Product Overview

ManageEngine NetFlow Analyzer 12.0

네트워크 트래픽 분석, 대역폭 관리
그리고 네트워크 비정상 상태 탐지를 위한
정교한 종합 도구

There's No Stopping ME
IT Software In Over 200 Countries & Growing

ManageEngine.com
Powering IT ahead

About ManageEngine

ManageEngine 제품 라인 소개

Network	Servers & Applications	Desktop	ServiceDesk	Windows Infrastructure	Event Log & Compliance	Security
Network Monitoring	Server Monitoring	Desktop Management	Helpdesk	Active Directory	Windows Event Logs	Vulnerability Analysis
NetFlow Analysis	Application Perf Monitoring	Asset Management	ITIL Service Desk	SQL Server	Syslog Management	Patch Management
Network Config Mgmt	End User Experience	Remote Control	Software License Tracking	Exchange Server	Firewall Log Analyzer	Password Management

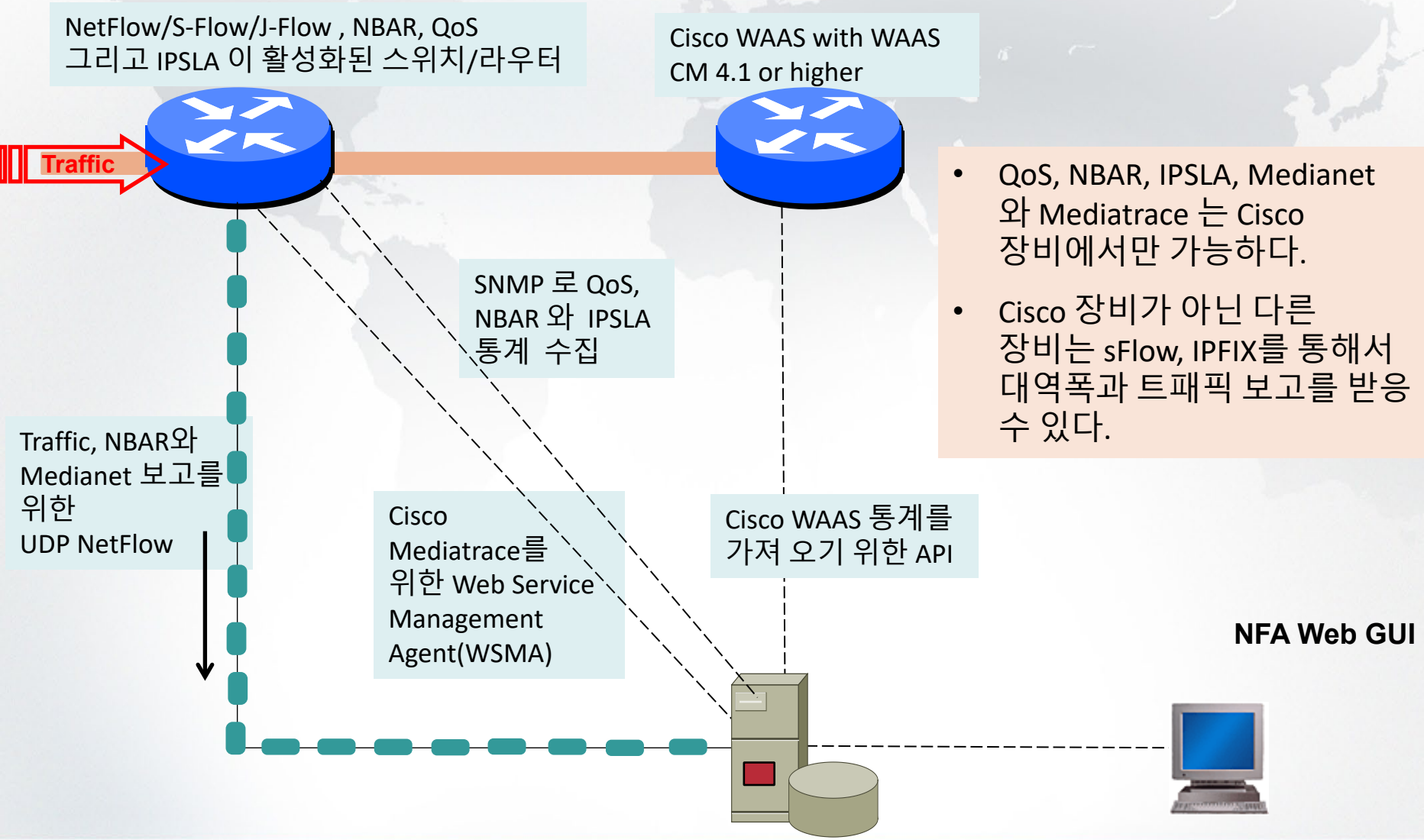
ManageEngine 은 모든 유형의 기업/기관에
완전한 IT 관리 도구를 공급합니다.

NetFlow Analyzer – 소개합니다.

- 대역폭 감시, 트래픽 분석 그리고 네트워크 비정상 상태를 탐지하는 소프트웨어 솔루션.
- 단일 솔루션 – 다양한 종류의 기술을 감시.

- ❖ NetFlow, sFlow, IPFIX, J-Flow, NetStream, Appflow 대역폭과 트래픽 분석용
- ❖ Cisco NBAR: DPI 기반 application 인식
- ❖ Cisco QoS 감시: QoS 정책 검증
- ❖ Cisco IPSLA : VoIP 와 WAN RTT 성능 보고서
- ❖ Cisco WAAS - WAN 최적화 보고서
- ❖ Cisco Medianet monitoring : 미디어(VIDEO/VOICE) 트래픽 성능 보고서
- ❖ Centralized monitoring: 분산 네트워크를 위한 솔루션(옵션)

NetFlow Analyzer – Working Architecture



- QoS, NBAR, IPSLA, Medianet 와 Mediatrace 는 Cisco 장비에서만 가능하다.
- Cisco 장비가 아닌 다른 장비는 sFlow, IPFIX를 통해서 대역폭과 트패픽 보고를 받응 수 있다.

주요 제품 기능

대역폭 감시 / 트래픽 분석 / 네트워크 회선 용량 계획

- 대역폭 감시
  - 인터페이스/포트 기준의 실시간 대역폭 사용량 보고서
  - Volume, Speed, Utilization, Packets 기반의 트래픽 보고서
- 트래픽 분석
  - Applications 과 Conversations 에 대한 상세 보고서
  - 1 년간 저장된 원천 플로우 데이터
  - 통합 플로우 데이터 통계 – 다양한 Top N 보고서
- 용량 계획 및 Application 증감 보고서
  - 지난 1 년간의 1 분 단위의 상세 트래픽 보고서
  - 트래픽과 어플리케이션의 증감 패턴을 그래프로 표시
  - 부서별 과금/사용량 보고서, 용량 계획 보고서

대역폭 감시 / 트래픽 분석 / 네트워크 회선 용량 계획

누가 ?
어디서 ?

Source IP Address
Destination IP Address

Source Port
Destination Port
Protocol

무엇을 ?

언제 ?

Conversation Time
Flow Start and End time

Volume
Speed
Utilization
Packet Count

사용량 ?

QoS ?

ToS
DSCP
TCP Flags

QoS ?

통로는 ?

Input and Output Interface
(ifindex)

NextHop
Source AS Information
Destination AS Information

Route ?

대역폭 감시 / 트래픽 분석 / 네트워크 회선 용량 계획

Traffic | Application | Source | Destination | QoS | Conversation | Multicast | Medianet | NBAR | CBQoS | Security Events

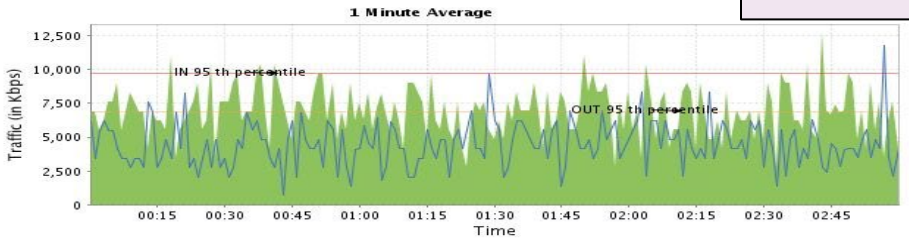
Refresh: Every 1 Minute

IN OUT Today Report From : 2012-08-14 00:00 To : 2012-08-14 03:00

Volume | Speed | Utilization | Packets

Data Points : 1 5 15 Minute(s) Average

대역폭 감시
속도



Category	Total	Max	Min	Avg	Standard Deviation	95th Percentile
IN	9.4 GB	12.7 Mbps	2.76 Mbps	6.92 Mbps	1.81 Mbps	9.71 Mbps
OUT	6.1 GB	11.8 Mbps	690.84 Kbps	4.49 Mbps	1.62 Mbps	6.9 Mbps

Traffic | Application | Source | Destination | QoS | Conversation | Multicast | Medianet | NBAR | CBQoS | Security Events

Refresh: Every 1 Minute

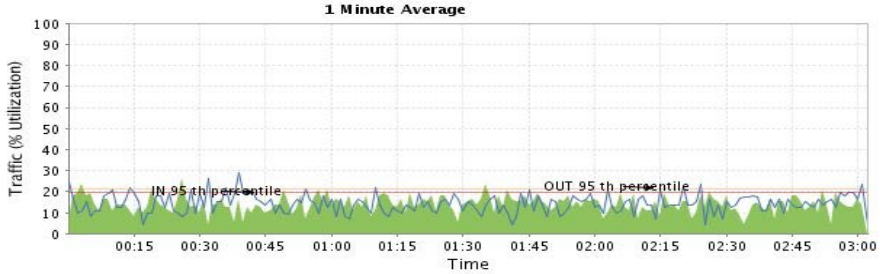
IN OUT Today Report From : 2012-08-14 00:00 To : 2012-08-14 03:02

Volume | Speed | Utilization | Packets

Capacity Planning Report

Data Points : 1 5 15 Minute(s) Average

대역폭 감시
사용률



* Utilization is calculated with Link Speed of 100.0 Mbps

Category	Total	Max	Min	Avg	Standard Deviation	95th Percentile
IN	19.15 GB	26.24%	4.14%	13.96%	3.90	19.44%
OUT	19.68 GB	29.01%	4.14%	14.34%	4.38	21.55%

There's No Stopping ME
IT Software In Over 200 Countries & Growing
ManageEngine.com
Powering IT ahead

대역폭 감시 / 트래픽 분석 / 네트워크 회선 용량 계획

Tata 70 MB PIL --> WAN

Action(s) | More Reports | Dashboards

Traffic | Application | Source | Destination | QoS | Conversation | Multicast | Medianet | NBAR

IN | OUT | Today Report | From: 2012-08-14 00:00 | To: 2012-08-14 15:22

어플리케이션 별 대역폭 점유률

Application | Application Gr

Protocol Distribution | Showing 1 to 50 | View per page 50

Application	Traffic(Total: 125.73 GB)	% of total traffic
http	79.97 GB	64%
https	32.29 GB	26%
TCP_App [Show Ports]	9.92 GB	8%
pop3s	1.56 GB	1%
ESP_App [Show Ports]	774.61 MB	1%
Netflow	381.0 MB	<1%
ssh	250.08 MB	<1%
domain	222.25 MB	<1%
imaps	190.42 MB	<1%
netmeeting	58.59 MB	<1%
smtp	27.29 MB	<1%

어플리케이션 종류

어플리케이션 별 트래픽

어플리케이션 별 점유율

Troubleshoot Generated from raw data and may take longer, especially for large time intervals.

Device : Tata 70 MB PIL > WAN | Select the Device

Match any of the following | Match all the following

Criteria 1 | Source Address

From 2012-08-14 00:00

Generate Report

대화 별 트래픽, 속도, 패킷 수, 등

원천 트래픽 데이터로부터 분석한 대화 보고서

현재 대화 중인 사내 IP와 상대방 IP

Traffic | Application | Conversation

Resolve DNS | IN | Sort by : Bytes

IN Traffic Details | Showing 1 to 100

Src IP	Dst IP	Appln	Src Port	Dst Port	Protocol	DSCP	TCP FLAGS	Flow Rate	Traffic	Packets	NextHop	FNF NbarApp
74.125.169.244	121.244.182.76	http	80	35284	TCP	Default	AP	2.98 Mbps	56.67 MB	37786	121.244.182.76	-
74.125.169.166	121.244.182.67	http	80	41727	TCP	Default	AP	3.17 Mbps	31.71 MB	21144	121.244.182.67	-
74.125.169.6	121.244.182.77	http	80	38536	TCP	Default	AP S	4.01 Mbps	28.12 MB	18751	121.244.182.77	-
74.125.169.169	121.244.182.77	http	80	37079	TCP	Default	AP	3.65 Mbps	25.55 MB	17040	121.244.182.77	-
74.125.169.244	121.244.182.76	http	80	35284	TCP	Default	AP	3.11 Mbps	21.78 MB	14521	121.244.182.76	-
74.125.169.166	121.244.182.67	http	80	33477	TCP	Default	AP	2.71 Mbps	21.72 MB	14483	121.244.182.67	-
74.125.169.244	121.244.182.76	http	80	35284	TCP	Default	AP	1.78 Mbps	17.83 MB	11893	121.244.182.76	-
74.125.169.166	121.244.182.67	http	80	41727	TCP	Default	AP	2.53 Mbps	17.76 MB	11843	121.244.182.67	-
74.125.169.166	121.244.182.67	http	80	41727	TCP	Default	AP	2.22 Mbps	15.58 MB	10393	121.244.182.67	-
74.125.169.244	121.244.182.76	http	80	35284	TCP	Default	AP	2.47 Mbps	14.86 MB	9913	121.244.182.76	-
74.125.169.244	121.244.182.76	http	80	35284	TCP	Default	AP	2.42 Mbps	14.56 MB	9713	121.244.182.76	-
74.125.169.166	121.244.182.67	http	80	41727	TCP	Default	AP	2.84 Mbps	14.21 MB	9476	121.244.182.67	-

대역폭 감시 / 트래픽 분석 / 네트워크 회선 용량 계획

Device/Interface : Tata 70 MB PIL --> WAN

Last Week Report | From : 2012-08-07 19:33 | To : 2012-08-14 19:33 | Business Hour Filter | Exclude weekends | Generate Bill

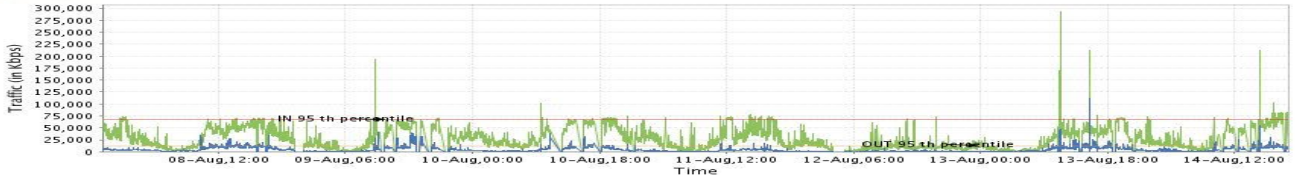
Report

Volume | Speed | Utilization | Packets

1 Minute Average

Data Points : 1 5 Minute(s) Average

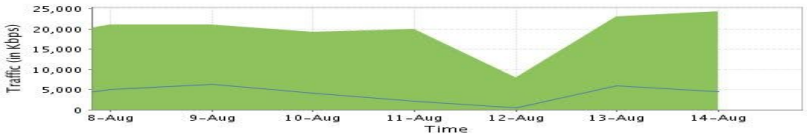
1분 평균



Category	Total	Max	Min	Avg	Standard Deviation	95th Percentile
IN	1.87 TB	293.08 Mbps	0.00	24.78 Mbps	21.1 Mbps	67.27 Mbps
OUT	298.01 GB	112.03 Mbps	0.00	3.94 Mbps	4.72 Mbps	12.63 Mbps

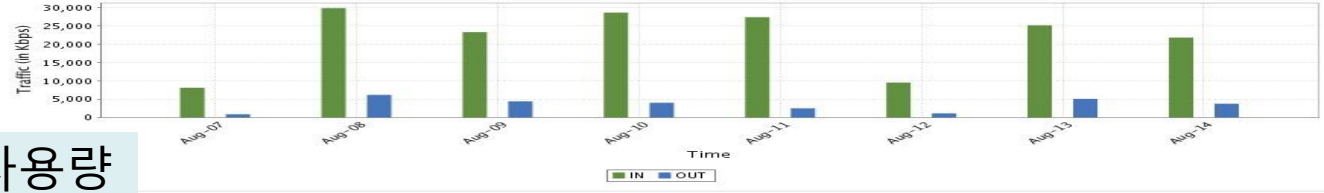
Standard Deviation Graph(Daily)

일일 표준 편차 보고서



네트워크 회선
용량 계획 보고서

Average Usage(Daily)



일일 평균 사용량

Data Points

Traffic IN Details

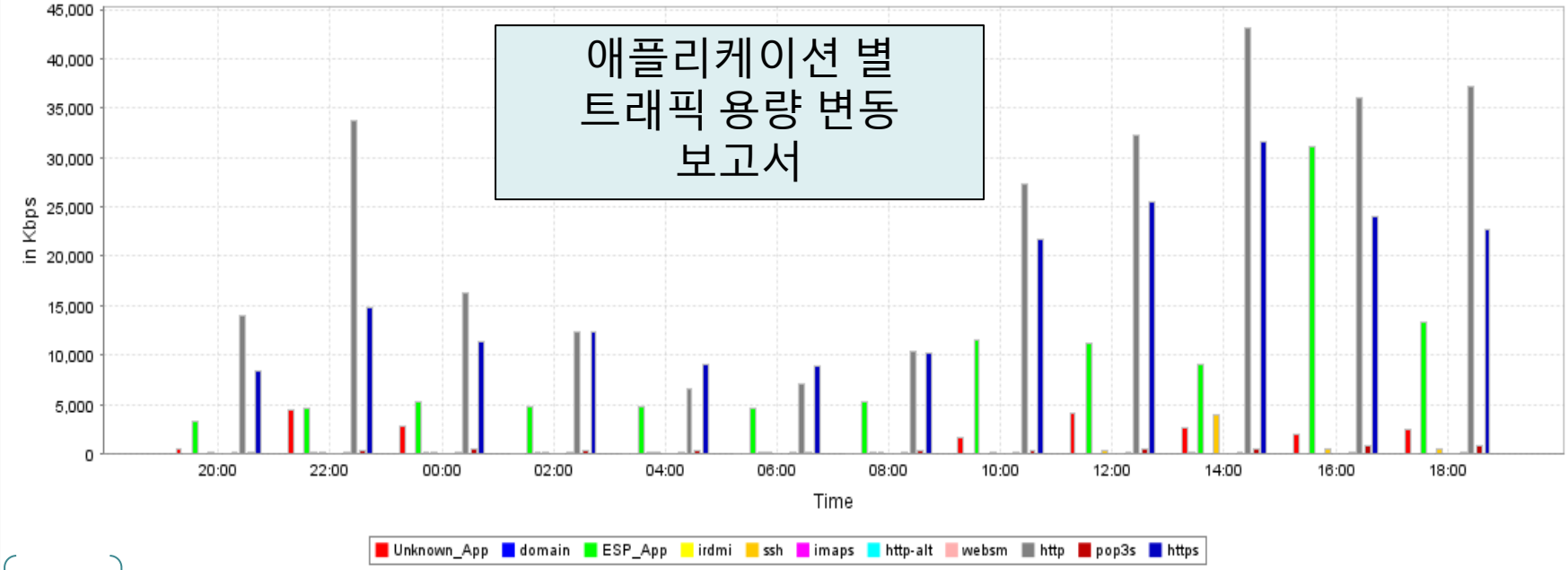
Time	Min	Max	Avg	Total
Aug-14-12	0.00	211.87 Mbps	21.78 Mbps	235.23 Gbps
Aug-13-12	0.00	293.08 Mbps	25.15 Mbps	271.68 Gbps
Aug-12-12	0.00	72.97 Mbps	9.48 Mbps	102.4 Gbps
Aug-11-12	1.51 Mbps	77.72 Mbps	27.35 Mbps	295.47 Gbps
Aug-10-12	0.00	100.9 Mbps	28.6 Mbps	308.88 Gbps
Aug-09-12	0.00	193.55 Mbps	23.25 Mbps	251.15 Gbps
Aug-08-12	0.00	71.76 Mbps	29.82 Mbps	322.13 Gbps
Aug-07-12	15.01 Mbps	74.27 Mbps	8.08 Mbps	87.29 Gbps

Traffic OUT Details

Time	Min	Max	Avg	Total
Aug-14-12	0.00	54.93 Mbps	3.7 Mbps	40.01 Gbps
Aug-13-12	0.00	112.03 Mbps	5.05 Mbps	54.6 Gbps
Aug-12-12	0.00	6.93 Mbps	1.08 Mbps	11.68 Gbps
Aug-11-12	531.39 Kbps	18.7 Mbps	2.45 Mbps	26.55 Gbps
Aug-10-12	0.00	37.48 Mbps	3.97 Mbps	42.93 Gbps
Aug-09-12	0.00	42.01 Mbps	4.37 Mbps	47.24 Gbps
Aug-08-12	0.00	35.12 Mbps	6.12 Mbps	66.11 Gbps
Aug-07-12	2.51 Mbps	9.25 Mbps	820.03 Kbps	8.85 Gbps

There's No Stopping ME
IT Software In Over 200 Countries & Growing
ManageEngine.com
Powering IT ahead

ApplicationIN Growth Report



외부에서 들어 오는
어플리케이션 종류

ApplicationIN	20:00	22:00	00:00	02:00	04:00	06:00	08:00	10:00	12:00	14:00	16:00	18:00	20:00
Unknown_App	562.72 Kbps	4.37 Mbps	2.74 Mbps	2.81 Kbps	6.38 Kbps	15.38 Kbps	14.07 Kbps	1.56 Mbps	4.09 Mbps	2.58 Mbps	2.04 Mbps	2.44 Mbps	-
domain	18.04 Kbps	30.18 Kbps	24.67 Kbps	21.35 Kbps	19.89 Kbps	20.36 Kbps	34.66 Kbps	65.24 Kbps	67.62 Kbps	74.86 Kbps	67.38 Kbps	61.8 Kbps	-
ESP_App	3.35 Mbps	4.55 Mbps	5.26 Mbps	4.77 Mbps	4.71 Mbps	4.51 Mbps	5.27 Mbps	11.46 Mbps	11.25 Mbps	9.12 Mbps	31.08 Mbps	13.31 Mbps	-
irdmi	66.73 Kbps	[illegible]	[illegible]	[illegible]	[illegible]	132.8 Kbps	104.42 Kbps	17.42 bps	1.58 bps	9.03 bps	4.76 bps	1.55 bps	-
ssh	117.59 [illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]83 Kbps	209.05 Kbps	230.77 Kbps	243.14 Kbps	3.85 Mbps	543.65 Kbps	460.92 Kbps	-
imaps	13.2 Kbps	[illegible]	[illegible]	[illegible]	[illegible]	16.62 Kbps	15.79 Kbps	21.34 Kbps	31.08 Kbps	53.23 Kbps	37.89 Kbps	58.38 Kbps	-
http-alt	18.95 Kbps	38.68 Kbps	37.94 Kbps	38.85 Kbps	40.55 Kbps	39.42 Kbps	40.17 Kbps	65.11 Kbps	67.34 Kbps	67.95 Kbps	56.96 Kbps	57.11 Kbps	-
websm	86.88 Kbps	162.33 Kbps	167.74 Kbps	182.94 Kbps	182.93 Kbps	197.37 Kbps	195.18 Kbps	198.67 Kbps	194.91 Kbps	191.69 Kbps	194.41 Kbps	198.6 Kbps	-
http	14.02 Mbps	33.75 Mbps	16.31 Mbps	12.29 Mbps	6.64 Mbps	7.13 Mbps	10.39 Mbps	27.34 Mbps	32.23 Mbps	43.17 Mbps	36.05 Mbps	37.2 Mbps	-
pop3s	157.25 Kbps	365.85 Kbps	444.23 Kbps	365.79 Kbps	237.03 Kbps	206.84 Kbps	283.04 Kbps	337.94 Kbps	430.93 Kbps	510.91 Kbps	768.78 Kbps	841.64 Kbps	-
https	8.36 Mbps	14.86 Mbps	11.34 Mbps	12.37 Mbps	8.99 Mbps	8.81 Mbps	10.12 Mbps	21.66 Mbps	25.53 Mbps	31.53 Mbps	23.95 Mbps	22.7 Mbps	-

There's No Stopping ME
IT Software In Over 200 Countries & Growing
ManageEngine.com
Powering IT ahead

IP 그룹 / 과금 / 경보 / 정기 보고서

- IP Groups
  - 원하는 보고서 생성을 위해 트래픽을 그룹화 하는 기능
  - 그룹의 종류
    - IP Address / IP Network / IP 범위 / Port / Port 범위
    - IP 와 Port 의 조합
- 사용량을 기준으로 과금
  - 과다한 사용에 대한 경보 가능
  - 사용량과 속도를 기준으로 자동 과금 정보 전송 가능
  - 대역폭 사용량에 따라 고객 / 부서 / 프로젝트 별로 과금 가능
- 임계치 위반 경보
  - 인터페이스/어플리케이션/포트/IP/DSCP 별로 임계치 위반 경보
  - 경보 발생 시, SNMP Manager 에 통지하거나, 이메일 발송 가능
- 주기 별 이메일 보고서 발송
  - 사용자가 정의하는 일정에 따라 원하는 보고서를 정한 시간에 자동 발송

IP 그룹 / 과금 / 경보 / 정기 보고서

IP Group 생성

IP Group Name:

IP Group Description:

IPGroup based on: ☑ IP Address ☑ Port/Protocol ☑ DSCP

Specify IP / IP Range / Network:

✖ Include | IP Network | Network IP | Netmask : 255.255.255.0

IP Network
IP Address
IP Range

Add More

Filter based on Port / Protocol: (Enter either a single port number or a single port range.Example 1001 or 1200-1600)

✖ Port Number: | Protocol: TCP

Add More

Filter based on DSCP Names:

✖ DSCP Name: Default

Add DSCP

Associated Interfaces: [Select the Device]

All Interfaces

IP Group Speed (this value will be used for calculation): 1000000 (in bps)

Save Cancel

IP 그룹 / 과금 / 경보 / 정기 보고서

과금 정보 생성

Enter Billing Details

Bill Plan Name

Bill Plan Description

Billing Type: Speed

Base Speed: [bps]

Base Cost: American Dollar-USD

Additional Speed: [bps] (Optional)

Additional Cost: USD (Optional)

95th Percentile Calculation: IN & OUT Merge

The IN and OUT values are merged and then the 95th percentile value is calculated from the merged records.

Billing Period: monthly

Billing TimeZone : Asia/Calcutta

Bill Genaration Date: 1

Your bill period is 1st to Last day of every month

Associating to

Router List

Router / Interface
ipfix-I (1.1.1.1)
IfIndex2
IfIndex5
IfIndex6

IP Group

IP Group
All IP Groups
between_site_ipaddr
between_site_ipntwk
DSCP

Interface Group

Interface Groups
All Interface Groups
cbqos-nbarIG
IPv6IG
medianetIG

There's No Stopping ME
IT Software In Over 200 Countries & Growing

ManageEngine.com
Powering IT ahead

IP 그룹 / 과금 / 경보 / 정기 보고서

Alert Profiles --> Add Alert Profile

Important : 1 Ensure that 'active time out' on the router is set to 1 minute
2 To parse the SNMP traps load NetFlow-Home/lib/ADVENTNET-NETFLOWANALYZER-MIB in your Manager Application.More

Add Alert Profile

Alert Profile Name :

Description :

Select Source : Interface | IP Groups | Interface Group

Selected Interfaces : All Interfaces (Modify Selection)

Define Alert Criteria : IN Traffic | OUT Traffic | Combined

Port/Protocol | DSCP | Application | IP Address

Define Thresholds and Action : Utilization | Volume | Speed | Packets

% times minutes; Severity Warning Select Action None

Add More

Business Hour Alerts : Enable | Disable

From : 00:00 Hrs;To: 00:00 Hrs;in Asia/Calcutta TimeZone

경보 발생
조건 설정

경보 보고서 생성

Schedule Report Configuration

Scheduler Name :

Description :

Select Source : Interface | IP Groups

Selected Interfaces : All Interfaces (Modify Selection)

Report Type : ...Select...

Report Format : PDF | CSV

Report TimeZone : Asia/Calcutta

Specify Time : Daily | Weekly | Monthly | Only Once

Generate report on the following days at the specified time

Generate report on : 02 Hrs ; 00 Mns; Asia/Calcutta TimeZone;

Generate report for : Previous Day(00:00-23:59)

Exclude weekends

The 30 most recent reports for this schedule can be accessed from the Schedule List page

Also email this report to Report accessing options : (Use comma "," for multiple mail id's)

E-mail Subject: Report From NetFlow Analyzer

보고서 형식
설정

보고서 주기
설정

정기 보고서 생성

Cisco NBAR, Cisco QoS 그리고 Cisco IPSLA Reports

- Cisco NBAR 보고서
  - Cisco NBAR에 의해 인식되는 어플리케이션 보고서
  - 수시로 포트를 달리하거나 잘 알려진 TCP, IP 포트를 사용하는 어플리케이션의 트래픽을 상세하게 관찰
  - 웜, Peer to Peer apps, Skype, 등을 식별
- Cisco QoS 보고서
  - QoS 정책 성능 검증
  - 정책 적용 전후의 통계를 비교
- Cisco IPSLA – VoIP 와 WAN RTT 보고서
  - VoIP 성능과 WAN RTT 성능지수
  - 지터(jitter), 지연, 패킷 손실과 VoIP 패킷에 대한 MoS (감도)
  - 데이터 패킷에 대한 Round-Trip time 과 링크 Up-Down

Cisco Flexible NetFlow를 이용한 NBAR 보고서

Traffic | Application | Source | Destination | QoS | Conversation | Medianet | NBAR | CBQoS

Select : FNF NBAR IN OUT Last 15 Minutes From: 2012-03-12 16:07 To: 2012-03-12 16:22

Resolve DNS Group by None Showing 1 to 100 View per page 100

Src IP	Dst IP	Application	Src Port	Dst Port	Protocol	DSCP	Traffic
172.18.66.250	228.8.7.9	unclassified	0	0	UDP	Default	2.06 MB
172.18.66.250	228.8.7.9	unclassified	35802	35802	UDP	Default	1.64 MB
172.18.66.250	228.8.47.52	unclassified	0	0	UDP	Default	981.28 KB
172.18.66.250	228.8.47.52	unclassified	9468	9468	UDP	Default	763.5 KB
172.18.4.62	232.0.1.10	unknown	0	0	UDP	Default	386.06 KB
192.168.24.158	172.18.2.101	unknown	0		ICMP	CS6	295.09 KB
192.168.24.158	172.18.2.101	snmp	47253			Default	135.37 KB
192.168.24.158	172.18.2.101	snmp				Default	135.08 KB
172.18.120.148	172.18.2.101	snmp				Default	134.97 KB
192.168.24.158	172.18.2.101	snmp				Default	134.63 KB
172.18.4.62	232.0.1.10	unknown				Default	131.94 KB
192.168.25.102	172.18.2.101	snmp	4560			Default	106.77 KB
172.18.98.139	172.18.2.101	snmp	56219		UDP	Default	106.57 KB
172.18.98.139	172.18.2.101	snmp	52122	161	UDP	Default	106.33 KB
192.168.25.102	172.18.2.101	snmp	5393	161	UDP	Default	106.11 KB
192.168.25.102	172.18.2.101	snmp	3	161	UDP	Default	105.3 KB
10.10.14.121	224.0.0.251	unknown		5353	UDP	Default	102.8 KB
172.18.2.151	224.0.0.251	unknown			UDP	Default	89.84 KB
172.18.93.211	224.0.0.251	unknown	5353			Default	81.65 KB
172.18.100.15	224.0.0.251	unknown	5353			Default	68.68 KB
172.18.2.170	224.0.0.251	unknown	5353			Default	68.27 KB
172.18.88.211	239.255.255.250	unclassifi	1900			Default	54.88 KB
172.18.2.170	172.18.255.255	netbio	138			CS1	52.8 KB
172.18.78.232	172.18.255.255	netbios	137			Default	49.92 KB
172.18.2.170	172.18.255.255	netbios	1		UDP	CS1	49.61 KB
172.18.120.148	172.18.2.101	snmp	62702	161	UDP	Default	48.16 KB
192.168.24.158	172.18.2.101	snmp	41876	161	UDP	Default	48.16 KB
172.18.120.148	172.18.2.101	snmp	61949	161	UDP	Default	48.16 KB
192.168.24.158	172.18.2.101	snmp	35761	161	UDP	Default	48.16 KB
172.18.120.148	172.18.2.101	snmp	55550	161	UDP	Default	48.16 KB
192.168.24.158	172.18.2.101	snmp	42341	161	UDP	Default	47.03 KB
172.18.78.223	224.0.0.251	unknown	5353	5353	UDP	Default	46.26 KB
172.18.2.197	172.18.255.255	netbios	137	137	UDP	CS1	42.58 KB
172.18.98.192	224.0.0.251	unknown	5353	5353	UDP	Default	42.09 KB
172.18.181.20	224.0.0.251	unknown	5353	5353	UDP	Default	39.59 KB
172.18.93.211	172.18.255.255	netbios	138	138	UDP	CS1	38.49 KB
172.18.2.164	172.18.255.255	netbios	137	137	UDP	CS1	38.06 KB
172.18.2.179	224.0.0.251	unknown	5353	5353	UDP	Default	37.61 KB
172.18.93.212	172.18.255.255	netbios	137	137	UDP	CS1	36.27 KB
10.0.2.1	10.0.2.255	netbios	137	137	UDP	CS1	36.03 KB
10.0.2.1	10.0.2.255	netbios	137	137	UDP	Default	36.03 KB
172.18.0.1	224.0.0.18	unknown	0	0	VRRP	Default	33.96 KB
172.18.98.99	224.0.0.251	unknown	5353	5353	UDP	Default	32.04 KB
172.18.97.154	224.0.0.251	unknown	5353	5353	UDP	Default	30.94 KB
172.18.120.148	172.18.2.101	snmp	55549	161	UDP	Default	30.12 KB
172.18.120.148	172.18.2.101	snmp	61948	161	UDP	Default	30.12 KB
172.18.2.146	224.0.0.251	unknown	5353	5353	UDP	Default	27.83 KB
172.18.255.254	224.0.0.251	unknown	5353	5353	UDP	Default	27.81 KB
172.18.145.96	172.18.255.255	netbios	137	137	UDP	Default	27.26 KB
172.18.93.211	172.18.255.255	netbios	137	137	UDP	CS1	26.76 KB
172.18.99.165	239.255.255.250	unclassified	1900	1900	UDP	Default	24.24 KB
172.18.43.103	239.255.255.250	unclassified	1900	1900	UDP	Default	24.24 KB
10.0.2.1	10.0.2.255	netbios	138	138	UDP	CS1	23.68 KB

사내, 사외 IP

어플리케이션

There's No Stopping ME
IT Software In Over 200 Countries & Growing

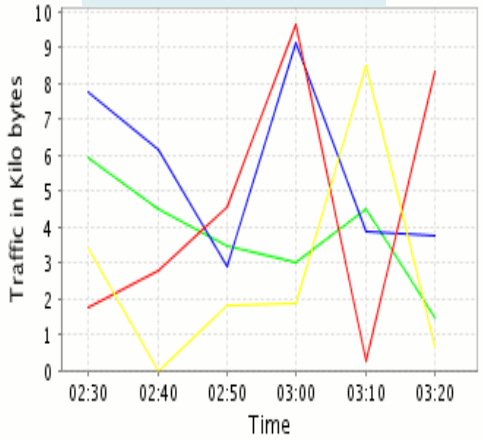
ManageEngine.com
Powering IT ahead

Volume Packets Speed Queue

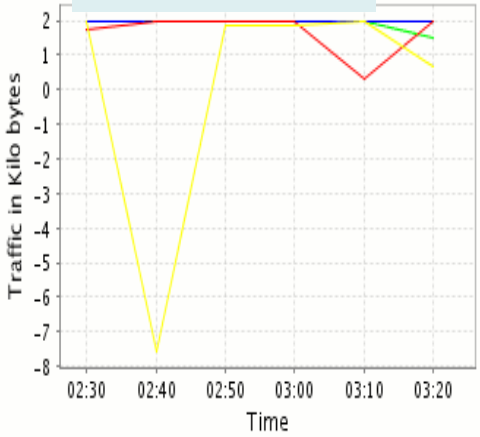
QoS 보고서

Policy Name : COS1

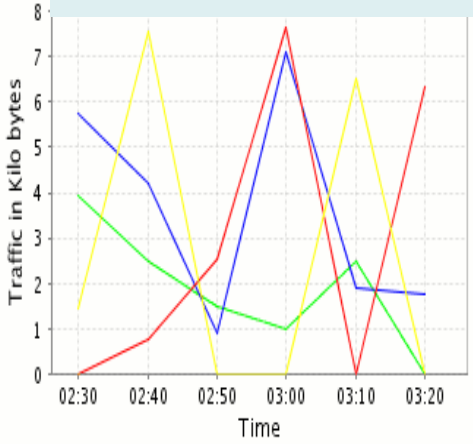
정책 적용 전



정책 적용 후



정책 적용 전후의 차이



Post Policy

Show Pie Chart : Post Policy

TransactionalData(COS1) MissionCritical(COS1) class-default(COS1) VOIP(COS1)

There's No Stopping ME
IT Software In Over 200 Countries & Growing
ManageEngine.com
Powering IT ahead

ManageEngine
NetFlow Analyzer *Professional Plus*

Trial period will expire in 28 days.. | Get Quote | Buy Online | Community | Upgrade | Themes | Help | Support | Register | About | Logout (admin)

Last Hour	0	0	0
All Alerts	0	0	5053

Dashboards | Devices | CBQoS/NBAR | IPSLA | Cisco WAAS | Medianet | Security Analytics | Billing | Reports | Admin

Device Groups | IP Groups | Alert Profiles | Schedule Reports | Application / QoS Maps | User Management | License Management | Search

IPSLA Dashboard | Configuration

IPSLA – VOIP 보고서

Overview | Top 10 | All Monitors | Settings | Switch To | Report | 1 Minute

Top Call Performance by Location - 22:07 Sep 28, 2011 To 23:07 Sep 28, 2011 | Configure VoIP Monitor

Locations	Score	Jitter	Packet Loss	Latency
cisco2081_routerss.csez.zohocorpin.com	0 Bad Calls			3 Links
172.18.2.101		1.0 ms	0.0%	1.0 ms
172.18.2.101		1.0 ms	0.0%	1.0 ms
172.18.2.101		1.0 ms	0.0%	1.0 ms

22 — 23
28 Sep 11 — 28 Sep 11

파형 왜곡이 심한 path

Top Call Paths by Jitter

Call Path	Max	Average
MainVoip -- cisco2081_rou ... → 172.18.2.101	1 msec	1.0 msec
branch -- cisco2081_rou ... → 172.18.2.101	1 msec	1.0 msec
Nestl -- cisco2081_rou ... → 172.18.2.101	1 msec	1.0 msec

More >>

Top Call Paths by Packet Loss

Call Path	Max	Average
MainVoip --cisco2081_rou ... → 172.18.2.101	0.0 %	0.0 %
branch --cisco2081_rou ... → 172.18.2.101	0.0 %	0.0 %
Nestl --cisco2081_rou ... → 172.18.2.101	0.0 %	0.0 %

More >>

음성 감도

Top Call Paths by MOS

Call Path	Max	Average
MainVoip -- cisco2081_rou ... → 172.18.2.101	4.3	4.3
branch -- cisco2081_rou ... → 172.18.2.101	4.3	4.3
Nestl -- cisco2081_rou ... → 172.18.2.101	4.3	4.3

More >>

Top Call Paths by Latency

Call Path	Max	Average
MainVoip --cisco2081_rou ... → 172.18.2.101	4 msec	1.0 msec
branch --cisco2081_rou ... → 172.18.2.101	7 msec	1.0 msec
Nestl --cisco2081_rou ... → 172.18.2.101	4 msec	1.0 msec

More >>

There's No Stopping ME
IT Software In Over 200 Countries & Growing
ManageEngine.com
Powering IT ahead

ManageEngine
NetFlow Analyzer *Professional Plus*

Trial period will expire in 28 days.. | Get Quote | Buy Online | Community | Upgrade | Themes | Help | Support | Register | About | Logout (admin)

Last Hour	0	0	0
All Alerts	0	0	5053

Dashboards | Devices | CBQoS/NBAR | IPSLA | Cisco WAAS | Medianet | Security Analytics | Billing | Reports | Admin

Device Groups | IP Groups | Alert Profiles | Schedule Reports | Application / QoS Maps | User Management | License Management | Search

IPSLA Dashboard ▾ | Configuration

IPSLA - WAN RTT 보고서

Overview | All Monitors | Settings | Switch To ▾ | Report | 1 Minute

Probe Snapshot cisco2081_router... → 192.168.17.93

Path Details | Threshold Details

Collector Details

Collector Name	MainPortland
Status	✓
Source IP Address	cisco2081_routerss.csez.zohocorpin.com
Destination IP Address	192.168.17.93
Souce IOS Version	15.1(3)T1,
Last Updated	Sep 28, 23:07 (Interval: 0 min)
Last Oper. Status	100.0 % Success

Test Parameters

Each Packet Size	24 KB
Frequency	60 seconds
Time Out	60 seconds

Todays Availability	ICMP Echo	Errors
	0.0%	0.0%

Min RTT	Average RTT	Max RTT
1.0 milliseconds	4.0 milliseconds	32.0 milliseconds

There's No Stopping ME
IT Software In Over 200 Countries & Growing
ManageEngine.com
Powering IT ahead

고급 보안 분석 모듈

- 수집되는 데이터를 분석하여 네트워크 트래픽의 이상 현상을 검출한다.
- Stream Mining Engine 을 이용하여 실시간 패턴 매칭과 이벤트 상호관계 분석
  - 웜, 바이러스, 의심스러운 트래픽, 스캔, DoS 공격 식별
  - 방화벽과 IDS를 초월하는 공격을 탐지하고 완화
- 공격자, 타깃 그리고 공격 경로에 대한 상세한 정보 보고서

ASAM(보안 분석) Dashboard

Scans / Probes

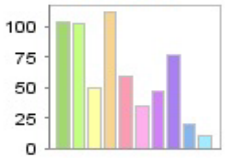
스캔 공격

Problem / Events / Resources

Short TCP Ack Port Scan(Reverse)	446	103
Short TCP Fin Ack Port Scan(Re...	425	102
Short TCP Ack Port Scan	331	49
TCP Rst Port Scan(Reverse)	329	112
Short TCP Fin Ack Port Scan	262	59
Short TCP Rst Ack Port Scan(Re...	224	35
TCP Syn Port Scan(Reverse)	149	46
TCP Syn Host Scan	122	76
TCP Rst Port Scan	111	19
Short TCP Syn Ack Port Scan(Re...	80	10
Others		

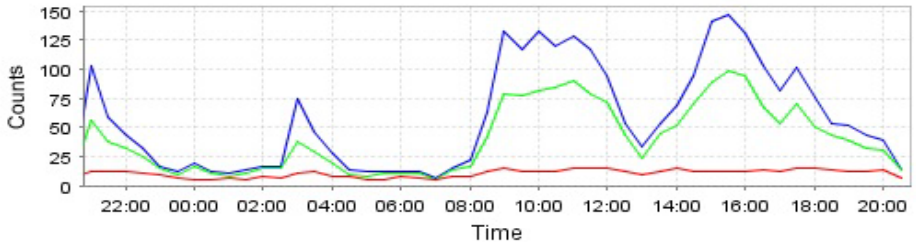
Events

Resources



Time Distribution

Events Resources Problems



DoS / Flash Crowd

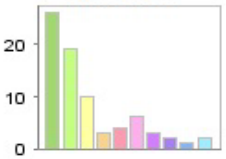
DoS / Flash

Problem / Events / Resources

Short TCP Ack Inflood	62	26
TCP Rst Inflood	50	19
TCP Syn Inflood	32	10
ICMP Port Unreachable Outflood	17	03
TCP Rst Outflood	14	04
Short TCP Psh Ack Inflood	09	06
Short TCP Psh Ack Outflood	09	03
Short TCP Fin Ack Inflood	09	02
Short TCP Syn Ack Inflood	08	01
Short TCP Rst Ack Inflood	07	02
Others		

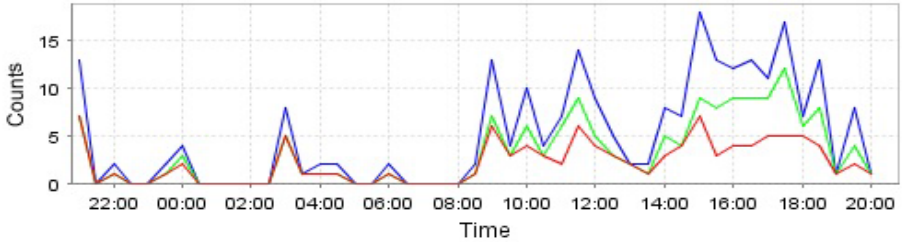
Events

Resources



Time Distribution

Events Resources Problems



There's No Stopping ME
IT Software In Over 200 Countries & Growing
ManageEngine.com
Powering IT ahead

ASAM(보안 분석) event 상세 자료 보기

Security Analytics Configuration

Security Events

Security Dashboards

- Last 24Hour(136)
  - Suspect Flows(136)
  - Scans / Probes(0)
  - Bad Src-Dst(0)
  - DoS / Flash Crowd(0)

Event List

Show Filter

White List | Manage | Algorithm Settings | Location | More Actions | Show IP

Flows Processed : 296080

Report Details 1 - 8 Per Page : 25

	ID	Problem		Offender(s)	Routed via		Target(s)	Time	Hits	
	193977	**Suspect Flows** - Malformed TCP Packets	NA	21: [192.168.181.2, 192.168.181.9, 192.168.181.16, 192.168.181.23, 192.16...	20: [RC_Datacenter (Serial 1/1), RC_Datacenter (FastEthernet 1), RC_Datac...	NA	21: [192.168.116.4, 192.168.116.11, 192.168.116.18, 192.168.116.25, 192.1...	2012-08-14 09:09:00 -- 2012-08-14 09:12:55	100	View
	193978	**Suspect Flows** - Malformed TCP Packets	NA	21: [192.168.181.2, 192.168.181.9, 192.168.181.16, 192.168.181.23, 192.16...	20: [RC_Datacenter (Serial 1/1), RC_Datacenter (FastEthernet 1), RC_Datac...	NA	21: [192.168.116.4, 192.168.116.11, 192.168.116.18, 192.168.116.25, 192.1...	2012-08-14 09:09:00 -- 2012-08-14 09:12:55	100	View
	193973	**Suspect Flows** - Malformed TCP Packets	NA	21: [192.168.181.11, 192.168.181.18, 192.168.181.25, 192.168.181.32, 192....	20: [RC_Datacenter (Serial 1/1), RC_Datacenter (FastEthernet 1), RC_Datac...	NA	21: [192.168.116.61, 192.168.116.68, 192.168.116.75, 192.168.116.82, 192....	2012-08-14 09:05:40 -- 2012-08-14 09:09:25	100	View
	193974	**Suspect Flows** - Malformed TCP Packets	NA	21: [192.168.181.11, 192.168.181.18, 192.168.181.25, 192.168.181.32, 192....	20: [RC_Datacenter (Serial 1/1), RC_Datacenter (FastEthernet 1), RC_Datac...	NA	21: [192.168.116.61, 192.168.116.68, 192.168.116.75, 192.168.116.82, 192....	2012-08-14 09:05:40 -- 2012-08-14 09:09:25	100	View
	193943	**Suspect Flows** - Malformed TCP Packets	NA	23: [192.168.181.83, 192.168.181.90, 192.168.181.97, 192.168.181.104, 192...	20: [RC_Datacenter (Serial 1/1), RC_Datacenter (FastEthernet 1), RC_Datac...	NA	23: [192.168.116.76, 192.168.116.83, 192.168.116.90, 192.168.116.97, 192....	2012-08-14 03:05:00 -- 2012-08-14 03:09:30	100	View
	193944	**Suspect Flows** - Malformed TCP Packets	NA	23: [192.168.181.83, 192.168.181.90, 192.168.181.97, 192.168.181.104, 192...	20: [RC_Datacenter (Serial 1/1), RC_Datacenter (FastEthernet 1), RC_Datac...	NA	23: [192.168.116.76, 192.168.116.83, 192.168.116.90, 192.168.116.97, 192....	2012-08-14 03:05:00 -- 2012-08-14 03:09:30	100	View
	193939	**Suspect Flows** - Malformed TCP Packets	NA	23: [192.168.181.6, 192.168.181.13, 192.168.181.20, 192.168.181.27, 192.1...	20: [RC_Datacenter (Serial 1/1), RC_Datacenter (FastEthernet 1), RC_Datac...	NA	23: [192.168.116.6, 192.168.116.13, 192.168.116.20, 192.168.116.27, 192.1...	2012-08-14 03:01:50 -- 2012-08-14 03:06:00	100	View

There's No Stopping ME
IT Software In Over 200 Countries & Growing
ManageEngine.com
Powering IT ahead

HighPerf Reporting 엔진

- 증강된 원천 데이터 저장 능력
- 즉각적인 보고서 생성
- Columnar Database 사용
  - Row 로 데이터를 저장하지 않고, column으로 저장하여 검색 속도를 높이는 데이터베이스. Disk 에 쓰고 읽는 속도가 빠름.

Professional Edition

- 실시간 보고서: Bandwidth, application, port, protocol, host, conversation, ToS, DSCP, TCP Flags.
- 임계치 위반 시 경보 발생: interface, IP, port and DSCP
- 자동 정기 보고서: 비교 보고서, 커스텀 대시 보드
- 그룹화 기능: 부서, 네트워크, IP 등
- Cisco ASA NSEL, Cisco Medianet , Cisco WAAS 보고서
- TimeZone 기준의 보고서
- Cisco AVC(Application Visibility and Control)

Add-Ons for Essential Edition

- **Cisco IPSLA Module** – 최대 100 까지의 모니터가 생성되고 감시됨.
- **Advanced Security Analytics Module** – 기준 인터페이스의 수와 동일하게 지원됨.
- **High Perf Engine – 최대 1 년까지** raw NetFlow 데이터 보유
- Cisco NBAR 보고서, Cisco QoS 보고서, 사용량 기준 과금, 용량 계획

Enterprise Edition (분산 에디션)

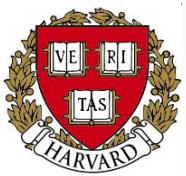
- 대역폭 감시와 트래픽 분석에 대한 모든 'Essential Edition' 기능 포함
- 분산 구조: Central reporting server & flow collectors
- 확장성 : 100,000 flows per second , 20,000 interfaces
- 최대 1 년의 raw NetFlow 데이터 유지, 통합 데이터는 영구히 유지
- Edition에서는 Essential Edition의 모든 Add-on 포함

지원되는 장비

Vendor	Flows	Device List
Cisco	NetFlow	800, 1700, 2600, 1800, 1900, 2800, 2900, 3660, 3800, 3900, 4500, 6500, 7200, 7300, 7500, 7600, 10000, 12000, Cisco ASA (IOS 8.2 onwards), Catalyst 4500 series, Catalyst 6500 series, Nexus 7000, Cisco ASR and even more
Hewlett-Packard	sFlow	ProCurve series
Juniper Networks	NetFlow, J-Flow	Juniper SRX series, M10i series and more Juniper devices
Nortel	IPFIX	5500 & 8600 Series
Adtran	NetFlow	NetVanta 3200, 3305, 4305, 5305, 1524, 1624, 3430, 3448, 3130, 340, and 344
3Com	NetFlow	8800 Series Switches
Extreme Networks	NetFlow	Alpine 3800 series, BlackDiamond 6800 series, BlackDiamond 8800 series, BlackDiamond 10808, BlackDiamond 12804C , BlackDiamond 12804R ,Summit X450 Series , Summit i series
Force10 Networks	sFlow	E series
Dell – Force 10 Networks	sFlow	PowerConnect 6200 series, PowerConnect 8200 series
Huawei	NetStream	Huawei AR1200, NE40EX3 and more

Customers

NetFlow Analyzer is used by more than 5000 Enterprises worldwide



www.netflowanalyzer.com

Technical Support Team in Korea:
inforeq@tmn.co.kr

NetFlow Analyzer Blogs:
https://blogs.netflowanalyzer.com

User Forums:
http://forums.netflowanalyzer.com

LinkedIn:
http://www.linkedin.com/groups?gid=4208806&trk=hb_side_g

There's No Stopping ME
IT Software In Over 200 Countries & Growing
ManageEngine.com
Powering IT ahead

감사합니다

텔리맨트 주식회사
https://www.tmn.co.kr
02) 588-7350

기술 질문: inforeq@tmn.co.kr
견적 요청: sales-info@tmn.co.kr