VIII JORNADAS

STIC CCN-CERT

La defensa del patrimonio tecnológico
frente a los ciberataques

10 y 11 de diciembre de 2014

ccn-cert
centro criptológico nacional

Servicio de Defensa frente a ataques de DDoS: Modelo colaborativo de detección

CCN
Centro Criptológico Nacional

Esquema de Evaluación y Certificación de la Seguridad de las Tecnologías de Información

C/Argentona 20, 28023 MADRID

www.ccn-cert.cni.es

Alex Lopez

Arbor Networks

alopez@arbor.net

Índice

1 ¿Que es el DDoS?

2 Tipos de ataque DDoS

3 Modelos de defensa frente a DDoS

4 Comparación de modelos de Servicios

5 Solución de Red Iris

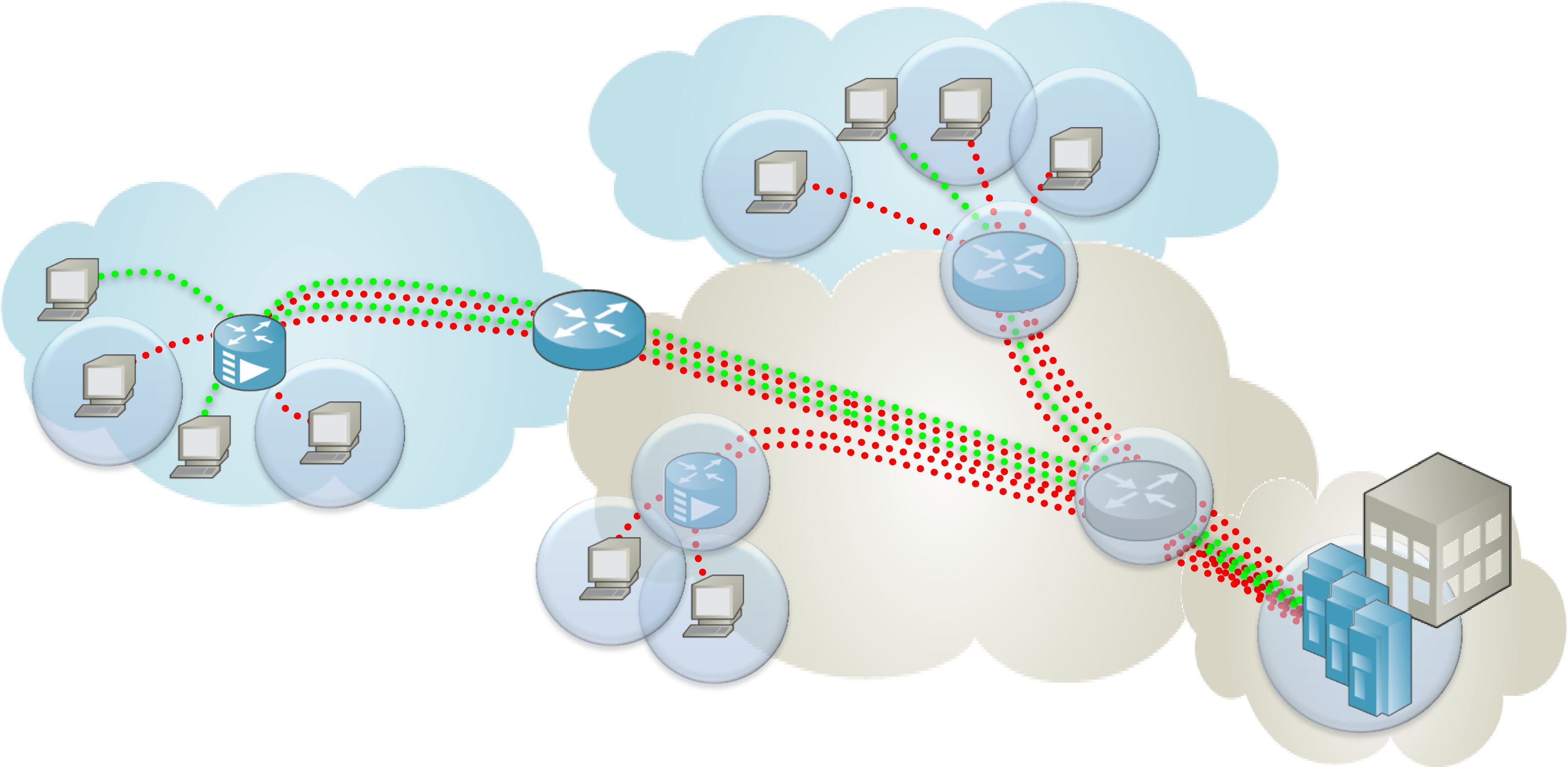
6 War Game

7 Preguntas/Debate

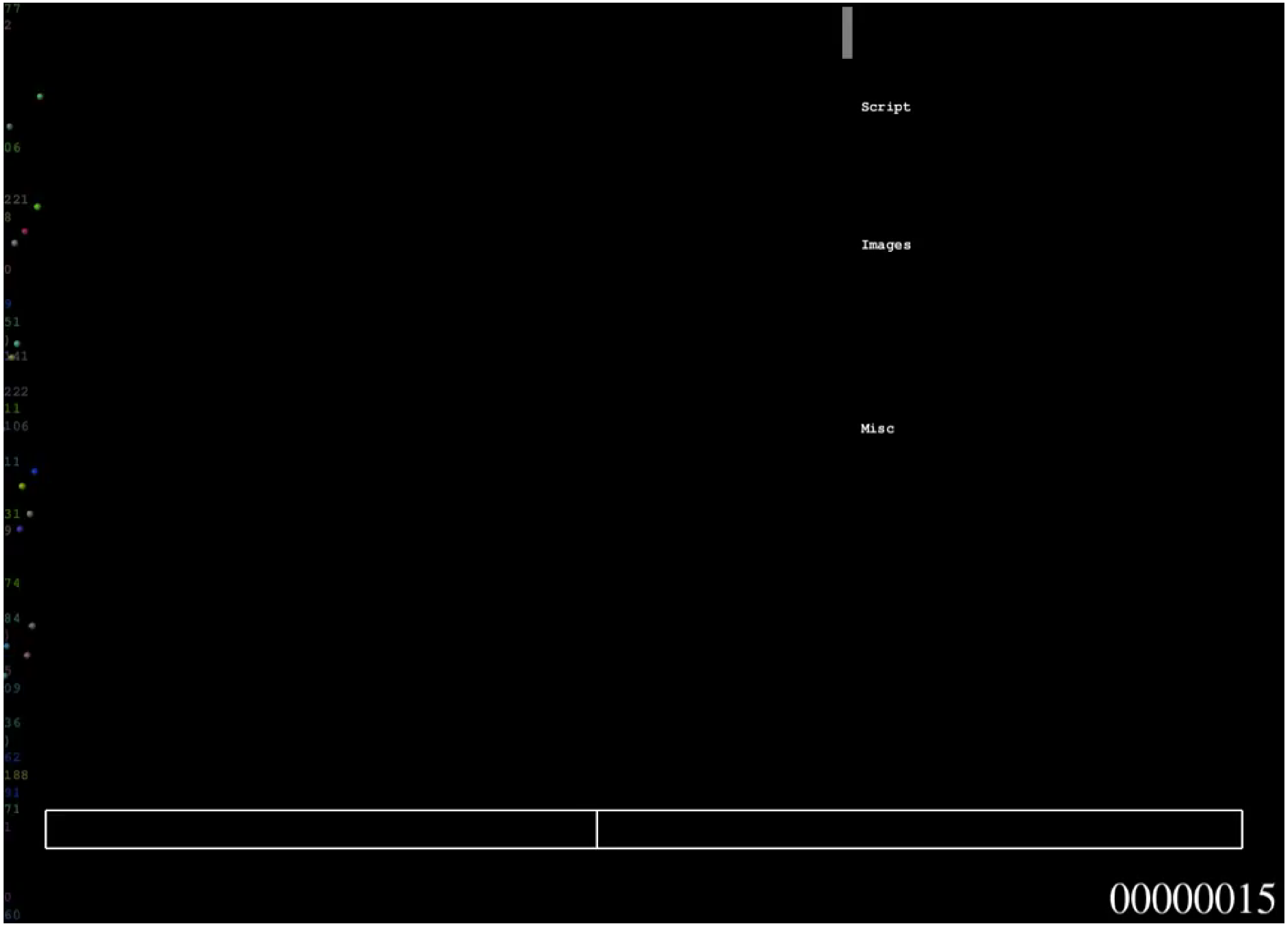
1

¿Que es el DDoS?

- En seguridad informática, un **ataque de denegación de servicios**, también llamado ataque **DoS** (de las siglas en inglés *Denial of Service*) o **DDoS** (de **D**istributed **D**enial of**S**ervice), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- Una ampliación del ataque DoS es el llamado **ataque distribuido de denegación de servicio**, también llamado ataque **DDoS** (de las siglas en inglés *Distributed Denial ofService*) el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión. La forma más común de realizar un DDoS es a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica.



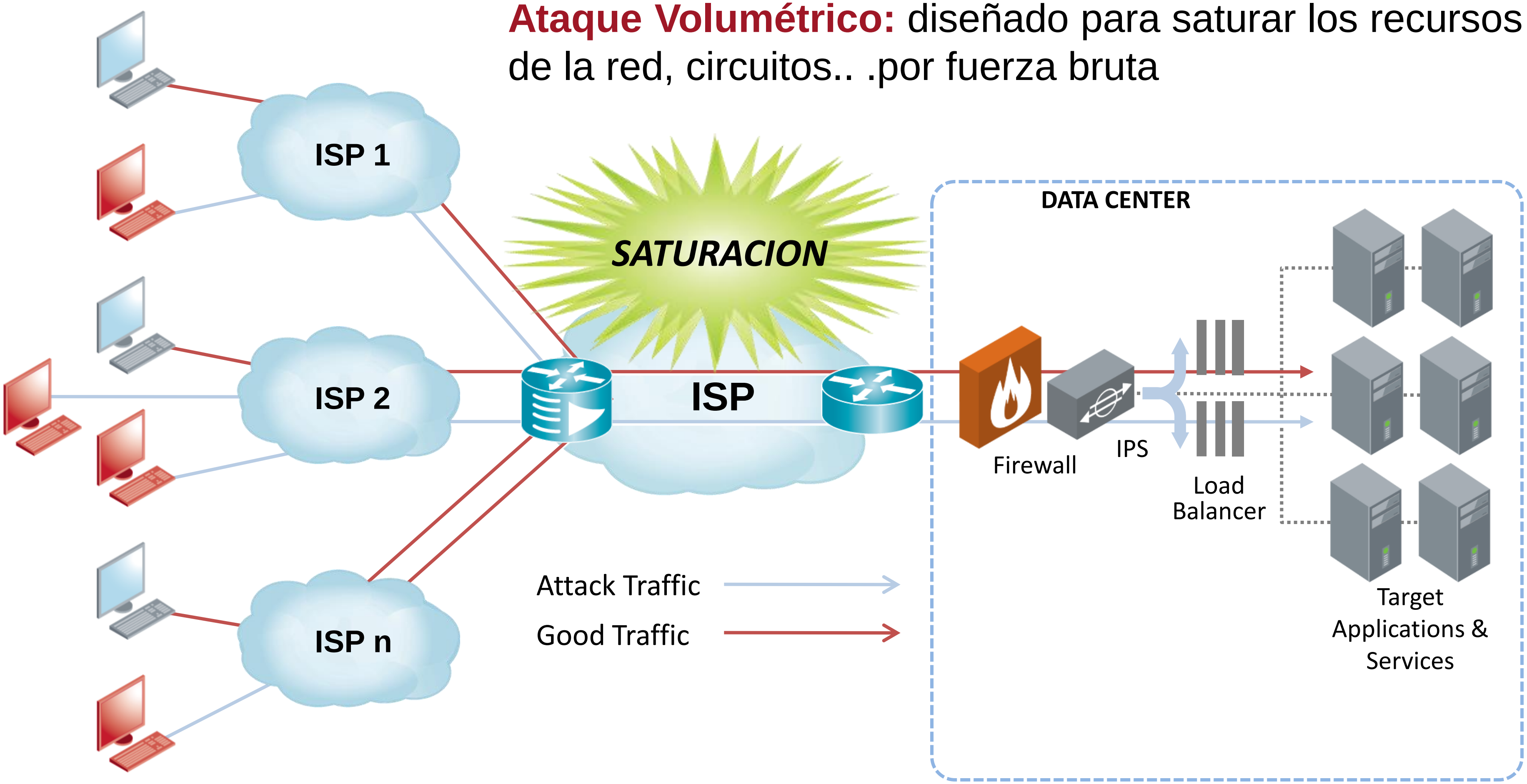
Durante un ataque de denegación de servicio distribuido (DDoS), hosts o bots comprometidos de fuentes dispersas abruman al objetivo con tráfico ilegítimo por lo que los servidores no pueden responder a los clientes legítimos.


Script
Images
Misc
00000015

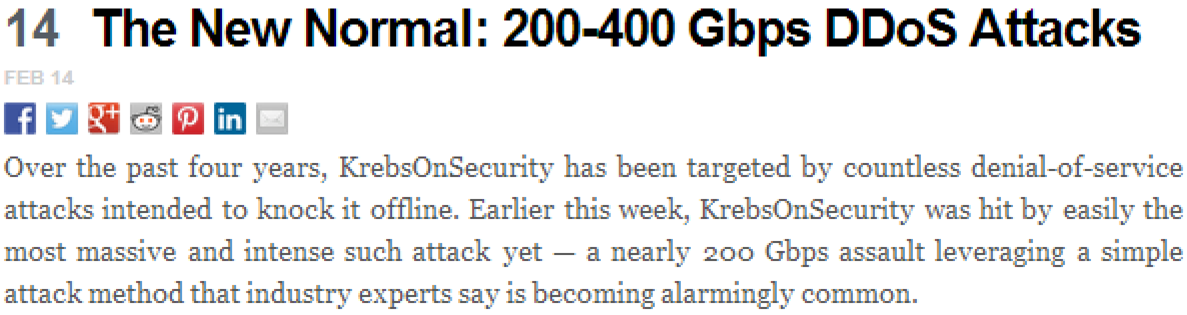
2

Tipos de ataques DDoS

Ataque Volumétrico: diseñado para saturar los recursos de la red, circuitos.. .por fuerza bruta



Ataques Típicos: TCP Flood, UDP Flood, Packet Flood, DNS Reflection, DNSSec Amplification…

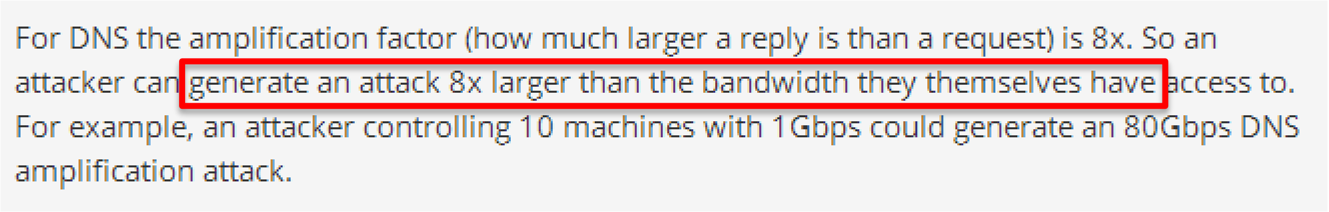


14 The New Normal: 200-400 Gbps DDoS Attacks

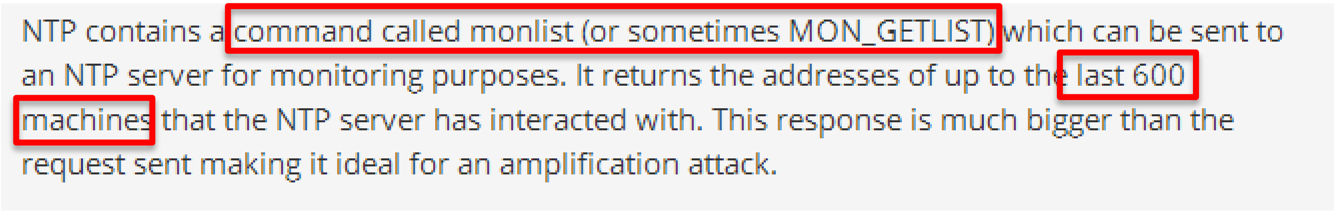
FEB 14

Over the past four years, KrebsOnSecurity has been targeted by countless denial-of-service attacks intended to knock it offline. Earlier this week, KrebsOnSecurity was hit by easily the most massive and intense such attack yet — a nearly 200 Gbps assault leveraging a simple attack method that industry experts say is becoming alarmingly common.

Technical Details Behind a 400Gbps NTP Amplification DDoS Attack



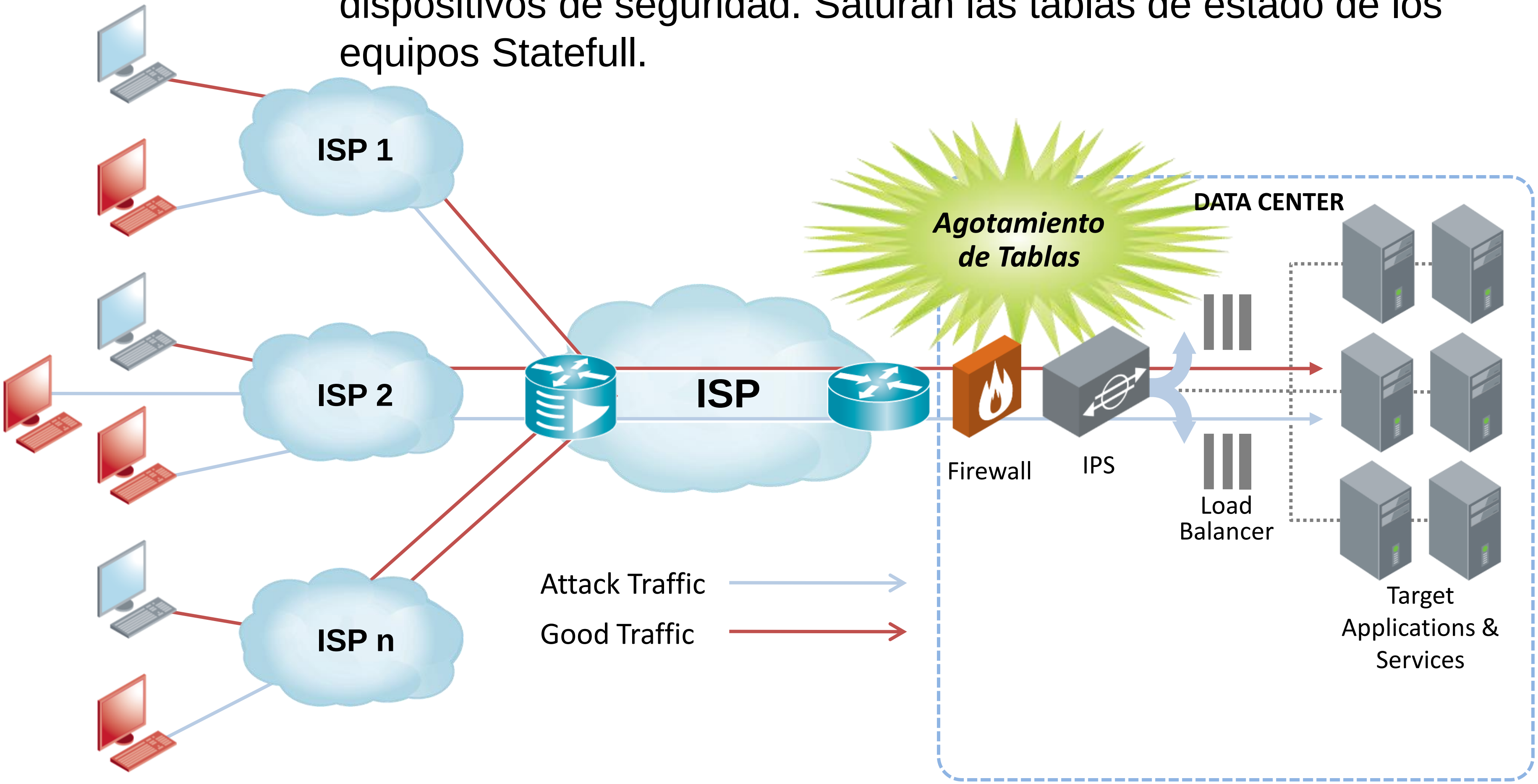
For DNS the amplification factor (how much larger a reply is than a request) is 8x. So an attacker can generate an attack 8x larger than the bandwidth they themselves have access to. For example, an attacker controlling 10 machines with 1Gbps could generate an 80Gbps DNS amplification attack.



NTP contains a command called monlist (or sometimes MON_GETLIST) which can be sent to an NTP server for monitoring purposes. It returns the addresses of up to the last 600 machines that the NTP server has interacted with. This response is much bigger than the request sent making it ideal for an amplification attack.

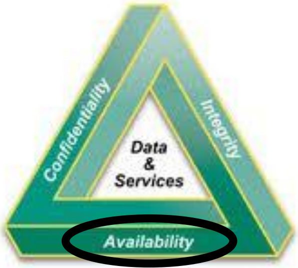
Abbreviation	Protocol	Ports	Amplification Factor	# Abusable Servers
CHARGEN	Character Generation Protocol	UDP / 19	~17.75x	Tens of thousands (~90K)
DNS	Domain Name System	UDP / 53	~160x	Millions (~30M)
NTP	Network Time Protocol	UDP / 123	~1000x	Over One Hundred Thousand (~128K)
SNMP	Simple Network Management Protocol	UDP / 161	~880x	Millions (~5M)

Ataque DDoS contra tablas de estado: atacan a los dispositivos de seguridad. Saturan las tablas de estado de los equipos Statefull.



Ataques Típicos: SYN Flood, RST Flood, FIN Flood, SockStress…

Los equipos de seguridad de perímetro se enfocan en la integridad y confidencialidad, pero no en la ***disponibilidad***



Information Security Triangle

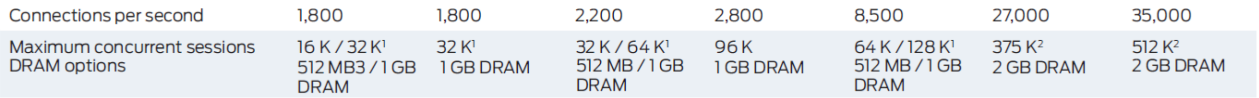
Firewall

Los **Firewalls** incluyendo los **WAFs** refuerzan la ***confidencialidad*** o que la informacion y funcionalidades puedan ser accesibles solo por quien esta autorizado

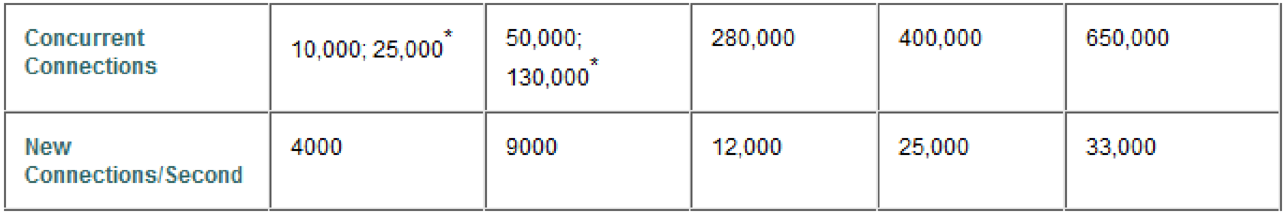
IPS

Los Intrusion Prevention Systems (IPS) ayudan a proteger la ***integridad***, o que la información pueda ser añadida, alterada o eliminada solo por las personas autorizadas

Todos los Firewalls, IPS, WAFS… son ***stateful*** y pueden sufrir ataques de DDoS contra sus tablas de estado

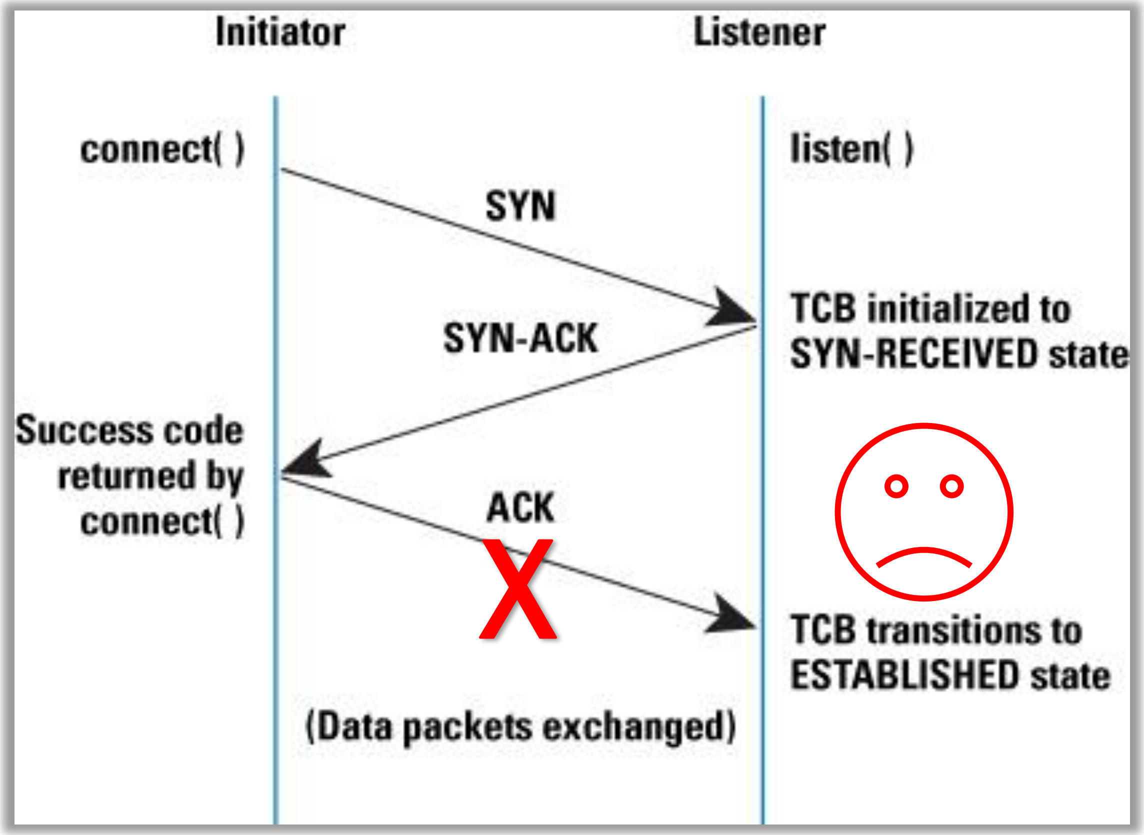


Connections per second	1,800	1,800	2,200	2,800	8,500	27,000	35,000
Maximum concurrent sessions DRAM options	16 K / 32 K[1] 512 MB3 / 1 GB DRAM	32 K[1] 1 GB DRAM	32 K / 64 K[1] 512 MB / 1 GB DRAM	96 K 1 GB DRAM	64 K / 128 K[1] 512 MB / 1 GB DRAM	375 K[2] 2 GB DRAM	512 K[2] 2 GB DRAM

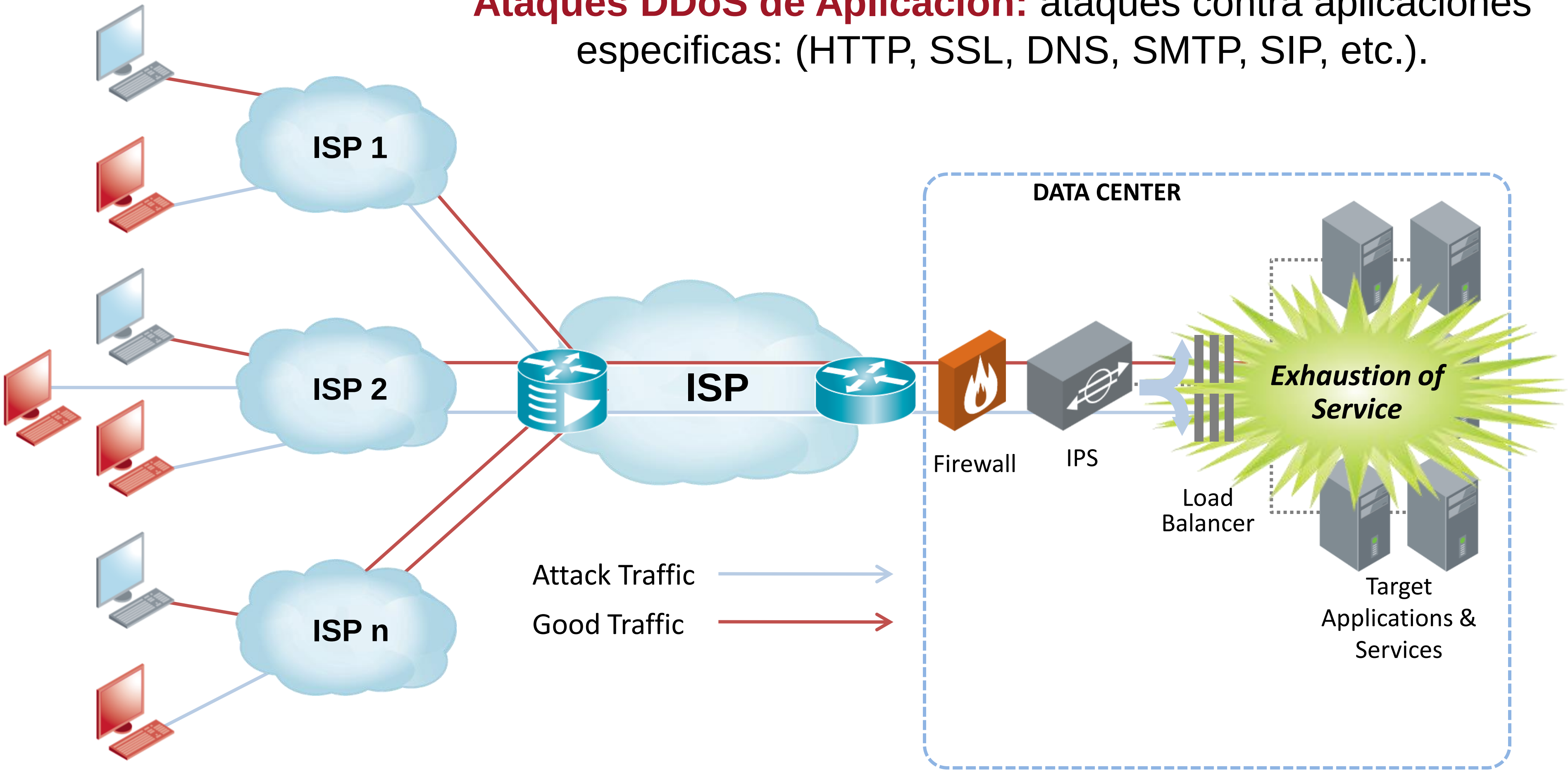


Concurrent Connections	10,000; 25,000*	50,000; 130,000*	280,000	400,000	650,000
New Connections/Second	4000	9000	12,000	25,000	33,000

TCP Stack Attack – Syn Attack



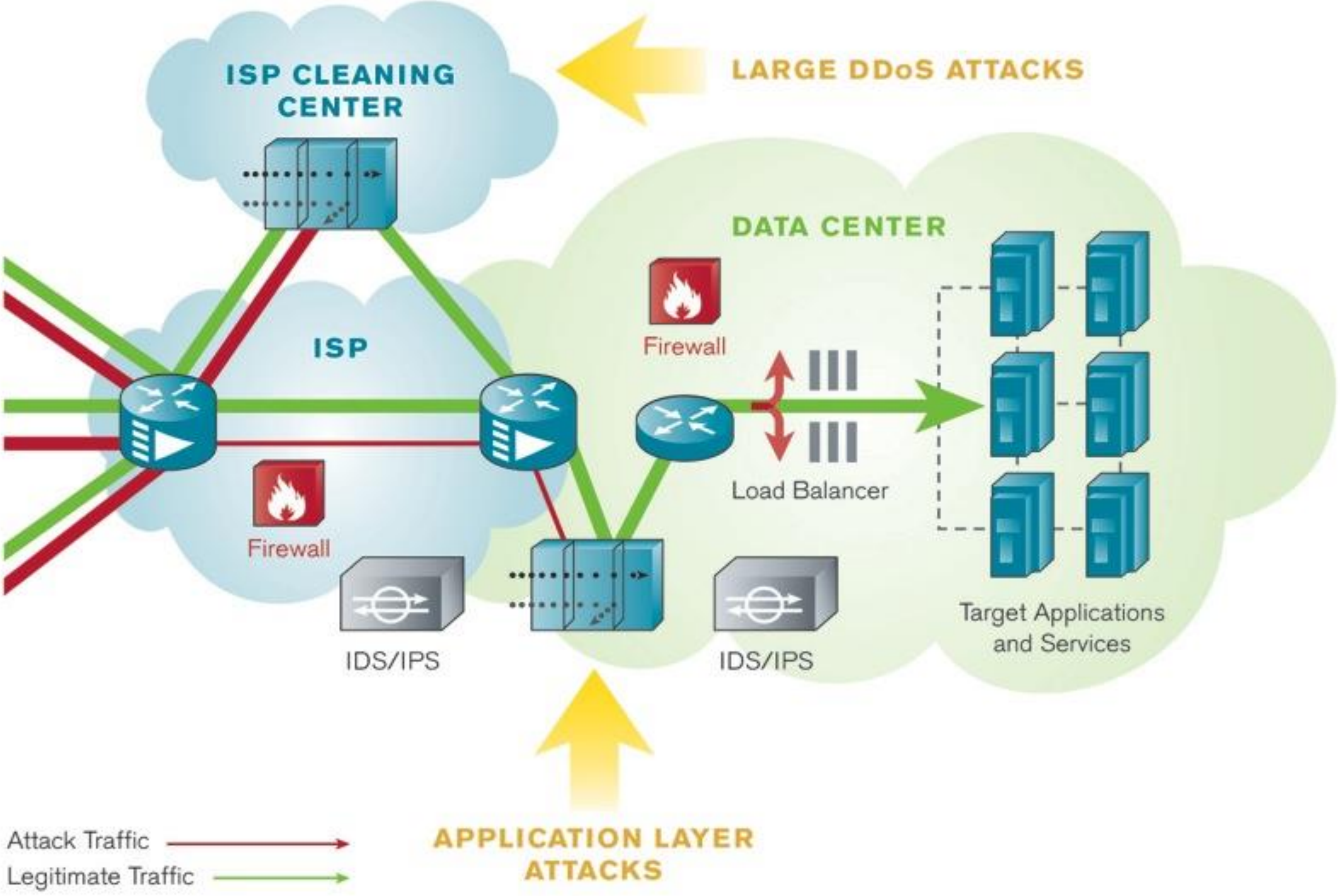
Ataques DDoS de Aplicación: ataques contra aplicaciones especificas: (HTTP, SSL, DNS, SMTP, SIP, etc.).



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

El servidor tiene que almacenar gran información en memoria para la reanudaciones… y muere

```
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        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        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,
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,
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,
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,
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,        -
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,        1,5-
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,        61,5-
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,        91,5-
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,        521,5-
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,  -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
```

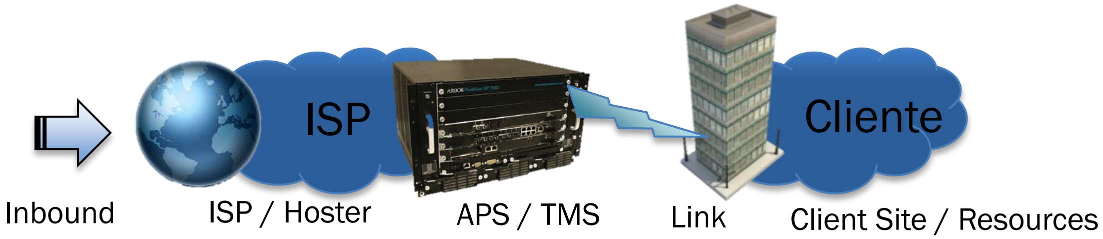


El DDoS es un problema que solo la red puede resolver

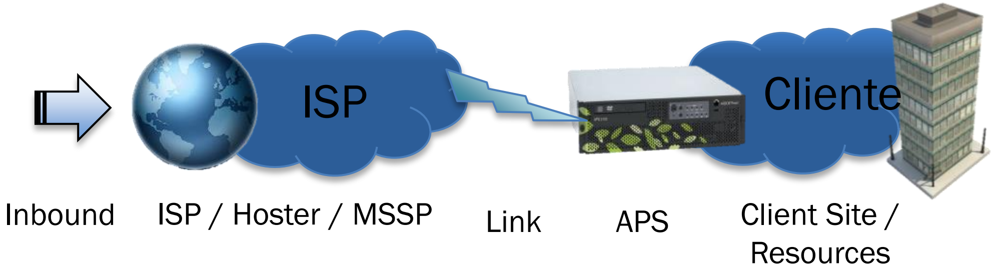
3

Modelos de defensa frente a DDoS

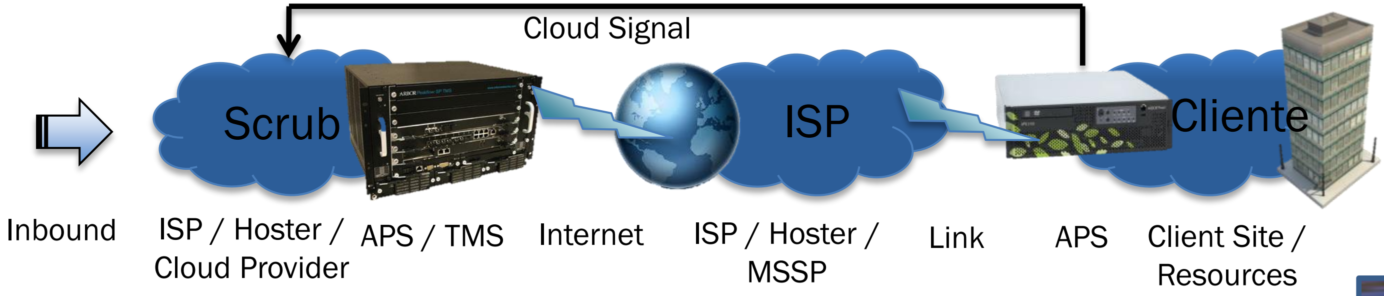
Servicios de Operador



Defensa basada en CPE



Servicios Híbridos



Tipo de Servicio: Operador

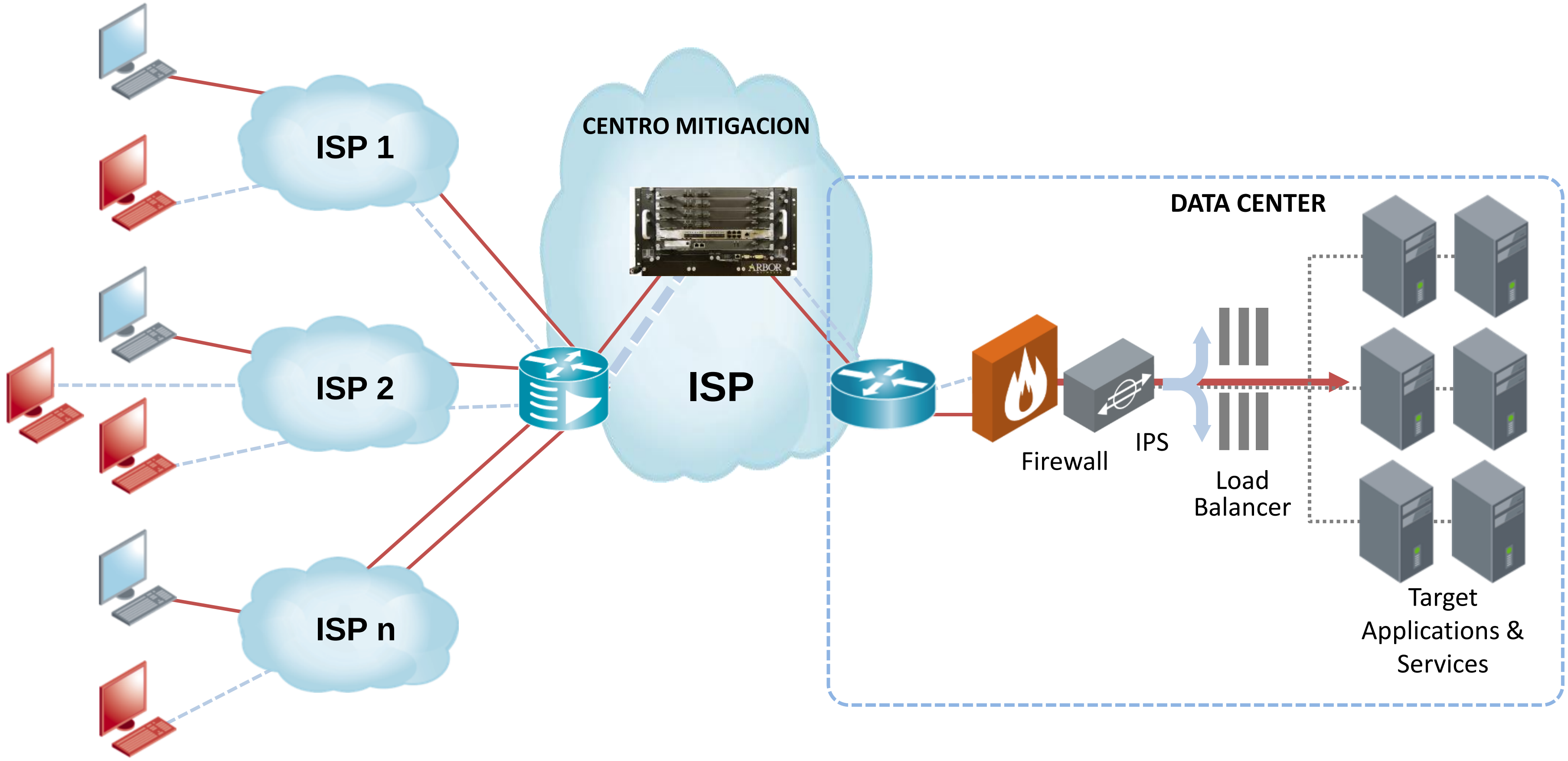
Descripción del Servicio: Son servicios de protección de DDoS prestados desde la red del operador. Estos servicios acostumbrar a proporcionarse junto a la conectividad a Internet, hosting, colocación, y servicios tipo cloud.

Ventajas del Servicio: El servicios se enfoca generalmente a los ataques volumétricos y ofrecen al cliente final un punto único confiable y responsable del acceso a Internet. El soporte se proporciona de un punto central único (el operador). Además, las soluciones de clean pipes ayudan a los clientes en la consolidación y simplificación de los servicios.

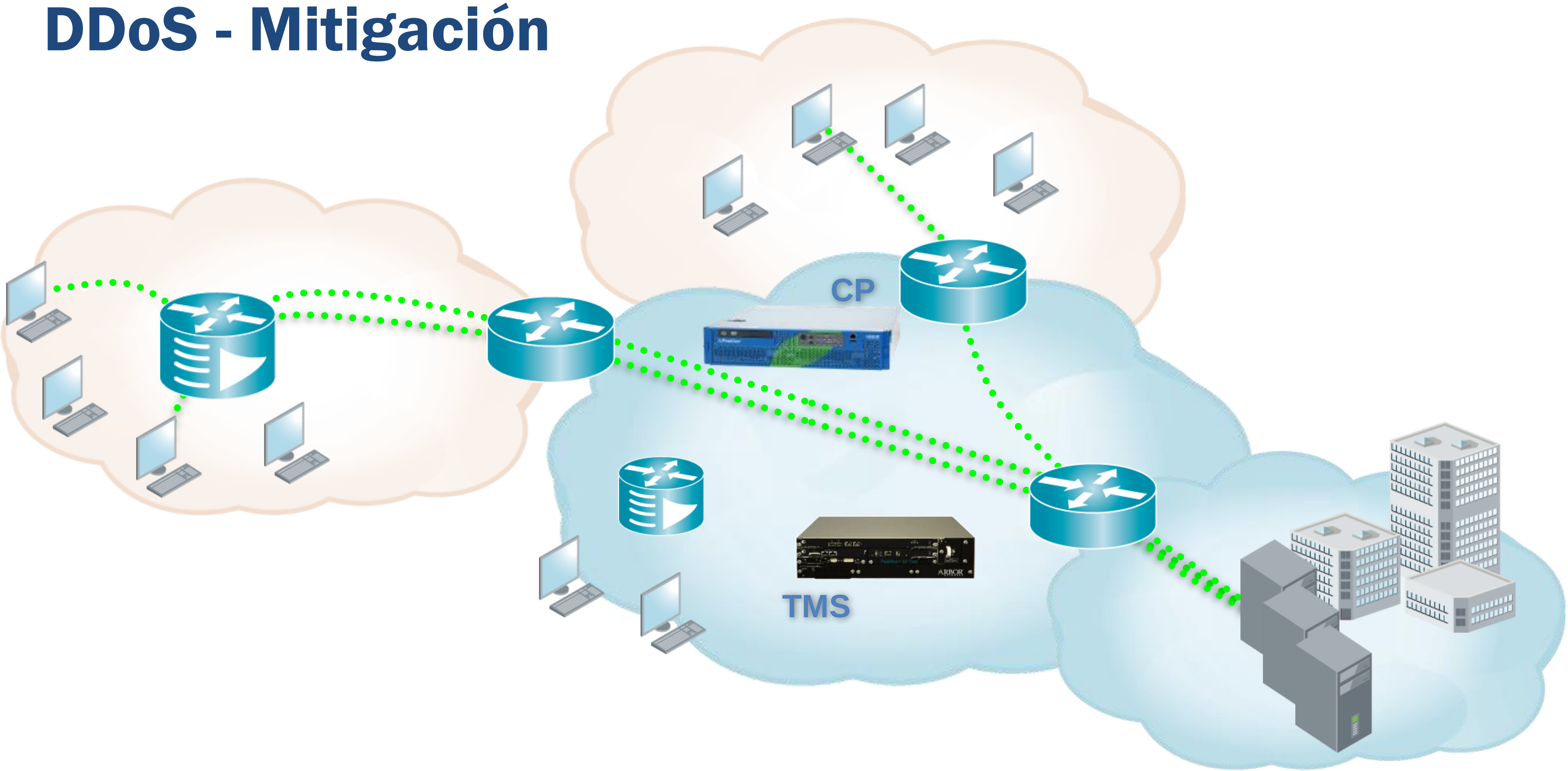
Desventajas del Servicio: Los servicios de operador enfatizan mucho la protección frente a ataques volumétricos en capa -3/4 pero no pueden afrontar la problemática de los ataques de nivel 7. Para muchas organizaciones esta protección puede ser suficiente, pero en la actualidad los ataques de aplicación están subiendo en popularidad y representan ya el 30%-40% del total de ataques de DDoS (fuente: grupo ASERT de Arbor).

Los servicios de operador tienen mucha dificultad en dar respuesta a los escenarios de clientes con varios proveedores de internet.

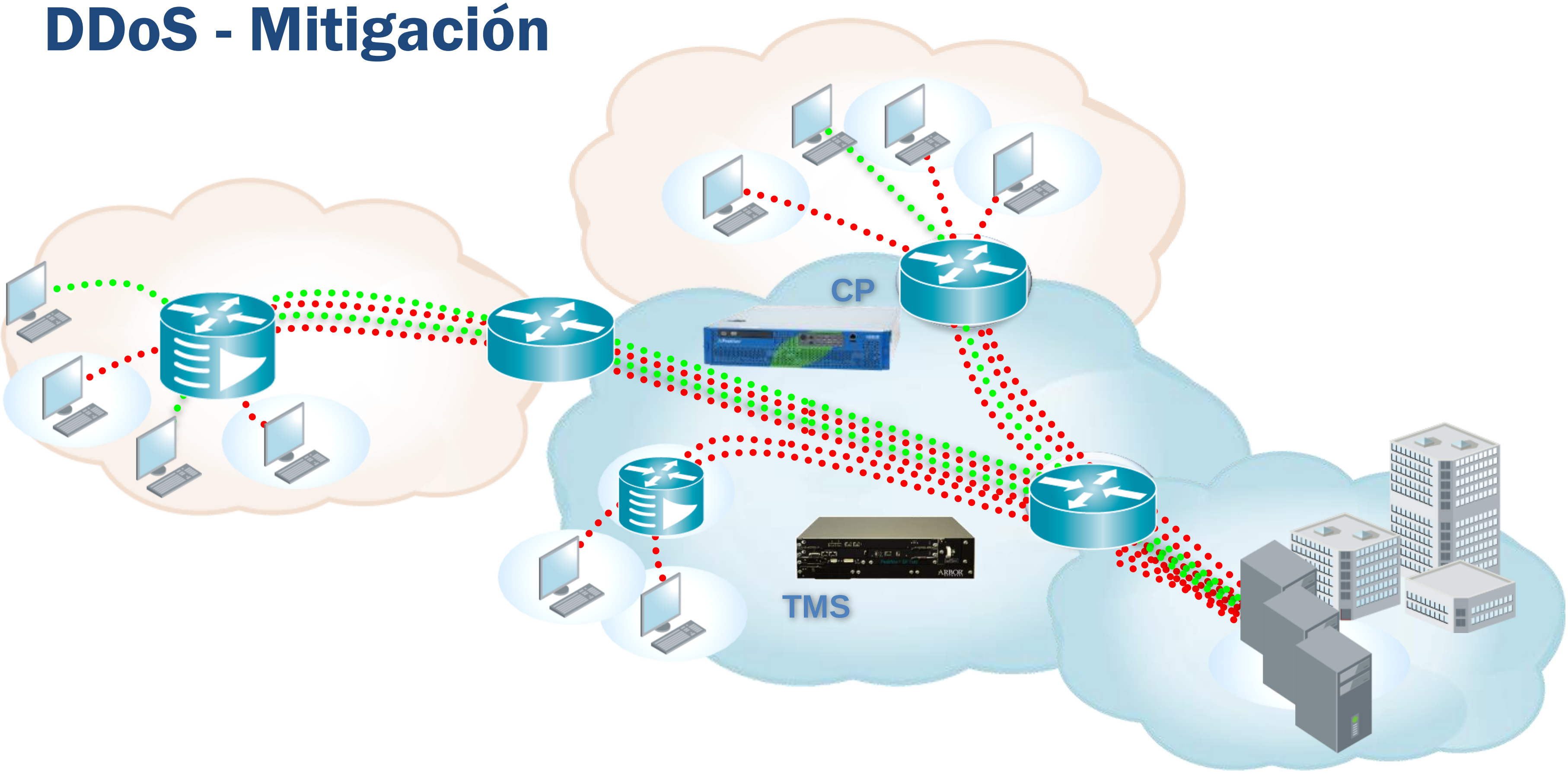
Servicio de Operador



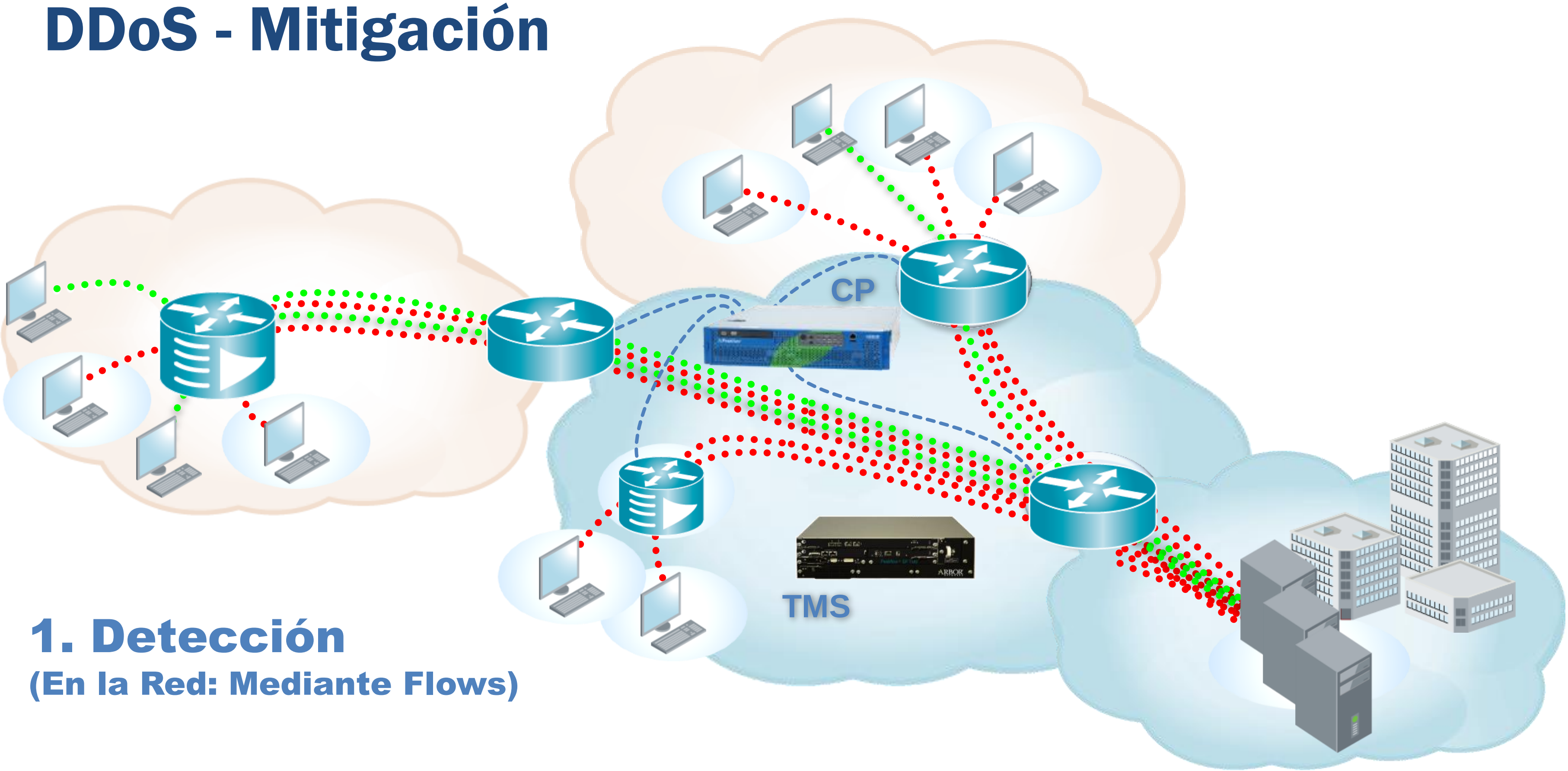
DDoS - Mitigación



DDoS - Mitigación



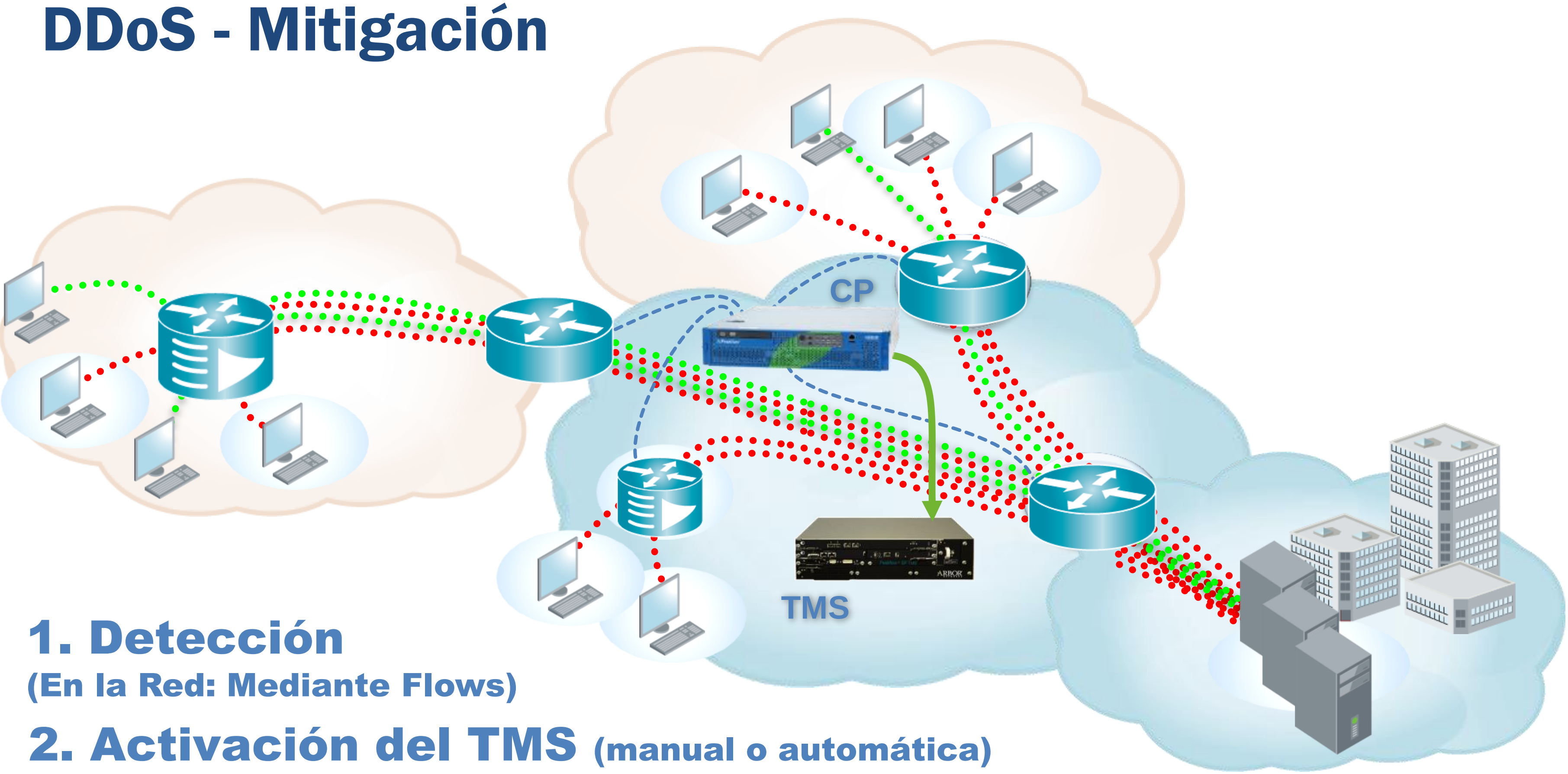
DDoS - Mitigación



1. Detección

(En la Red: Mediante Flows)

DDoS - Mitigación

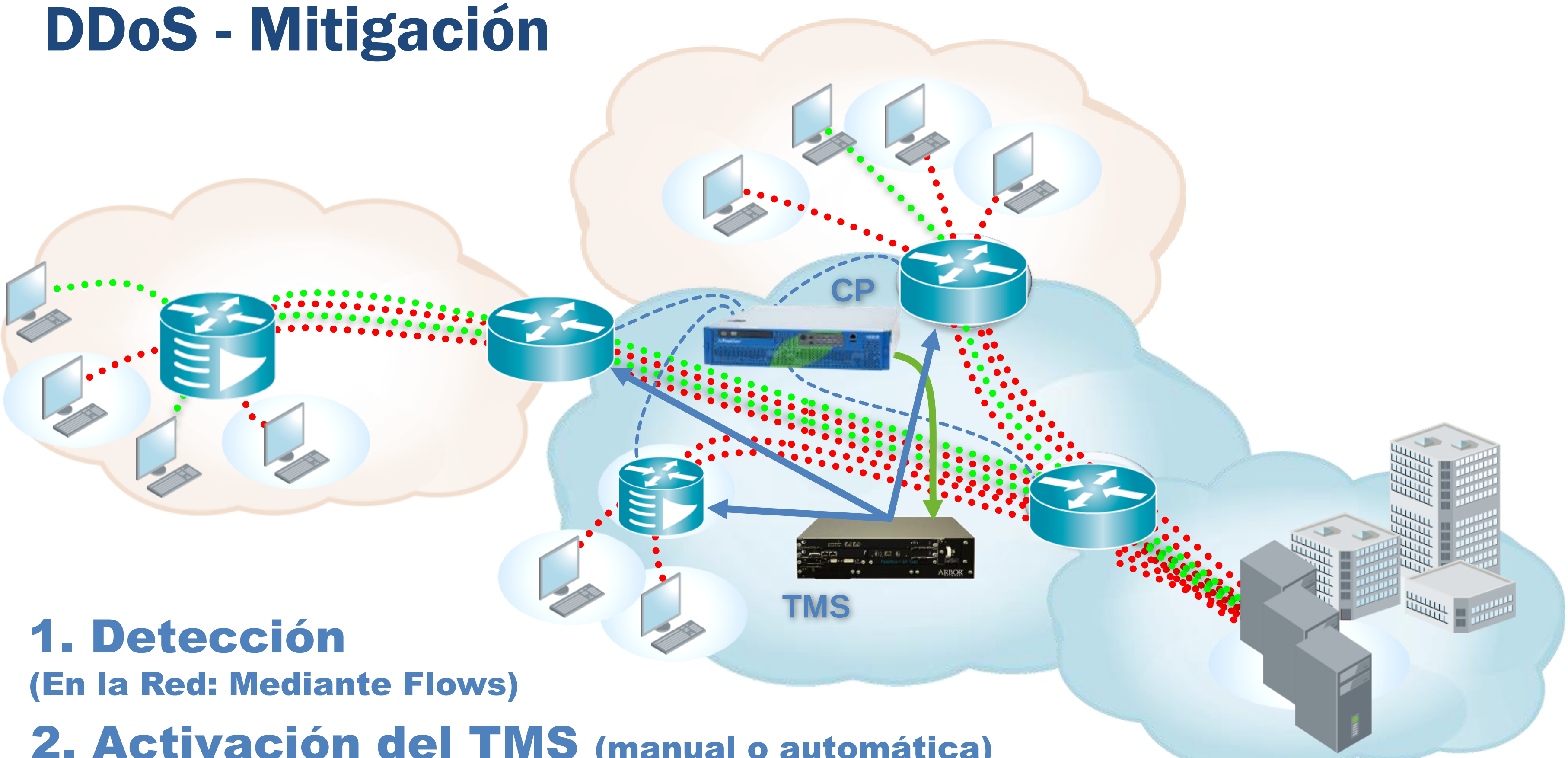


1. **Detección**

   (En la Red: Mediante Flows)

2. **Activación del TMS** (manual o automática)

DDoS - Mitigación

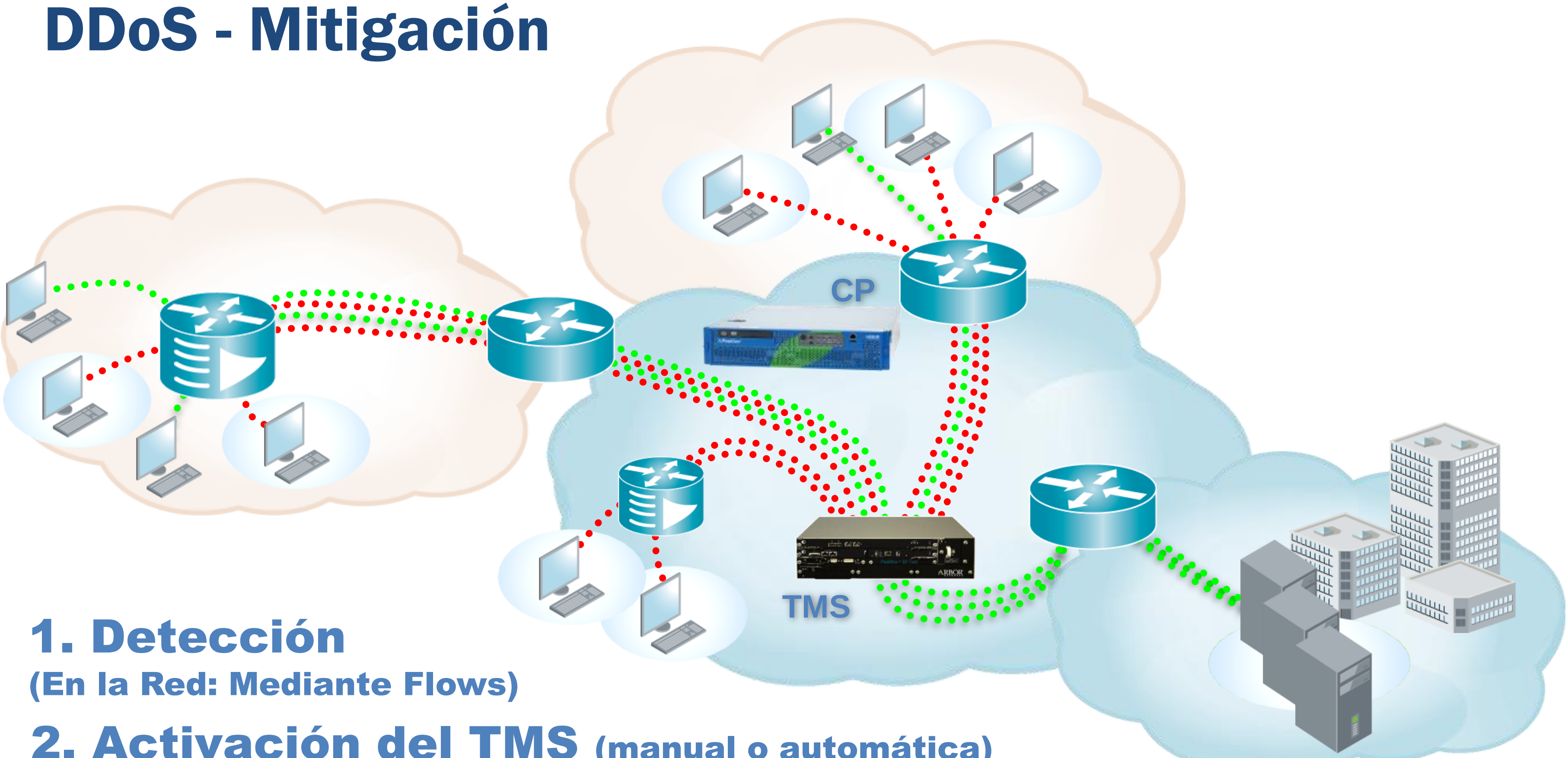


1. **Detección**
(En la Red: Mediante Flows)

2. **Activación del TMS** (manual o automática)

3. **Diversión del Trafico** (en la Red : anuncio BGP OFF-Ramp

DDoS - Mitigación



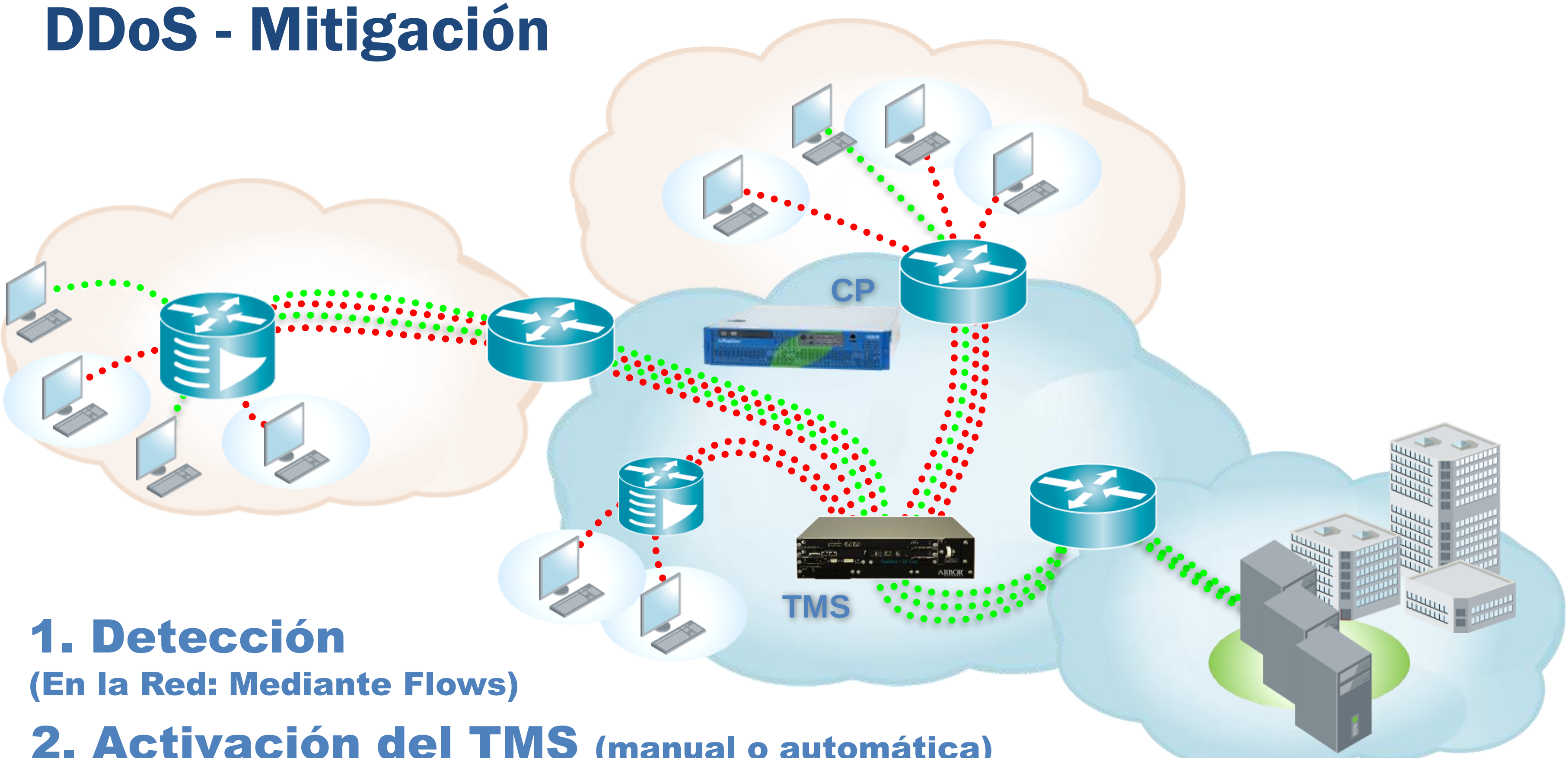
1. Detección
(En la Red: Mediante Flows)

2. Activación del TMS (manual o automática)

3. Diversión del Trafico (en la Red : anuncio BGP OFF-Ramp

4. Limpieza de trafico y reenvío del legitimo (en la red: usando técnicas ON-Ramp [MPLS, GRE, VLAN, …])

DDoS - Mitigación



1. Detección

(En la Red: Mediante Flows)

2. Activación del TMS (manual o automática)

3. Diversión del Trafico (en la Red : anuncio BGP OFF-Ramp

4. Limpieza de trafico y reenvío del legitimo (en la red: usando técnicas ON-Ramp [MPLS, GRE, VLAN, …])

5. Protection

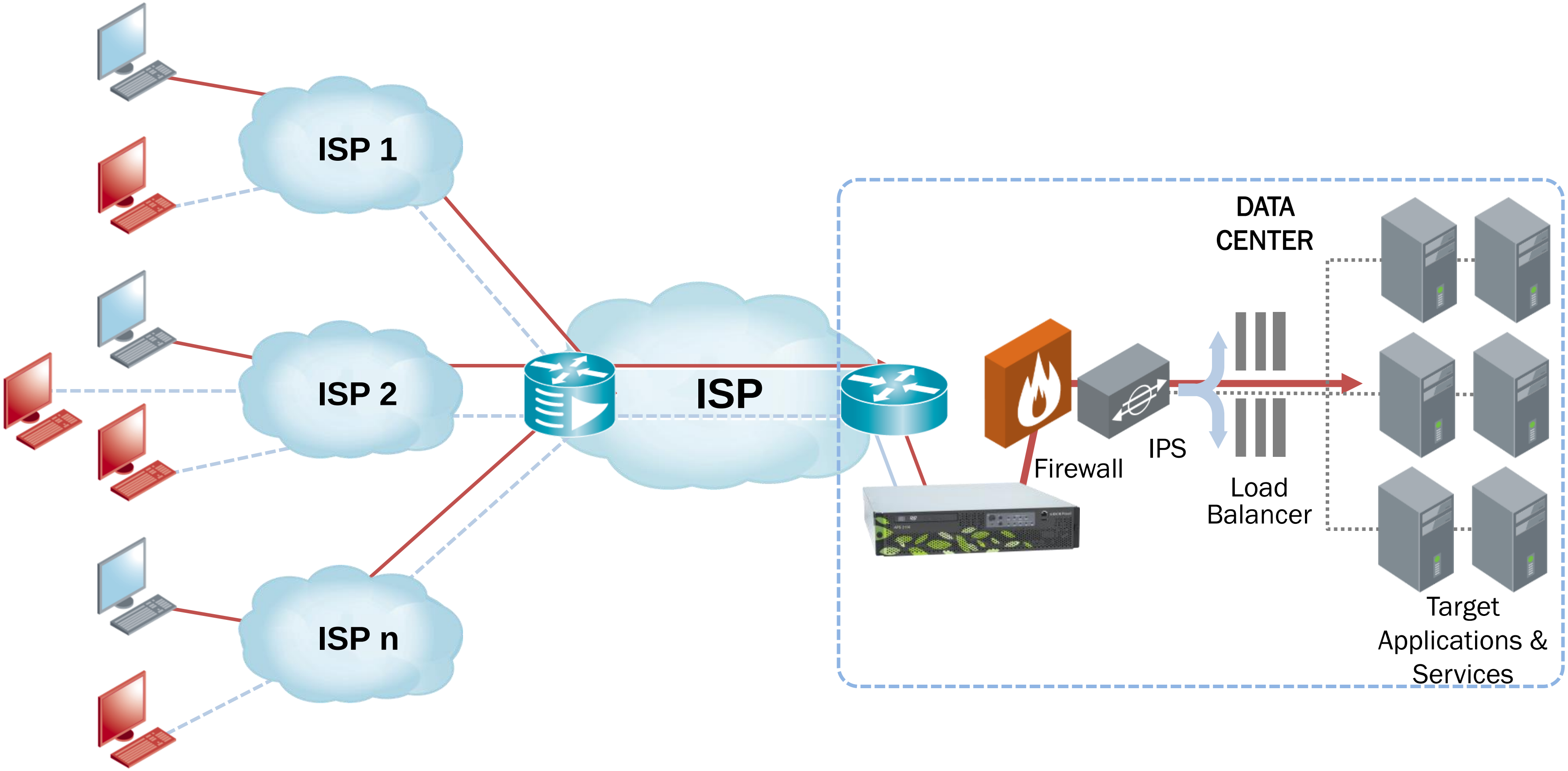
Tipo de Servicio: Basado en CPE

Descripción del Servicio: Las soluciones basadas en CPE como el Arbor Pravail APS son appliances que se instalan en el datacenter del cliente en linea en el borde de la red, justo en el punto de demarcación del cliente. Estos dispositivos están pensados para monitorizar en tiempo real el trafico y mitigar los ataques de DDoS tanto volumétricos como de aplicación.

Beneficios del servicio: Proporciona detección y mitigación activa, en línea y en tiempo real. El cliente tiene gran flexibilidad en la definición de políticas y la configuración del equipo. Permite activar las defensas hibridas que combinan soluciones tipo CPE con soluciones de Operador.

Desventajas del Servicio: La efectividad del servicio se limita a las capacidades de mitigación del equipo y al ancho de banda existente. Estas soluciones requieren de personal técnico capacitado para la operación del equipo y responsabilizarse de las mitigaciones. Estas soluciones suponen una inversión CAPEX por parte del cliente.

CPE


ISP 1
ISP 2
ISP n
ISP
DATA CENTER
Firewall
IPS
Load Balancer
Target Applications & Services

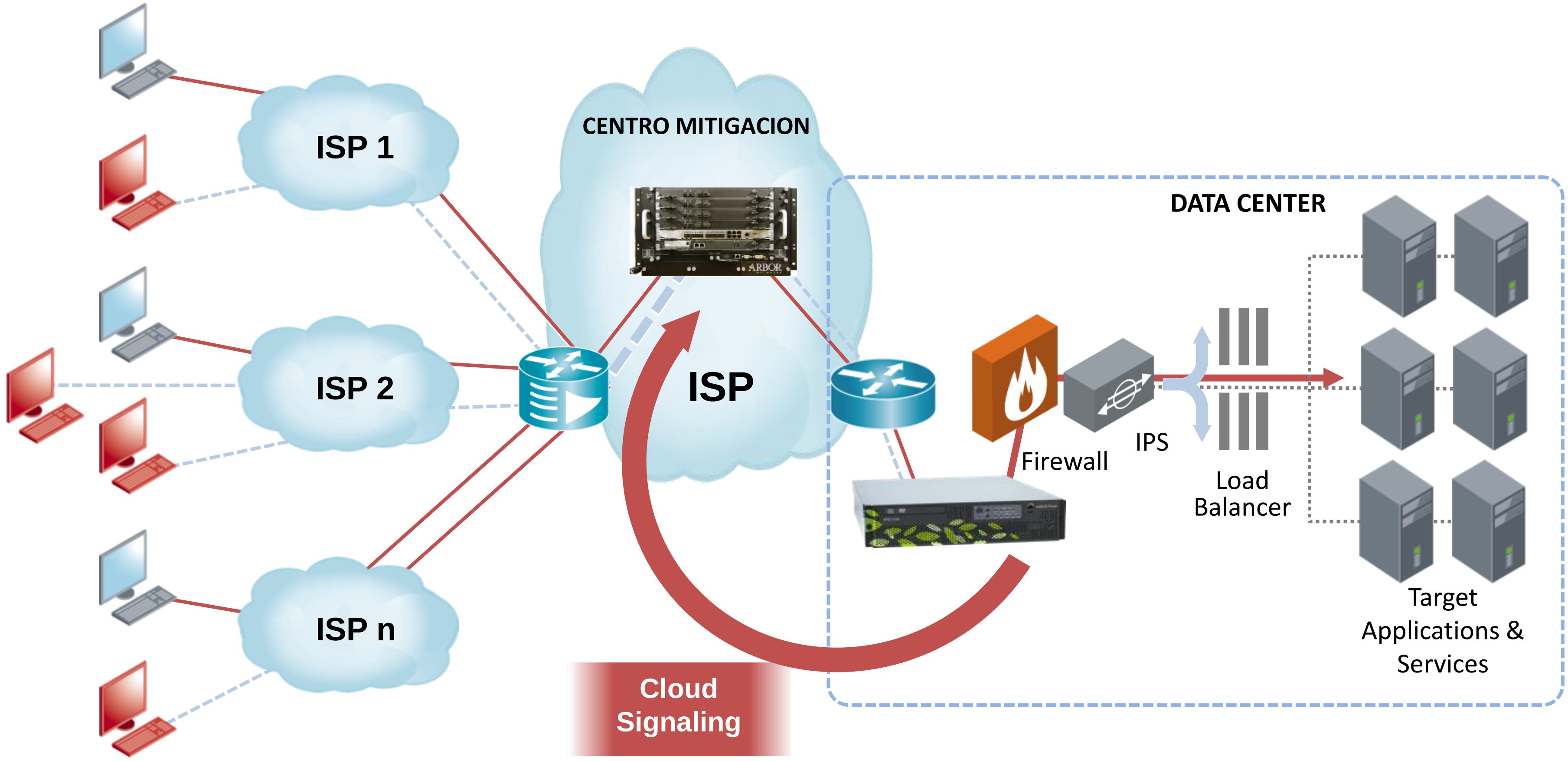
Tipo de Servicio: Hibrido

Descripción del Servicio: Combina la tecnología CPE con el servicio de operador.

Beneficios del Servicio: Protección superior. Detección y mitigación en tiempo de real de todo tipo de ataques

Del Servicio: Normalmente mas costoso.

Modelo de protección hibrido



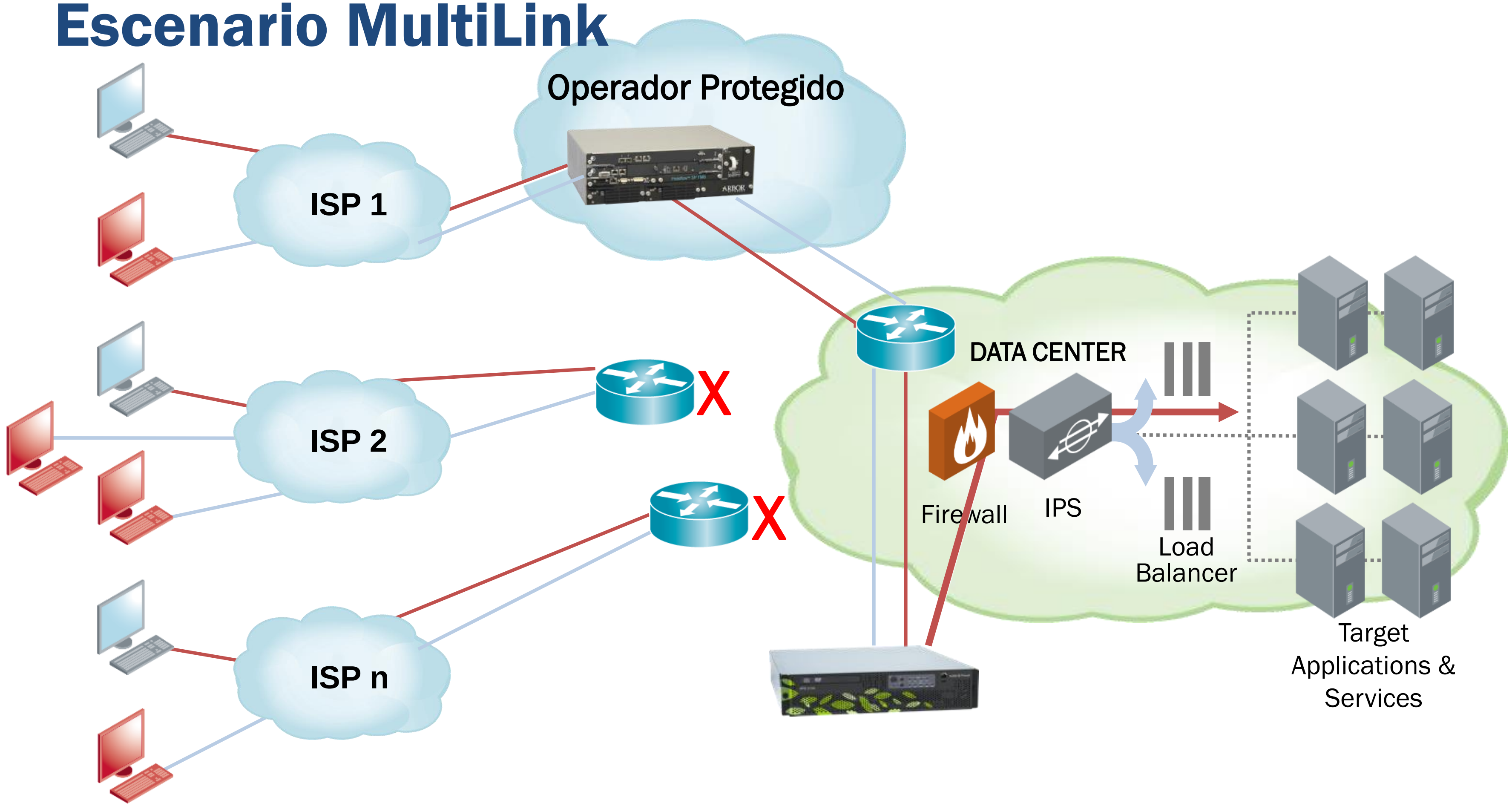
Tipo de Servicio: Protección para clientes Multilink

Descripción del Servicio: Combina la tecnología CPE con el servicio de operador para clientes con varios links de diferentes operadores. Hay que tener en cuenta si el cliente tiene o no su propio AS

Beneficios del Servicio: Mejor control de la inversión, ya que no hay que contratar el servicio de operador con todos ellos. Minimiza también los costes de operador, ya que el cliente puede mitigar los ataques hasta el ancho de banda disponible

Desventajas del Servicio: Supone un gasto tipo Capex inicial para el CPE. Requiere gestión local del CPE y operación para la desconexión delos links no protegidos cuando hay un ataque volumétrico que sature las líneas, así como la reconexión una vez se acabe el ataque

Escenario MultiLink



Mejor solución para escenarios Multi-Link

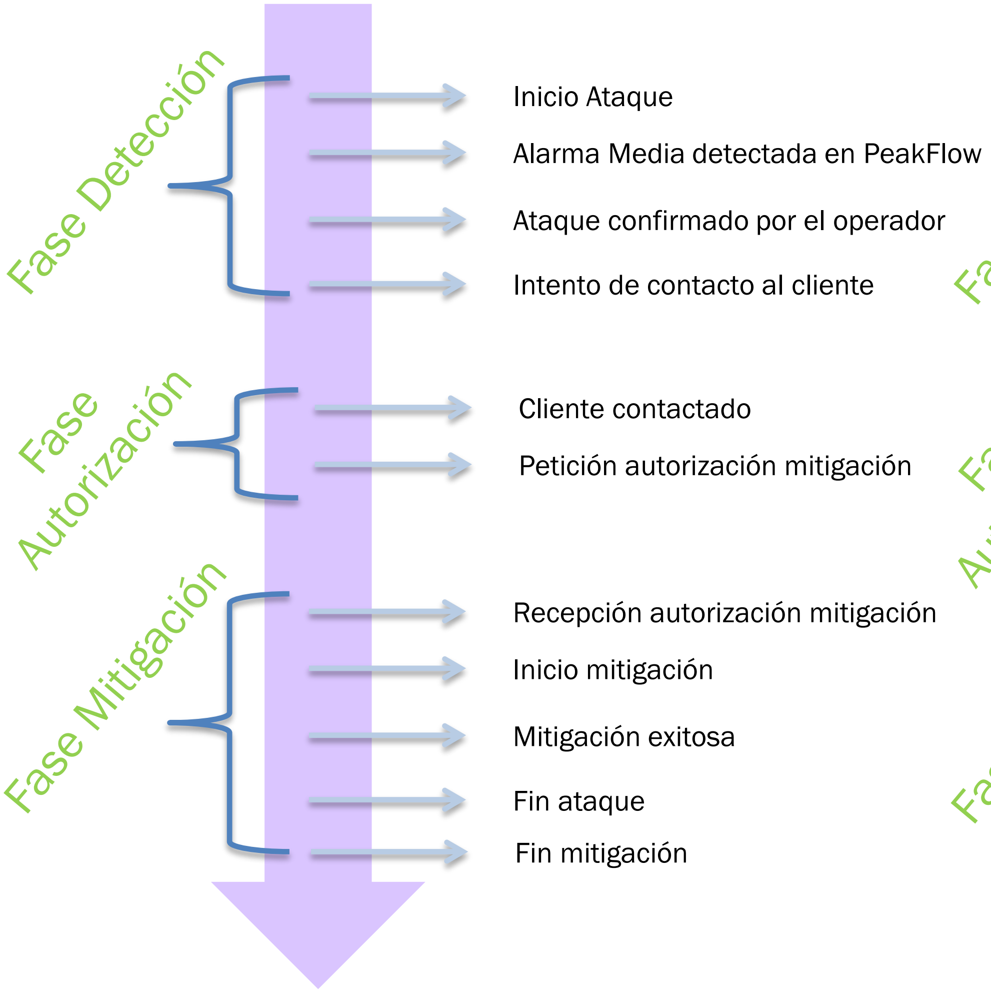
4

Comparación de modelos de Servicio

	Operador	Servicio Hibrido	CPE
Deteccion Proactiva L3	✓	✓	✓
Deteccion Proactiva L7	✗	✓	✓
Mitigacion L3	✓	✓	✓
Mitigacion L7	✓	✓	✓
Mitigacion Volumetrica	✓	✓	✗
Diversion Trafico	BGP	BGP	✗
Re-Inyeccion Trafico	VRF/GRE	VRF/GRE	✗
Tiempo Respuesta Deteccion	🐢	🐇	🐇
Tiempo Respuesta Mitigacion	🐢	🐇	🐇
Independiente ISP	✗	✓	✓

Ejemplos de WorkFlow

Detección Proactiva

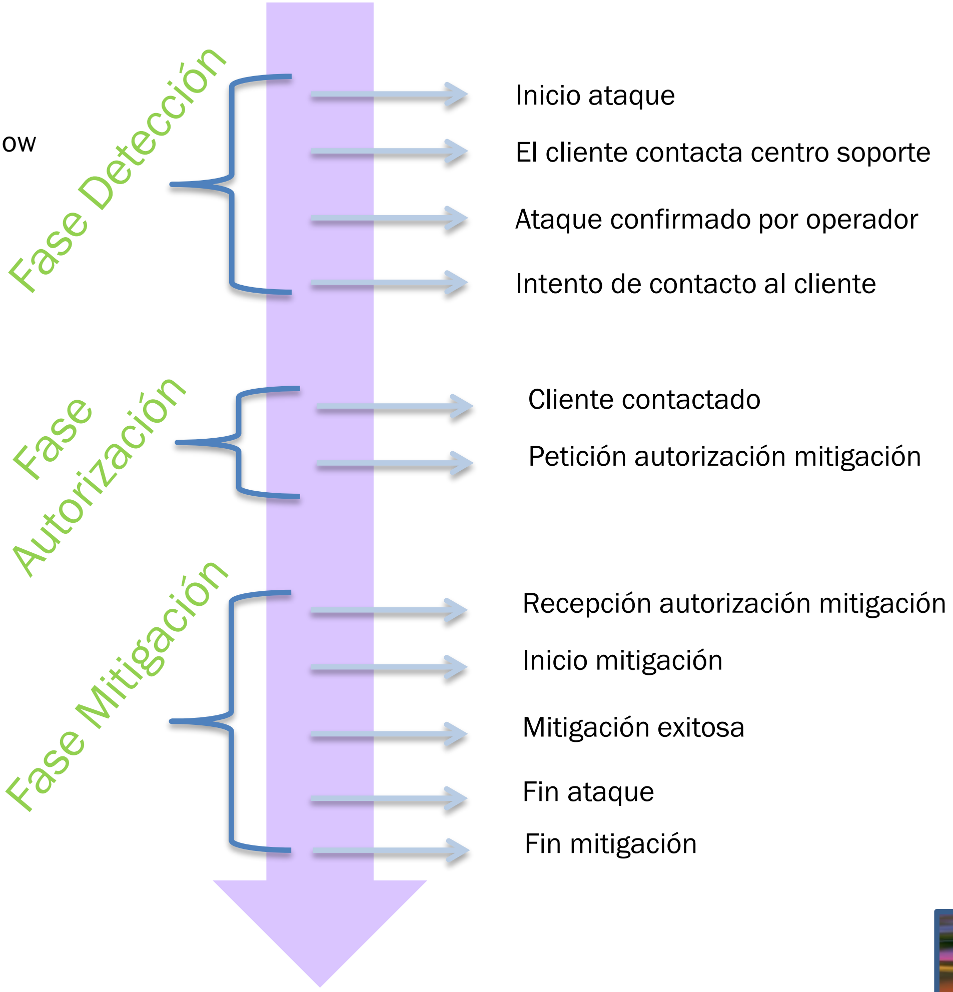


Fase Detección
- Inicio Ataque
- Alarma Media detectada en PeakFlow
- Ataque confirmado por el operador
- Intento de contacto al cliente

Fase Autorización
- Cliente contactado
- Petición autorización mitigación

Fase Mitigación
- Recepción autorización mitigación
- Inicio mitigación
- Mitigación exitosa
- Fin ataque
- Fin mitigación

Detección Reactiva



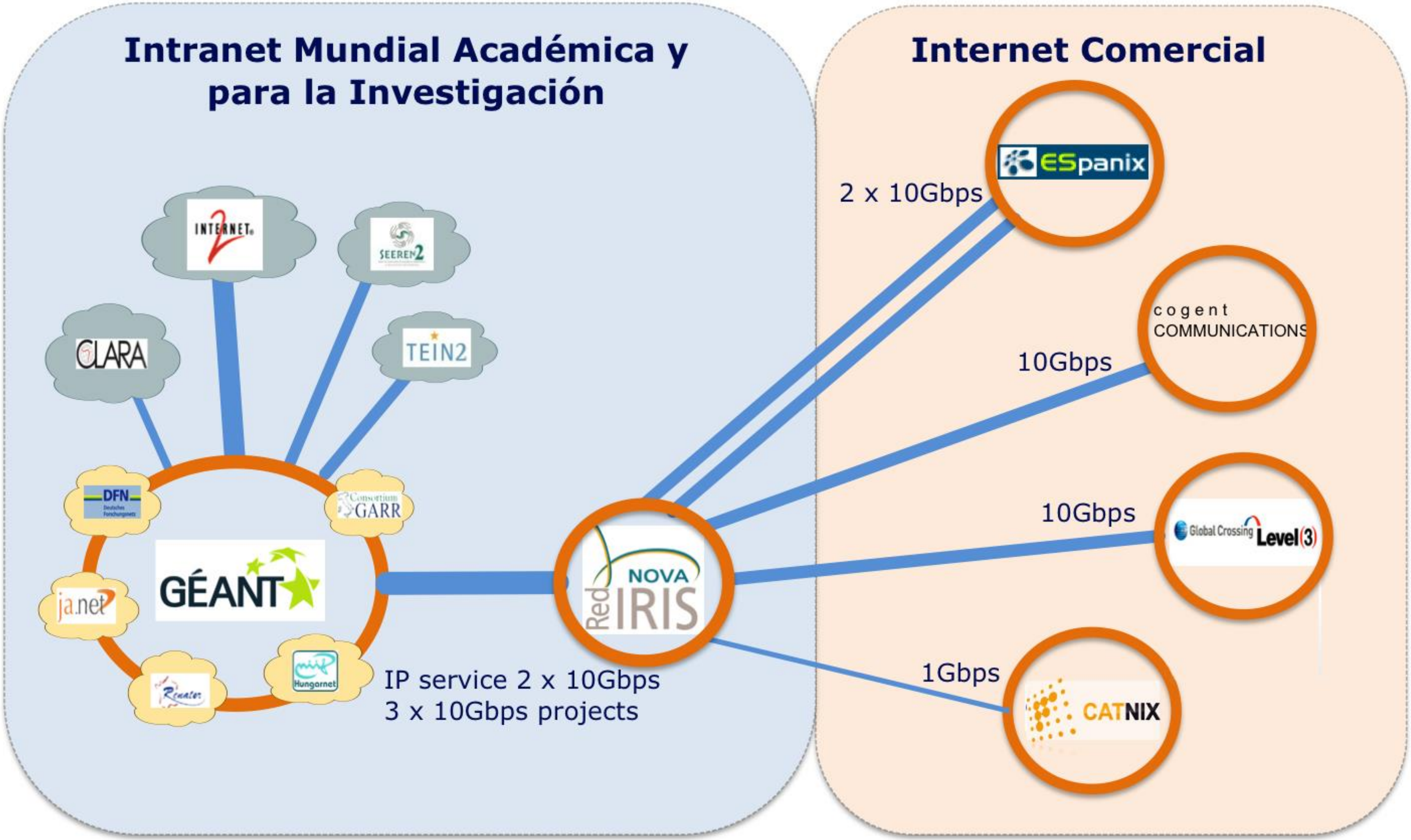
Fase Detección
- Inicio ataque
- El cliente contacta centro soporte
- Ataque confirmado por operador
- Intento de contacto al cliente

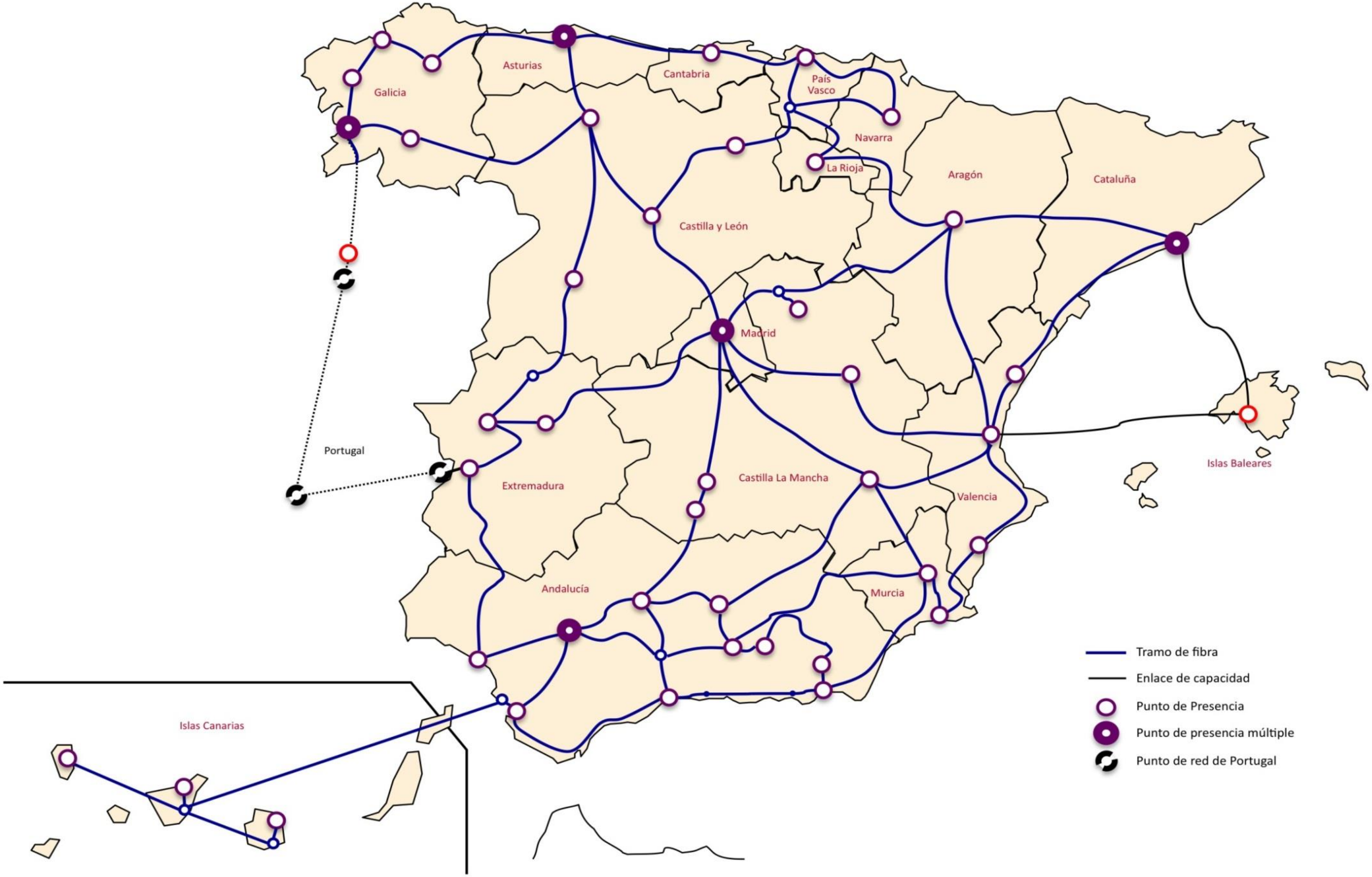
Fase Autorización
- Cliente contactado
- Petición autorización mitigación

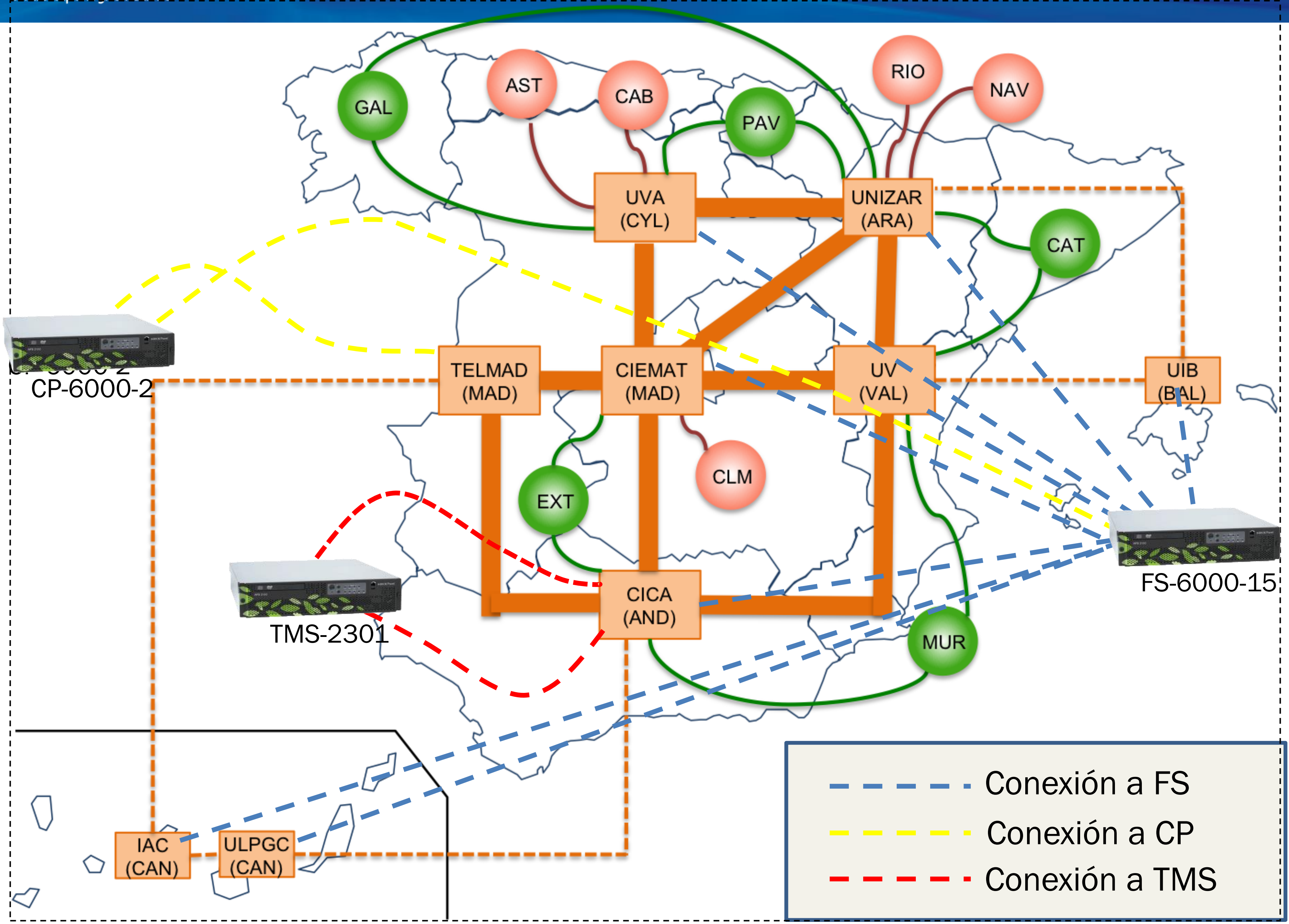
Fase Mitigación
- Recepción autorización mitigación
- Inicio mitigación
- Mitigación exitosa
- Fin ataque
- Fin mitigación

5

Servicio de Red Iris


Intranet Mundial Académica y para la Investigación
Internet Comercial
INTERNET2
SEEREN2
CLARA
TEIN2
DFN
Consortium GARR
GÉANT
ja.net
Renater
Hungarnet
IP service 2 x 10Gbps
3 x 10Gbps projects
NOVA RedIRIS
ESpanix
2 x 10Gbps
cogent COMMUNICATIONS
10Gbps
Global Crossing Level(3)
10Gbps
1Gbps
CATNIX


Asturias
Cantabria
País Vasco
Galicia
Navarra
La Rioja
Aragón
Cataluña
Castilla y León
Madrid
Portugal
Islas Baleares
Castilla La Mancha
Valencia
Extremadura
Andalucía
Murcia
Islas Canarias
Tramo de fibra
Enlace de capacidad
Punto de Presencia
Punto de presencia múltiple
Punto de red de Portugal



- - - - - Conexión a FS

- - - - - Conexión a CP

- - - - - Conexión a TMS

Blu ray Disc
MATTHEW BRODERICK
DABNEY COLEMAN
JOHN WOOD
ALLY SHEEDY
WARGAMES
MGM
Is it a game, or is it real?

Conexionado del Servicio – Detalles

Router de Interconexión conectado al CP-6000-2:

- CIEMAT (Madrid)

Routes de Distribución conectados al FS-6000-15:

- TELMAD (Madrid)
- UVA (Noroeste)
- UNIZAR (Noreste)
- UIB (Baleares)
- UV (Valencia)
- CICA (Andalucia)
- IAC (Canarias)
- ULPGC (Canarias)

TMS Conectado a CICA en Andalucía off-ramp/on-ramp.

- **E-Mails**
  - ccn-cert@cni.es
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - sondas@ccn-cert.cni.es
  - redsara@ccn-cert.cni.es
  - carmen@ccn-cert.cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es

ccn-cert
centro criptológico nacional

Síguenos en Linked in