Types of attacks detected
Context: SATAN probes, port and ping sweeps, etc
Contents: sendmail, loadmodule, org, policy violations, etc

Event levels
1) info only - call detail records, etc
2) admin - policy violations, config, etc
3) alarm - minor security violation
4) alarm - major security violation
5) alarm - attack in progress
Distributed Network Security Management

Director Tier 1

Director Tier 2

Director Tier 3

Director Tier 3

Enterprise Strategic Management

Regional Operational Management

Local Network Security Management
NetRanger NSX

- Expert system
  Real-time intrusion detection and instantaneous "surgical" response
- Content and Context monitoring
  Redundant, robust, communications architecture for assured event notification
- Secure VPN
- 56k, T1/E1, Ethernet, T3, 100Mbps
- Plug-and-play
- Sun (SPARC & PC), HP, IBM
# NetRanger NSX Alarm Levels

<table>
<thead>
<tr>
<th>Alarm Level</th>
<th>Network Config Events</th>
<th>Network Usage Events</th>
<th>Network Security Events</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LEVEL 0</strong></td>
<td>Misc Ignored Ports</td>
<td>Misc Ignored Ports</td>
<td></td>
</tr>
<tr>
<td><strong>LEVEL 1</strong></td>
<td>Misc Network Traffic</td>
<td>Packets From Blocked Services</td>
<td></td>
</tr>
<tr>
<td><strong>LEVEL 2</strong></td>
<td>Misc Failed Packets</td>
<td>Packets Travelling to Blocked Sites</td>
<td></td>
</tr>
<tr>
<td><strong>LEVEL 3</strong></td>
<td></td>
<td></td>
<td>Authentication tcp P 13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failed DNS Attempts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failed SNMP Attempts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failed FTP Attempts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failed Telnet Attempts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failed X Session Attempts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failed Finger Attempts</td>
</tr>
<tr>
<td><strong>LEVEL 4</strong></td>
<td>Lost Heartbeat</td>
<td></td>
<td>Failed SNMP Attempts</td>
</tr>
<tr>
<td></td>
<td>Router Interface Down</td>
<td></td>
<td>Failed RPC Attempts</td>
</tr>
<tr>
<td></td>
<td>Failed NSX</td>
<td></td>
<td>Failed TFTP Attempts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failed Rsh Attempt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failed Rlogin Attempt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failed Rexec Attempt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Login To Router</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Password Change On Router</td>
</tr>
</tbody>
</table>
|             |                       |                      | Sendmail w/ from: [tail |IFS/]
|             |                       |                      | Port Sweeping (tcp/udp) |
|             |                       |                      | ICMP Sweeping         |
|             |                       |                      | Source Routing        |
|             |                       |                      | IP Spoofing           |
|             |                       |                      | Fragmented TCP Headers |
|             |                       |                      | SATAN Attack          |
| **LEVEL 5** |                       |                      | Multiple Hacking Attempts |
| **LEVEL 6** |                       |                      |                        |
Hardware Specifications

NSX Sensor
- 7” high
- 19” wide (including rabbit ears)
- 20” deep (including rabbit ears)
- Weighs 32 pounds

BorderGuard 1000
- 2” high
- 10” wide (including rabbit ears)
- 17.5” deep
- Weighs 15 pounds

BorderGuard 2000
- 6.5” high
- 19” wide
- 17.5” deep
- Weighs 25 pounds
Considerations
NetKarger Pre-Installation

WheelGroup Corporation
Analyze Current Network Architecture

- Identify what to protect:
  - Internet
  - Remote sites
  - Business partners
  - Departments
- Define all entry and exit points to the protected network:
  - One geographic location, no existing internet connections
  - One geographic location, existing internet connections
  - Multiple geographic locations, existing internet connections
- Identify current security measures:
  - Existing Firewalls
  - Security Filters
Option 1: Install the Border Guard as a Bridge

Internet

Local Area Network (LAN)
Option 2: Install the BorderGuard as an Internet Router.
Options 3-6: Unable to Replace Existing Router

- Class B Address
- One or more Unused Class C Addresses
- No Unused Class C Addresses
- Class C Address that Cannot be Subnetted
Option 5: No Unused Class C Addresses
Option 6: (cont.)

Internet

Existing Internet Router

Internet

BenderGuard

Proxy Server

Local Area Network (LAN)

Local Area Network (LAN)

Internal IP Address: 193.20.20.x

Network Mask: 255.255.255.0

External IP Address: 193.20.20.32

Network Mask: 255.255.255.0
NetRanger NSX Sensor Installation Options

- Install the NSX Sensor on a Separate, Isolated Network
  - Most Secure NSX Connection
    - Only with the NSX 2000 or 5000
- Install the NSX Sensor on the Corporate Network
  - Can be used with NSX 1000, 2000 or 5000
- Install the NSX Sensor on a Switched Ethernet Network
  - Can be used with NSX 1000, 1000 or 5000
NSX Sensor on a Separate, Isolated Network.
Install the NSX Sensor on the Corporate Network