

Traffic to/from Extranet may be further analyzed in FW

Traffic from/to Intranet may be analyzed in FW

in VLAN GRE interfaces Separate GRE tunnels may be used to guarantee different QoS levels for

different services (http, smtp, dns, ldap, ftp etc.)

Source of terminology: e.g. www.wikipedia.org Version 1.3.9 © 23.5.2007, Mika.Panhelainen@iki.fi 1) IPS Gateway System can also be used to protect other public services like smtp, dns, ldap, ftp etc. It may be possible to implement an IPS Analyzer Sensor functionality inside an associated Corporate NIC. In this case a dedicated line connection to the Corporate via separate interfaces (ICs) is not needed

IPS Data Center can be connected to the Operator's Site Backbone Routers

VLAN_EXT interfaces and Priority or Class based WFQ (based on DSCP)

Traffic Flows inside NIC

Inbound VLAN EXT: Queuing

Blacklist ACL

Traffic shaping GRE tunnel encapsulation and DiffServ marking Forwarding based on route selection (Linux based route cache, RPDB and RTs)

Outbound VLAN GRE: Queuing 802.1p marking (based on DSCP) Forwarding

Inbound VLAN GRE: Queuing ACL

GRE tunnel decapsulation ACL Traffic shaping Forwarding based on route selection (Linux based route cache, RPDB and RTs)

Outbound VLAN EXT: Queuing Forwarding

There is a bidirectional communication between active CP and every NIC. ICs are used for secure connections to the IPS Analyzer Sensors. Active CP is responsible of Fault management including alarms, logs, system failures and NIC failovers, Configuration management including maintaining and pushing configuration to the NICs, Accounting management including administration and gathering statistics of system components, Performance management including collecting performance data and Security management including controlling access to the system.