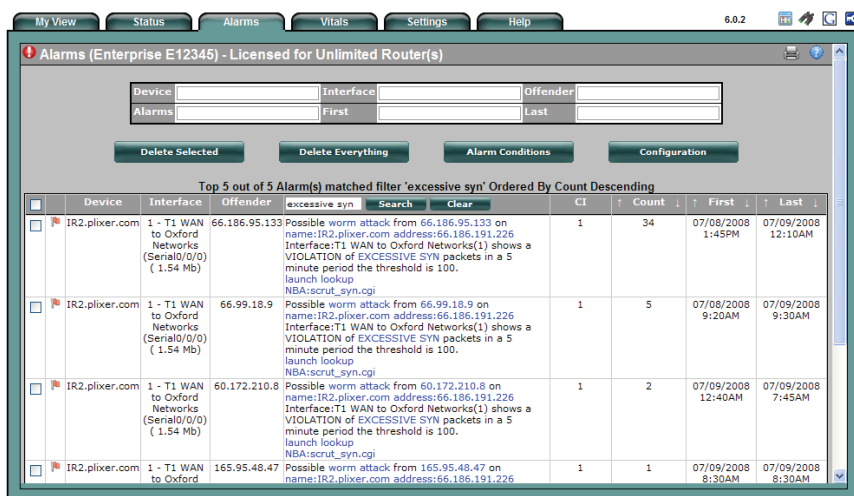


Scrutinizer Network Behavior Analysis



Scrutinizer Network Behavior Analysis

Scrutinizer NBA (Network Behavior Analysis) is an expert system that interrogates every conversation from every host for traffic behavior pattern anomalies. Imagine all conversations through potentially hundreds of routers across your enterprise being monitored at all times for traffic that shouldn't be there.



Alarms (Enterprise E12345) - Licensed for Unlimited Router(s)

Device: [] Interface: [] Offender: []
 Alarms: [] First: [] Last: []

Delete Selected Delete Everything Alarm Conditions Configuration

Top 5 out of 5 Alarm(s) matched filter 'excessive syn' Ordered By Count Descending

Device	Interface	Offender	excessive syn	Search	Clear	CI	Count	First	Last
IR2.plixer.com	1 - T1 WAN to Oxford Networks (Serial0/0/0) (1.54 Mb)	66.186.95.133	Possible worm attack from 66.186.95.133 on name: IR2.plixer.com address: 66.186.191.226 Interface: T1 WAN to Oxford Network(s1) shows a VIOLATION of EXCESSIVE SYN packets in a 5 minute period the threshold is 100. launch lookup NBA:scrut_syn.cgi			1	34	07/08/2008 1:45PM	07/09/2008 12:10AM
IR2.plixer.com	1 - T1 WAN to Oxford Networks (Serial0/0/0) (1.54 Mb)	66.99.18.9	Possible worm attack from 66.99.18.9 on name: IR2.plixer.com address: 66.186.191.226 Interface: T1 WAN to Oxford Network(s1) shows a VIOLATION of EXCESSIVE SYN packets in a 5 minute period the threshold is 100. launch lookup NBA:scrut_syn.cgi			1	5	07/08/2008 9:20AM	07/09/2008 9:30AM
IR2.plixer.com	1 - T1 WAN to Oxford Networks (Serial0/0/0) (1.54 Mb)	60.172.210.8	Possible worm attack from 60.172.210.8 on name: IR2.plixer.com address: 66.186.191.226 Interface: T1 WAN to Oxford Network(s1) shows a VIOLATION of EXCESSIVE SYN packets in a 5 minute period the threshold is 100. launch lookup NBA:scrut_syn.cgi			1	2	07/09/2008 12:40AM	07/09/2008 7:45AM
IR2.plixer.com	1 - T1 WAN to Oxford	165.95.48.47	Possible worm attack from 165.95.48.47 on name: IR2.plixer.com address: 66.186.191.226			1	1	07/09/2008 8:30AM	07/09/2008 8:30AM

Figure 1: Advanced Alarming

Quickly sort on peculiarities of the problem and narrow down to the culprit to a specific interface. A Concern Index is maintained on all computer systems causing alerts. The Concern Index increases for individual hosts as they participate in questionable behaviors. Thresholds can be set on behavioral probabilities.

Scrutinizer NBA continually tallies and sizes up the conversations from all flow sending devices and helps identify:

- Zero-day worms, SYN Floods and DoS attacks
- ICMP Destination Unreachable
- Bleeding Edge Attacks
- Policy violations and internal misuse
- Poorly configured and unauthorized devices
- Unauthorized Application Deployments
- Suspicious NetBIOS-based services
- Excessive Multicast Traffic
- Unauthorized or incorrectly configured server activity
- P2P traffic, such as BitTorrent (even if encrypted)
- Root causes of network slow downs
- Serious vs. trivial network incidents

"We have been using another product, but I use Scrutinizer on a large network. It's an invaluable tool for determining the "who, what, and where" of network activity. Scrutinizer is a world-class product with an intuitive and easy-to-use interface. It's feature rich and a much lower cost than other NetFlow management products."

- State of Maine

"I started using the freeware version of this new tool and I must say it's already been helpful. It takes the per packet info from the NetFlow streams you configure on your Cisco router and displays it in an easy to use web interface. I've known how much traffic I had on my interfaces, but didn't know what the content of the traffic was. I was able to identify the cause of a network link running slow because of one user transferring a huge file during the day over a slow link. Scrutinizer saved me a lot of time troubleshooting the old fashion way!"

- Central Maine Power

We deliver the tools you need...

Plixer International, Inc. designs, develops and services NetFlow products and solutions for mission critical businesses. Our technical support and installation services ensure that every installation works with your existing software investments.

Product Overview

Simply counting protocol volumes and user traffic levels or monitoring for high interface utilization is helpful, but many anomalies exist in a realm where typical counter detection systems don't look.

Scrutinizer NBA complements existing security measures.

- No agents need to be installed or deployed anywhere.
- Works by collecting NetFlow, sFlow, IPFIX and NetStream from existing routers/switches.
- Works differently than a typical IDS because its focus is on numerous conversation patterns and not on individual packets.
- Looks at all traffic across hundreds of routers and switches, not just periodic snap shots.
- Useful at the network perimeter, as well as across highly switched internal networks.
- Requires almost no initial configuration. However, has a flexible modeling architecture to create additional behavior monitors.

Since typical NetFlow exports don't contain the detail necessary for more involved IDS functions, such as parsing applications, Scrutinizer NBA makes decisions by utilizing proprietary algorithms that watch patterns of behavior.

Algorithms define:

- What is considered normal/abnormal behavior
- What can be excluded (e.g. hosts and or protocols which need to break the rules)

Architecture

Scrutinizer NBA goes to work right away without customization. The flexible host and protocol profile architecture allows for easy tweaks of the default algorithms, which go to work immediately to identify existing threats on the corporate network. The algorithms can be configured to run against all or only a few of the flow sending devices.

The most sophisticated IDS appliances search through the packet stream's payload for multiple string patterns which is a computationally expensive task. Since NetFlow contains pre-summarized conversations, this sophisticated approach

is easier in some cases. However, searching above Layer 5 of the OSI model is impossible with most NetFlow packets today.

Standards for NetFlow (e.g. Flexible NetFlow) are on the way, which will allow for deeper analysis. Scrutinizer NBA maintains FIFO conversation tables for virtually every host and protocol even on wire speed interfaces. The tables are scanned with behavior profiles every few minutes and events are triggered when abnormal patterns are identified.

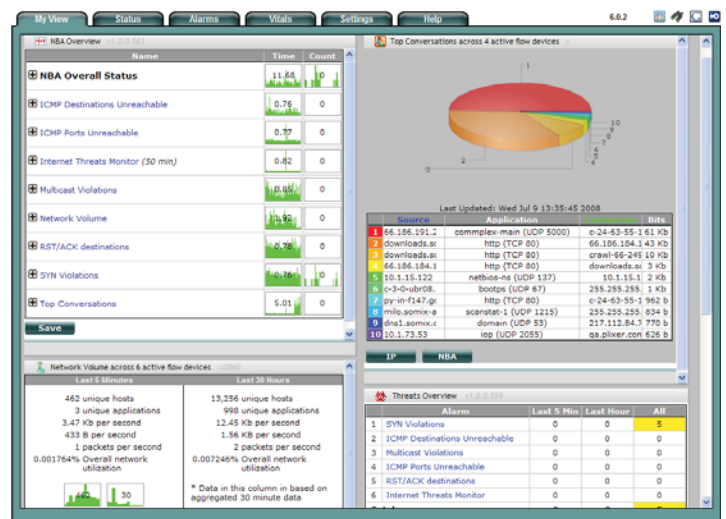


Figure 2: NBA MyView Gadgets

Similar to IDS Systems, Scrutinizer NBA shares the same basic mechanism: As an IP packet traverses the firewall, the headers are parsed and the results are compared to a rule set defined by a system administrator. The rule set (commonly based upon source and/or destination IP address, source and/or destination port, or a combination) defines what type of traffic is subsequently acceptable or not.

Scrutinizer NBA compares conversations in each flow to the anomaly algorithms. As the network behavior is learned, exceptions can be made to prevent false positives and threat algorithms are frequently updated via an Internet connection.

Advanced alarming allows users to launch historical trends on the data by IP addresses or Port numbers that help identify how long the issue has been at large and what other hosts are involved.

Mitigation

Scrutinizer can take action by disabling ports or making changes to the firewall and or necessary routers to assist in mitigating and stopping the virus.

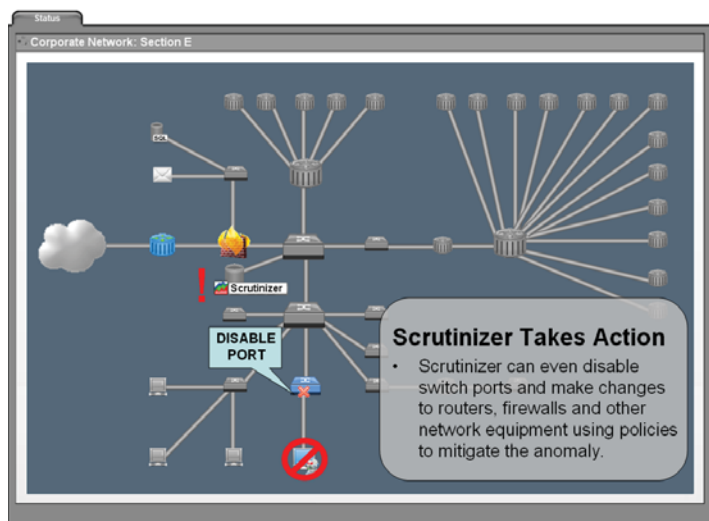


Figure 3: Threat Mitigation

Vitals

Scrutinizer NBA provides details on how often a particular policy is being violated.

How many routers/switches can Scrutinizer NBA handle? It really depends on the volume of NetFlow and the capacity of the hardware it is installed on. See the minimum hardware requirements on our web site.

Notifications

Syslogs are sent to the existing NMS when policies are violated.

Summary

Traditional Intrusion Protection Systems are certainly an asset. Scrutinizer provides another layer of security. Be they intentional or unintentional, internal computers are one of the largest threats to a business' electronic assets.

The bottom line today is that in order to exercise sound bandwidth and security controls, organizations and service providers need to monitor traffic inside the network as many attacks get past the existing IDS and firewall. Once the threat is inside, administrators need multiple ways to watch for problems.

Scrutinizer NBA capitalizes on existing flow technologies and can provide clear diagnosis. It is a great additional way to protect hosts, networks and applications against attacks and misuse.

Policy	Owner	Board	Count	Time (first)	Time (last)	Last Alert	Violation List
SCRUTINIZER (194.193.193) has been disabled by	[Take]	Default	165489	Mon Jun 23 16:00:57 2008	Tue Jul 8 16:59:37 2008	Email (jmd@plixer.com) No-repeat	66.186.184.202 (195489)
Denika Threshold CPU	[Take]	Default	3426	Mon Jun 23 16:10:34 2008	Tue Jul 8 16:55:18 2008		MINOTR (118) lab plixer.com (384) IR2 plixer.com (865) HANDY (2041) Ecdysis (18)
Scrutinizer (194.193.193) has been disabled by	[Take]	Default	490	Mon Jun 23 17:07:45 2008	Tue Jul 8 16:37:01 2008	Email (dale@plixer.com) No-repeat	66.186.184.202 (490)
Possible port scan dropped	[Take]	Firewall	674	Mon Jun 23 21:05:13 2008	Tue Jul 8 14:49:19 2008	Email (Raut@plixer.com) No-repeat	66.186.184.193 (674)
SCRUTINIZER has exceeded its configured threshold of traffic	[Take]	Default	1687	Mon Jun 23 23:13:40 2008	Tue Jul 8 14:20:34 2008		66.186.184.202 (1687)
Denika has disabled a report	[Take]	Default	315	Tue Jun 24 01:17:37 2008	Tue Jul 8 01:18:17 2008		127.0.0.1 (315)
Antisense - Unable to create channel of type (AA/OSP)	[Take]	Default	1705	Mon Jun 23 16:02:21 2008	Mon Jul 7 16:57:05 2008		66.186.184.194 (1705)
VOP Packet Loss Threshold Violation	[Take]	Default	134	Tue Jun 24 13:45:12 2008	Mon Jul 7 14:55:42 2008		lab plixer.com (4) IR2 plixer.com (130)

Figure 3: NMS Alerting

Minimum Hardware Specifications

- Windows 2000/XP/2003
- 2 Gigs of RAM
- 15,000 RPM IDE or SATA Hard Disk
- 2 GHz+ processor
- Minimum 100 Megs of hard drive space for program files
- Minimum 300 Gigs of hard drive space for database files