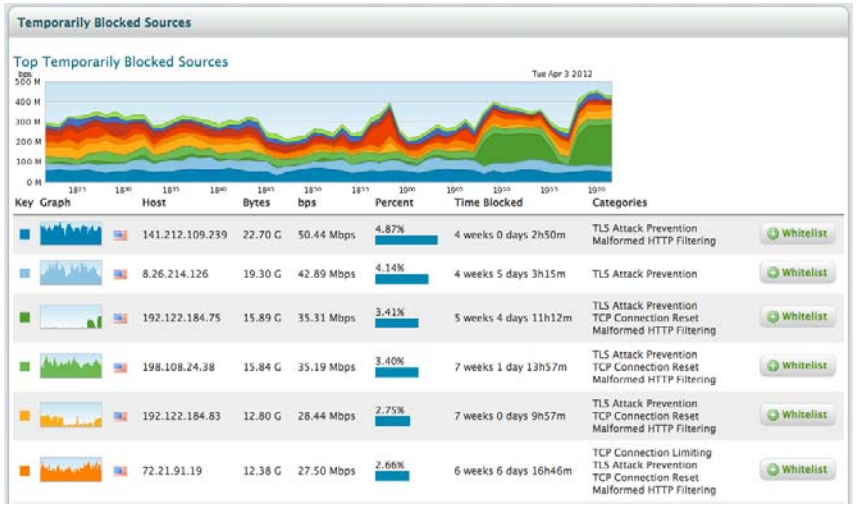
Pravail APS

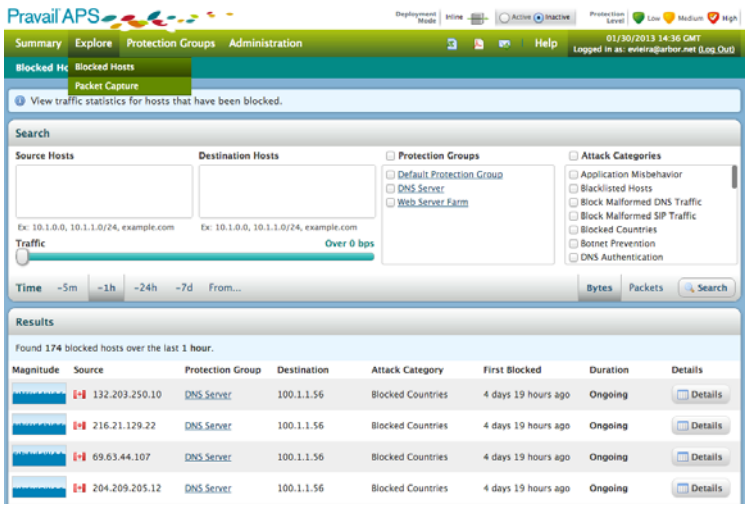
Models: APS 2202, APS-2203- APS 2004, APS-2104, APS-2105, APS-2107, APS-2108

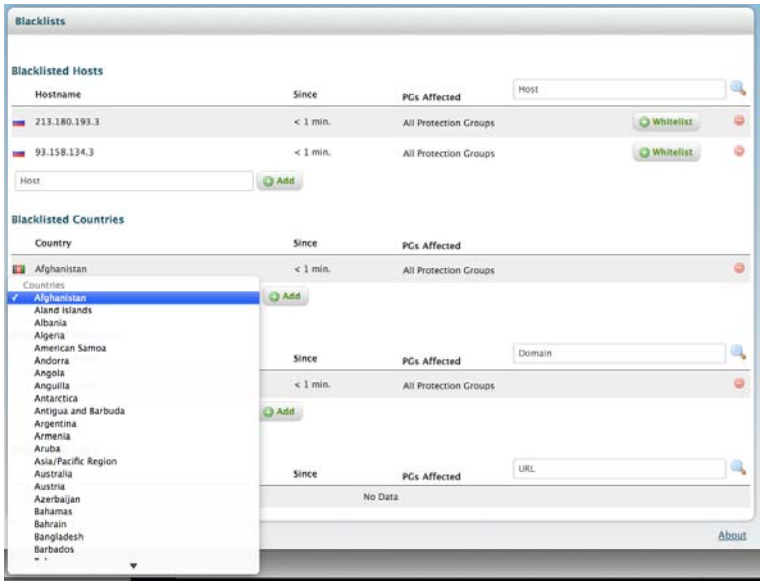
The **Pravail Availability Protection System (APS)** provides out-of-box protection for attacks while being immune to state-exhausting attacks; blocks complex application-layer DDoS; supports a dynamic threat from ATLAS to stop botnets; supports inline deployment models; and ability to send cloud signals upstream.

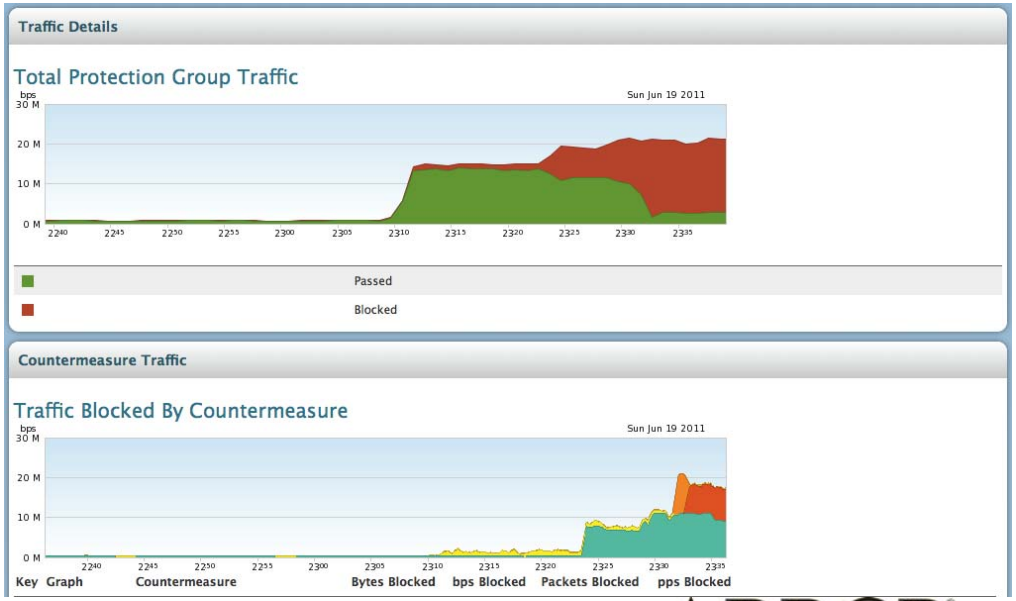
ARBOR NETWORKS

Pravail capabilities



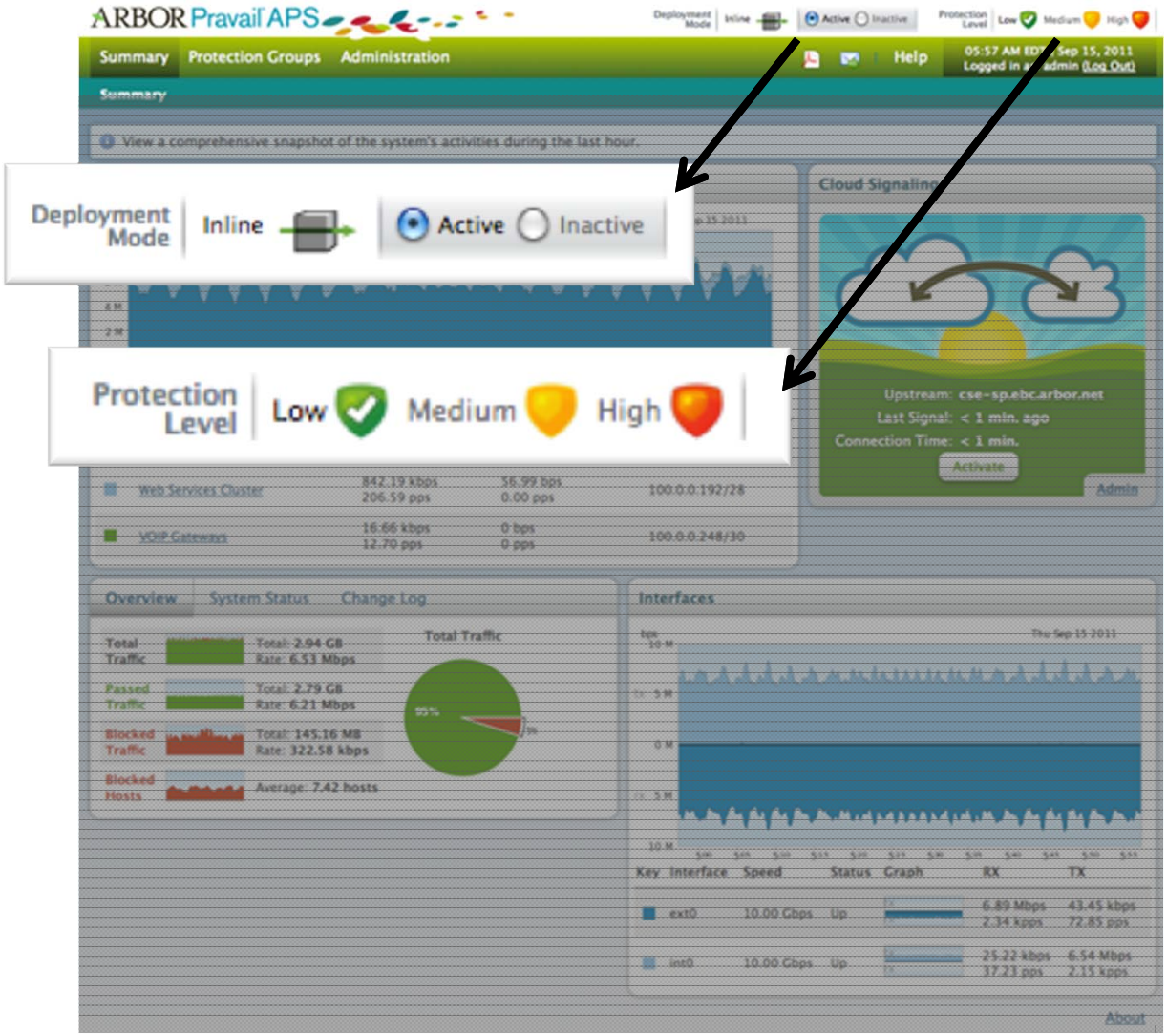






ARBOR NETWORKS

Customer Basic Self Mitigation



- Mode:
  - Active
  - Inactive
- Protection Level:
  - Low
  - Medium
  - High
- Cloud Signaling
  - Status
  - Automatic
  - Manually

ARBOR NETWORKS

ARBOR®
NETWORKS

Thank You