



SP2000-Series Platform

Intelligent Service Management

The XMCS solution provides application-layer intelligence to the network, empowering organizations with the ability to deploy new mail-centric services at the network-layer.

By combining highly sophisticated spam and virus detection algorithms with network-based traffic management, XMCS regulates network traffic by prioritizing network bandwidth for valid mail traffic while reducing the network bandwidth consumed by connections transporting spam and/or malicious content such as viruses.

SP2000-Series Platform

The SP2000-series solution consists of up to 40 SP2100 Service Engines and the SP2500 Cluster Manager.



Dynamic Spam Detection

XMCS uses sophisticated content analysis to provide accurate spam detection. An SMTP protocol analyzer also plays a key role in detecting untrustworthy and/or malicious servers. Historical data is stored and reused in providing a server/client history analysis tool to prevent new spamming techniques from slipping through the mail system as spam techniques change.

Content analysis

The XMCS employs a real-time content analysis engine to detect suspect mail messages. Using text word matching, regular expression string matching, word repetition and an automatic message decode agent messages are scanned and weighted based on their content and structure. XMCS also utilizes a sophisticated decoding system to keep message weighting accurate. The decode process includes HTML code parsing, quoted printable mime decoding and base 64 message decoding. These decoding processes help to ensure accurate message weighting.

Protocol analysis

Communication between the XMCS and remote mail servers/clients are monitored for any erroneous protocol communication. Often protocol analysis can detect a spam server before the message content has been transmitted. Within the protocol analysis subsystem, XMCS utilizes mail-probe blocking technology to keep remote systems from using brute force or dictionary attacks in attempts to detect valid local user accounts.

SP2000-Series Specifications

- 1U/4U Multiple appliance solution
- Up to 4Gbps+ per SP2000-Series Cluster
- 100Mbps+ performance per SP2100
- 40 SP2100s per SP2500 Cluster Manager
- MX & SMTP-relay integration w/ SMTP server
- Supports MX Clustering w/ DNS System
- Supports SMTP Clustering w/ Content Switch
- 5000 to unlimited user licensing
- Hundreds of millions of messages per day

Spam Detection Subsystems

- Content Analysis
- Protocol Analysis
- Historical/Statistical Analysis
- 3rd Party/Plug-Ins

Virus Detection Subsystem

- F-Prot Antivirus (licensed optionally)

Group Management

- Configurable IP/DNS grouping
- Blacklisting and Whitelisting
- Dynamic Control Lists
- External Control Lists via SQL API
- 3rd Party Control Lists

Message Controls

- Forward Message
- Drop Message
- Flag Message and Forward
- Flag Message and Forward to Alternate Destination

Connection Controls

- Process Connection
- Drop Connection
- Drop Connection w/ SMTP Error Message
- Maintain Connection with XMCS Traffic Shaping

XMCS Traffic Shaping

- Dynamic Weighted Traffic Shaping: The greater the offence, the greater the bandwidth reduction to the connection and/or server/client
- Multi-tiered Whitelist/Blacklist traffic shaping
- 3rd-Party trigger list traffic shaping

Device Management

- GUI Device Management over HTTPS
- Enhanced Device Management over SQL
- Customizable Alerting, Logging and Reporting