

Niksun Technology Overview



Security Event

Stop

Events Top Sources: LINK		Events Top Alarms: IP			ICMP Bit Rate: LINK: proto 1	Total Bit Rate: LINK
Alarm Time	Source	Alarm Time	Name	Description	GROUP/Network Bit Rate (bits/sec)	GROUP/Network Bit Rate (bits/sec)
7:34:28	210.17.17.149	7:34:28	TPS Alarm [1:...	[1:2050:8] MS...		
7:34:28	210.17.17.149	7:34:28	TPS Alarm [1:...	[1:2003:8] MS...		
7:34:28	216.191.44.67	7:34:28	TPS Alarm [1:...	[1:1417:9] SN...		
7:34:28	216.191.44.67	7:34:28	TPS Alarm [1:...	[1:1411:10] S...		
7:34:28	47.129.241.69	7:34:28	TPS Alarm [1...	[122:23:0] po...		
7:34:28	47.248.0.43	7:34:28	TPS Alarm [1...	[119:4:1] http...		
7:34:28	47.248.0.43	7:34:28	TPS Alarm [1...	[119:4:1] http...		
7:34:28	47.135.152.84	7:34:28	TPS Alarm [1...	[122:23:0] po...		
7:34:28	47.248.0.43	7:34:28	TPS Alarm [1...	[119:4:1] http...		
7:34:28	47.248.0.43	7:34:28	TPS Alarm [1...	[119:4:1] http...		
7:34:28	210.17.17.149	7:34:28	TPS Alarm [1:...	[1:2050:8] MS...		
7:34:28	210.17.17.149	7:34:28	TPS Alarm [1:...	[1:2003:8] MS...		

Events Top Sources: LINK	Events Top Alarms: IP	ICMP Bit Rate: LINK: proto 1	Total Bit Rate: LINK
<p>GROUP/West-Region Connections (count)</p>	<p>GROUP/West-Region Avg Thruput (bytes/sec)</p>	<p>GROUP/West-Region Bit Rate (bits/sec)</p> <p>560</p> <p>low: 56.0 high: 14.9 K</p> <p>poll intrvl: 10 sec(s)</p>	<p>GROUP/West-Region Bit Rate (bits/sec)</p>

Events Top Sources: LINK	Events Top Alarms: IP	ICMP Bit Rate: LINK: proto 1	Total Bit Rate: LINK																																																																	
<table border="1"> <thead> <tr> <th>Alarm Time</th> <th>Source</th> </tr> </thead> <tbody> <tr><td>7:34:28</td><td>210.17.17.149</td></tr> <tr><td>7:34:28</td><td>210.17.17.149</td></tr> <tr><td>7:34:28</td><td>216.191.44.67</td></tr> <tr><td>7:34:28</td><td>216.191.44.67</td></tr> <tr><td>7:34:28</td><td>47.129.241.69</td></tr> <tr><td>7:34:28</td><td>47.248.0.43</td></tr> <tr><td>7:34:28</td><td>47.248.0.43</td></tr> <tr><td>7:34:28</td><td>47.135.152.84</td></tr> <tr><td>7:34:28</td><td>47.248.0.43</td></tr> <tr><td>7:34:28</td><td>47.248.0.43</td></tr> <tr><td>7:34:28</td><td>210.17.17.149</td></tr> <tr><td>7:34:28</td><td>210.17.17.149</td></tr> </tbody> </table>	Alarm Time	Source	7:34:28	210.17.17.149	7:34:28	210.17.17.149	7:34:28	216.191.44.67	7:34:28	216.191.44.67	7:34:28	47.129.241.69	7:34:28	47.248.0.43	7:34:28	47.248.0.43	7:34:28	47.135.152.84	7:34:28	47.248.0.43	7:34:28	47.248.0.43	7:34:28	210.17.17.149	7:34:28	210.17.17.149	<table border="1"> <thead> <tr> <th>Alarm Time</th> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>7:34:28</td><td>TPS Alarm [1:...</td><td>[1:2050:8] MS...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1:...</td><td>[1:2003:8] MS...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1:...</td><td>[1:1417:9] SN...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1:...</td><td>[1:1411:10] S...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1...</td><td>[122:23:0] po...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1...</td><td>[119:4:1] http...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1...</td><td>[119:4:1] http...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1...</td><td>[122:23:0] po...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1...</td><td>[119:4:1] http...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1...</td><td>[119:4:1] http...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1:...</td><td>[1:2050:8] MS...</td></tr> <tr><td>7:34:28</td><td>TPS Alarm [1:...</td><td>[1:2003:8] MS...</td></tr> </tbody> </table>	Alarm Time	Name	Description	7:34:28	TPS Alarm [1:...	[1:2050:8] MS...	7:34:28	TPS Alarm [1:...	[1:2003:8] MS...	7:34:28	TPS Alarm [1:...	[1:1417:9] SN...	7:34:28	TPS Alarm [1:...	[1:1411:10] S...	7:34:28	TPS Alarm [1...	[122:23:0] po...	7:34:28	TPS Alarm [1...	[119:4:1] http...	7:34:28	TPS Alarm [1...	[119:4:1] http...	7:34:28	TPS Alarm [1...	[122:23:0] po...	7:34:28	TPS Alarm [1...	[119:4:1] http...	7:34:28	TPS Alarm [1...	[119:4:1] http...	7:34:28	TPS Alarm [1:...	[1:2050:8] MS...	7:34:28	TPS Alarm [1:...	[1:2003:8] MS...	<p>beta.mj.niksun.com/ftp1 Bit Rate (bits/sec)</p>	<p>beta.mj.niksun.com/ftp1 Bit Rate (bits/sec)</p>
Alarm Time	Source																																																																			
7:34:28	210.17.17.149																																																																			
7:34:28	210.17.17.149																																																																			
7:34:28	216.191.44.67																																																																			
7:34:28	216.191.44.67																																																																			
7:34:28	47.129.241.69																																																																			
7:34:28	47.248.0.43																																																																			
7:34:28	47.248.0.43																																																																			
7:34:28	47.135.152.84																																																																			
7:34:28	47.248.0.43																																																																			
7:34:28	47.248.0.43																																																																			
7:34:28	210.17.17.149																																																																			
7:34:28	210.17.17.149																																																																			
Alarm Time	Name	Description																																																																		
7:34:28	TPS Alarm [1:...	[1:2050:8] MS...																																																																		
7:34:28	TPS Alarm [1:...	[1:2003:8] MS...																																																																		
7:34:28	TPS Alarm [1:...	[1:1417:9] SN...																																																																		
7:34:28	TPS Alarm [1:...	[1:1411:10] S...																																																																		
7:34:28	TPS Alarm [1...	[122:23:0] po...																																																																		
7:34:28	TPS Alarm [1...	[119:4:1] http...																																																																		
7:34:28	TPS Alarm [1...	[119:4:1] http...																																																																		
7:34:28	TPS Alarm [1...	[122:23:0] po...																																																																		
7:34:28	TPS Alarm [1...	[119:4:1] http...																																																																		
7:34:28	TPS Alarm [1...	[119:4:1] http...																																																																		
7:34:28	TPS Alarm [1:...	[1:2050:8] MS...																																																																		
7:34:28	TPS Alarm [1:...	[1:2003:8] MS...																																																																		

Niksun Technology Overview

Who is Niksun?

Niksun is the only single-point totally integrated solution that immediately replaces three or more network performance monitoring, security surveillance and forensic analysis tools. Niksun's scalable architecture easily adapts to Data centre, Core network, Remote Branch or Central office. Niksun's solution is scalable for LAN, MAN and WAN requirements such as Ethernet and 10Gb to OC-48.

What makes Niksun Different

The key to Niksun's technology is its ability to capture huge amounts of data multi Terabytes, and interrogate it extremely quickly.

The way that it works is to interrogate every packet as it enters the system, index information on the packet in various high speed lookup tables and then write the packet to disk. In the event of searching on terabytes of data file, the system only queries the much smaller high speed lookup tables. This results in speedy responses to queries. The actual packet data only get accessed when doing things such as decoding the protocol or reconstructing a session. The indexing means that the packet data can be immediately retrieved without looking through multiple time slices.

The large amount of data captured means that you don't have to know what you are looking for prior to an event. After something has happened such as malicious event or network outage you can go back and review exactly what happened.

This process is the key to Niksun's solution, once this data is in place and rapidly available, it is up to you what to do with it. Niksun provides modules for;

- Security (IDS, anomaly alerting, forensic reconstruction)
- Network Analysis (QOS, network analysis, reporting, multicast, RMON, VOIP)
- Enterprise solutions (Enterprise wide reporting, security and network management)

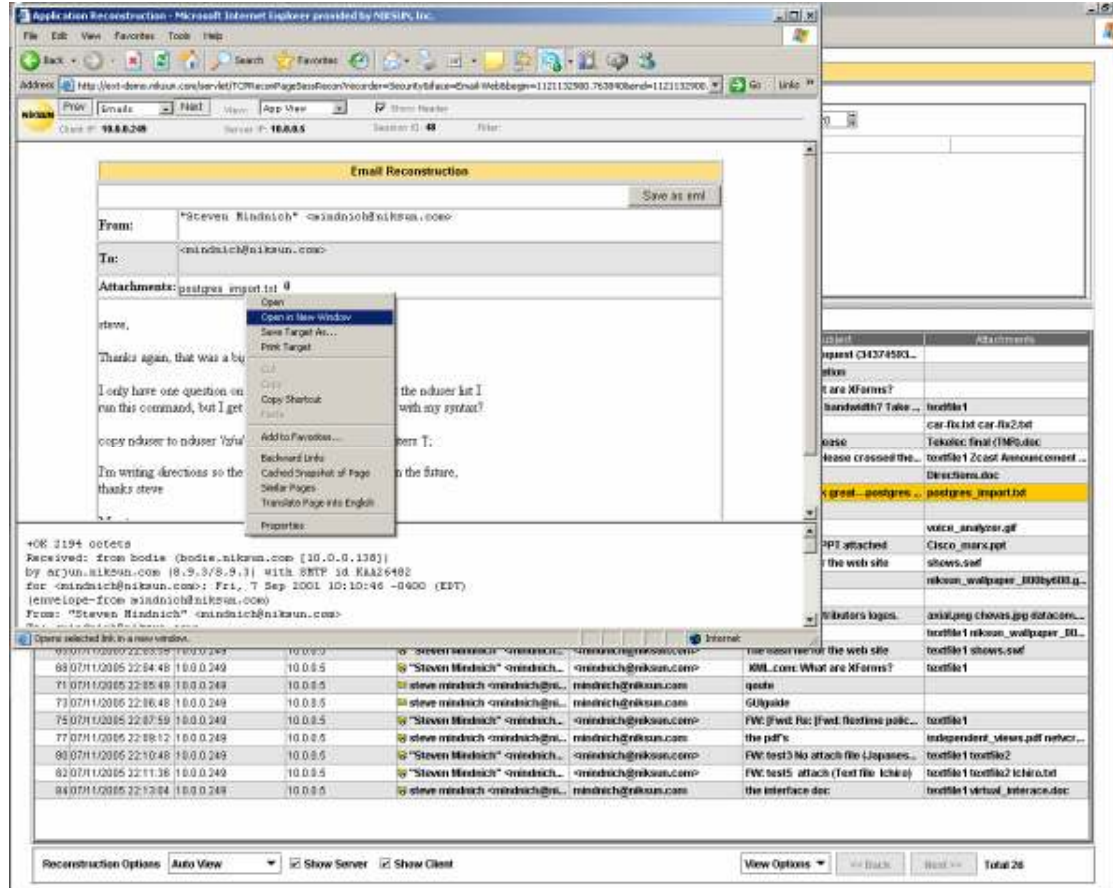
Niksun Technology Overview

Network Security and Forensics

NetDetector contains Niksun's security toolset. It allows real time on the fly intrusion detection as well as application reconstruction.

The types of sessions that can be reconstructed are;

- web (HTTP & HTTPS)
- email (SMTP/POP3/IMAP4)
- Telnet
- FTP with embedded images
- MIME attachments and files transferred
- instant messaging (IM from ICQ, Yahoo, MSN, AOL)
- ASCII
- HEX, Offers string search (including Base-64 encoding)



Individual sessions can be isolated in a few mouse clicks; furthermore if you are trying to identify an event such as a leaked document, keywords from that document can be searched upon to find its movements.

As well as the ability to put sessions back together post event, Niksun can intelligently alert on network anomalies such as;

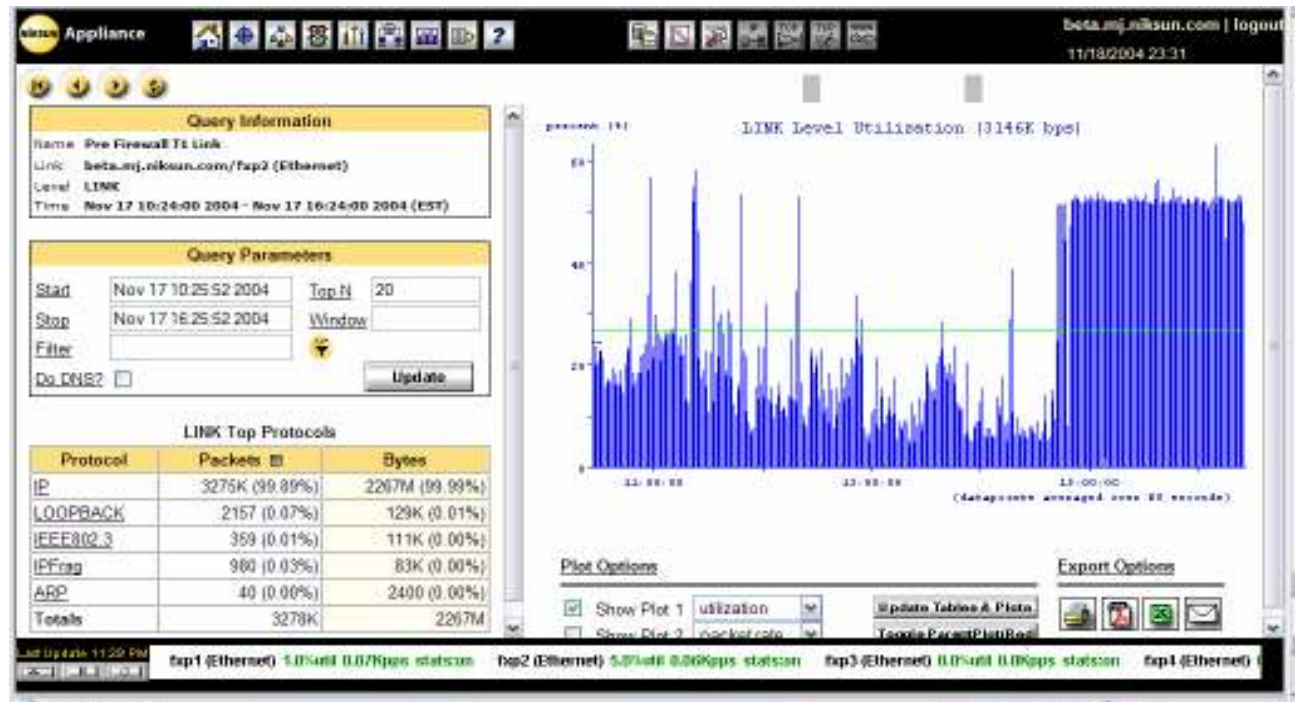
- User-defined Threshold-based Anomaly Detection: Numerous alerts can be customized to any environment. Alerting options include screen pop-ups, email/pager notifications, SNMP traps, custom messages, Syslogs & 3rd party security consoles (e.g., IBM Tivoli Risk Manager, Micromuse NetCool Secure)
- Signature-based Intrusion Detection: Integrated internal signature based IDS or external Cisco based IDS alerts.
- Detect and alert on keywords passing over a network link, projects names etc.

Niksun Technology Overview

Network Analysis

The combination of the large quantities of data, statistical and analysis tools gives Niksun an extremely quick time to resolution on network issues. This is due to the data and a powerful array of tools to interpret it. Some of the tools available are;

- Application performance;
 - round-trip response times
 - application/server response times
 - re-transmission rates
 - Application overhead
- For web-based traffic statistics on user abort rates
- VOIP analysis
- Expert analysis (Intelligent interpretation of IP traffic)
- Multicast Tools
- Automated and on demand reporting
- RMON statistics
- Dynamic IP flow data exporting
- QOS and service level monitoring



In the event of an application failure, Niksun will have recorded the application session right up to the point of failure; this provides visibility as to what was going on as application performance started degrading.

The important thing to take into consideration is that all the information is there and it can be accessed extremely quickly, often without the need to look at packet data.

Niksun Technology Overview

Enterprise Suite

Niksun's management suite provides the capability to get real time updates from your entire Niksun deployment. This provides a true indication as to the state of network performance cross infrastructure. The console interface can be configured to suit your needs. The security department can have one view that displays very different information to Network teams, VOIP team, applications team, etc. The charts that you see can be configured to suit your needs.

The true power of this solution really becomes evident when you start performing queries, it is important to note that the processing takes place on each remote Niksun unit. This minimises the network overhead as only the results are passed back to the management interface.

In the event that you are following up a malicious event or network issue, perform the following steps;

1. Tell the enterprise interface what you want to know
2. A global query will be sent to all Niksun units
3. Each unit will perform the query locally
4. The answers are returned to the management console

You have just queried your entire infrastructure and have a complete picture of the event in a matter of seconds.

