



Zentyal Cloud Report

January 2010 - October 2010
organization: Widgets Networks
for: Daily Planet

Table of contents

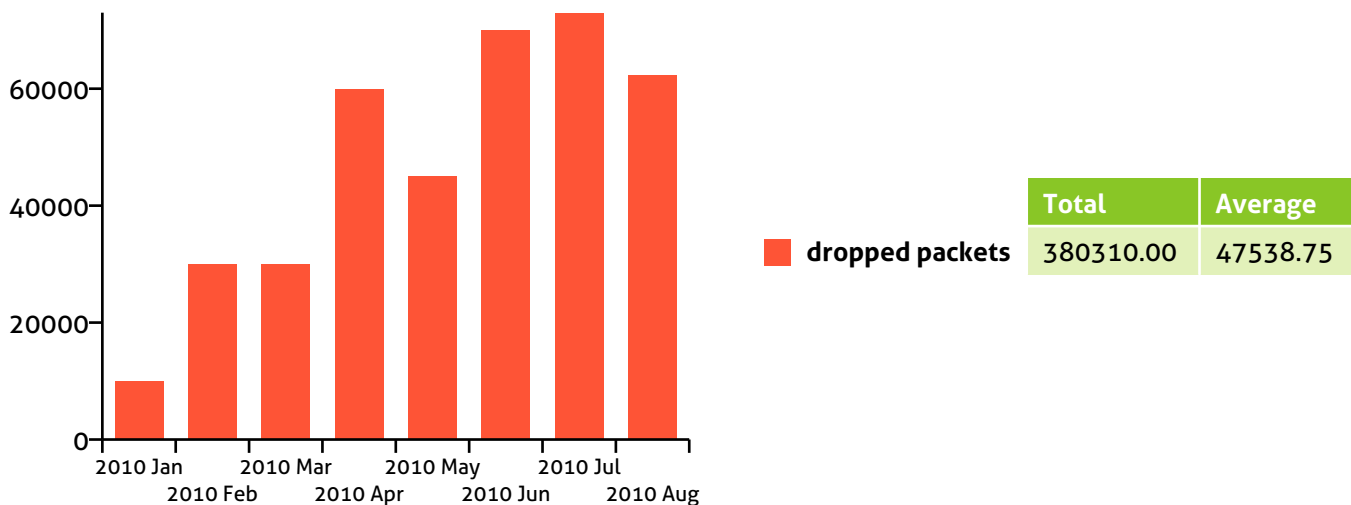
Table of contents	2
UTM profile	3
Firewall	3
Intrusion Detection System	4

UTM profile

Firewall

Dropped packets

Number of packets dropped by the firewall. Dropped packets are only logged when firewall is explicitly configured to do so.



Top dropped sources

The IP address sources sending the highest number of packets dropped by the firewall. Dropped packets are only logged when firewall is explicitly configured to do so. You can search for infected software from those sources.

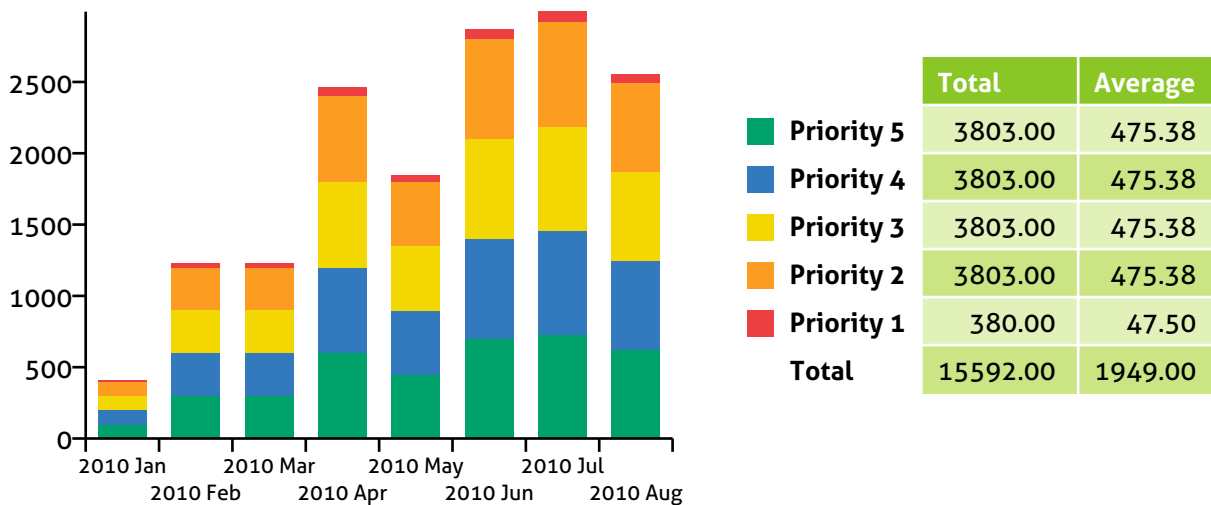
Source	Packets
10.45.12.12	27300
192.168.4.5	27000
34.23.12.1	16231
98.34.12.12	16000
154.12.12.12	14500
192.168.5.6	13000
101.45.22.12	12900
46.23.12.12	9000

Intrusion Detection System

The alerts are prioritised by severity: **The lower the number, the more severe the alert is.** Priority 1 - high alert, Priority 5 - low alert.

IDS Alerts

Number of IDS alerts by severity.



Top IDS alert sources

The IP address sources triggering the greatest number of alerts.

Source	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5
10.45.12.12	10	100	100	100	100
192.168.4.5	30	300	300	300	300
34.23.12.1	30	300	300	300	300
98.34.12.12	60	600	600	600	600
154.12.12.12	45	450	450	450	450
192.168.5.6	70	700	700	700	700
101.45.22.12	73	730	730	730	730
46.23.12.12	62	623	623	623	623