

RedSpam – ‘In the Cloud’ Technical Specification

The existing security infrastructure in many organisations is no longer sufficient to protect against today’s cyber threats. The continued discovery of vulnerabilities in commercially deployed software puts servers and client workstations at risk for becoming compromised by Spyware, viruses, botnet programs and other malicious code.

THREE DIMENSIONAL PROTECTION

Protection against malicious content, undesired access, and botnet-based attacks.

DIRTY FEED - CLEAN FEED

Eradicate malicious traffic from your network and enjoy ‘clean’ exploit free traffic. Our solution ensures that only legitimate traffic reaches your network via our Guardian DDoS network.

PERFORMANCE

High throughput especially while blocking attacks, ensures excellent network performance.

LOW NETWORK LATENCY

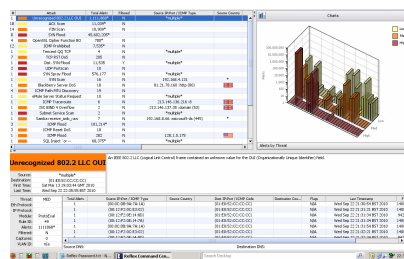
Low latency infrastructure to ensure critical applications run within expected time sensitive parameters

RELIABILITY

Protection Cluster configurations, port bypass and redundant power ensure reliability.

HIGH AVAILABILITY

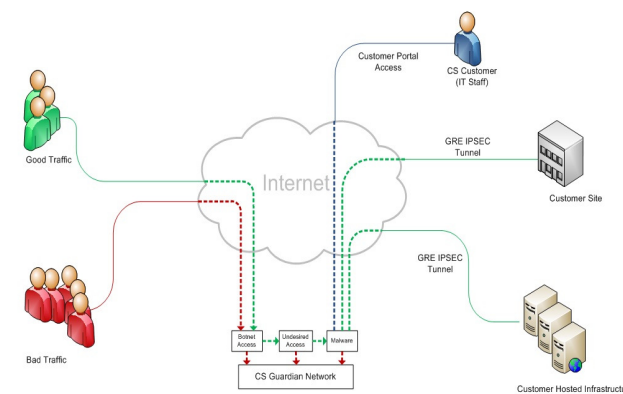
- Active-Active Infrastructure
- Asymmetric traffic handling
- Scalable performance and capacity
- Seamless fail-over that ensures non-stop protection
- Highly resilient including Hot swappable power supply and fans
- No rotating media or chip fans



At the heart of our ‘In the Cloud’ solution is the RedSpam Guardian Network, the most advanced third generation family of DDoS and Intrusion Prevention network security hardware, utilising the leading and pioneering security vendor - Top Layer Networks. The RedSpam solution is designed to deliver non-disruptive protection against constantly evolving threats. It provides maximum protection for critical IT assets while allowing full access to legitimate users and applications. Security threats are constantly changing and your network needs to rapidly be protected from zero-day attacks. RedSpam in conjunction with Top Layer Networks provides a protection service ensuring proactive protection for your network and assets.

The development of more targeted attack methods and clever social engineering makes it more likely that even careful educated users can become victims. Finally the appearance of true zero-day exploits of commonly deployed software makes patching an ineffective defense.

‘In the Cloud’ Topology



COMPREHENSIVE FUNCTIONLITY

- Prevent exploits of critical vulnerabilities
- Keep Spyware, viruses, botnet programs and other malware out of your network
- Thwart advanced hybrid and application level attacks
- Provide P2P Security, blocking BitTorrent, Gnutella, eDonkey, Winny, Skype, and FastTrack
- Provide protection of VoIP infrastructure
- Block DDoS and botnet-based attacks
- Prevent undesired access

RedSpam Includes:-

- Proactive protection against threats while patches are being tested and deployed
- Improved security posture through acceptable application usage enforcement
- Regulatory compliance through protection of confidential data
- Protection against theft of intellectual property due to undesired access
- Reduction in IT hours devoted to fixing/remediating systems infected by viruses, worms, and spyware
- Reduction of downtime from DDoS attacks and Botnet threats

Comprehensive Network Security through Three Dimensional Protection

THREE DIMENSIONAL PROTECTION

Protection against malicious content, undesired access, and botnet-based attacks.

CLEAN FEED

Eradicate malicious traffic from your network and enjoy 'clean' exploit free vulnerabilities.

PERFORMANCE

High throughput especially while blocking attacks, ensures excellent network performance.

LOW NETWORK LATENCY

Low latency infrastructure to ensure critical applications run within expected time sensitive parameters

RELIABILITY

Protection Cluster configurations, port bypass and redundant power ensure reliability.

HIGH AVAILABILITY

- Active-Active Infrastructure
- Asymmetric traffic handling
- Scalable performance and capacity
- Seamless fail-over that ensures non-stop protection
- Highly resilient including Hot swappable power supply and fans
- No rotating media or chip fans

PROTECTION BENEFITS	DESCRIPTION
Prevents desktop computers and servers from being compromised by remote exploits and malware.	
Acceptable Application Use Policies	<ul style="list-style-type: none"> • Deep packet inspection for HTTP, FTP, DNS, SMTP, Telnet, SSH, MS-RPC, MS-CIFS, and other application protocols • Critical vulnerability protection against injection attacks, access attacks, DoS attacks, unauthorized servers, backdoors, etc. • Transaction and data protection rules for application-level checking of HTTP, FTP, DNS, SMTP, Telnet, SSH, MS-RPC, MS-CIFS, and other application protocols • Configurable data validation modules that inspect the content and format of known and unknown file types when carried as payloads of supported L3, L4, and L5 protocols
Protocol & File Validation	<ul style="list-style-type: none"> • Configurable transport layer protection rules for TCP and UDP including flexible enforcement criteria • Protocol normalization for reordering and coalescing IP fragments, and reordering TCP segments • Configurable file-format protection rules for files carried in protocol payloads • File format usage policies
Vulnerability Signatures	Unlike the attack signatures, our vulnerability signatures provide protection against a whole group of attack variants, and are also very useful in providing protection against zero day attacks. For example, a vulnerability signature that simply checks that the HTTP host field length is smaller than 410 bytes can stop multiple known MS IIS exploits.
Attack Signatures	Stateful matching signatures for IP, UDP, and reassembled TCP session payloads. In addition to the factory provided signatures, users can add and edit their own signatures.
Prevents undesired access to business-critical systems, applications, and data.	
Stateful Firewall Filtering	<ul style="list-style-type: none"> • Policy-based undesired access protection through stateful firewall filtering with no performance degradation • Configurable data link protection against illegal or ill-formed MAC and data link headers, IEEE 802.1Q VLAN filters, MAC address filters • Configurable protection against attempts to use TCP retransmissions and segment overlap as evasion mechanisms • Configurable network protocol protection rules for IPv4, ICMP header fields, IP address filters
Ensures the availability of applications and services, even when under botnet-initiated attacks.	
Denial of Service & DDoS Protection	Patented algorithms for protection against SYN floods, ICMP floods, UDP floods, and application overload attacks.
Application Rate Limits	Policy based rules that limit traffic rates
Connection Limits	Configurable rules that protect your network resources (such as servers and routers) from being overwhelmed by too many active connections
Client Request Limits	Configurable rules that limit the rate at which individual clients or groups of clients can initiate transactions

RED SPAM



303 - 306 High Holborn
Northumberland House
London
WC1V 7JZ
T: 0870 352 1007
E: info@matec.co.uk