河北联通金石机房
DDOS 防护报表

报表周期：2014 年 5 月 20 日~2014 年 5 月 20 日

制表日期：2014 年 5 月 20 日

DDOS 报告目录

1 基本信息

订单编号：201405200001JYYL

防护时间：05/20/2014

清洗带宽：1 Gbps

应用防护服务的 IP 地址列表（1 个）:

- 110.249.213.30

2 DDOS 防护简报

5 月 20 日，共遭受的 DDOS 攻击总量为 75 次。

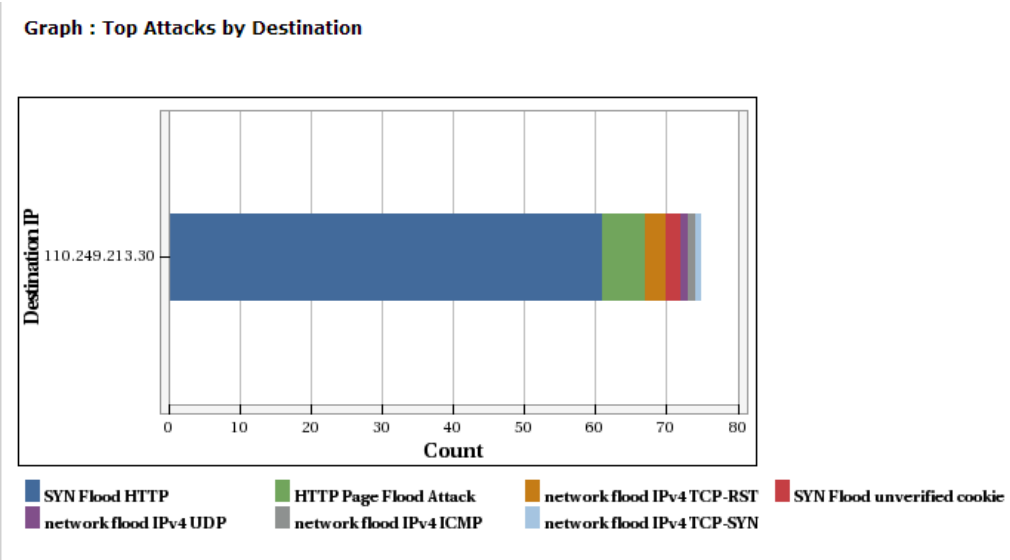
在受防护的 IP 地址中，以 110.249.213.30 所遭受的攻击比较多。

从遭受的攻击种类看，绝大多数是 SYN Flood HTTP，HTTP page Flood Attack。

3 DDOS 防护报告详情

3.1 受攻击 IP 地址报告

DDOS 攻击 IP 地址分布如下：



DDOS 攻击 IP 详细列表如下：

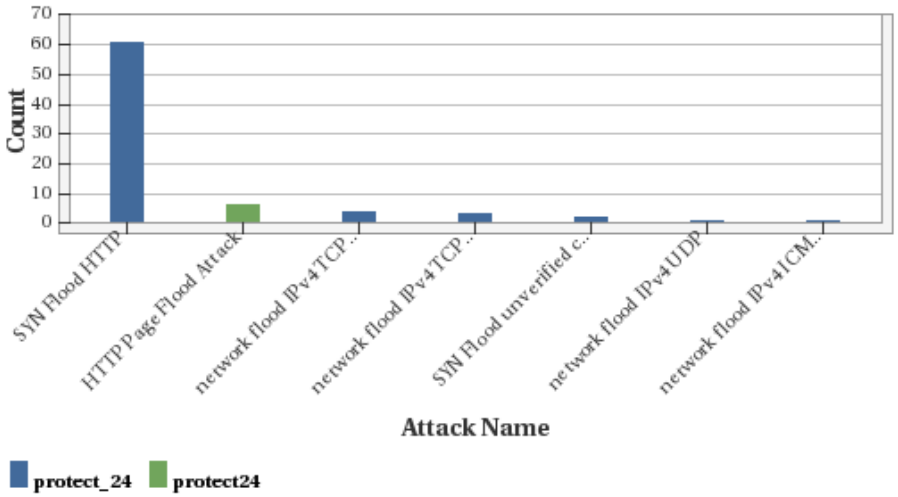
Table : Top Attacks by Destination

Destination IP	Attack Name	Rule Name	VLAN Tag	Count	%Count
110.249.213.30	SYN Flood HTTP	protect_24	Multiple	61	81.33%
110.249.213.30	HTTP Page Flood Attack	protect24	N/A	6	8.00%
110.249.213.30	network flood IPv4 TCP-RST	protect_24	N/A	3	4.00%
110.249.213.30	SYN Flood unverified cookie	protect_24	Multiple	2	2.67%
110.249.213.30	network flood IPv4 UDP	protect_24	N/A	1	1.33%
110.249.213.30	network flood IPv4 ICMP	protect_24	N/A	1	1.33%
110.249.213.30	network flood IPv4 TCP-SYN	protect_24	N/A	1	1.33%
Total				**75**	**100.00%**

3.2 受攻击 DDOS 类型报告

DDOS 攻击类型分布如下：

Graph : Top Attacks



DDOS 攻击类型详情如下：

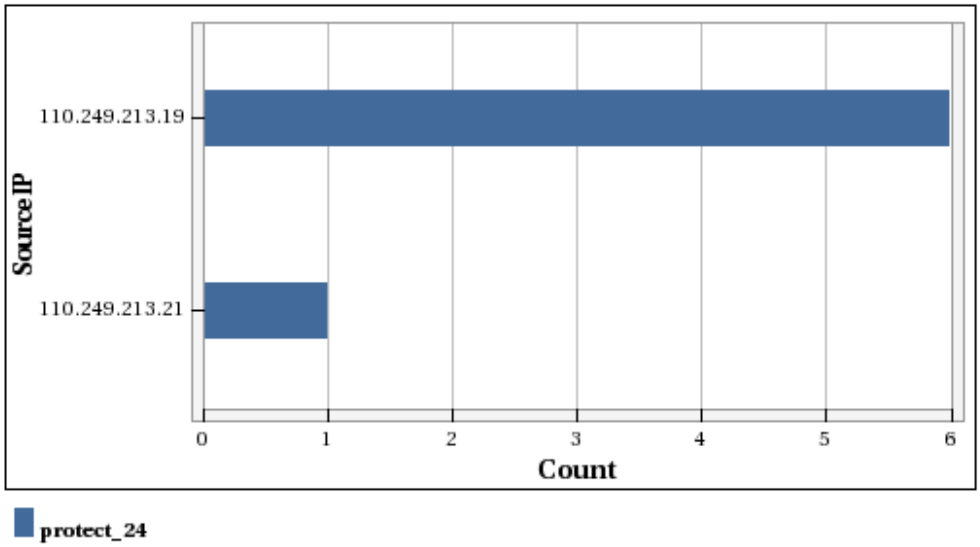
Table : Top Attacks

Attack Name	Rule Name	VLAN Tag	Count	%Count
SYN Flood HTTP	protect_24	Multiple	61	78.21%
HTTP Page Flood Attack	protect24	N/A	6	7.69%
network flood IPv4 TCP-RST	protect_24	N/A	4	5.13%
network flood IPv4 TCP-SYN	protect_24	N/A	3	3.85%
SYN Flood unverified cookie	protect_24	Multiple	2	2.56%
network flood IPv4 UDP	protect_24	N/A	1	1.28%
network flood IPv4 ICMP	protect_24	N/A	1	1.28%
Total			**78**	**100.00%**

3.3 攻击源报告

DDOS 攻击源地址分布如下：

Graph : Top Attack Sources



DDOS 攻击源地址详情如下：

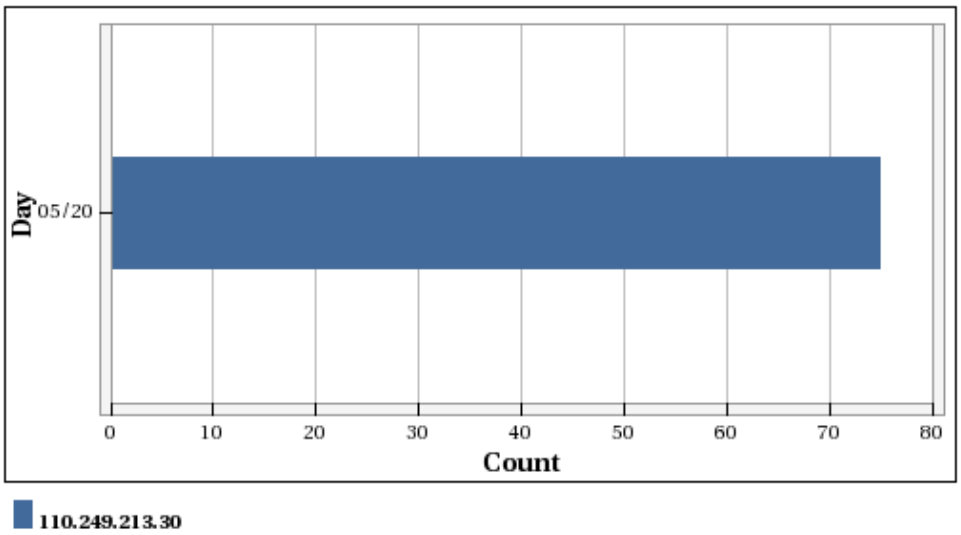
Table : Top Attack Sources

Source IP	Rule Name	VLAN Tag	Country	Count	%Count
110.249.213.19	protect_24	N/A	CN	6	85.71%
110.249.213.21	protect_24	Multiple	CN	1	14.29%
Total				**7**	**100.00%**

3.4 攻击日期分布报告

DDOS 攻击日期分布如下：

Graph : Top Attacks per Hour and Day



DDOS 攻击时间详情如下(UTC 时间)：

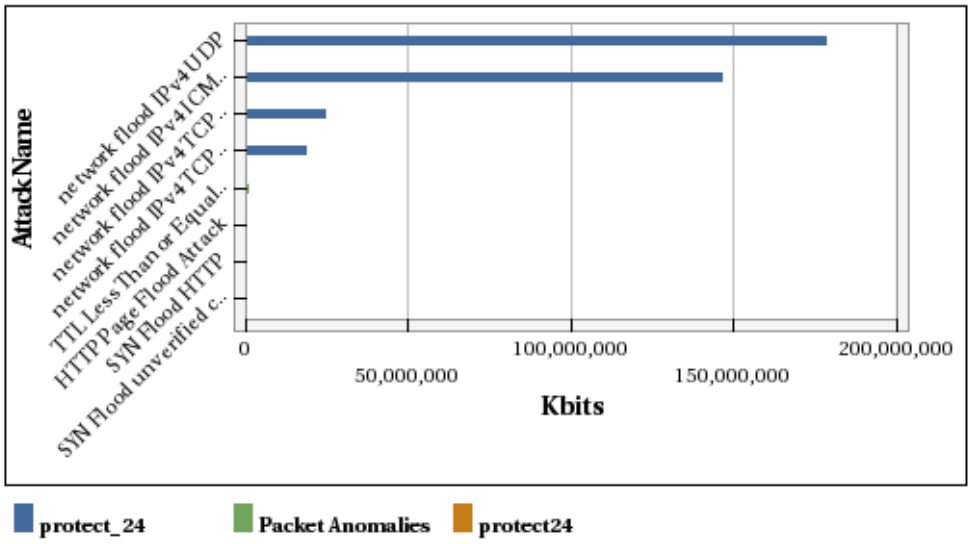
Table : Top Attacks per Hour and Day

Day	Hour	Attack Name	Rule Name	VLAN Tag	Count	%Count
05/20/2014	2:00	network flood IPv4 TCP-RST	protect_24	N/A	4	1.56%
05/20/2014	2:00	network flood IPv4 TCP-SYN	protect_24	N/A	2	0.78%
05/20/2014	2:00	network flood IPv4 UDP	protect_24	N/A	1	0.39%
05/20/2014	2:00	HTTP Page Flood Attack	protect24	N/A	1	0.39%
05/20/2014	2:00	network flood IPv4 ICMP	protect_24	N/A	1	0.39%
05/20/2014	3:00	SYN Flood HTTP	protect_24	Multiple	56	21.88%
05/20/2014	3:00	HTTP Page Flood Attack	protect24	N/A	4	1.56%
05/20/2014	3:00	network flood IPv4 TCP-SYN	protect_24	N/A	1	0.39%
05/20/2014	4:00	SYN Flood HTTP	protect_24	Multiple	5	1.95%
05/20/2014	4:00	HTTP Page Flood Attack	protect24	N/A	1	0.39%
05/20/2014	5:00	SYN Flood unverified cookie	protect_24	Multiple	2	0.78%
05/20/2014	18:00	TTL Less Than or Equal to 1	Packet Anomalies	N/A	178	69.53%
Total					**256**	**100.00%**

3.5 攻击流量分布报告

DDOS 攻击流量分布如下：

Graph : Top Attacks by Bandwidth



DDOS 攻击流量分布如下：

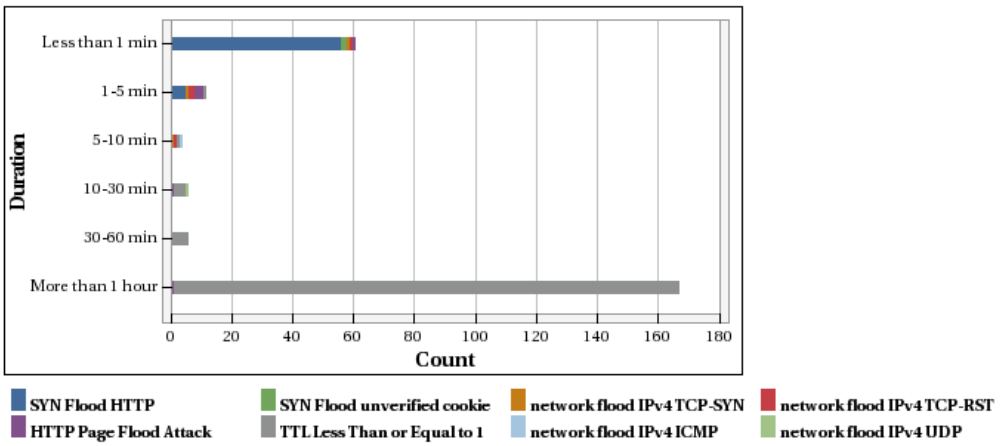
Table : Top Attacks by Bandwidth

Attack Name	Rule Name	VLAN Tag	Packets	%Packets	Kbits	%Kbits
network flood IPv4 UDP	protect_24	N/A	41,082,028	24.73%	179,081,728	48.13%
network flood IPv4 ICMP	protect_24	N/A	33,799,211	20.35%	147,335,312	39.60%
network flood IPv4 TCP-RST	protect_24	N/A	50,566,468	30.44%	25,210,796	6.78%
network flood IPv4 TCP-SYN	protect_24	N/A	38,198,739	23.00%	19,073,310	5.13%
TTL Less Than or Equal to 1	Packet Anomalies	N/A	2,415,554	1.45%	1,366,870	0.37%
HTTP Page Flood Attack	protect24	N/A	35,954	0.02%	32,240	0.01%
SYN Flood HTTP	protect_24	Multiple	9,216	0.01%	4,268	0.00%
SYN Flood unverified cookie	protect_24	Multiple	30	0.00%	8	0.00%
Total			**166,107,200**	**100.00%**	**372,104,480**	**100.00%**

3.6 攻击持续时长报告

DDOS 攻击流量分布如下：

Graph : Top Attacks by Duration



DDOS 攻击流量详情如下：

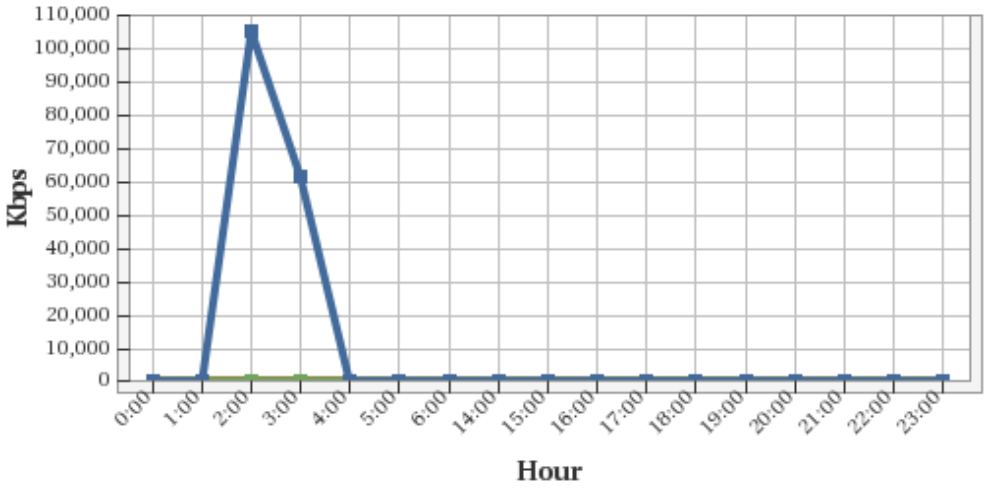
Table : Top Attacks by Duration

Duration	Attack Name	Rule Name	VLAN Tag	Count	%Count
Less than 1 min	SYN Flood HTTP	protect_24	Multiple	56	21.88%
Less than 1 min	SYN Flood unverified cookie	protect_24	Multiple	2	0.78%
Less than 1 min	network flood IPv4 TCP-SYN	protect_24	N/A	1	0.39%
Less than 1 min	network flood IPv4 TCP-RST	protect_24	N/A	1	0.39%
Less than 1 min	HTTP Page Flood Attack	protect24	N/A	1	0.39%
1-5 min	SYN Flood HTTP	protect_24	Multiple	5	1.95%
1-5 min	HTTP Page Flood Attack	protect24	N/A	3	1.17%
1-5 min	network flood IPv4 TCP-RST	protect_24	N/A	2	0.78%
1-5 min	network flood IPv4 TCP-SYN	protect_24	N/A	1	0.39%
1-5 min	TTL Less Than or Equal to 1	Packet Anomalies	N/A	1	0.39%
5-10 min	TTL Less Than or Equal to 1	Packet Anomalies	N/A	1	0.39%
5-10 min	network flood IPv4 TCP-SYN	protect_24	N/A	1	0.39%
5-10 min	network flood IPv4 TCP-RST	protect_24	N/A	1	0.39%
5-10 min	network flood IPv4 ICMP	protect_24	N/A	1	0.39%
10-30 min	TTL Less Than or Equal to 1	Packet Anomalies	N/A	4	1.56%
10-30 min	network flood IPv4 UDP	protect_24	N/A	1	0.39%
10-30 min	HTTP Page Flood Attack	protect24	N/A	1	0.39%
30-60 min	TTL Less Than or Equal to 1	Packet Anomalies	N/A	6	2.34%
More than 1 hour	TTL Less Than or Equal to 1	Packet Anomalies	N/A	166	64.84%
More than 1 hour	HTTP Page Flood Attack	protect24	N/A	1	0.39%
Total				**256**	**100.00%**

3.7 DDOS 流量统计报告

DDOS 流量统计如下：

Graph : Bandwidth by Hour of Day(Kbps)



4 安全建议

本次 DDOS 攻击，发生在 5 月 20 日上午 10 点至 12 点之间，攻击源主要来自 110.249.213.19 和 110.249.213.21，攻击方法主要使用了 SYN Flood 和 CC 等攻击方式，攻击在发生当时已被顺利清洗，正常业务不受干扰。

此外，经查询，由于主要攻击源 IP 地址位于相同的地址段，并且不属于公众客户 IP，建议可以在服务器端屏蔽 110.249.213.16/29 地址段的全部 IP 地址。