cressida™ Software To Be Sure *presents:*

NitroSecurity Intrusion Prevention Overview for OSSIR (Groupe SUR)

Marc Berlow, Cressida France

nitrosecurity

January 11, 2005

Cressida Int'l Company History

- **Created by Systems Administration and Security Experts in 2001**
- **Distributes and supports software across all European markets**

- **Main products:**
  - NitroSecurity Suite
    - Intrusion Prevention Systems
  - Ecora
    - Configuration & Change Reporting, Baseline & Compare settings, Automated Patch Management, Devices Security
  - Akonix
    - Real time solutions for Secure, Managed, Productive Enterprise Instant Messaging
  - MQ Message Assurance
    - Track, Record, Audit, Replay, Edit WMQ Messages
  - RepliWeb
    - Industrialized Strength Disaster Recovery cross platform tool, replication, distribution, synchronization

NitroSecurity Company History

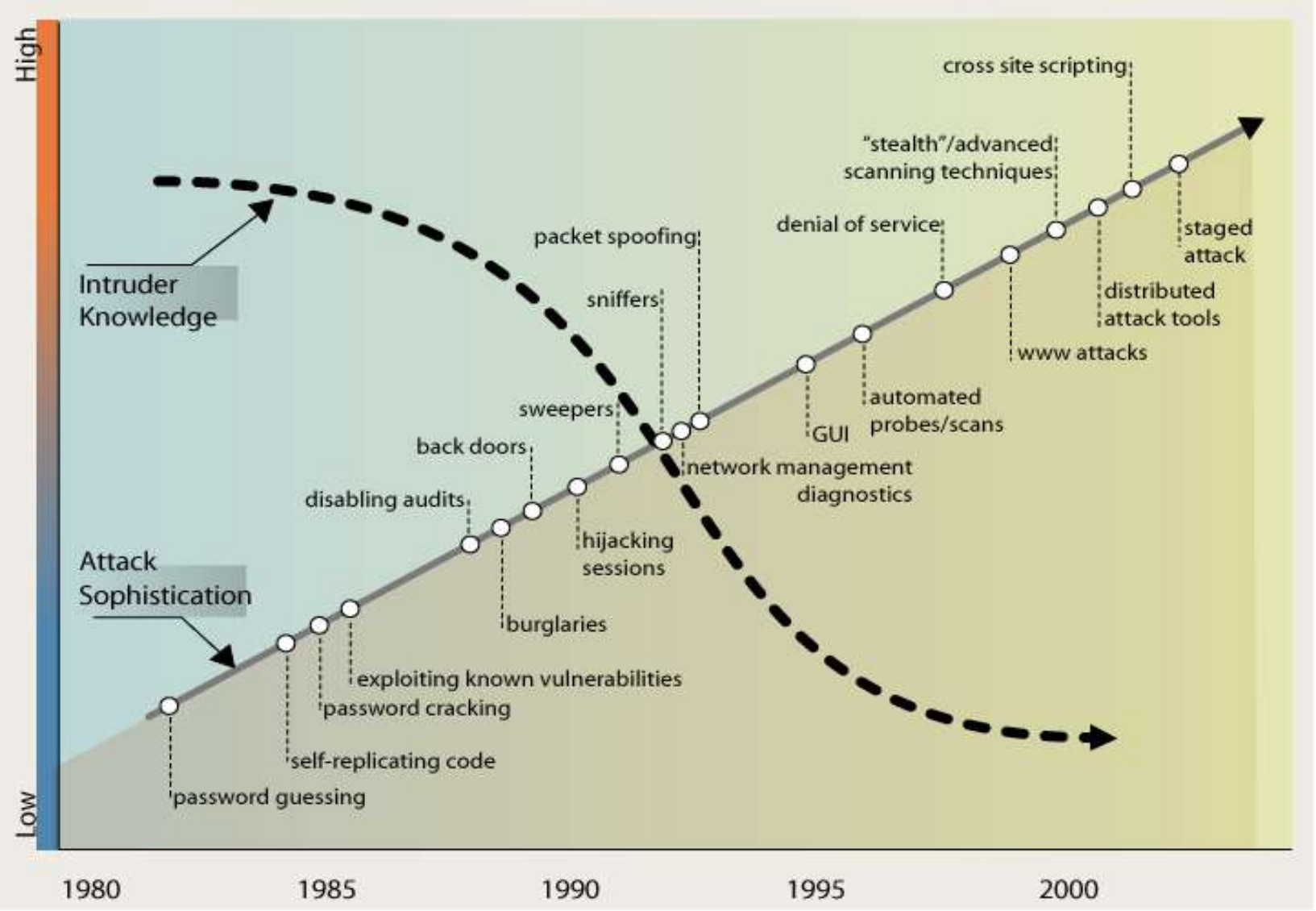
Technology origins U.S. Department of Energy's Idaho National Engineering and Environmental Laboratory (INEEL) (Sister to Los Alamos, Sandia, Oakridge)

Products

- **NitroEDB- High performance embedded relational database**
  - Built to handle exact, high speed data demands of nuclear power industry
  - $30M and 65 man years invested
  - Commercialized in 1999 for the OEM community
- **NitroGuard IPS-In line intrusion prevention solution**
  - Open Source Debut in 2001 at DEFCON
  - Commercialized in 4th Quarter of 2001
  - 2002 version 3.0 introduced new Technologies for Detection, Analysis including integrating in-line SNORT, and Remote Communications
  - 2003 version 4.0 introduced improved Device Analysis and more comprehensive Management Console queries and analysis capabilities

nitrosecurity

So many attacks, so little time…



NitroGuard Concepts

- **Next Generation Network-Based Intrusion Prevention System**
  - No client agents
  - No version management or interoperability issues
  - Scalable to any size enterprise
- **Ultra-fast database**
  - Same database used to correlate data from all U.S nuclear power plants
  - Highly scalable
  - Technology embedded in upcoming Cisco monitoring products
- **Enterprise management console**
  - Enterprise wide correlation from all IPSs
  - Robust reporting

A Layered Security Approach

Security Threat	Firewall	Antivirus	NitroSecurity
Limits access to parts of the network	FULL		FULL
Translates internal addresses to external addresses	FULL		No IP Address
Protects against virus attacks		FULL	PARTIAL
Protects against worms		FULL	PARTIAL
Protects against combination worm/intrusion attacks (Nimda, CodeRed)		PARTIAL	FULL
Protects against intrusion			*FULL
Prevents outbound attacks			*FULL
Prevents outbound critical data loss			*FULL
Enforces policy rules (porn, gambling, webmail, IM, etc)			*FULL
Logs intrusion alerts for post-analysis			*FULL

NitroGuard Security Architecture

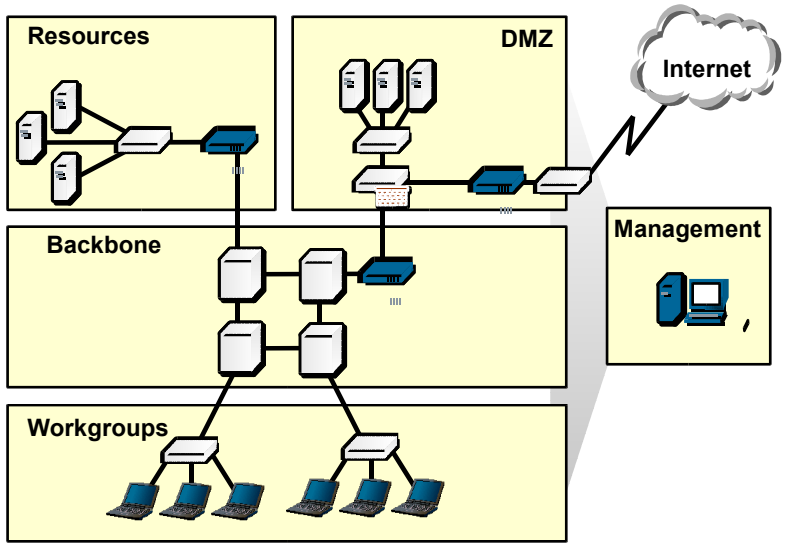
nitrosecurity

NitroSecurity IPS Family

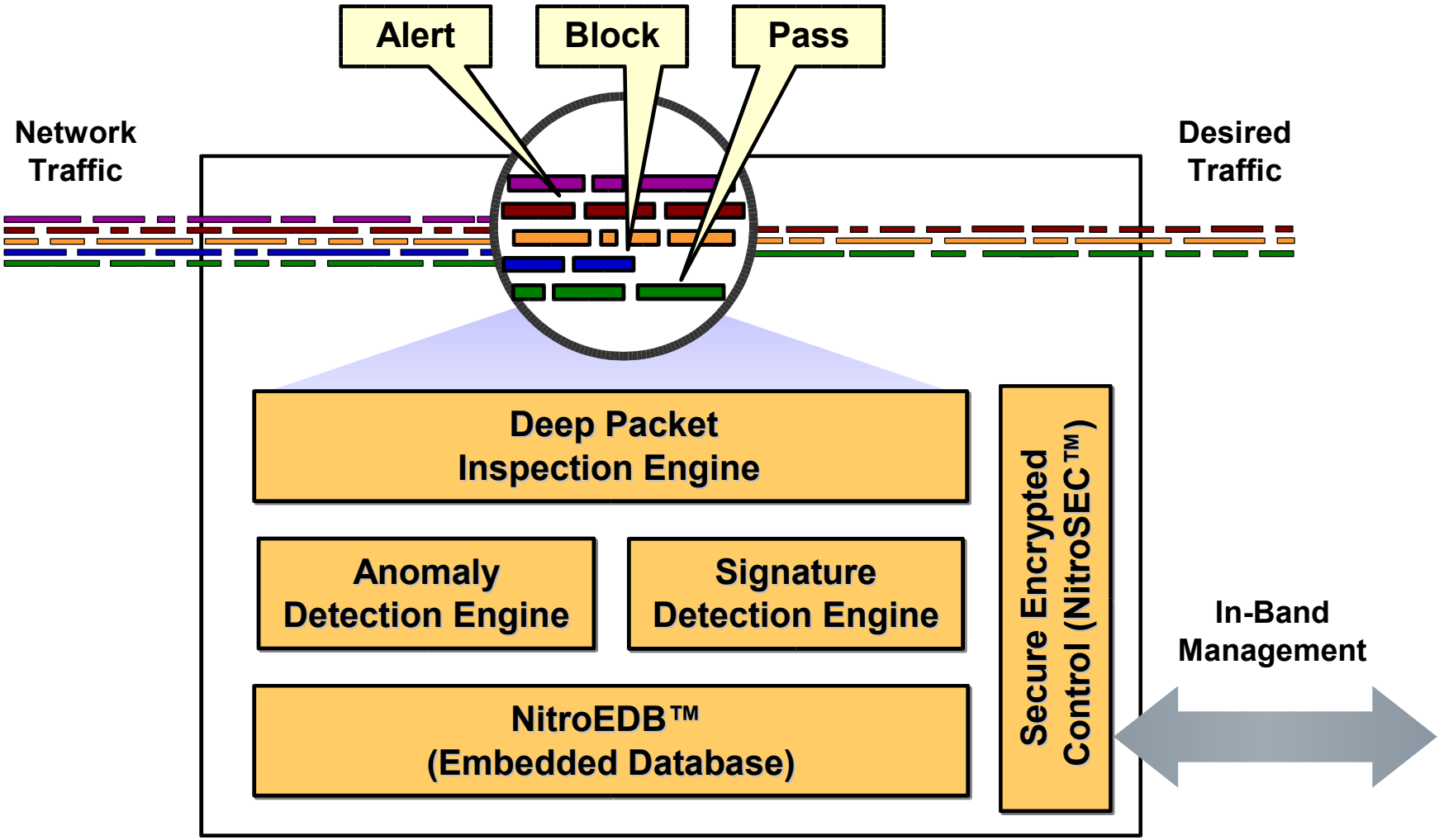
- **Enterprise-Scale, In-line IPS**
  - Active (IPS) or promiscuous (IDS) mode in single device
  - Real-time event correlation and analysis across entire enterprise via embedded security database architecture
- **Integrated Signature/Anomaly Detection**
  - Industry's largest signature (3600+) library
  - Fully customizable signatures/reports
  - Protocol and behavioral anomaly support
- **Stealth Operation Mode**
  - Industry's only IPS that has no IP address using in-band management
  - Invisible to typical network attacks

NitroSecurity IPS

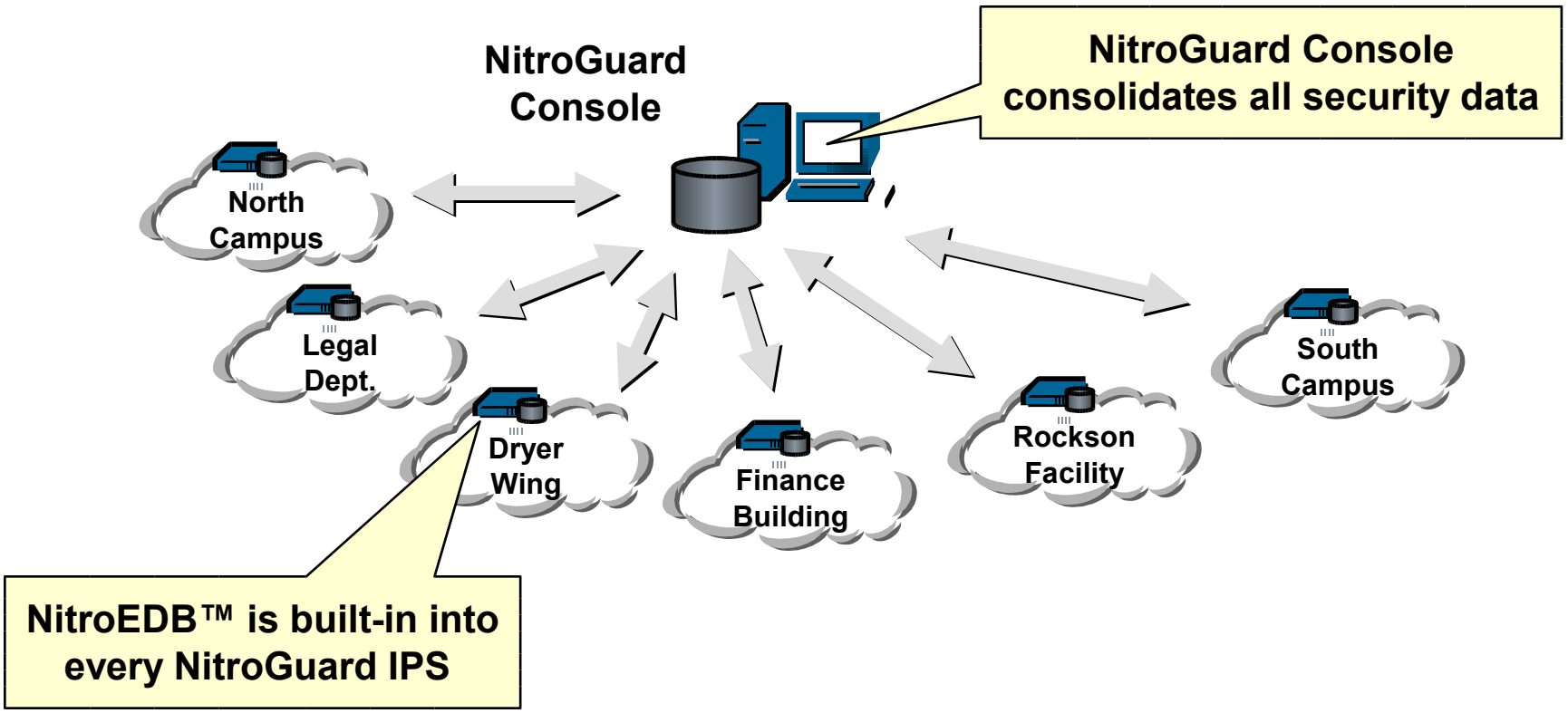
Hardware either supplied by NitroSecurity or purchased based on exact specifications



NitroSecurity IPS Architecture

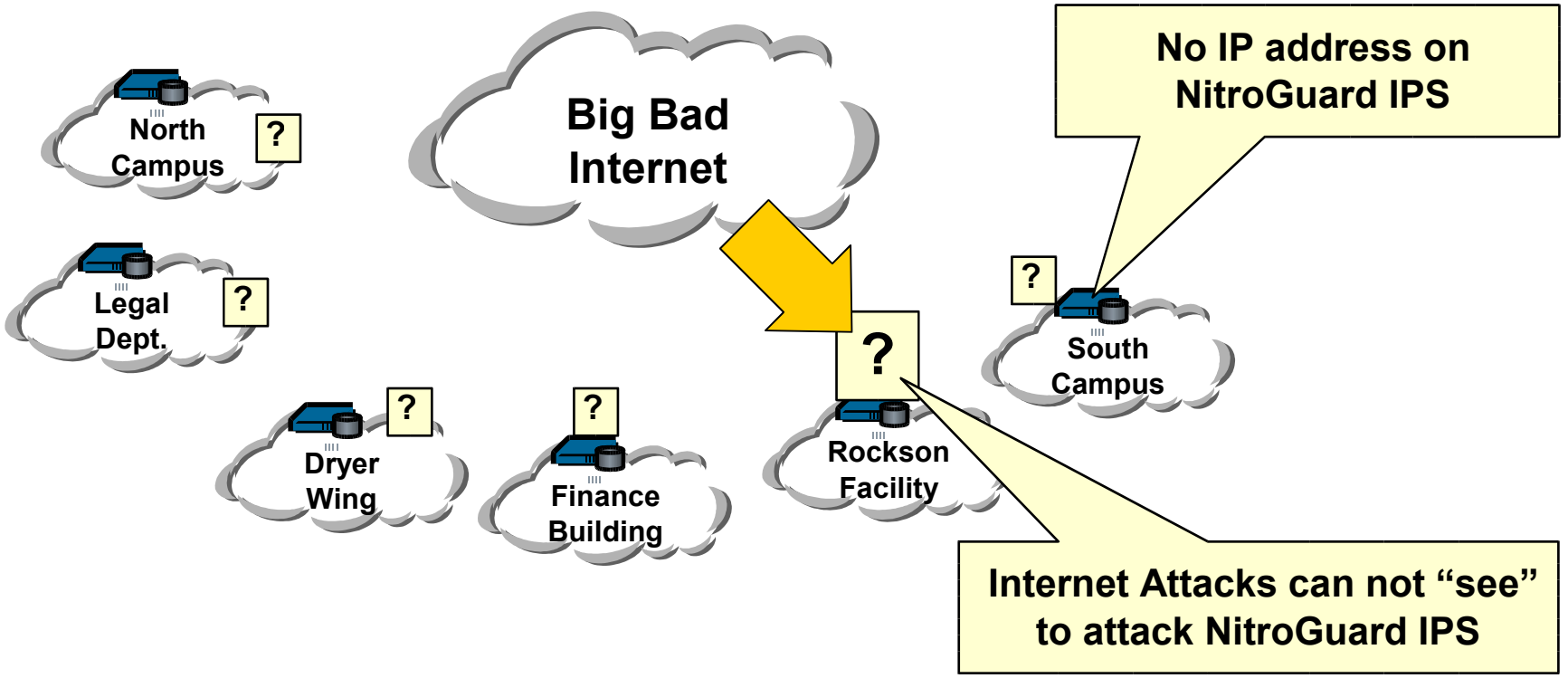


NitroEDB™ Overview



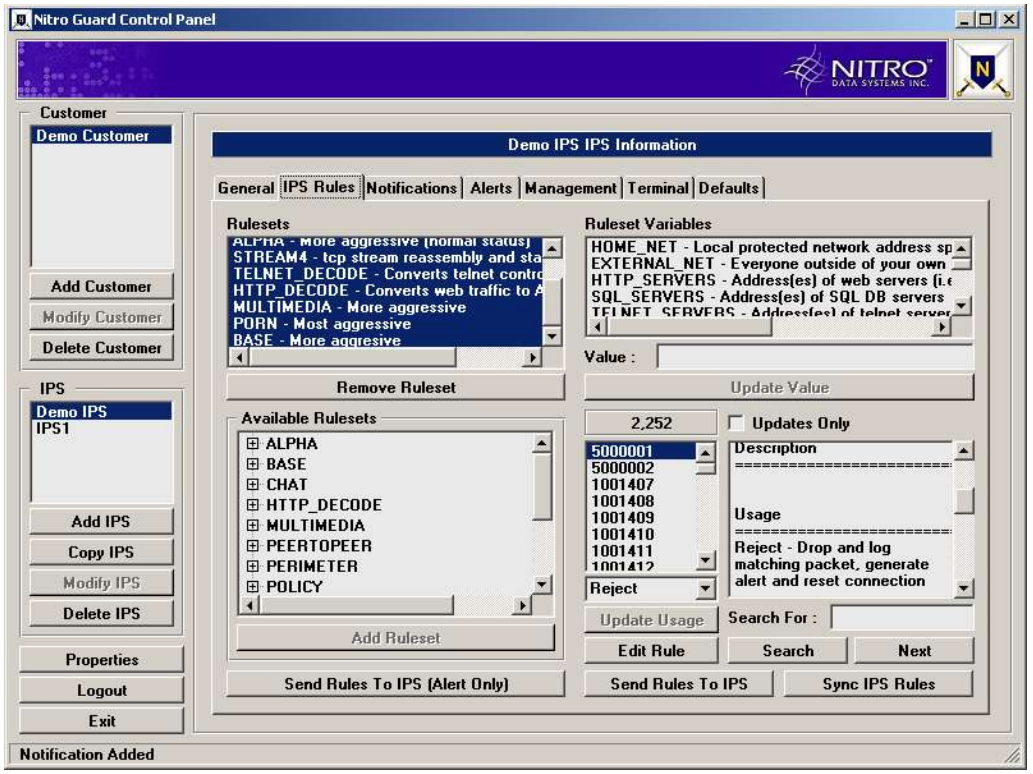
- NitroEDB™ enables real-time, enterprise-wide correlation of security data across an unlimited number of NitroGuard IPS
- Traditional IPS designs decrease in performance and correlation capabilities as security data increases

NitroSEC™ Overview

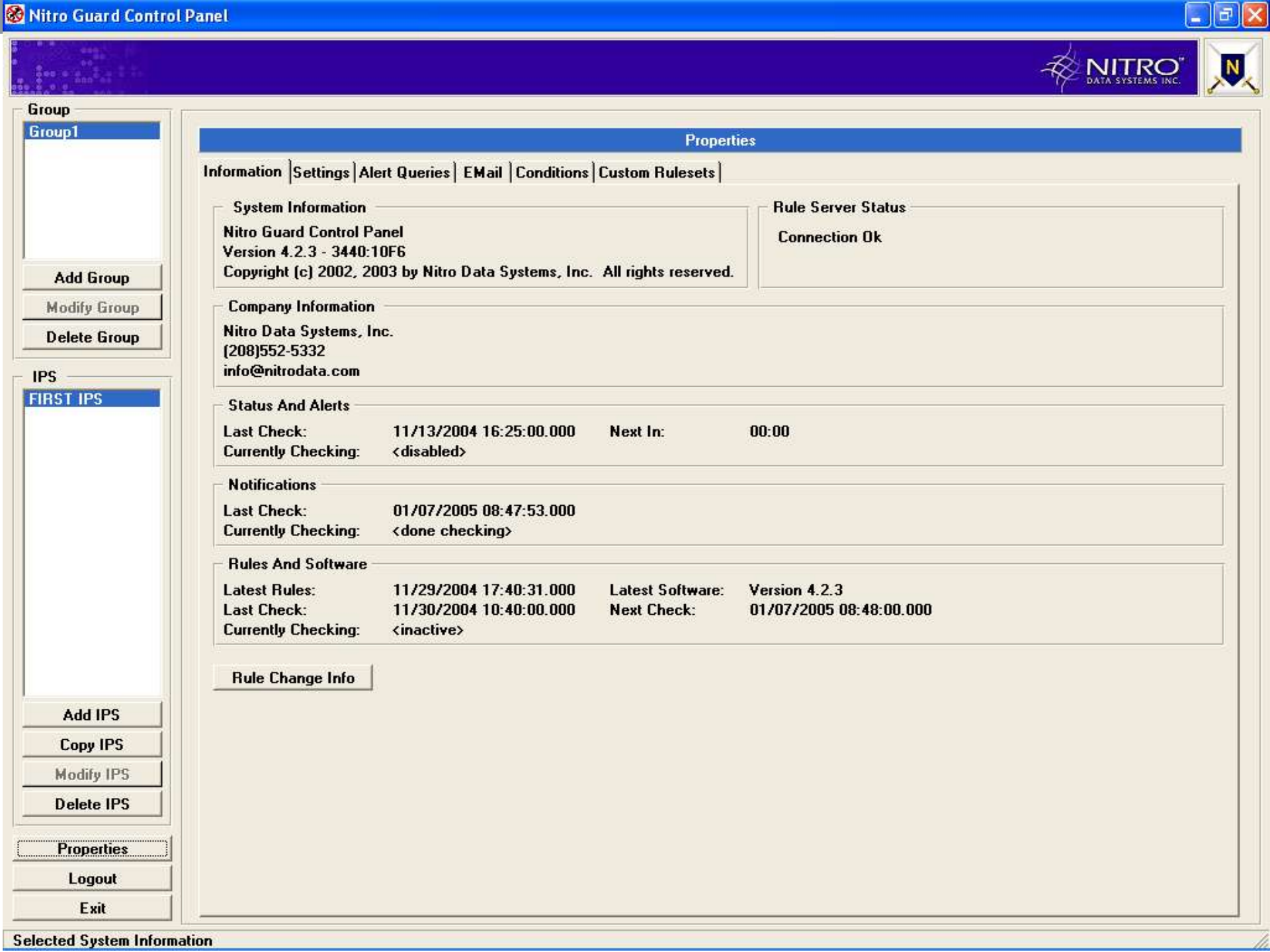


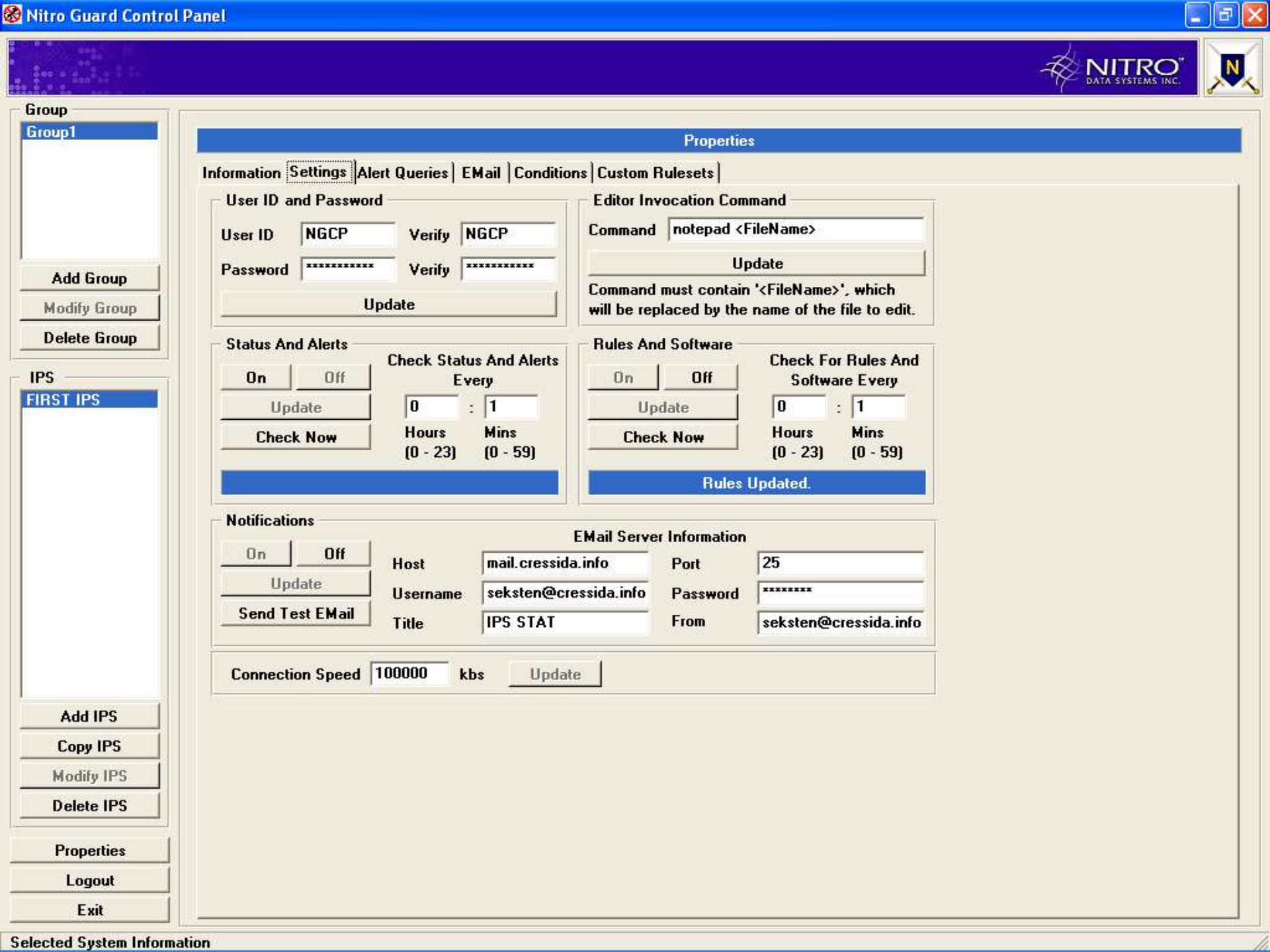
- NitroSEC™ makes NitroGuard IPS virtually impossible to attack (and does not require out-of-band management)
- Traditional IPS designs use an IP address for management (or require an out-of-band management interface and network)

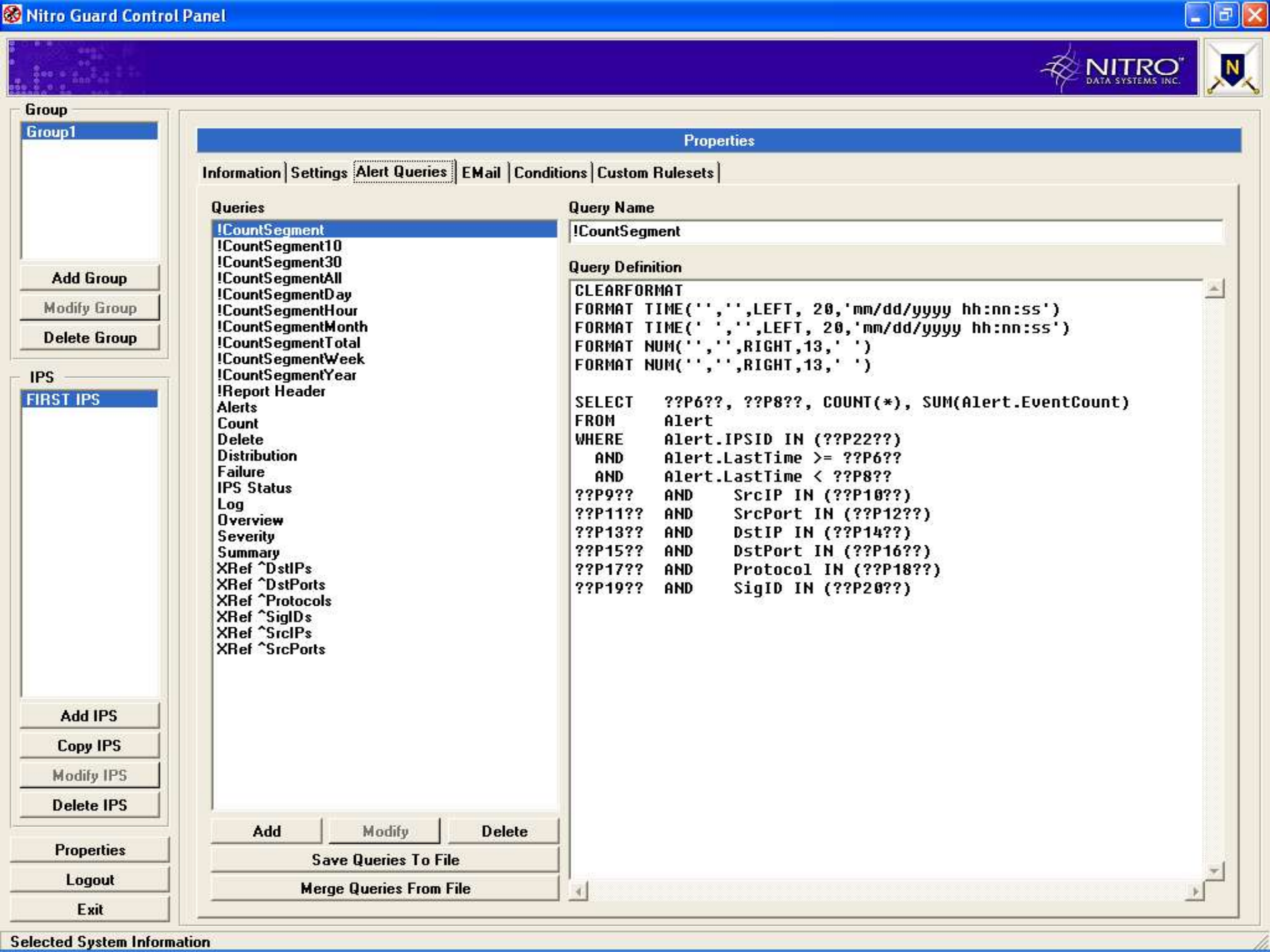
NitroSecurity Demonstration

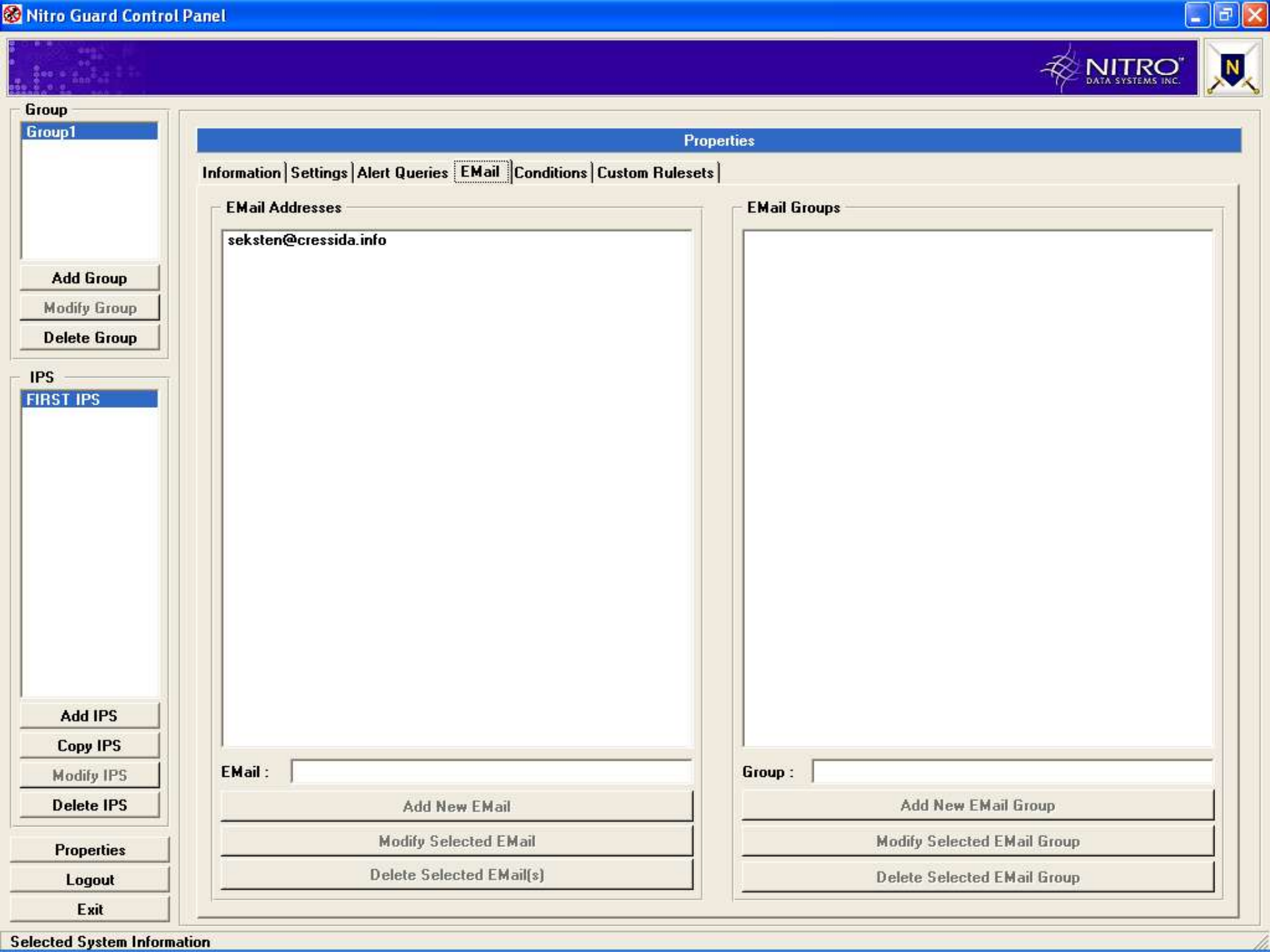


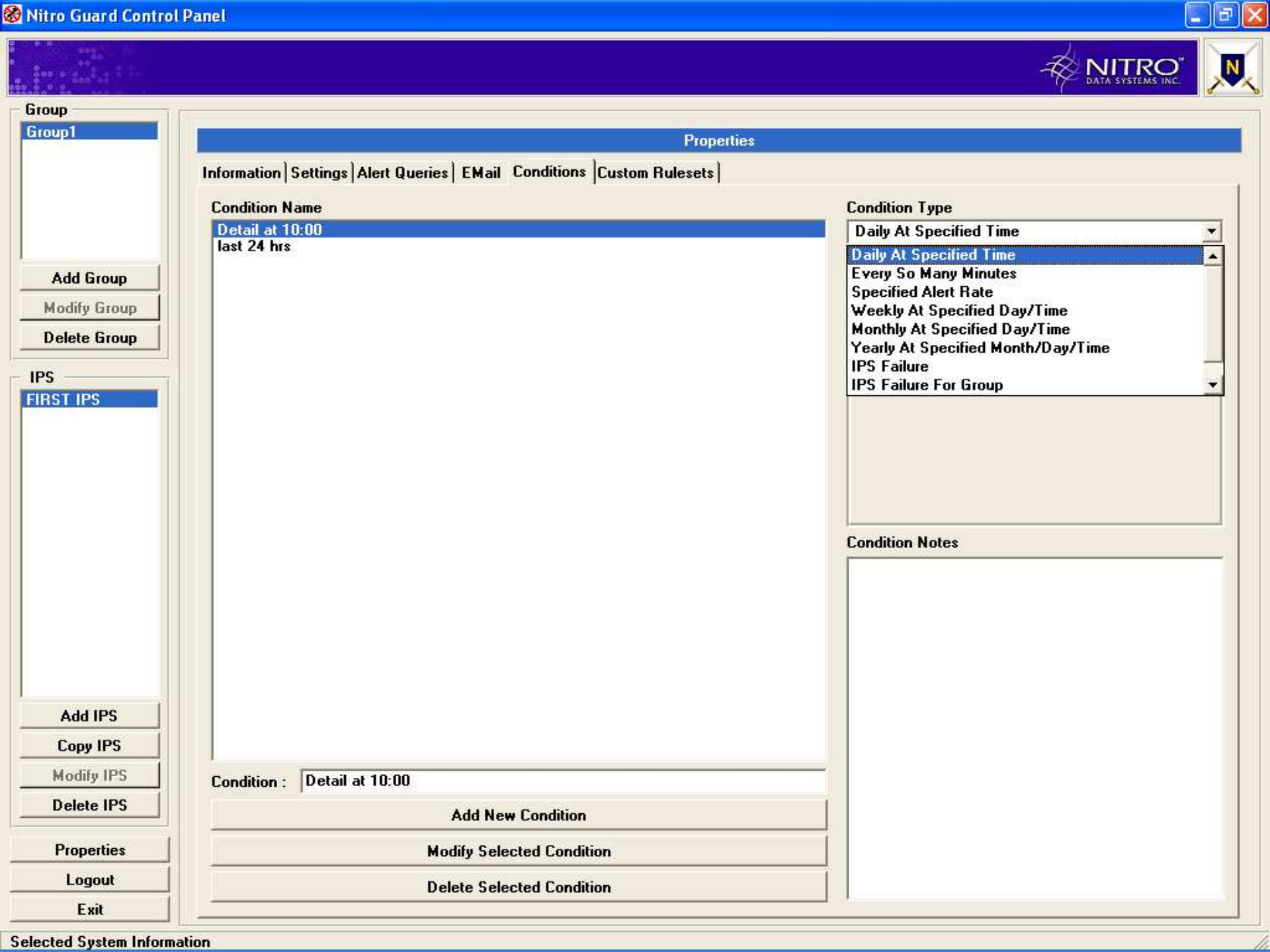
Please contact us at www.cressida.info for a live demo

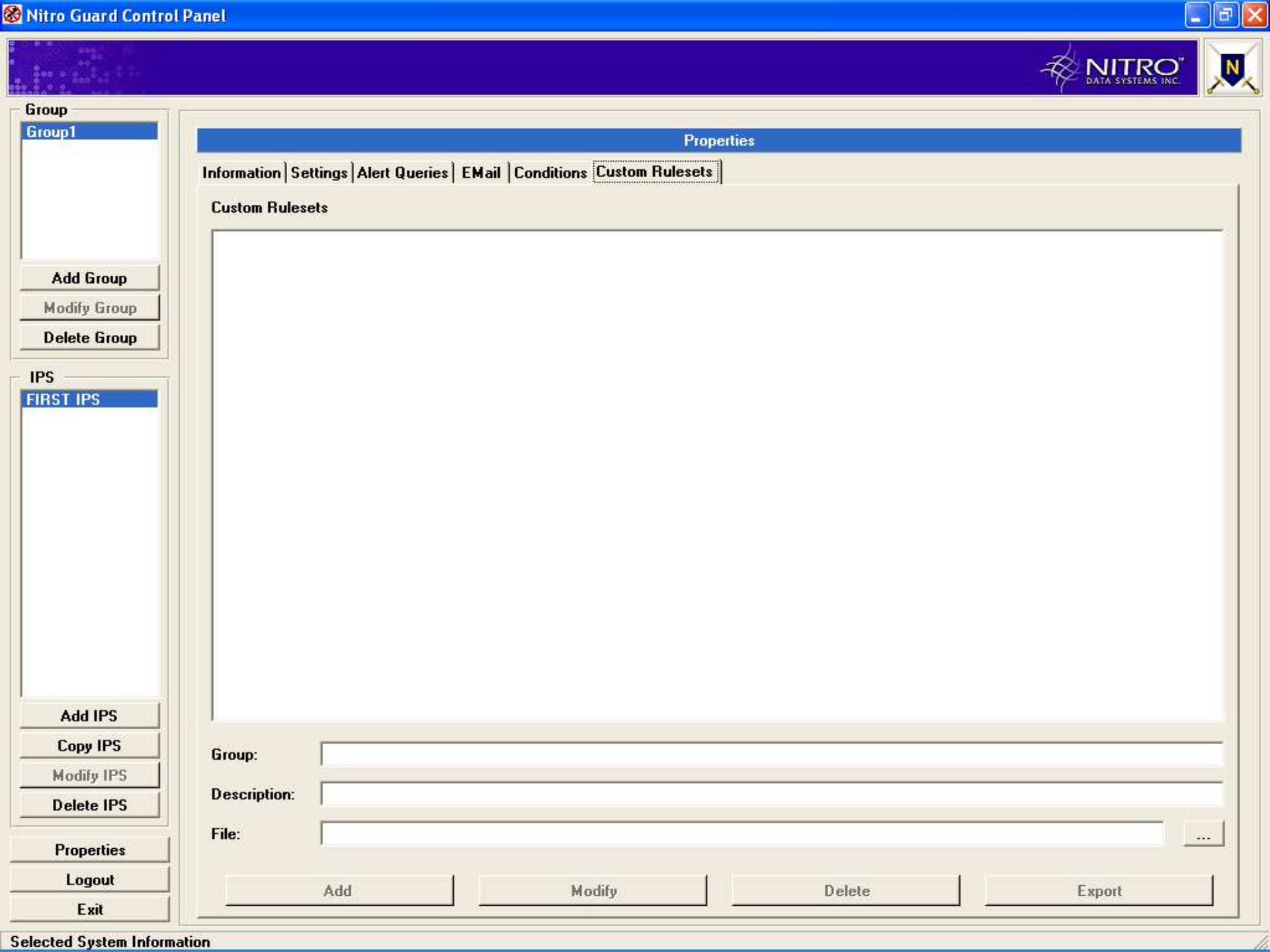

Nitro Guard Control Panel
NITRO
DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
Properties
Information
Settings
Alert Queries
EMail
Conditions
Custom Rulesets
System Information
Nitro Guard Control Panel
Version 4.2.3 - 3440:10F6
Copyright (c) 2002, 2003 by Nitro Data Systems, Inc. All rights reserved.
Rule Server Status
Connection Ok
Company Information
Nitro Data Systems, Inc.
(208)552-5332
info@nitrodata.com
Status And Alerts
Last Check: 11/13/2004 16:25:00.000
Next In: 00:00
Currently Checking: <disabled>
Notifications
Last Check: 01/07/2005 08:47:53.000
Currently Checking: <done checking>
Rules And Software
Latest Rules: 11/29/2004 17:40:31.000
Latest Software: Version 4.2.3
Last Check: 11/30/2004 10:40:00.000
Next Check: 01/07/2005 08:48:00.000
Currently Checking: <inactive>
Rule Change Info
Selected System Information

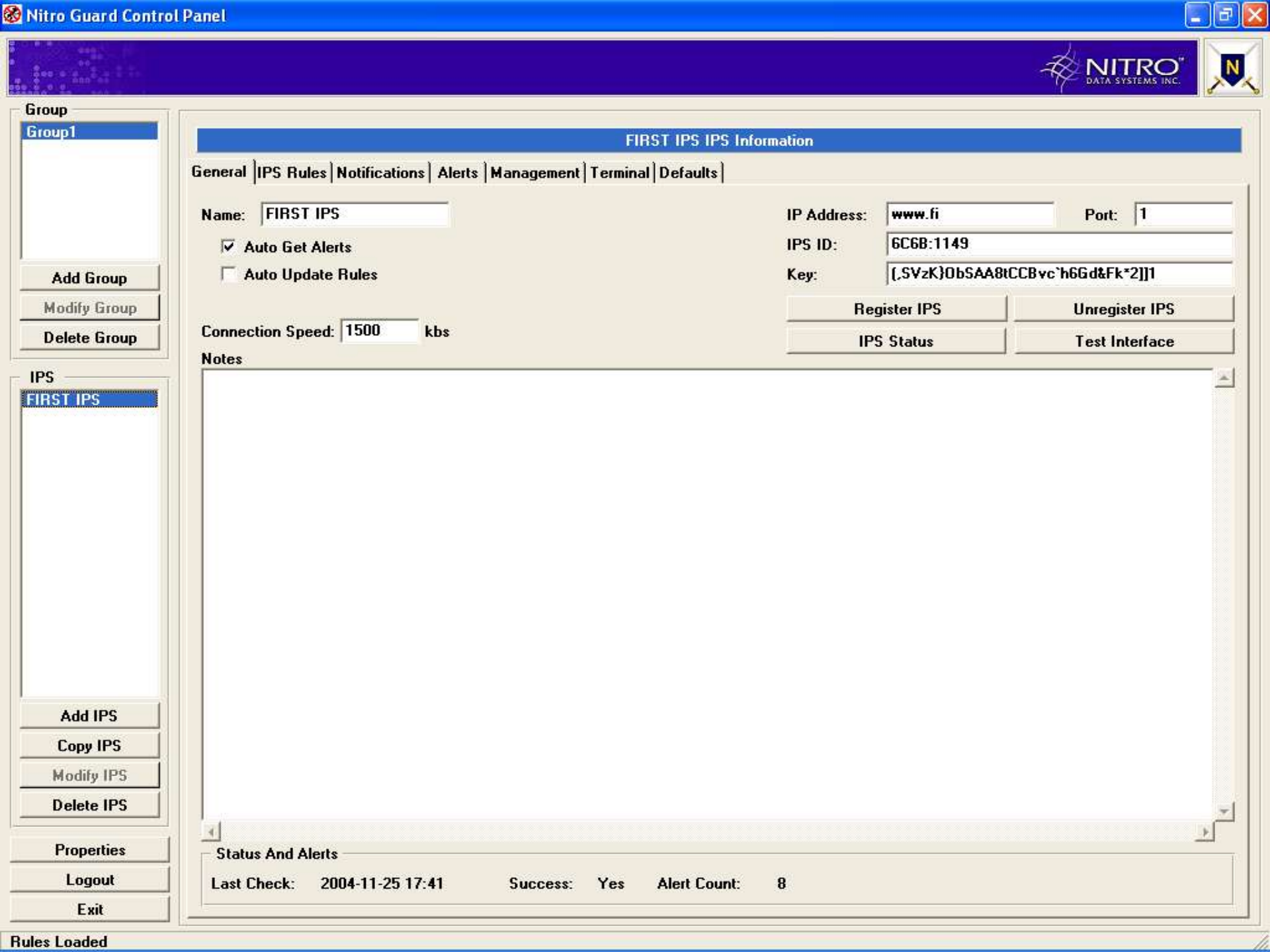

Nitro Guard Control Panel
NITRO DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
Properties
Information
Settings
Alert Queries
EMail
Conditions
Custom Rulesets
User ID and Password
User ID
NGCP
Verify
NGCP
Password
Verify
Update
Editor Invocation Command
Command
notepad <FileName>
Update
Command must contain '<FileName>', which will be replaced by the name of the file to edit.
Status And Alerts
On
Off
Update
Check Now
Check Status And Alerts Every
0
1
Hours (0 - 23)
Mins (0 - 59)
Rules And Software
On
Off
Update
Check Now
Check For Rules And Software Every
0
1
Hours (0 - 23)
Mins (0 - 59)
Rules Updated.
Notifications
On
Off
Update
Send Test EMail
EMail Server Information
Host
mail.cressida.info
Port
25
Username
seksten@cressida.info
Password
Title
IPS STAT
From
seksten@cressida.info
Connection Speed
100000
kbs
Update
Selected System Information

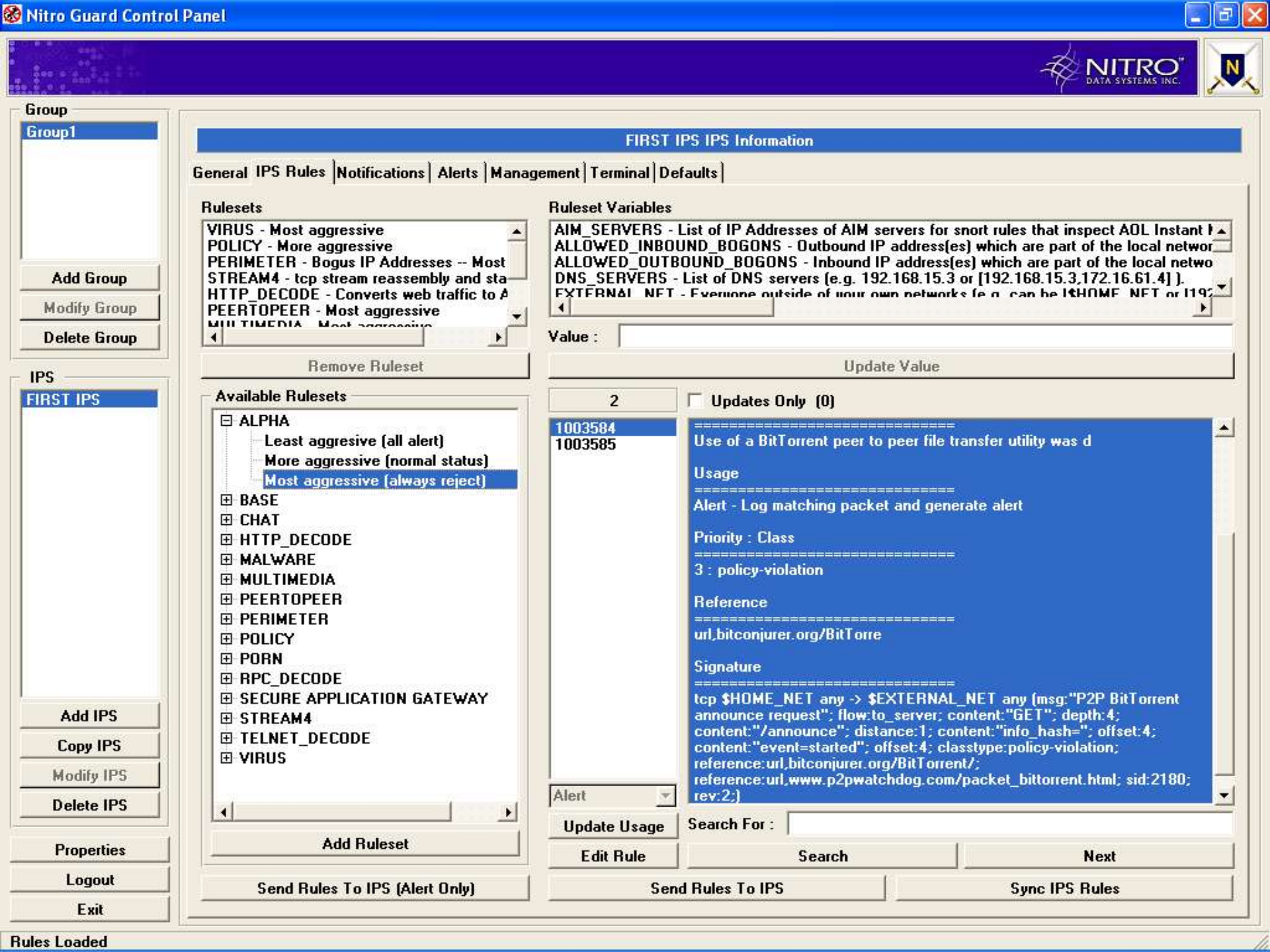

Nitro Guard Control Panel
NITRO
DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
Properties
Information
Settings
Alert Queries
EMail
Conditions
Custom Rulesets
Queries
!CountSegment
!CountSegment10
!CountSegment30
!CountSegmentAll
!CountSegmentDay
!CountSegmentHour
!CountSegmentMonth
!CountSegmentTotal
!CountSegmentWeek
!CountSegmentYear
!Report Header
Alerts
Count
Delete
Distribution
Failure
IPS Status
Log
Overview
Severity
Summary
XRef ^DstIPs
XRef ^DstPorts
XRef ^Protocols
XRef ^SigIDs
XRef ^SrcIPs
XRef ^SrcPorts
Add
Modify
Delete
Save Queries To File
Merge Queries From File
Query Name
!CountSegment
Query Definition
CLEARFORMAT
FORMAT TIME('','',LEFT, 20,'mm/dd/yyyy hh:nn:ss')
FORMAT TIME(' ','',LEFT, 20,'mm/dd/yyyy hh:nn:ss')
FORMAT NUM('','',RIGHT,13,' ')
FORMAT NUM('','',RIGHT,13,' ')
SELECT ??P6??, ??P8??, COUNT(*), SUM(Alert.EventCount)
FROM Alert
WHERE Alert.IPSID IN (??P22??)
AND Alert.LastTime >= ??P6??
AND Alert.LastTime < ??P8??
??P9?? AND SrcIP IN (??P10??)
??P11?? AND SrcPort IN (??P12??)
??P13?? AND DstIP IN (??P14??)
??P15?? AND DstPort IN (??P16??)
??P17?? AND Protocol IN (??P18??)
??P19?? AND SigID IN (??P20??)
Selected System Information

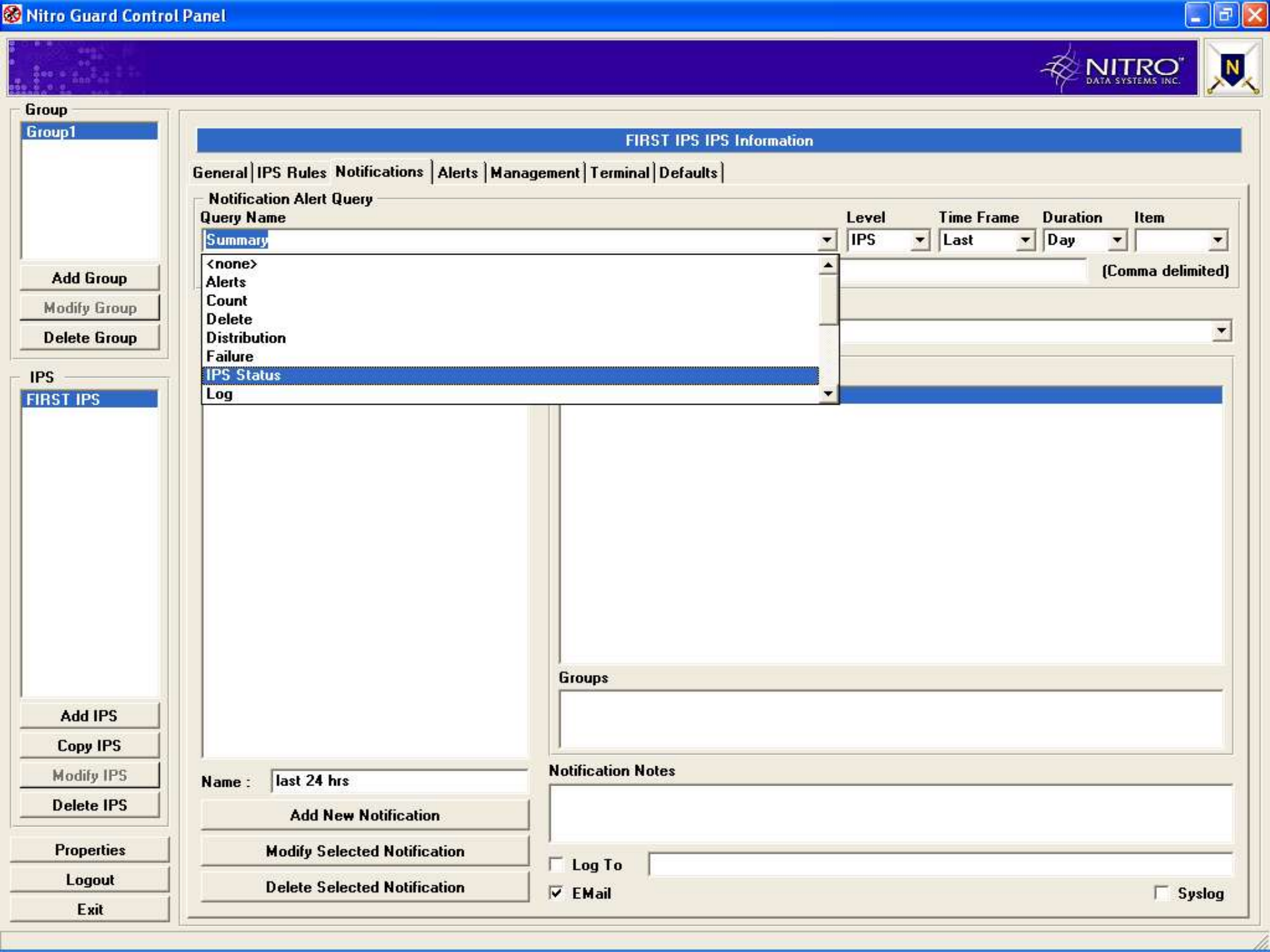

Nitro Guard Control Panel
NITRO
DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
Properties
Information
Settings
Alert Queries
EMail
Conditions
Custom Rulesets
EMail Addresses
seksten@cressida.info
EMail :
Add New EMail
Modify Selected EMail
Delete Selected EMail(s)
EMail Groups
Group :
Add New EMail Group
Modify Selected EMail Group
Delete Selected EMail Group
Selected System Information

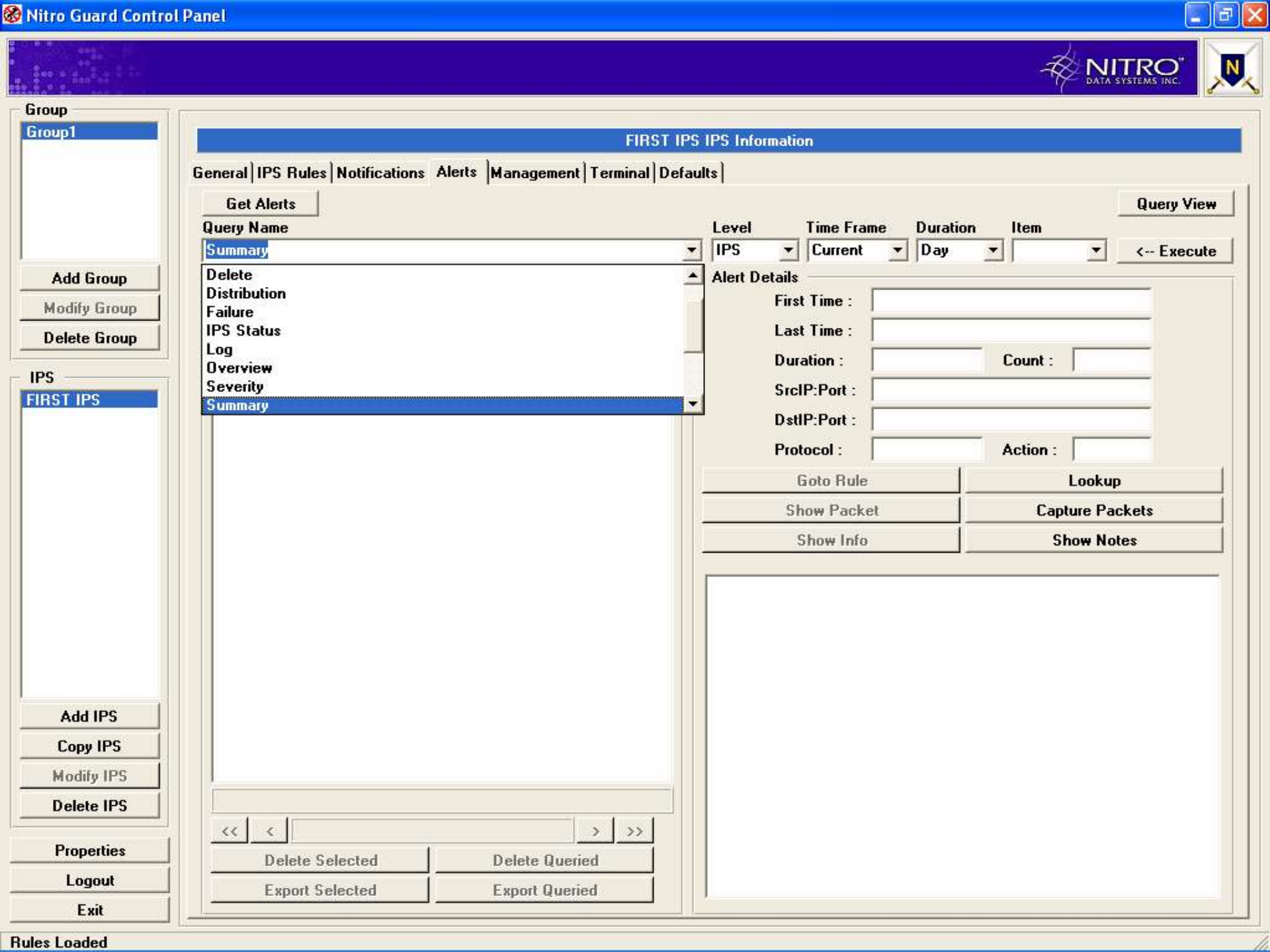

Nitro Guard Control Panel
NITRO
DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
Properties
Information
Settings
Alert Queries
EMail
Conditions
Custom Rulesets
Condition Name
Detail at 10:00
last 24 hrs
Condition :
Detail at 10:00
Add New Condition
Modify Selected Condition
Delete Selected Condition
Condition Type
Daily At Specified Time
Daily At Specified Time
Every So Many Minutes
Specified Alert Rate
Weekly At Specified Day/Time
Monthly At Specified Day/Time
Yearly At Specified Month/Day/Time
IPS Failure
IPS Failure For Group
Condition Notes
Selected System Information


Nitro Guard Control Panel
NITRO
DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
Properties
Information
Settings
Alert Queries
EMail
Conditions
Custom Rulesets
Custom Rulesets
Group:
Description:
File:
...
Add
Modify
Delete
Export
Selected System Information


Nitro Guard Control Panel
NITRO
DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
FIRST IPS IPS Information
General
IPS Rules
Notifications
Alerts
Management
Terminal
Defaults
Name: FIRST IPS
Auto Get Alerts
Auto Update Rules
Connection Speed: 1500 kbs
IP Address: www.fi
Port: 1
IPS ID: 6C6B:1149
Key: (.SVzK}ObSAA8tCCBvc`h6Gd&Fk*2]]1
Register IPS
Unregister IPS
IPS Status
Test Interface
Notes
Status And Alerts
Last Check: 2004-11-25 17:41
Success: Yes
Alert Count: 8
Rules Loaded


Nitro Guard Control Panel
NITRO DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
FIRST IPS IPS Information
General IPS Rules
Notifications
Alerts
Management
Terminal
Defaults
Rulesets
VIRUS - Most aggressive
POLICY - More aggressive
PERIMETER - Bogus IP Addresses -- Most
STREAM4 - tcp stream reassembly and sta
HTTP_DECODE - Converts web traffic to A
PEERTOPEER - Most aggressive
Remove Ruleset
Available Rulesets
ALPHA
Least aggresive (all alert)
More aggressive (normal status)
Most aggressive (always reject)
BASE
CHAT
HTTP_DECODE
MALWARE
MULTIMEDIA
PEERTOPEER
PERIMETER
POLICY
PORN
RPC_DECODE
SECURE APPLICATION GATEWAY
STREAM4
TELNET_DECODE
VIRUS
Add Ruleset
Send Rules To IPS (Alert Only)
Ruleset Variables
AIM_SERVERS - List of IP Addresses of AIM servers for snort rules that inspect AOL Instant
ALLOWED_INBOUND_BOGONS - Outbound IP address(es) which are part of the local
ALLOWED_OUTBOUND_BOGONS - Inbound IP address(es) which are part of the local
DNS_SERVERS - List of DNS servers (e.g. 192.168.15.3 or [192.168.15.3,172.16.61.4]).
Value :
Update Value
2
Updates Only (0)
1003584
1003585
Use of a BitTorrent peer to peer file transfer utility was d
Usage
Alert - Log matching packet and generate alert
Priority : Class
3 : policy-violation
Reference
url,bitconjurer.org/BitTorre
Signature
tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"P2P BitTorrent announce request"; flow:to_server; content:"GET"; depth:4; content:"/announce"; distance:1; content:"info_hash="; offset:4; content:"event=started"; offset:4; classtype:policy-violation; reference:url,bitconjurer.org/BitTorrent/; reference:url,www.p2pwatchdog.com/packet_bittorrent.html; sid:2180; rev:2;)
Alert
Update Usage
Edit Rule
Search For :
Search
Next
Send Rules To IPS
Sync IPS Rules
Rules Loaded


Nitro Guard Control Panel
NITRO DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
FIRST IPS IPS Information
General
IPS Rules
Notifications
Alerts
Management
Terminal
Defaults
Notification Alert Query
Query Name
Summary
<none>
Alerts
Count
Delete
Distribution
Failure
IPS Status
Log
Level
IPS
Time Frame
Last
Duration
Day
Item
(Comma delimited)
Groups
Name :
last 24 hrs
Add New Notification
Modify Selected Notification
Delete Selected Notification
Notification Notes
Log To
EMail
Syslog


Nitro Guard Control Panel
NITRO
DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
FIRST IPS IPS Information
General
IPS Rules
Notifications
Alerts
Management
Terminal
Defaults
Get Alerts
Query View
Query Name
Summary
Level
IPS
Time Frame
Current
Duration
Day
Item
<-- Execute
Delete
Distribution
Failure
IPS Status
Log
Overview
Severity
Summary
Alert Details
First Time :
Last Time :
Duration :
Count :
SrcIP:Port :
DstIP:Port :
Protocol :
Action :
Goto Rule
Lookup
Show Packet
Capture Packets
Show Info
Show Notes
<<
<
>
>>
Delete Selected
Delete Queried
Export Selected
Export Queried
Rules Loaded

Nitro Guard Control Panel

NITRO DATA SYSTEMS INC.

Group

Group1

Add Group | Modify Group | Delete Group

IPS

FIRST IPS

Add IPS | Copy IPS | Modify IPS | Delete IPS

Properties | Logout | Exit

FIRST IPS IPS Information

General | IPS Rules | Notifications | Alerts | Management | Terminal | Defaults

Get Alerts | Export Results | Alert View

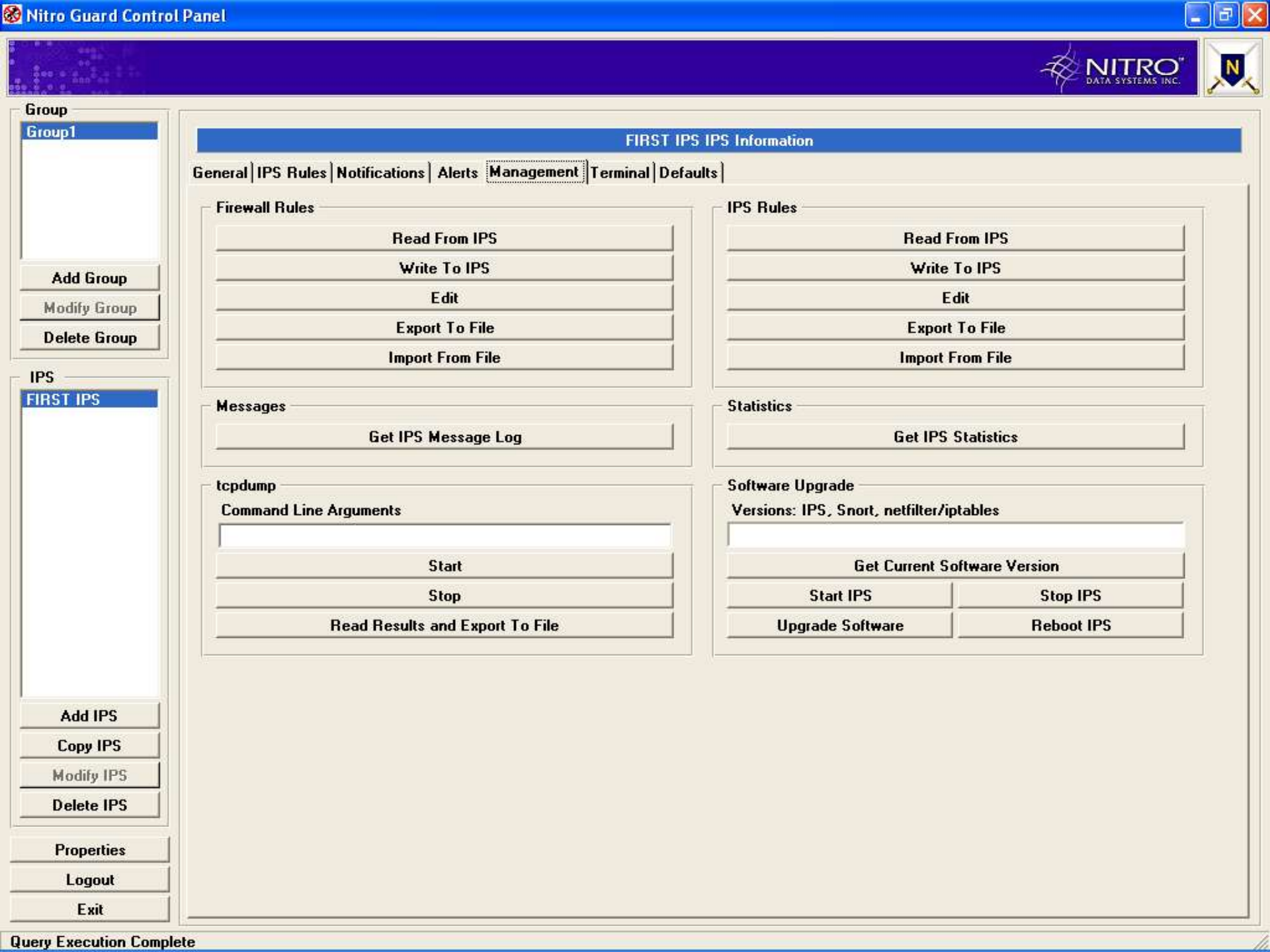
Query Name: Summary | Level: IPS | Time Frame: All | Duration | Item | <-- Execute

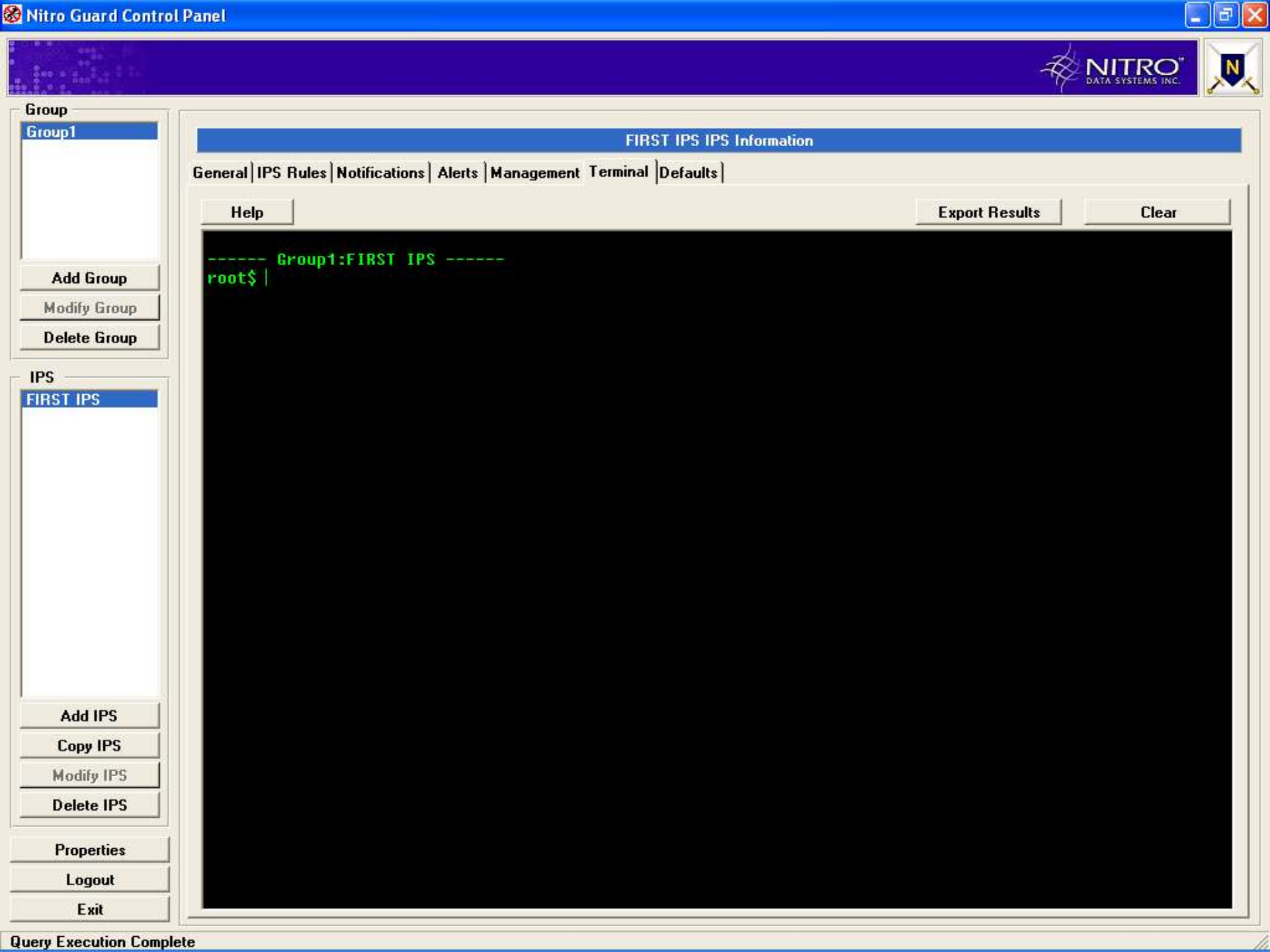
Drill Down | Alerts | Sig->Src | Sig->Dst | IP->Sig | Src<->Dst | < Sort > | Clear

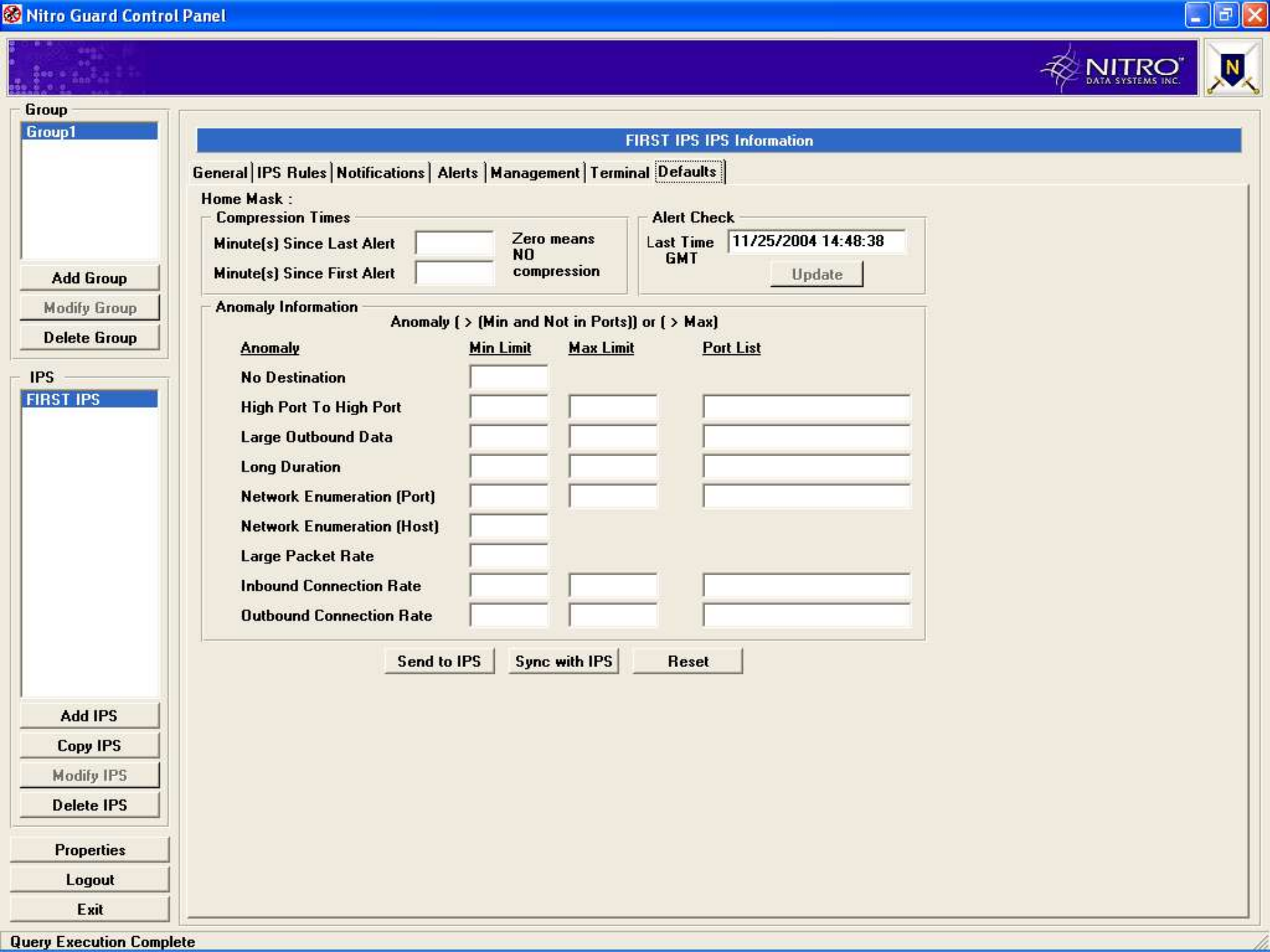
```
^=====================================================
= Report    : Summary All
= IPS       : Group1 : FIRST IPS : 2

=====================================================
```

SigID	Count	Total	Usage	Description
1001403	2	2,760	Alert	MISC UPNP malformed advertisement
1003048	3	106	Reject	MISC WATCHLIST - 20030613-window size 0xDA00
1002981	4	49	Alert	SCAN Traceroute UDP
1001358	6	44	Alert	ICMP Time-To-Live Exceeded in Transit
1001375	12	34	Reject	ICMP Communication Prohibited by Filtering
1002873	5	33	Reject	NETBIOS name-query
1000276	2	30	Reject	ICMP L3retriever ICMP PING
1002486	5	19	Alert	ICMP PING zeros
1001316	4	18	Alert	ICMP Port Unreachable
1003583	4	8	Alert	SMTP Non-SMTP Server Emails
1001299	2	7	Alert	ICMP Traceroute
1003604	1	7	Drop	EDONKEY connection to server
1001322	1	6	Alert	ICMP Echo Reply
1003583	1	6	Drop	SMTP Non-SMTP Server Emails
1001379	1	3	Alert	ICMP Large ICMP Packet
1001986	1	2	Alert	WEB-CGI adcycle access
1001375	1	1	Alert	ICMP Communication Prohibited by Filtering
3116054	1	1	Alert	DECODE_TCPOPT_BADLEN
Total =	56	3,134		

Query Execution Complete


Nitro Guard Control Panel
NITRO
DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
FIRST IPS IPS Information
General
IPS Rules
Notifications
Alerts
Management
Terminal
Defaults
Firewall Rules
Read From IPS
Write To IPS
Edit
Export To File
Import From File
IPS Rules
Read From IPS
Write To IPS
Edit
Export To File
Import From File
Messages
Get IPS Message Log
Statistics
Get IPS Statistics
tcpdump
Command Line Arguments
Start
Stop
Read Results and Export To File
Software Upgrade
Versions: IPS, Snort, netfilter/iptables
Get Current Software Version
Start IPS
Stop IPS
Upgrade Software
Reboot IPS
Query Execution Complete


Nitro Guard Control Panel
NITRO
DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
FIRST IPS IPS Information
General
IPS Rules
Notifications
Alerts
Management
Terminal
Defaults
Help
Export Results
Clear
------ Group1:FIRST IPS ------
root$
Query Execution Complete


Nitro Guard Control Panel
NITRO DATA SYSTEMS INC.
Group
Group1
Add Group
Modify Group
Delete Group
IPS
FIRST IPS
Add IPS
Copy IPS
Modify IPS
Delete IPS
Properties
Logout
Exit
FIRST IPS IPS Information
General
IPS Rules
Notifications
Alerts
Management
Terminal
Defaults
Home Mask :
Compression Times
Minute(s) Since Last Alert
Minute(s) Since First Alert
Zero means NO compression
Alert Check
Last Time GMT
11/25/2004 14:48:38
Update
Anomaly Information
Anomaly (> (Min and Not in Ports)) or (> Max)
Anomaly
Min Limit
Max Limit
Port List
No Destination
High Port To High Port
Large Outbound Data
Long Duration
Network Enumeration (Port)
Network Enumeration (Host)
Large Packet Rate
Inbound Connection Rate
Outbound Connection Rate
Send to IPS
Sync with IPS
Reset
Query Execution Complete

NitroGuard Product Line

- **NitroGuard 500 IPS**
  - *Ready for the enterprise*
  - *Redundant hardware*
- **NitroGuard 200 IPS**
  - *SME and departmental solution*
- **NitroGuard WG IPS**
  - *Work Group Solution*
  - *Protects internal assets*
- **NitroGuard M IPS**
  - *Built for SMB*
  - *Managed by a partner*

Hardware either supplied by NitroSecurity or purchased based on exact specifications

In the US, Nitroguard is delivered embedded within a hardware box.

In Europe, NitroGuard is mostly provided as a software suite in order to run on hardware based on NitroSecurity exact specifications.

The NitroGuard Advantage

- **User Customizable**
  - Custom Signatures / Alerts
  - Custom Reports
  - Secure Application Gateway
- **Signature updates**
  - Based upon the industry's most widely deployed Intrusion Detection System core – SNORT
  - Over 3,000 built in attack signatures
  - Multiple source vs. proprietary
  - Automated signature updates

- **World Class Service and Support**
  - 24X7 and managed service options available
  - Alpha response available

Intrusions: What should you do?

nitrosecurity

Gartner

In an October 2003 release, Gartner advised clients to purchase a network-based IPS and states, "*A true network-based intrusion prevention system must:*"

- *Operate as an in-line network device at wire speeds.* √
- *Perform packet normalization, assembly and inspection.* √
- *Apply rules based on several methodologies to packet streams, including (at a minimum) protocol anomaly analysis, signature analysis and behavior analysis.* √
- *Drop malicious sessions - don't simply reset connections.* √

"Enterprises that have not yet made large investments in network IDSs should delay investment while investigating the advantages of Intrusion Prevention Solutions."

Other Cressida Security Solutions: Ecora

- **Enterprise Auditor**

  Ensure proper implementation and use of Security settings & policies

  - Automatically generate configuration settings and change reports,
  - For security audits and compliance.
  - Covers all critical OS's, databases, network devices, and applications, including Cisco, Citrix, IBM, Microsoft and Oracle.

- **Patch Manager**

  Make sure latest Operating System Security capabilities are effective

  - Automate and accelerate patch management –
  - Easy to install and use,
  - Unsurpassed graphical reports.
  - Agentless or agent-based – your choice.

- **Device Lock**

  Stop improper use of mobile and volatile storage devices

  - Prevent users with USB drives from stealing your data.
  - Halt unauthorized Wi-Fi networks and manage user access to devices.

Other Cressida Security Solutions: Akonix

- **Full and Comprehensive of Management of Public and Enterprise IM**
  - Public IM - AOL, ICQ, IRC, MSN and Yahoo!
  - EIM – Lotus SameTime and Microsoft Live Communication Server (LCS)
- **IM Logging and Report for other selected Enterprise IM solutions**
  - Reuters Instant Messaging
  - Bloomberg Instant Message
  - Authenticates user/screen name
    - Integrates with Active Directory
  - Manages by single user, groups of users or everyone
  - Full Access Controls – Chinese Walls
  - File Transfer Controls
  - IM Feature Controls
  - Full or Selective Content Filtering
  - Anti-virus scanning (with 3rd party)
  - IM conversation logging and reporting
  - IM Content Archiving Integration (with 3rd party)
  - Compliance Reporter and protocol
  - Dynamic update for protocol changes
  - Auto install, no downtime
  - Offers full scalability

Other Cressida Security Solutions: ReQuest

- **Recovery**
  - Time Stamp Recovery
  - Detection of valid recovery points
  - Cross Queue Manager
  - Allows MQ data to be recovered in sync with DBMS data.
  - Recover deleted queues and purged data.
  - Forward Recovery
  - Individual Q's or group of Q's, possibly cross queue manager
  - Mass recovery in fail over situation.
  - Purged Queues
- **Reporting**
  - Granularity is MQ-call
  - Cross Queue Manager
  - By Q, By application, By Time-span
  - "Message Propagation"-report
  - MQPUT by appl A on RemoteQ in QMGR_A
  - Put on transmission Q for QMGR_intermediate
  - Put on transmission for QMGRB by QMGR_intermediate
  - Put on Q_Receiving in QMGRB by receiver.
  - MQGET from Q_Receiving
  - MQPUT of reply message (correlid!) by appl B on…
  - Filtering options
  - Raw data, in fixed documented format
  - To interface with other reporting tools

Other Cressida Security Solutions: RepliWeb

- **Recovery**
  - Fire and forget
    Recovers from networks failures or system crashes down to block level
- **Data transfer**
  - Integrity
  - Compression
  - Bandwidth control
    - Absolute
    - Relative
    - Time frames
  - Differential Transfer
    on large files only transfer the differences

Thank You

- Interesting free downloads:
  - NitroSecurity:
    - White papers on IPS (Intrusion Prevention System)
    - **http://www.cressida.info/whitepapers_page.htm#NitroGuard**
  - Akonix RogueAware software:
    - *free monitoring tool that detects and reports on IM and P2P File Sharing use within corporate network*
    - **http://www.akonix.com/products/test_drive.asp**
  - Ecora
    - Free software evaluation (Systems Configuration Audit & Patch Management)
    - **http://www.cressida.info/products_ecora_overview.htm**

Cressida, NitroSecurity Distributor for Europe,

In France: 03 20 38 06 46, Int'l HQ: +44 1483 23 93 00, *www.cressida.info*