



**Global
Technology
Associates, Inc.**

Internet Firewall Developer since 1994

Threat Management Intrusion Prevention

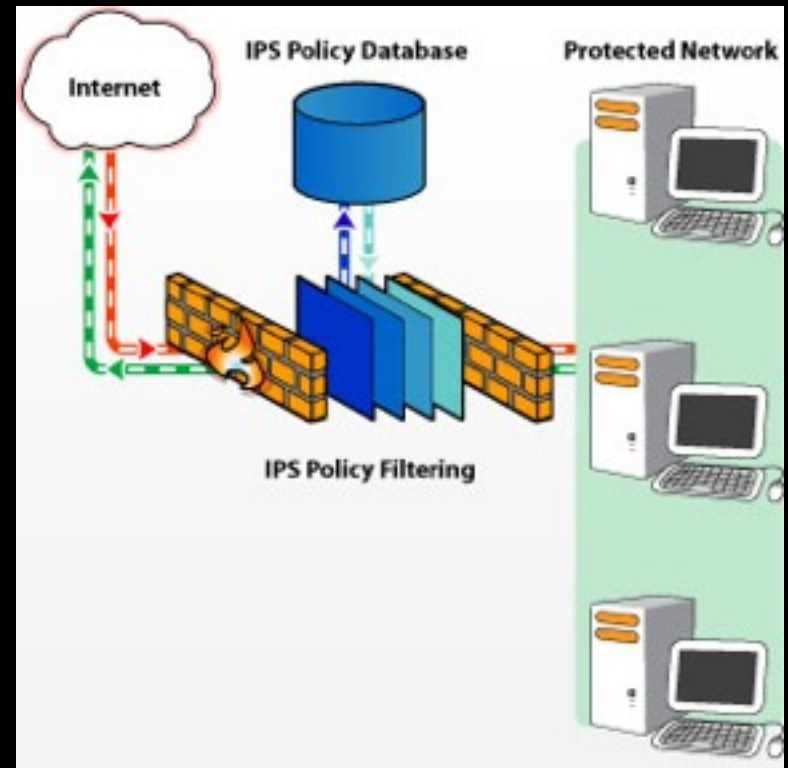
Course # 3303

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

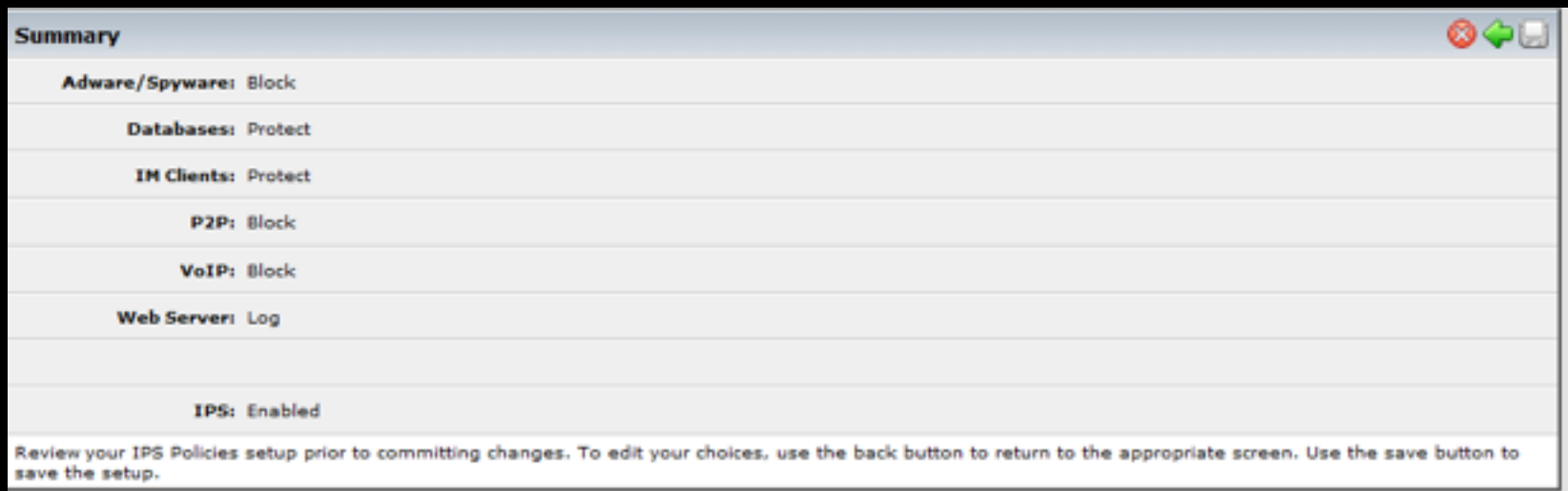
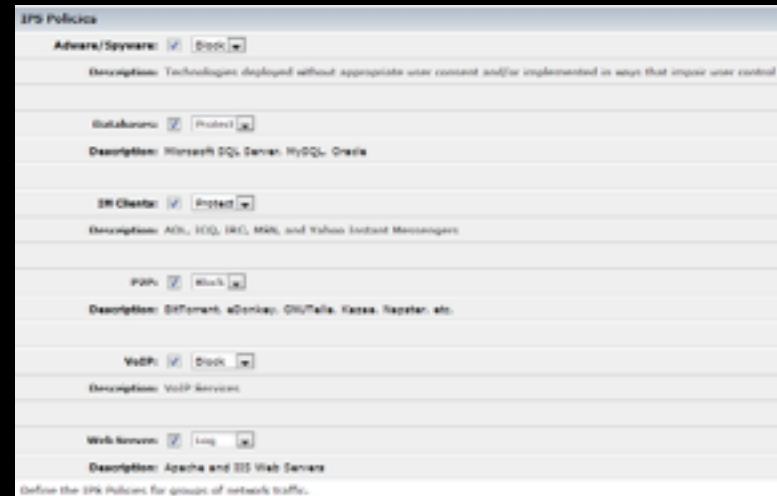
The screenshot shows a window titled "IPS Policies" with a light blue header. Below the header, there are several rows of configuration options, each with a label, a checkbox, and a description. The "Adware/Spyware" row has a checked checkbox and a "Log" dropdown menu. The other rows have unchecked checkboxes. The descriptions provide details about the technologies or services being configured.

Policy Name	Enabled	Description
Adware/Spyware	<input checked="" type="checkbox"/>	Technologies deployed without appropriate user consent and/or implemented in ways that impair user control
Databases	<input type="checkbox"/>	Microsoft SQL Server, MySQL, Oracle
IM Clients	<input type="checkbox"/>	AOL, ICQ, IRC, MSN, and Yahoo Instant Messengers
P2P	<input type="checkbox"/>	BitTorrent, eDonkey, GRUTella, Kazaa, Napster, etc.
VoIP	<input type="checkbox"/>	VoIP Services
Web Server	<input type="checkbox"/>	Apache and IIS Web Servers

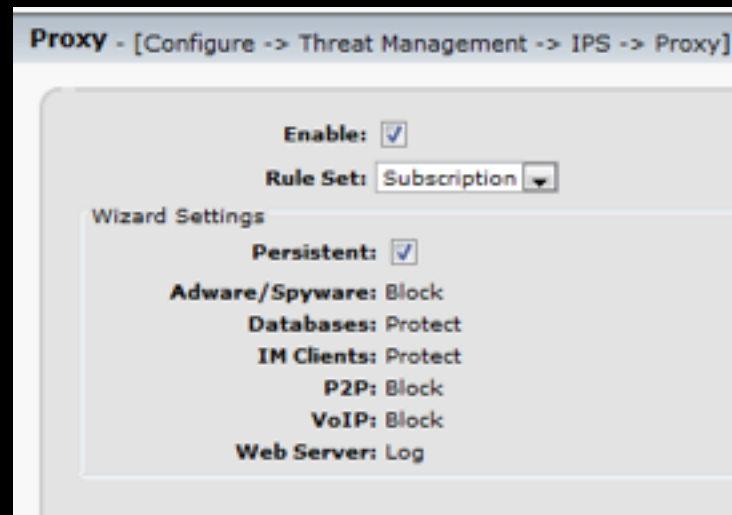
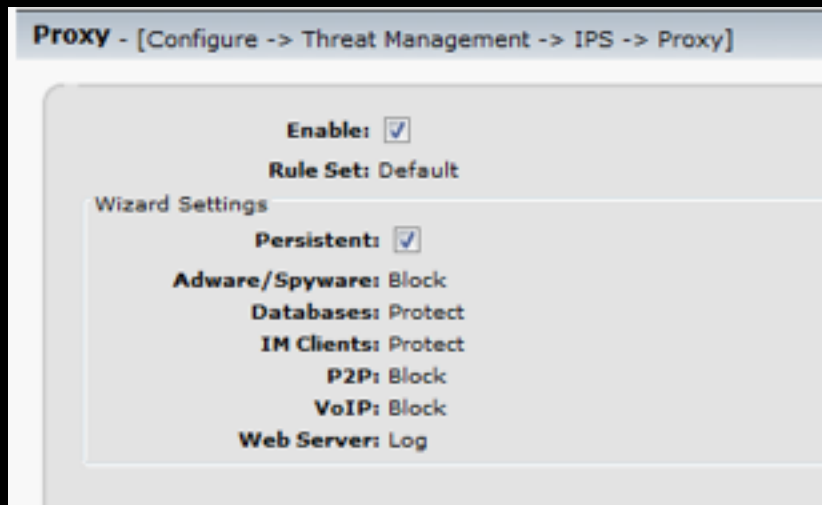
Wizard – 2 Steps

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

Welcome, fwadmin Filter Logout

Policies - [Configure -> Threat Management -> IPS -> Policies] 2011-10-05 13:18:38 EDT (-0400)

Filter

Row: 1 / 1345 ↓ ↑ Rows Per Page: 50

Column - Enable

Filter:

Field: Yes

Policies

Index	Enable	Log	Alarm	Action	Group	Name
1	Yes	Yes	No	Pass	Attack Response	IRC - Channel JOIN on non-std port
2	Yes	Yes	No	Pass	Attack Response	IRC - channel join on non-std port
3	Yes	Yes	No	Pass	Attack Response	IRC - DCC chat request on non-std port
4	Yes	Yes	No	Pass	Attack Response	IRC - DCC file transfer request on non-std port
5	Yes	Yes	No	Pass	Attack Response	IRC - dns request on non-std port
6	Yes	Yes	No	Pass	Attack Response	IRC - Name response on non-std port
7	Yes	Yes	No	Pass	Attack Response	IRC - Nick change on non-std port
8	Yes	Yes	No	Pass	Attack Response	IRC - Private message on non-std port

- Persistent – while enable the Policies are non-editable

IPS Wizard

Step 2 -

- Enable IPS on
 - Policiesor
 - 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.

This screenshot shows the configuration page for a security policy. The 'Enabled' checkbox is checked. The description is 'Allow Remote Desktop with VPN'. The service is set to 'RDP', and the source and destination are both 'ANY_IP'. The 'Automatic Accept All Policy' checkbox is checked. Under the 'Options' section, 'Authentication Required' is unchecked, 'IPS' is checked, and 'VPN Coexist' is unchecked.

This screenshot shows the configuration page for a tunnel. The 'Enabled' checkbox is unchecked. The description is 'Default: Allow protected interface access to anywhere.'. The type is 'Accept', the interface is 'Protected', the service is 'ANY_SERVICE', the time group is 'ANYTIME', and both source and destination addresses are 'ANY_IP'. Under the 'Options' section, 'Priority' is 'Inherit' and 'NAT' is 'Default NAT'. Under the 'Action' section, 'IPS' is checked and 'Alerts' is unchecked.

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

The screenshot displays the 'Policies' management interface. At the top, there are navigation buttons: 'Default', 'Filter', 'Reset', and 'Save'. The breadcrumb path is 'Policies - [Threat Management -> IPS -> Policies]' and the timestamp is '2007-04-21 06:53:46 EST (+1000)'. Below the navigation is a 'Filter' section with 'Row: 1 / 4132' and 'Rows Per Page: 30'. An 'Advanced' button is visible on the right. The 'Column' dropdown is set to 'Name'. The 'Filter' checkbox is checked, 'NDT' is unchecked, and the 'Field' is set to 'Contains' with the search term 'Spy' entered in the adjacent text box. Below the filter section is a table of policies with columns for Index, Enable, Log, Alarm, Action, Name, ID, and Group.

Index	Enable	Log	Alarm	Action	Name	ID	Group
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Drop	Toggle values of all visible policies		
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	ATTACK-RESPONSES 403 Forbidden	1201	Attack Responses
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	ATTACK-RESPONSES Invalid URL	1200	Attack Responses
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	ATTACK-RESPONSES Microsoft cmd.exe banner	2123	Attack Responses
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	ATTACK-RESPONSES command completed	494	Attack Responses

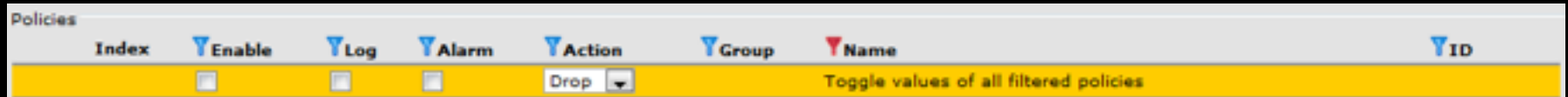
Multiple search criteria can be used.

Display option allows 50, 100, 500, ALL

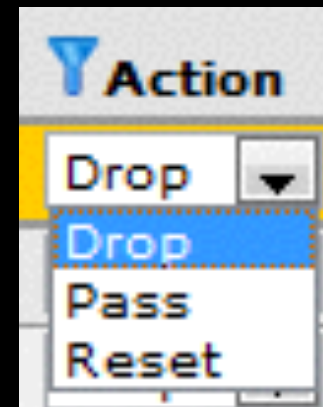
Page ICON moves to the next page.

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

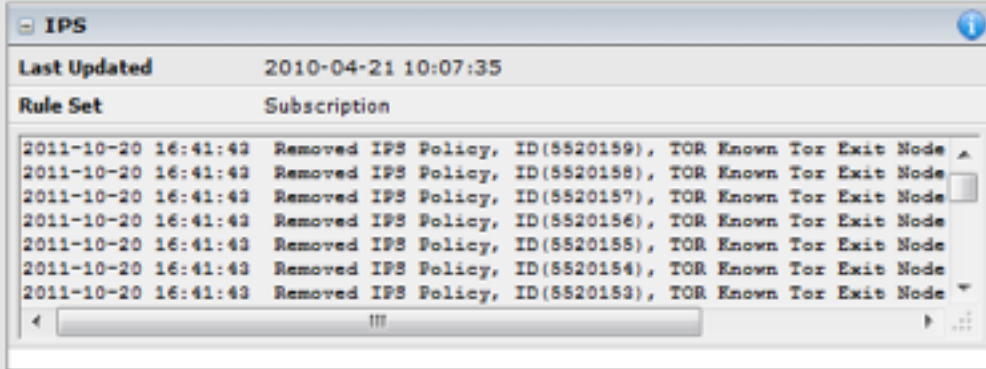
- Overview -> IPS – Displays IPS enabled or disabled and Rule Set Used – Subscription or Default (loaded in config)
- Monitor-> Activity -> Threat Management -> IPS] : Display any updates automatically downloaded when using Subscription set.
- System -> Overview -> IPS : smaller set of logs show updates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

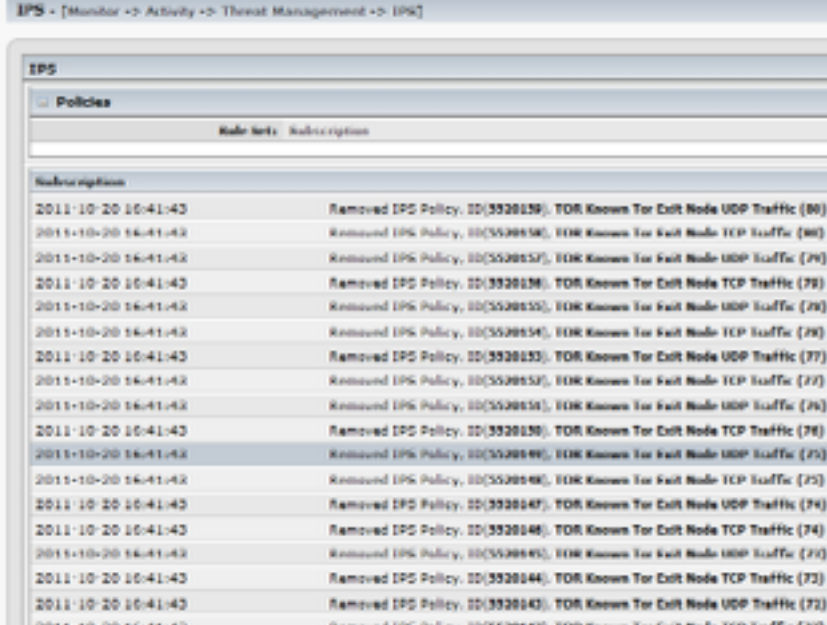
System Overview



IPS

Last Updated: 2010-04-21 10:07:35

Rule Set	Subscription
2011-10-20 16:41:43	Removed IPS Policy, ID(5520159), TOR Known Tor Exit Node
2011-10-20 16:41:43	Removed IPS Policy, ID(5520158), TOR Known Tor Exit Node
2011-10-20 16:41:43	Removed IPS Policy, ID(5520157), TOR Known Tor Exit Node
2011-10-20 16:41:43	Removed IPS Policy, ID(5520156), TOR Known Tor Exit Node
2011-10-20 16:41:43	Removed IPS Policy, ID(5520155), TOR Known Tor Exit Node
2011-10-20 16:41:43	Removed IPS Policy, ID(5520154), TOR Known Tor Exit Node
2011-10-20 16:41:43	Removed IPS Policy, ID(5520153), TOR Known Tor Exit Node



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

IPS

Policies

Rule Set	Subscription
2011-10-20 16:41:43	Removed IPS Policy, ID(5520158), TOR Known Tor Exit Node UDP Traffic (80)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520158), TOR Known Tor Exit Node TCP Traffic (80)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520157), TOR Known Tor Exit Node UDP Traffic (79)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520156), TOR Known Tor Exit Node TCP Traffic (79)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520155), TOR Known Tor Exit Node UDP Traffic (78)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520154), TOR Known Tor Exit Node TCP Traffic (78)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520153), TOR Known Tor Exit Node UDP Traffic (77)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520152), TOR Known Tor Exit Node TCP Traffic (77)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520151), TOR Known Tor Exit Node UDP Traffic (76)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520150), TOR Known Tor Exit Node TCP Traffic (76)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520149), TOR Known Tor Exit Node UDP Traffic (75)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520148), TOR Known Tor Exit Node TCP Traffic (75)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520147), TOR Known Tor Exit Node UDP Traffic (74)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520146), TOR Known Tor Exit Node TCP Traffic (74)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520145), TOR Known Tor Exit Node UDP Traffic (73)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520144), TOR Known Tor Exit Node TCP Traffic (73)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520143), TOR Known Tor Exit Node UDP Traffic (72)
2011-10-20 16:41:43	Removed IPS Policy, ID(5520142), TOR Known Tor Exit Node TCP Traffic (72)

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

Using Log to search IPS

Default Filter Reset Save

Policies - [Threat Management -> IPS -> Policies] 2007-07-25 16:59:16 EDT (-0400)

Filter

Row: 1 / 1 Rows Per Page: 50

Advanced

Column - ID

Filters:

NOT:

Field: Equals 5002192

Policies

	Index	Enable	Log	Alarm	Action	Group	Name	ID
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Drop		Toggle values of all filtered policies	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pass	P2P/Chat	MSN status change	5002192

GTA IPS Web Page

GTA Threat Viewer - Windows Internet Explorer


http://ips.gta.com/viewref.php?id=5001972

Google

Go + M + Bookmarks + 306 blocked + Check + AutoLink + AutoFill + Send to + Settings +

Norton AntiVirus

GTA Threat Viewer

 **Global
Technology
Associates, Inc.**

Threat Management Center
Intrusion Prevention System Threat Information

Threat ID: 5001972
Name: Network Scan - Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection

Description
For a detail description of the threat please investigate the links below

Detailed References
No references

Threat ID:

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
 - TELNET
 - HTTP

The screenshot displays the 'Performance Tuning' configuration page, organized into four main sections: Networks, External Servers, Internal Servers, and Services. Each section contains several dropdown menus for configuration.

- Networks:** External: <ANY_IP>, Protected: ANY_IP
- External Servers:** AIM: AIM Server List
- Internal Servers:** DNS: ANY_IP, Email: ANY_IP, SNMP: ANY_IP, Telnet: ANY_IP, Web: ANY_IP
- Services:** DNS: DNS lookups, FTP: FTP, Email: SMTP, SSH: SSH, Telnet: TELNET, Web: 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.



**Global
Technology
Associates, Inc.**

Internet Firewall Developer since 1994

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