DoS, DDoS & DrDoS mitigation and traffic policy enforcement software.

Andrisoft WANGuard Platform™
WANGuard Filter 3.0

OVERVIEW

WANGuard Filter is the WANGuard Platform component designed to protect networks from internal and external threats (availability attacks on DNS, VoIP, Mail and similar services, unauthorized traffic resulting in network congestion), botnet-based attacks, zero-day worm and virus outbreaks. WANGuard Filter includes sophisticated traffic analysis algorithms that are able to detect and filter the attack patterns contained in the malicious traffic, while re-injecting the cleaned traffic back into the network.

TRAFFIC DIVERSION AND INJECTION TECHNIQUES

Traffic diversion is the mechanism by which an upstream router in the core network is instructed to send suspect traffic (syn floods, spoofed packets, and so on) to the WANGuard Filter system. After scrubbing off anomalous packets, the WANGuard Filter performs traffic injection to insert cleaned traffic back to the network - to a downstream router - using one of the following techniques:

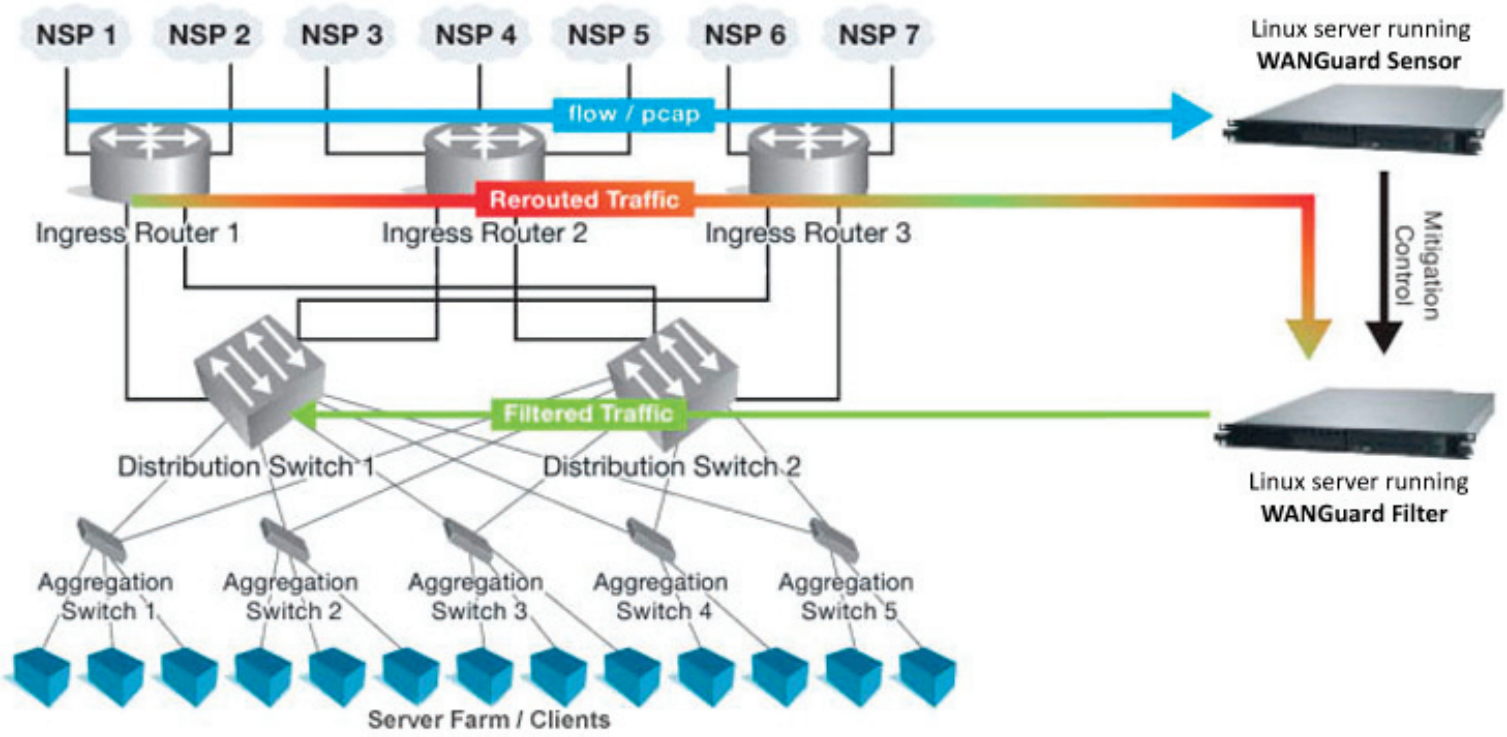
Static Routing - In a Layer 2 topology, WANGuard Filter will forward cleaned traffic to a statically configured next-hop address
GRE/IPIP Tunneling - In a Layer 3 topology, WANGuard Filter will forward cleaned traffic via a GRE/IP over IP tunnel
Inline Deployment - When the WANGuard Filter system is deployed inline, no traffic diversion and injection is needed

FEATURES

- Quickly see detailed live and historical information about traffic anomalies in your network from any location by accessing WANGuard Console with your web browser
- Defends against known, unknown and evolving attack patterns
- Recognizes and filters malicious traffic in under 5 seconds
- Does not block/blacklist valid customer traffic
- WANGuard Filter can be deployed in-line or out-of-line by diverting the malicious traffic towards the server running it. The cleaned traffic can be re-injected back to the network using Static Routing or GRE / IPIP tunneling
- Per endpoint flexible threat management tools and an easy to use API for scripting the reaction to attack patterns:
  - alert the NOC staff by email using user-defined email templates
  - alert the ISPs of the attackers via email using user-defined email templates
  - send custom syslog messages to remote log servers
  - execute custom scripts that extend the built-in capabilities, such as:
    - configure ACLs or execute PIX “shun” command to filter attack patterns
    - filter attacking IP addresses by executing “route blackhole” commands
    - send SNMP TRAP messages to SNMP monitoring stations
- Does not require network baseline training and operator intervention
- Easy and non-disruptive installation on common server hardware
- The most cost-effective DoS, DDoS and DrDoS mitigation and traffic policy enforcement solution on the market

Requirements

Single WANGuard Filter Deployment Example



Minimum System Requirements for protecting 1 Gigabit Network Interface

Architecture	x86 (32 or 64 bit)
CPU	1 x Xeon 2.5 GHz or 1 x Opteron 1.8 GHz
RAM	500 MBytes
Network Cards	2 x Gigabit Ethernet (NAPI support strongly recommended)
Operating System	Red Hat Enterprise 5, CentOS 4, CentOS 5, OpenSuSE 10, SUSE Linux Enterprise 10, Debian Linux 4, Ubuntu Linux Server 8
Installed Packages	perl 5.x quagga or zebra Net::Telnet iptables mysql 5.x perl-DBD-MySQL tcpdump WANGuard-Filter 3.0 WANGuard-BGPSupport 3.0 WANGuard-Controller 3.0
Disk Space	5 GB (including OS)

Andrisoft SRL
Str. Lunei L30 Ap. 11
300109 Timisoara
Romania

office@andrisoft.com

Andrisoft is a network security company that offers IT organizations network monitoring and protection software and solutions.
Andrisoft WANGuard Platform is built on a scalable and performant architecture and offers unparalleled granularity, accuracy and precise, non-intrusive mitigation.