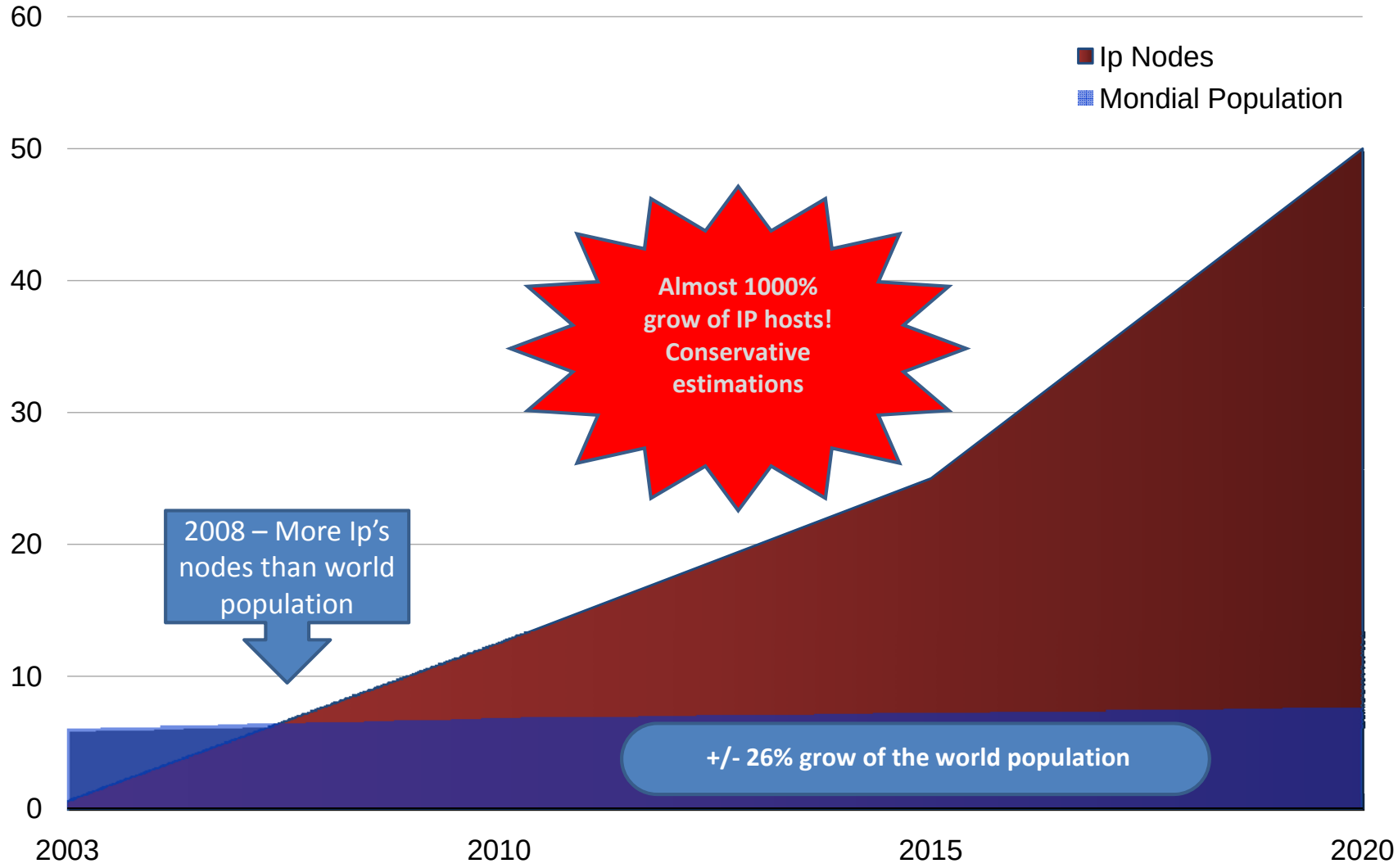
PineApp
Our innovation - Your SeCurity

IPv6
The Battle Against Botnet

PineApp
Our innovation - Your SeCurity

World Population Vs IP Nodes Worldwide



PineApp
Our innovation - Your SeCurity

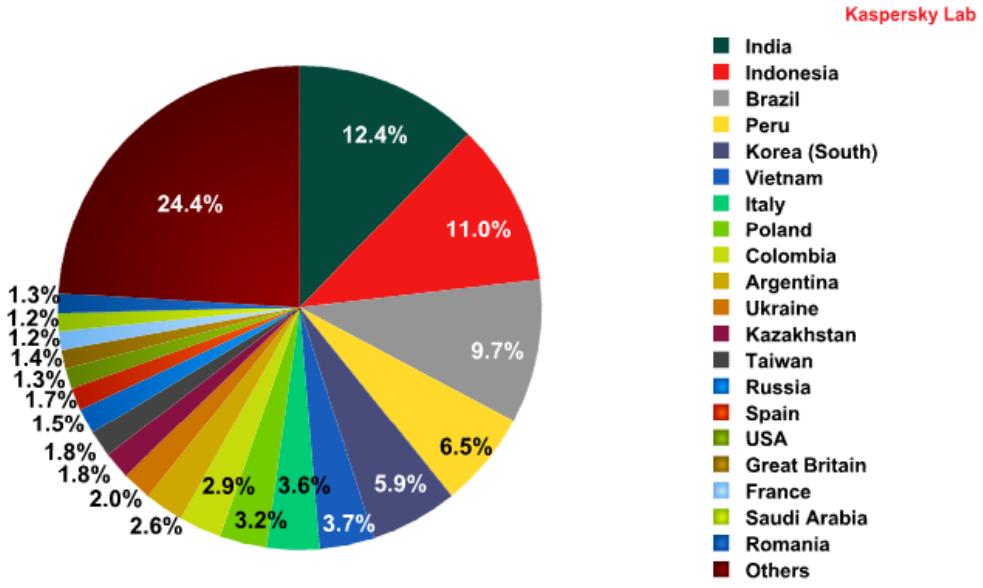
Migration to IPv6 Incentives.

- Need for more address space (exhaustion of IPv4 Space)
- Government mandate
- Mobile communication and 4G
- Population growth in APAC
- More appropriate model for emerging services

PineApp
Our innovation - Your SeCurity

Spam Latest World Numbers

- The percentage of global spam – November 2011



*Securelist Kaspersky

PineApp
Our innovation - Your SeCurity

More IP Space Means

- More available sources of spamming
- More available spamming targets
- More space to mask sources of spam
- More overall spam!

PineApp
Our innovation - Your SeCurity

Botnet and SPAM mechanism

- Botnet deploy on malware and worms.
- Botnet are usually activated through IRC, HTTP or P2P protocols for DDoS and SPAM
- Botnet are spreading SPAM using SMTP

All the mechanisms are application layers!

PineApp
Our innovation - Your SeCurity

Botnet Vs Host Vs SPAM

Date created	Date dismantled	Name	Estimated no. of bots	Spam capacity	Aliases
1999	!a	999,999,999	100000	!a	
2009 (May)	2010-Oct (partial)	BredoLab	30,000,00030,000,000[20]	3.6 billion/day	Oficla
2008 (around)	2009-Dec	Mariposa	12,000,000[21]	0 ?	
0?		Conficker	10,500,000+[22]	10 billion/day	DownUp, DownAndUp, DownAdUp, Kido
2010 (around)		TDL4	4,500,000[23]	0 ?	TDSS, Alureon
0?		Zeus	3,600,000 (US Only)[24]	-1n/a	Zbot, PRG, Wsnpoem, Gorhax, Kneber
2007 (Around)		Cutwail	1,500,000[25]	74 billion/day	Pandex, Mutant (related to: Wigon, Pushdo)
2008 (Around)		Sality	1,000,000[26]	?	Sector, Kuku
0?		Grum	560,000[27]	39.9 billion/day	Tedroo
0?		Mega-D	509,000[28]	10 billion/day	Ozdok
0?		Kraken	495,000[29]	9 billion/day	Kracken
2007 (March)		Srizbi	450,000[30]	60 billion/day	Cbeplay, Exchanger

http://en.wikipedia.org/wiki/Botnet

PineApp
Our innovation - Your SeCurity

Impact of SPAM on IPv4 Hosts and SP

- Exposition of Hosts to criminal content
- Exposition of SP to complain from customers
- Black listing systems usage prevent from users to communicate through SMTP
- Overhead of administration for SP to delist networks

PineApp
Our innovation - Your SeCurity

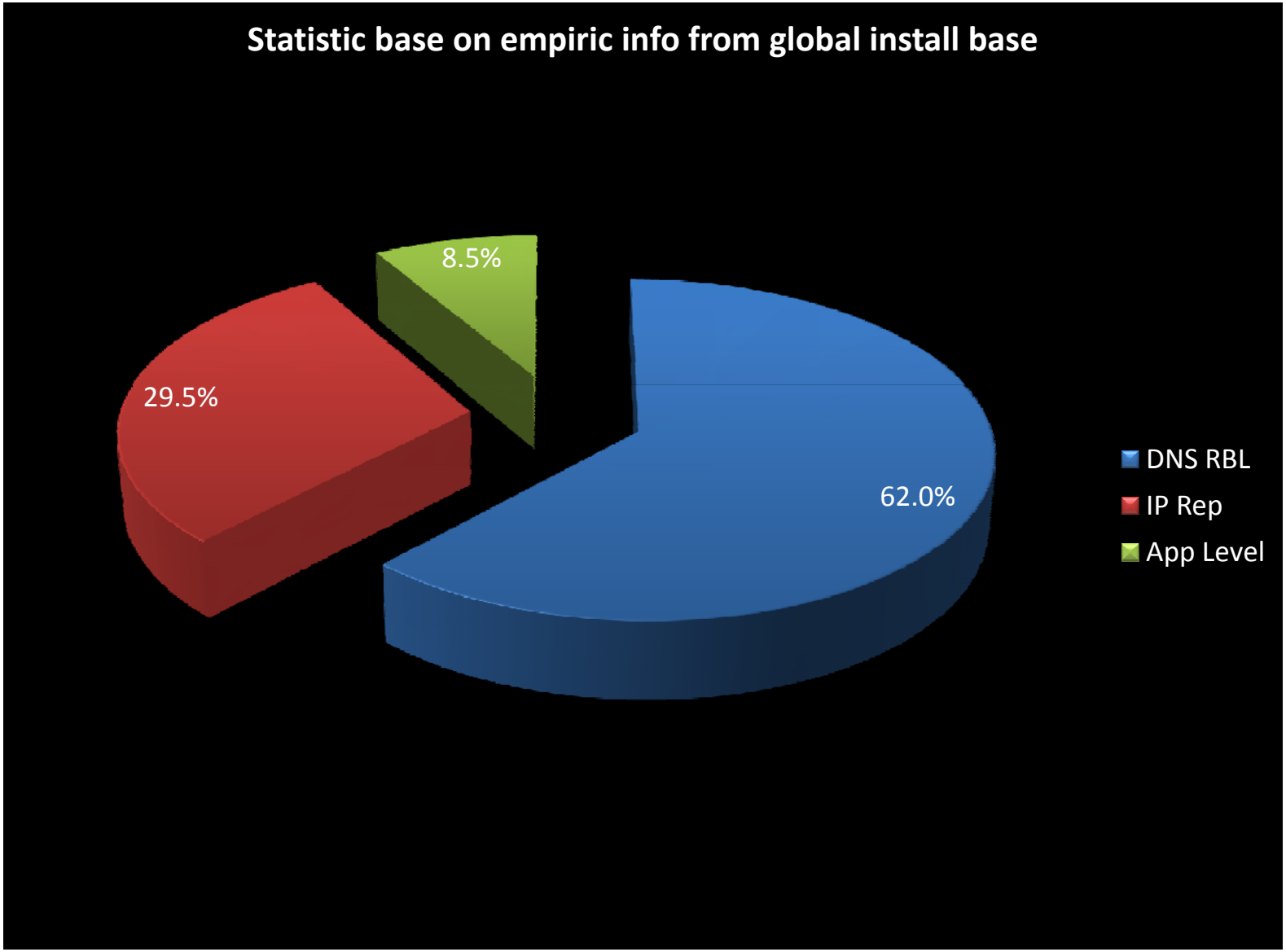
Traditional IPv4 prevention systems

Inbound SPAM filtering based on:

- IP RBL
- IP reputation
- SMTP analysis
- Signatures

PineApp
Our innovation - Your SeCurity

IPv4 Filter Efficiency



PineApp
Our innovation - Your SeCurity

Address based filter

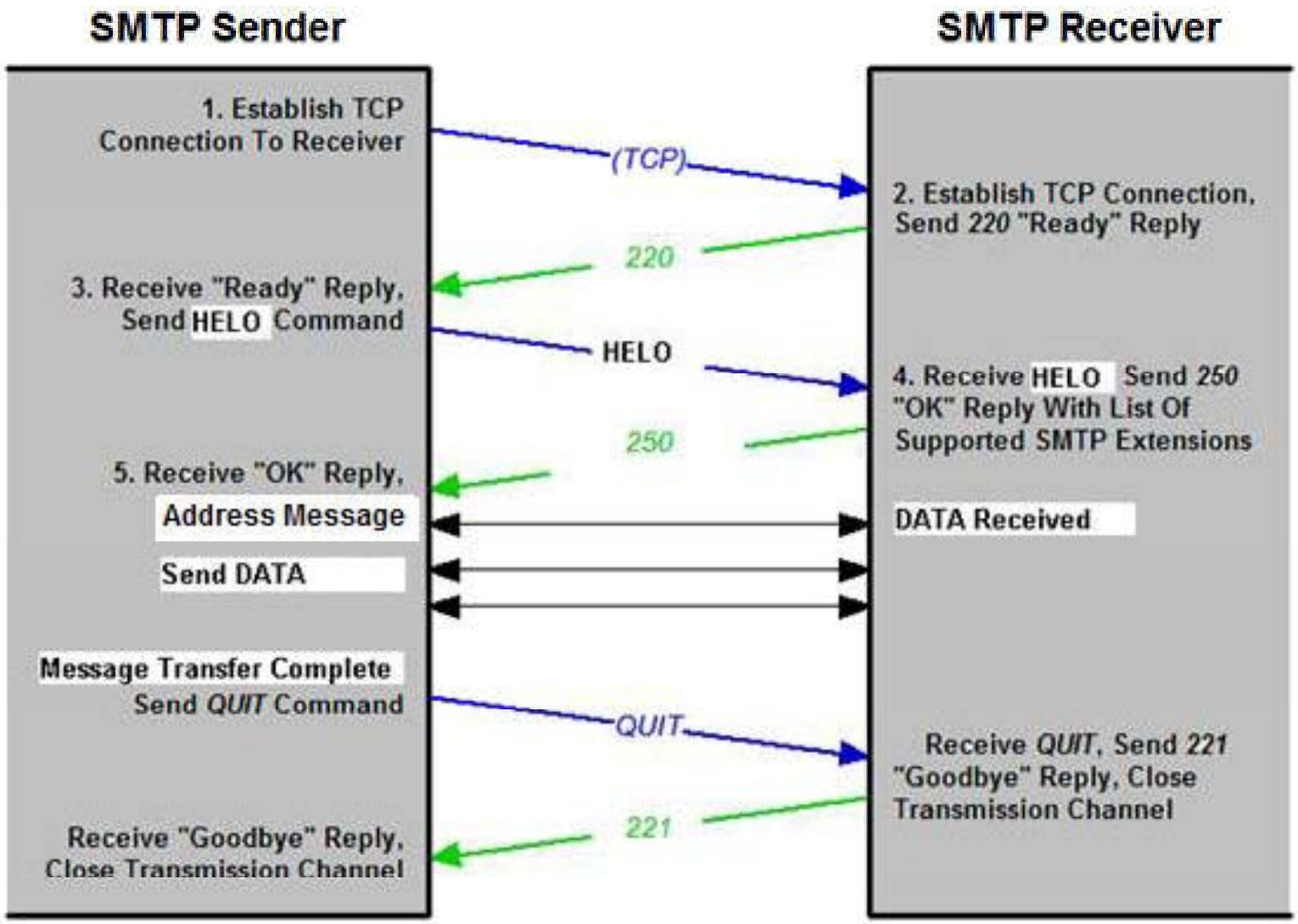
- With time the most effective filter tool
- RBL and IP reputation list block 90% of SPAM

BUT

- Not yet clear plan of migration to IPV6 scale ip reputation lists
- Not clear model of efficiency of this kind of list on IPV6 addressing model
- Not yet a clear practice of IP distribution model - Black Listing not yet possible

PineApp
Our innovation - Your SeCurity

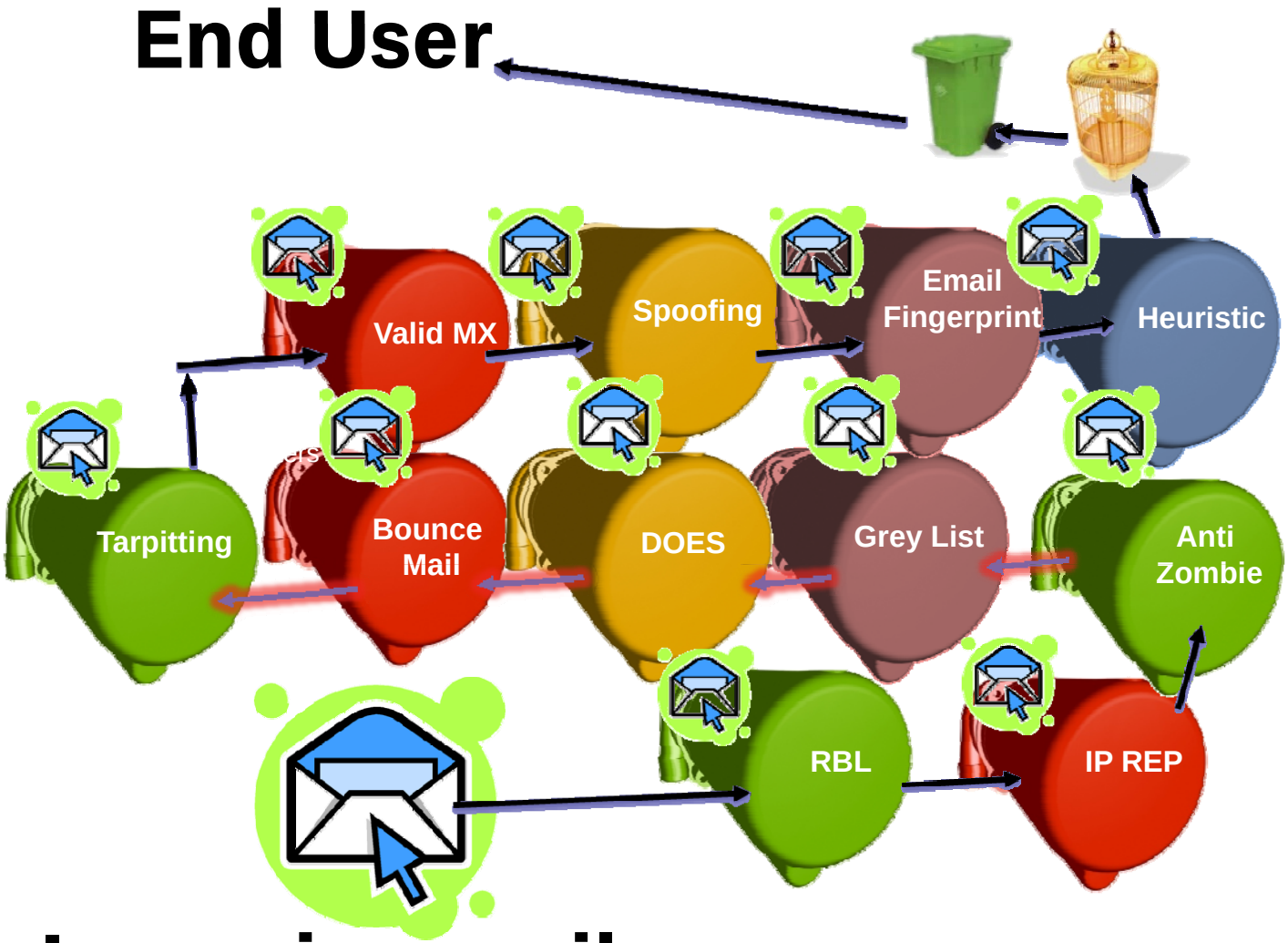
SMTP Model.



SMTP Transaction Session Establishment and Termination

PineApp
Our innovation - Your SeCurity

SMTP Filtering Model



PineApp
Our innovation - Your SeCurity

Impact of IPv6 on SPAM

The huge address space and growing devices connected, will provide and almost unlimited space for Spammer to operate!
IP based reputation system won't be scalable to 2^128 address space. On IPv4 we reach 4.3B entry database
The address space assignation for users (/48 or /64) will permit SPAM mechanism to virtually never use the same address twice.
All the well known mechanisms of SPAM will remain effective – The application layer in IPV6 is the same than IPV4
Growing of Hosts infected will permit creation of so huge DoS that Data inspection based system will overload.

PineApp
Our innovation - Your SeCurity

What About The Transition Period ?

Migration to IPv6 will take time. Meanwhile we will have several model of dual stack network or tunneling solutions

- Transition period will be optimal for SPAM
- Most network operators will focus energy on migration – not on SPAM battle.
- Dual stack and/or tunneling models will masquerade the originator of SPAM

PineApp
Our innovation - Your SeCurity

Mail Services and IPv6

- Most of the SMTP services will remain IPv4 for the foreseeable future
- Need for Dual stack or IPv4 dedicated relay
- Black listing for a relay will affect a lot of end users
- DNS BL cache won’t be able to scale to the V6 size

PineApp
Our innovation - Your SeCurity

IPv4 Exhaustion Implications

- Many provider will have a transition period based on IPv4 solution
- NAT 44 may permit to provider to consider later the move to IPv6
- Masking number of user with one public IP is also masking the real source of SPAM
- Black list will again affect a lot of users

PineApp
Our innovation - Your SeCurity

SPAM Battle for the Next Years

- Preventing SPAM on the connection level will be, more than ever, the best way to prevent SPAM
- Anti-spam systems that operate on the application protocol and transport layer will remain the most effective solutions
- **Awareness of customers**: Anti virus, P2P protection, dedicated anti-spam software