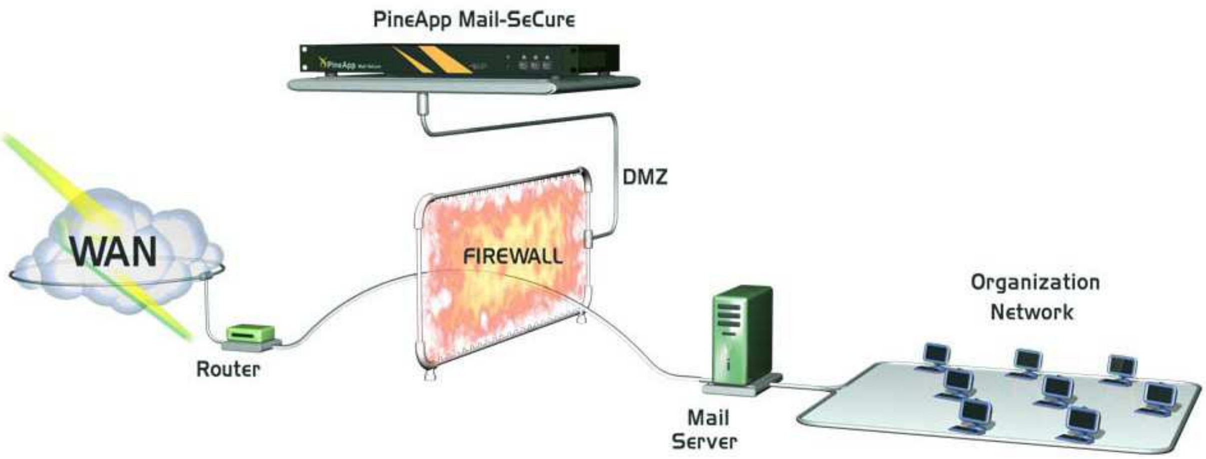
PineApp IP Reputation System™ Whitepaper

PineApp is pleased to announce its new IP Reputation System™ based on Commtouch™' IP Reputation Service.

Reduction of Incoming Spam & Malware and Bandwidth Saving

With spam comprising over 90% of all email, enterprises face extensive IT costs, and deterioration of quality of service (QoS) for valid traffic. PineApp's IP Reputation is available as an additional layer in Mail-SeCure system. To date, IP addresses can not easily be defined as "black" (i.e. definitely spammers), or "white" (i.e. known good senders). Thus, the need for a reputation mechanism that is able to deal with these "grey" addresses, or the "Grey Zone", is awakening. The ability to control unknown or suspicious traffic guarantees faster delivery of valid messages into the organization. In its defense against spam and email borne Malware, PineApp's IP Reputation System analyzes hundreds of millions of messages per day in real-time.



Benefits

- ✓ **Increases Security**: The majority of malicious mail is blocked at the perimeter, resulting increase of organization's security.

- ✓ **Saves Bandwidth, Enhancing Performance**: Bandwidth requirements are significantly reduced, guaranteeing better Quality of Service.

- ✓ **Reduces System Resources**: Eliminates the need for additional hardware and software due to mail traffic growth.

- ✓ **Eliminates False Positives**: by using a wide range of techniques such as temporary failures, false positives are virtually eliminated.

- ✓ **Improves Detection Rate**: by using this feature, in conjunction with other Anti-Spam technologies, a higher detection rate is achieved.

- ✓ **Global Email Coverage**: Billions of messages are classified across global networks and geographies

- ✓ **Global Rate Limiting**: fights distributed zombie attacks, since each individual zombie attacks thousands of targets, but sends just a few messages to each individual location

- ✓ **Accurate Risk Level Classification of Email Senders**: Advanced techniques are implemented to provide highly accurate spam risk and classification levels

- ✓ **Seamless Integration**: As an SMTP relay, as a transparent bridge*, or with Checkpoint firewalls

- ✓ **Support for High-Scalability Scenarios**: Reduced network load enables performance incensement

Classification of Grey Traffic

- ✓ Statistical analysis of averages, over time and recent changes of:
  - ❖ Mail volume and elevation of mail volume.
  - ❖ Spam ratio
  - ❖ Valid bulk ratio
- ✓ Real-time Zombie/BotNet detection
- ✓ Use of IP, DNS and WHOIS attributes such as: domain age, geography, known dynamic IP, and so on.

The Nature of Zombies

Zombies and Bots typically send large amounts of email messages, yet they deceive local defense systems by sending each message to a different organization; therefore, an organization under spam or Malware attack may receive similar messages, each coming from a different zombie-infected machine with a different IP address. A Zombie lifetime is limited, in order to prevent detection by real-time solutions such as RBL systems.

Risk-based Dynamic Policy

Commtouch has classified over 50 million IP addresses in its database, identifying the majority of zombies and other generators of high risk email traffic. PineApp IP Reputation relies on Commtouch huge database, and uses various flow control policies in order to block, throttle or reject high risk IP addresses, saving organizations from unwanted traffic. Quality of Service can also be achieved by mapping low and medium risk IP addresses to a high QoS class, to be guaranteed high performance (only on relay-mode).
High-risk traffic would be mapped to a low class ("thin pipe"), resulting in a substantial Spam and Malware reduction.

Seamless integration with Checkpoint™ firewalls

PineApp IP Reputation system can be easily integrated with Checkpoint firewalls using SAM. When an SMTP session is created, Checkpoint firewall validates the IP against PineApp's IP Reputation system and applies the policy given by the IP Reputation System. All logs are written on Checkpoint firewall thus preventing additional TCO.