Global Technology Associates, Inc.

Internet Firewall Developer since 1994

Threat Management
Intrusion Prevention

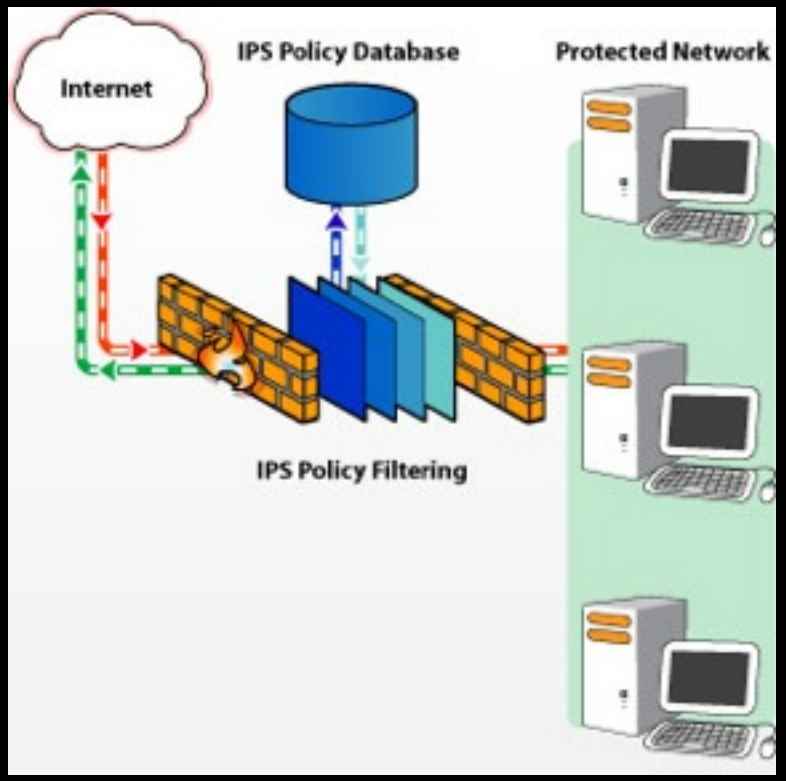
Course # 3303

IPS

- Part of GTA's Threat Management
  - Mail Sentinel and Surf Sentinel
  - Uses signature based policy definitions to recognize attacks.
  - IPS analyzes traffic before it reaches internal hosts and can blocks attacks before they can reach the internal network.
  - Comes with a standard (built in) set of predefined policies.
- IPS engine is based on SNORT
- Available on all GTA Firewalls
- Requirements
  - Configured DNS server (For updates)
  - Allowed SSL connections to als.gta.com
  - Optional Support or Maintenance contract – Dynamic Updates
  - Optional IPS code – Dynamic Updates
  - Only supports IPv4 IPS. IPV6 support for IPS is in development.

How does IPS work?

- Packet is received by the firewall.
- If IPS is enabled on the matching policy the packet is passed to the IPS engine.
  - Packet is then checked against known signatures in the IPS database.
  - If the packet matches a signature the actions specified for the signature are applied. Such as drop, pass or send a reset.
    - Part of the signature matching is based on the source and destination Address, and service. For example, IPS may be configured on an outbound policy. However, IPS signature is based on a connection to an internal web server.
  - If does not match a signature. It is passed back to the firewall to be match against the rest of the policy actions.
- If IPS is not enabled it processed against the reset of the policy.



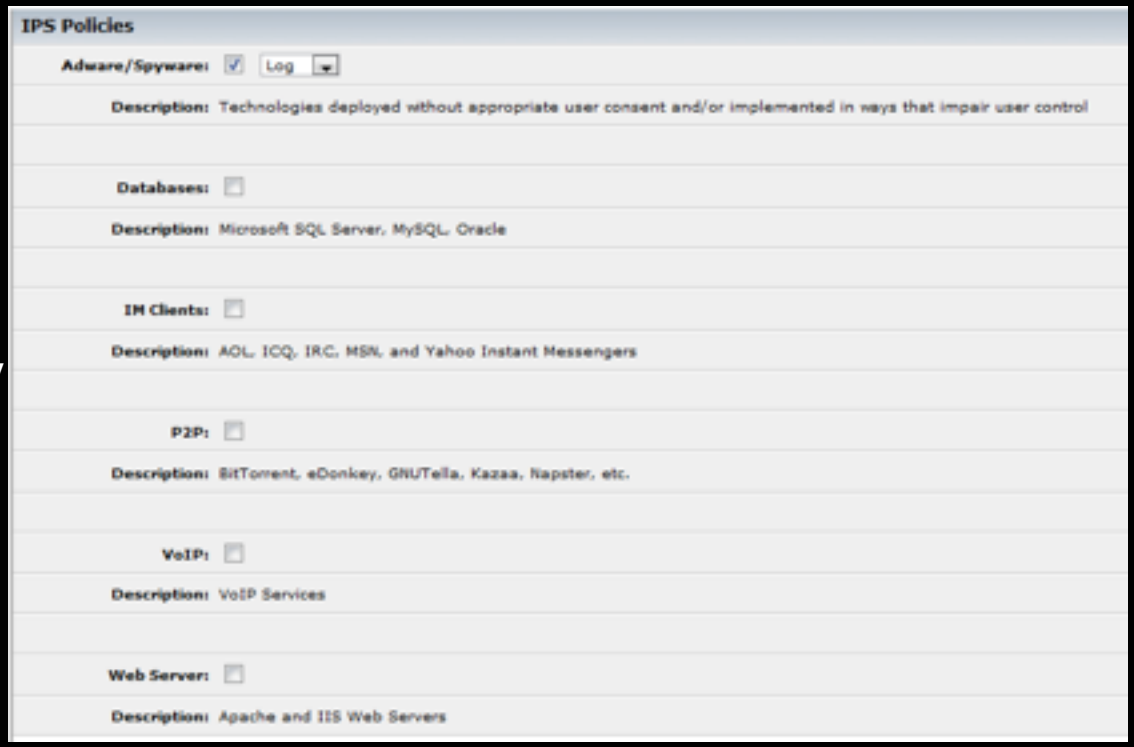
2 Types of Rules Sets

- Default –
  - Static set built into the GB-OS.
  - Static set is updated on new builds.
- Subscription (Dynamic) –
  - Requires a valid support or maintenance contract.
  - Activation code for IPS
  - Updates are downloaded automatically from GTA.

IPS Wizard

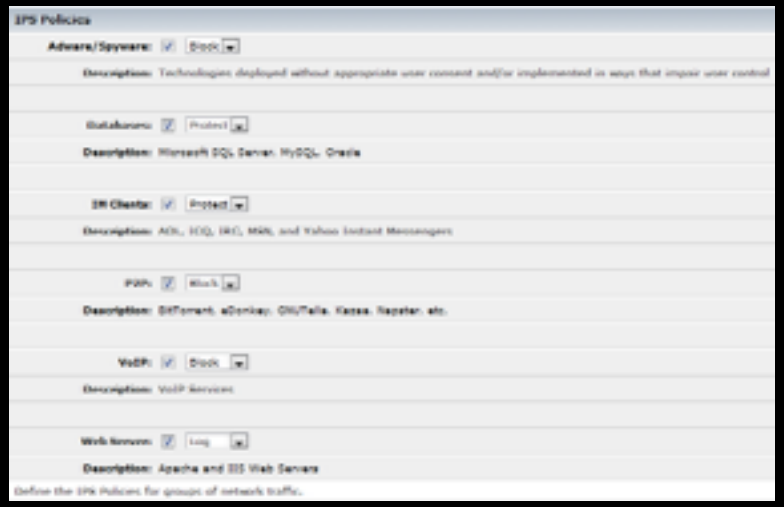
Wizards -> IPS

- Quick easy set up of common IPS policies
  - Spyware
  - Databases
  - IM Clients
  - P2P
  - VOIP
  - Web Servers
- Can be updated dynamically by GTA for firewalls with Maintenance or Support contracts
- Two to Three possible functions depending on service -
  - Protect
  - Block
  - Log

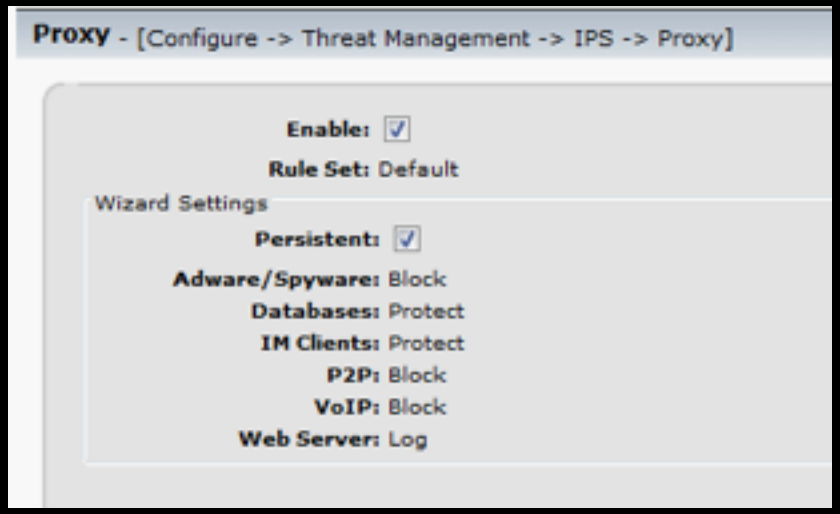


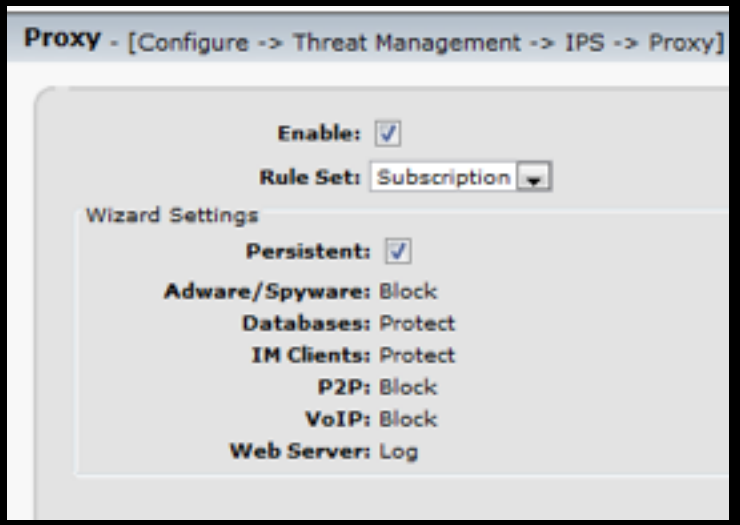
Wizard – 2 Steps
Step 1

- Step 1 – Run the Wizard
  - Select the service to protect or block
  - Apply – depending on the number of policies the apply may take a few moments.



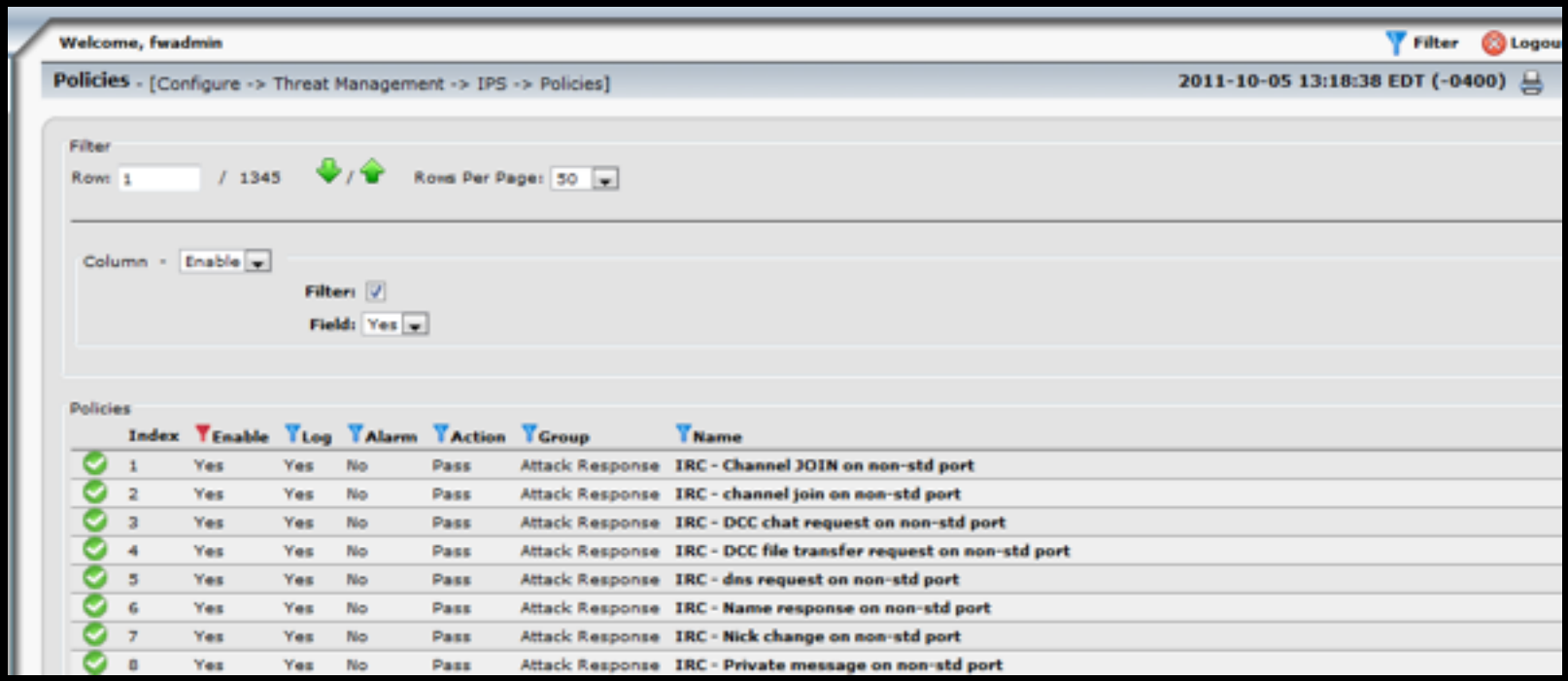
IPS Proxy After the Wizard





- Rule Set: Default – No IPS code on firewall
- Rule Set – Subscription – IPS code is present and firewall will download updates (If support contract is valid).
- Wizard Settings are set to “Persistent”

IPS Policy Settings After Wizard is run



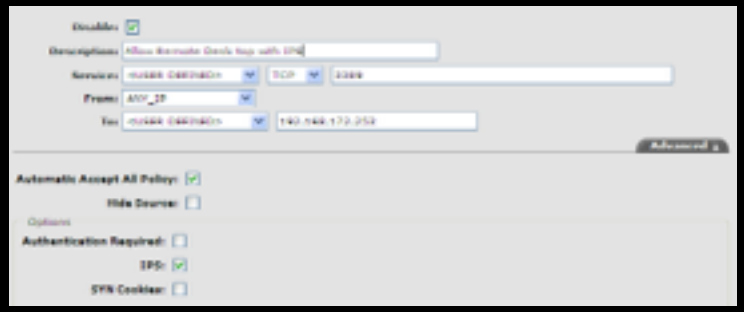
- Persistent – while enable the Policies are non-editable

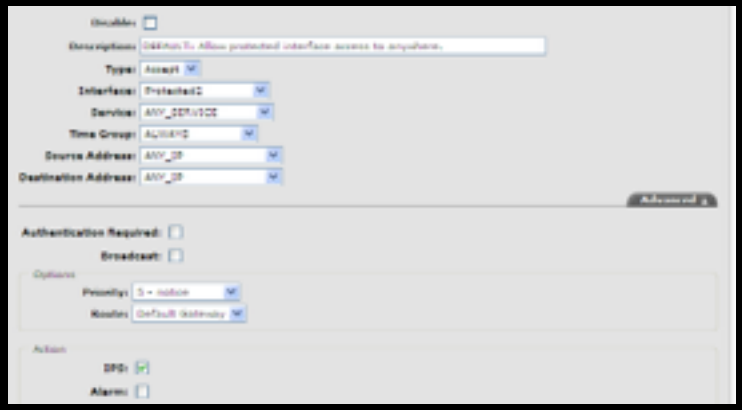
IPS Wizard

Step 2 -

- Enable IPS on
  - Policies

  or
  - Tunnels that you wish to have IPS server protect.
  - By default all policies and tunnels have IPS enabled.
- IPS is located in the Advanced section of tunnels or security policies.

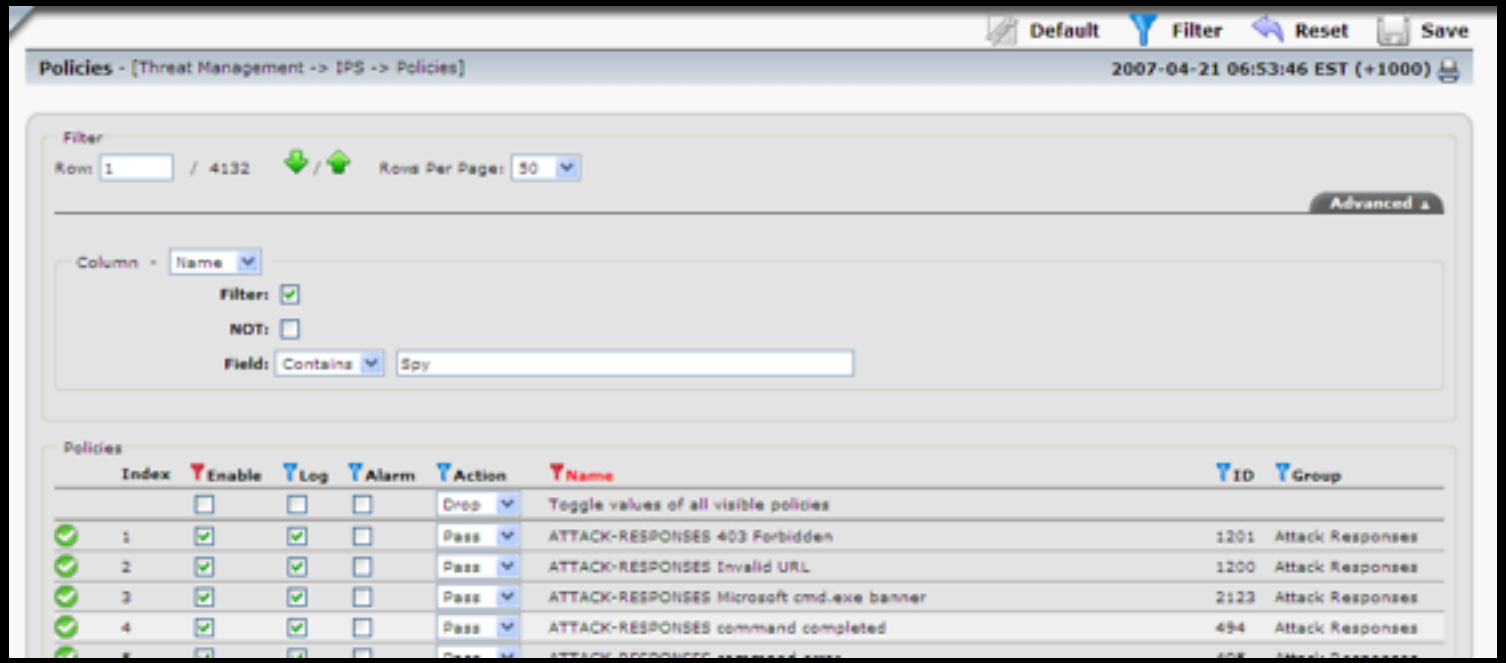




Manual Configuration - 3 Parts

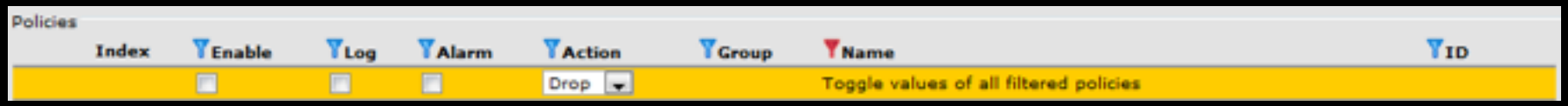
- Enable IPS Proxy -
  - [Threat Management -> IPS -> Proxy]
- Set IPS policies –
  - [Threat Management -> IPS -> Policies]
  - Currently 6000 + policies
- Apply IPS to
  - Tunnels
  - Policies (Outbound, Pass Through, Remote Access)

Searching and Sorting IPS Policies

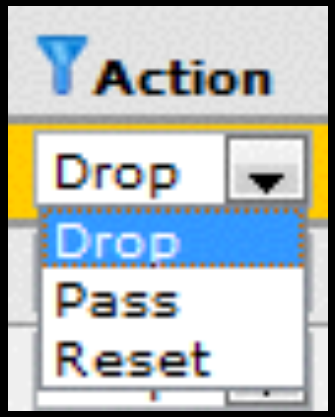


Multiple search criteria can be used.
Display option allows 50, 100, 500, ALL
Page ICON moves to the next page.
You can enable move next page and enable then save.

Policy Options



- Enable – Enables or disables policy
- Log – determines is policy is logged or not logged
- Alarm – generate an alarm on matching policy.
- Action –
  - Drop – drops packets
  - Pass – Allows Packets
  - Rest – Send reset



IPS Logging

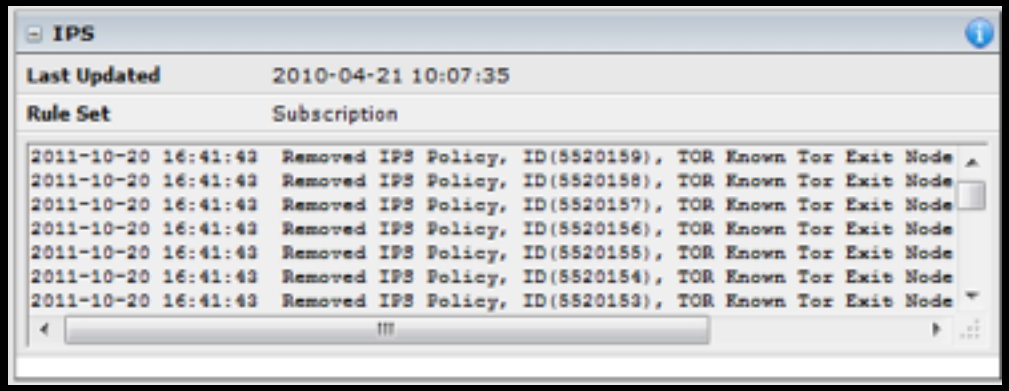
- Overview -> IPS – Displays IPS enabled or disabled and Rule Set Used – Subscription or Default (loaded in config)
- Monitor-> Activity -> Threat Management -> IPS] : Display any updates automatically downloaded when using Subscription set.
- System -> Overview -> IPS : smaller set of logs show updates and status (default or subscription set)
- Monitor -> Log Messages -> IPS

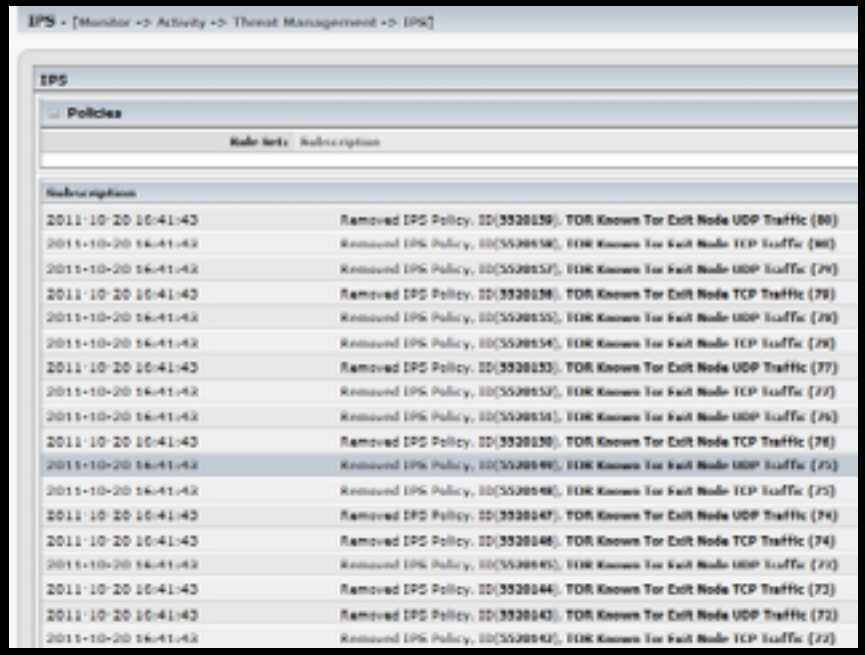
  Jul 25 12:44:27 pri=5 msg="IPS: P2P/Chat - MSN status change" action=pass rule_id=5002192 rule_rev=2 classification="Potential Corporate Privacy Violation" proto=1863/tcp src=10.10.1.247 srcport=1221 dst=207.46.109.18 dstport=1863

  Jun 5 08:15:03 pri=4 msg="IPS: Malware - Fun Web Products Agent Traffic" action=drop rule_id=5001034 rule_rev=14 classification="Potential Corporate Privacy Violation" proto=80/tcp src=10.10.1.25 srcport=3941 dst=65.207.183.56 dstport=80

Updates

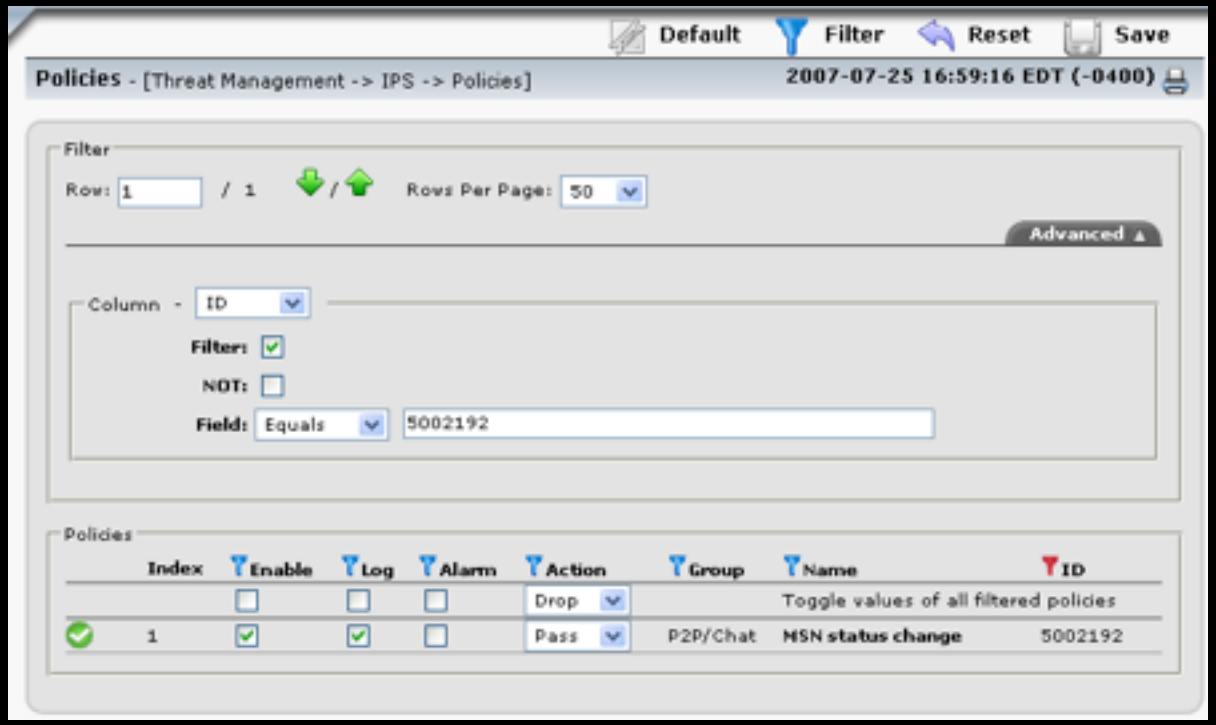
System Overview



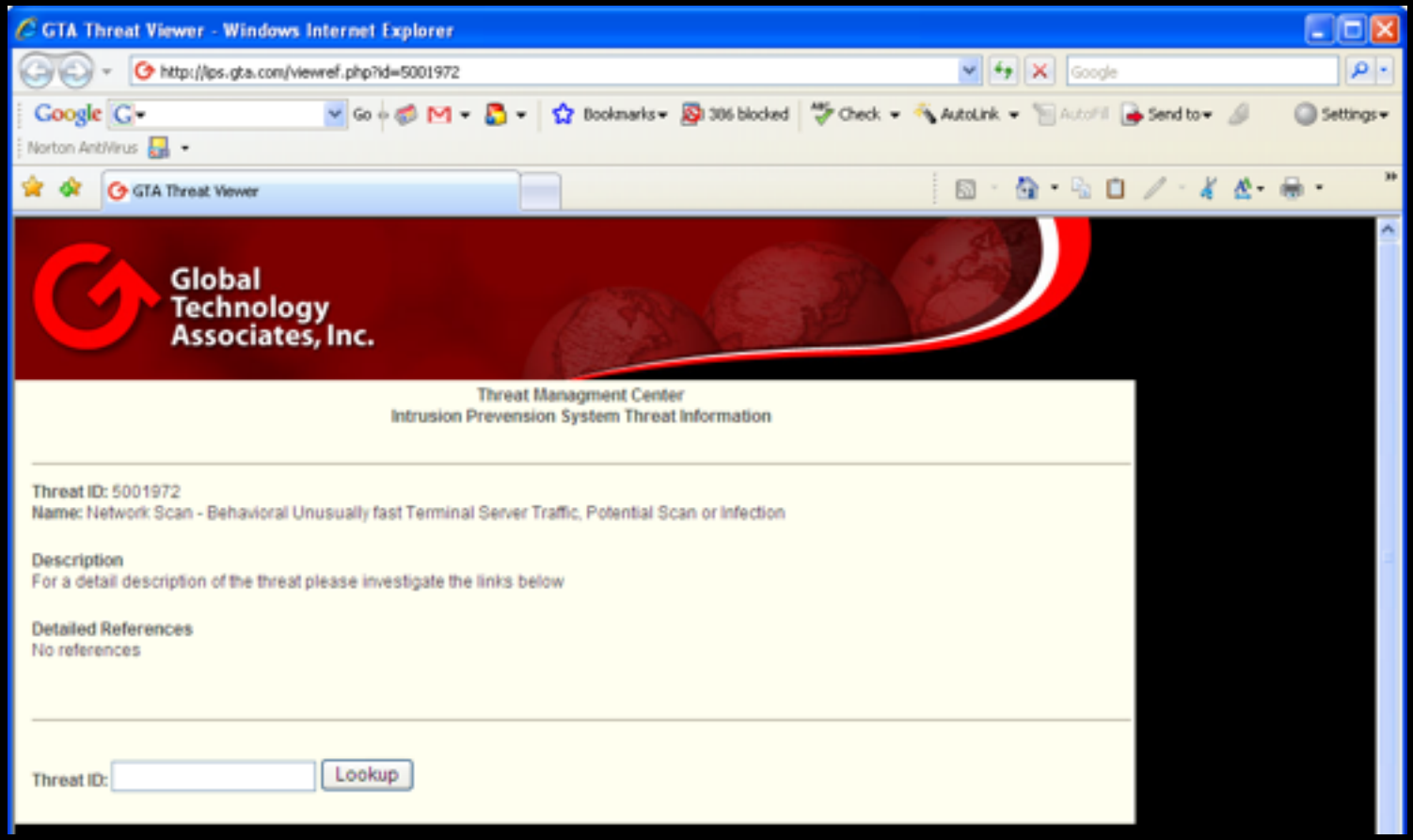


[Monitor -> Activity -> Threat Management -> IPS]

Using Log to search IPS

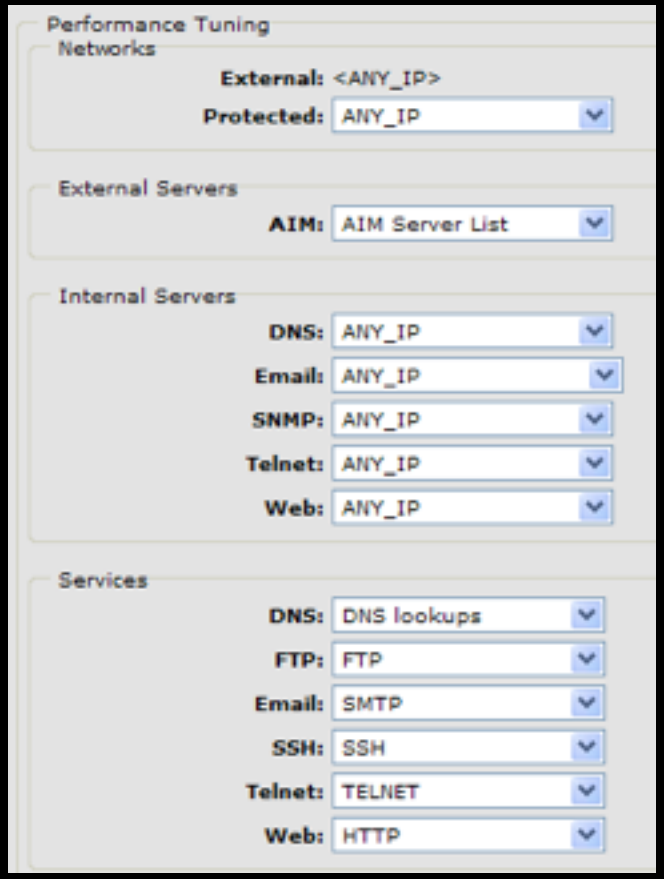


GTA IPS Web Page



IPS Performance Tuning

- Advanced section of the IPS -> Proxy is advanced performance tuning options
- External Servers
  - AIM Server List
- Internal Servers
  - Email
  - SNMP
  - Telnet
  - Web
- Services.
  - DNS
  - FTP
  - SMTP
  - SSH
  - TELNE
  - HTTP



IPS FAQ

- Global – you cannot have a separate IPS policy for two different web servers. For example one set for an Apache server and one set for IIS.
- VPN – does not support IPS on VPN policies.
- Does IPS Proxy Slow down connections
  - Yes, the inspection service will slow down connections.
  - How much is base on firewall and amount and types of traffic. Optimization can help in improving speed some.
- Optimization –
  - IPS Proxy Advanced
    - Protected networks – IP/Subnets to apply for IPS internally
    - AIM Servers – list of AIM server if a customer only wishes to block AIM.

FAQ – IPS and Hard to Block Protocols

Skype, AIM, Bit torrent can use SSL. This makes the service harder to block. However, it is possible with a strict policy.

- First Step is to create Address and service objects for Allowed IP Addresses and Services and denied IP Addresses and services.
- Second step is to configure Surf Sentinel Traditional Proxy.
- Third Step is to configure IP Service
- Step Four is to configure Outbound or Pass Through Policies.

IPS + Antivirus and Compact Flash cards below 1 GB

- Due to the increase in size of a IPS policies, and Anti-virus rules running a combination of Email Anti-Virus and IPS on firewalls with compact flash card of less than 1 GB can be problematic.
- System may slow down or have issue with amount of available memory.

References

- GTA Online Documentation - http://www.gta.com/support/documents
- IPS Information - http://emergingthreats.net/
- GTA IPS Information - http://online.gta.com/gb-os/ips.html

If you require additional assistance or have additional questions please contact GTA Technical Support.

- Email: support @gta.com
- Support Line Phone: 1.407.482.6925
- Normal Hours – 0830-1900 EST U.S.
- Free User Support – http://forum.gta.com

Global
Technology
Associates, Inc.

Internet Firewall Developer since 1994

The End