트래픽 제어를 통한 보안가이드
(Proactive Network Enforcement)

네트워크의 미래를 제시하는 세미나 **NetFocus 2003 :**
IT 관리자를 위한 네트워크 보안 방법론

on the NET
Network Intelligence for Leading Networkers

㈜인터콘웨어 / 과장
김 지 환
Jhkim@interconware.com

Agenda

IT Manager Requirements

IT관리 **Trend**의 변화

Proactive Network Enforcement

1.25대란 대응사례

QoS 매커니즘 비교표

통합보안서비스의 구축

실시간 경보 자동화 시스템

NMS와의 연동서비스

IDS/Firewall과의 연동

Proactive Network Enforcement의 장점

Reference site

IT 관리 Trend의 변화

- 급격한 **IT**환경의 변화에 따라 **IT Business**와 **Organization**의 성장속도 및 규모를 예측하기 힘듦

  →투자예산 시기 및 규모 측정이 어려워짐
- 단순한 네트워크 관리 측면을 지나 현재 상황에 대한 인지와 향후 대책 수립의 근거 자료가 요구됨
- **1.25** 인터넷 대란을 통한 손실은 **TCO**와 **ROI** 접근으로는 측정이 불가능함
- 소수의 인원으로 수많은 기회손실 요인에 대한 해결과 능동적인 대응이 어려움
- 능동적이고 중앙 집중적인 네트워크 관리는 계속기업**(Going Concern)**을 유지하기 위한 **IT Manager**의 최종 과제임

IT Manager Requirements

Real time Traffic Analysis

Historical Traffic Reporting & Trend Analysis

(day, week, Month, year)

Central Management with NMS

Business 지향적인 **Traffic** 관리

- **ERP, VoIP,**화상회의 등 **Mission Critical Application** 대역폭 보장
- 비업무용 트래픽**(P2P, FTP)**의 차등화된 대역폭 제공

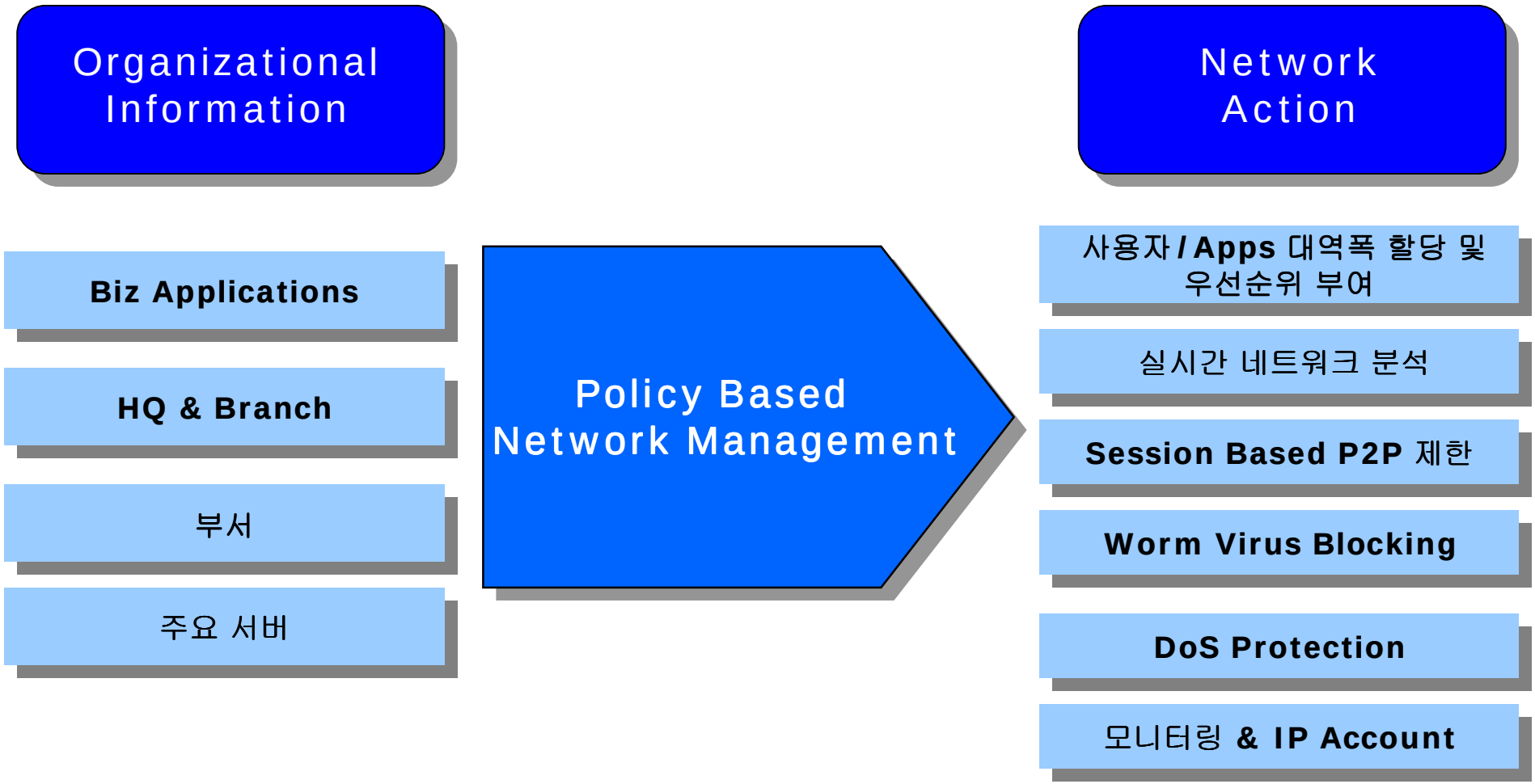
Build a Proactive Security Environment

- Dos Attack Protection
- Worm Virus Protection(Slammar, Nimda, Codered, etc)
- Firewall 및 IDS와의 연동 및 기능 강화

SLA Service의 제공

- Tiered Service 제공(Gold/Silver/Bronze)
- Accounting & Billing

Proactive Network Enforcement



사이버테러 현황 자료(Slammer Worm)

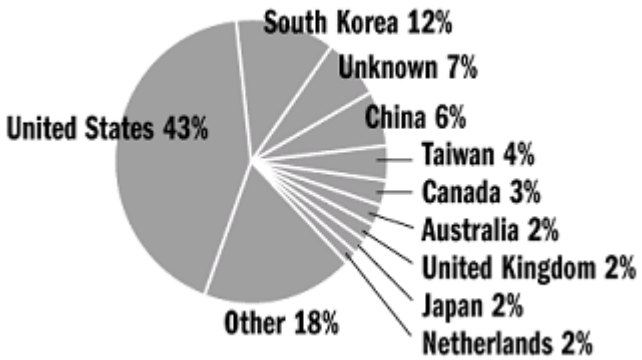
- 다량의 Slammer Worm 패킷 발생으로 네트워크 트래픽 마비
- ISP의 DNS서버 장애로 인터넷 접속 장애 또는 지연이 발생

국내 8,800여 SQL서버에 감염

전세계 감염대수의 11.8%

일본의 7배, 중국의 2배

<국가별 감염현황표>



출처: 인터넷 데이터 분석 협력협회(CAIDA)

1.25대란 대응사례 (S증권사)

- 실시간 네트워크 진단의 필요성 대두
- 사내 악성 사용자의 발견 및 조치
- **1.25** 대란으로 인한 증권 서비스망 및 내부망에 대한 진단 분석 솔루션의 필요성 제기
- 월별/분기별 리포팅 솔루션의 필요
- 능동적 보안 솔루션**(Worm Protection** 및 **DOS Protection)**의 필요

1.25대란 대응사례

- 이상징후의 포착

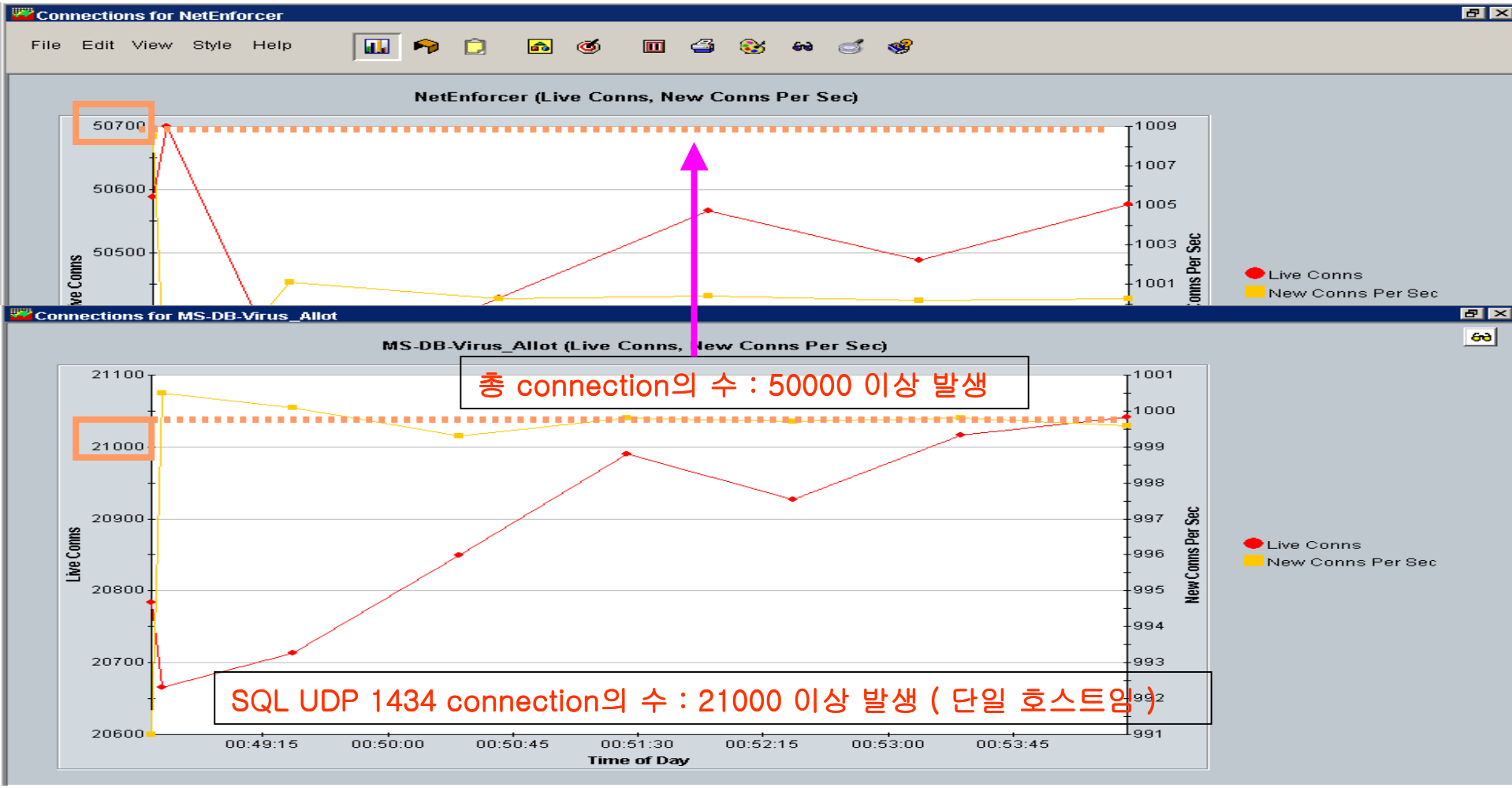
```
UDP    210.205.      :2348    64.133.243.70:1434    WIRED Allot    MS-DB-V    1 d
UDP    210.205.      :2348    142.38.7.137:1434     WIRED Allot    MS-DB-V    1 d
UDP    210.205.      :2348    8.21.80.180:1434      WIRED Allot    MS-DB-V    1 d
UDP    210.205.      :2348    80.62.177.239:1434    WIRED Allot    MS-DB-V    1 d
UDP    210.205.      :2348    222.168.161.214:1434  WIRED Allot    MS-DB-V    1 d
UDP    210.205.      :2348    116.228.101.110:1434  WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    210.182.149.171:1434  WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    162.122.86.174:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    24.98.96.51:1434      WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    70.210.121.98:1434    WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    140.223.142.146:1434  WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    202.173.8.111:1434    WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    96.6.78.247:1434      WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    46.38.43.211:1434     WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    148.35.183.65:1434    WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    114.204.4.166:1434    WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    150.233.134.237:1434  WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    28.237.77.92:1434     WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    154.190.192.136:1434  WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    112.107.19.206:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    126.196.61.37:1434    WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    36.4.35.148:1434      WIRED Allot    MS-DB-V    0 d
UDP    210.205       :2348    66.236.129.190:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205       :2348    56.188.108.246:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    128.86.135.30:1434    WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    60.106.228.4:1434     WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    30.187.135.206:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    88.174.187.128:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    134.99.34.28:1434     WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    204.89.20.75:1434     WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    160.190.11.248:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    110.147.45.118:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    178.159.38.72:1434    WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    104.192.196.150:1434  WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    176.187.128.199:1434  WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    192.62.109.191:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    118.107.32.62:1434    WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    142.152.155.15:1434   WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    116.125.17.50:1434    WIRED Allot    MS-DB-V    0 d
UDP    210.205.      :2348    210.131.216.118:1434  WIRED Allot    MS-DB-V    0 d
AC401:~# netstat
-----
TCP    : 29457
UDP    : 20840
anyIP  : 17
nonIP  : 3
-----
TOTAL  : 50317
AC401:~#
```

총 컨넥션의 수가 증가했으며 특히 UDP 컨넥션수가 많음

```
number of new connections per second was achieved
ax Connections 12000" triggered
number of new connections per second was achieved
number of new connections per second was achieved
ax Connections" resolved
number of new connections per second was achieved
ax Connections 12000" triggered
ax Connections" resolved
ax Connections 12000" triggered
ax Connections" resolved
ax Connections 12000" triggered
ax Connections" resolved
ck of the type 'UDP flood' started
ax Connections 12000" triggered
ck of the type 'UDP flood' ended
number of new connections per second was achieved
ax Connections 12000" triggered
number of new connections per second was achieved
ax Connections" resolved
number of new connections per second was achieved
ax Connections 12000" triggered
number of new connections per second was achieved
ax Connections" resolved
ck of the type 'UDP flood' started
ck of the type 'UDP flood' ended
ck of the type 'UDP flood' started
ck of the type 'UDP flood' ended
ck of the type 'UDP flood' started
ax Connections 12000" triggered
ck of the type 'UDP flood' ended
number of new connections per second was achieved
Jan 25 14:59:08 AC201-2M kernel: Alarm "Max Connections" resolved
Jan 25 14:59:23 AC201-2M kernel: Alarm "Max Connections 12000" triggered
Jan 25 14:59:24 AC201-2M kernel: Alarm "Max Connections" resolved
Jan 25 14:59:24 AC201-2M kernel: Alarm "Max Connections 12000" triggered
--More--
```

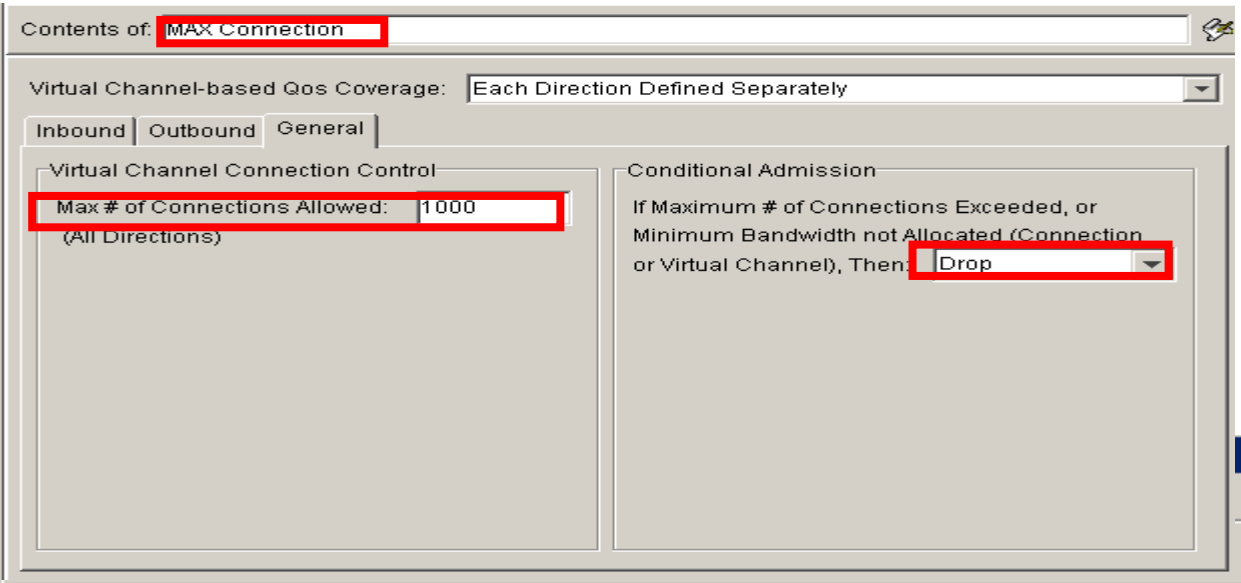
1.25대란 대응사례

- 실시간 세션 분석



1.25대란 대응사례

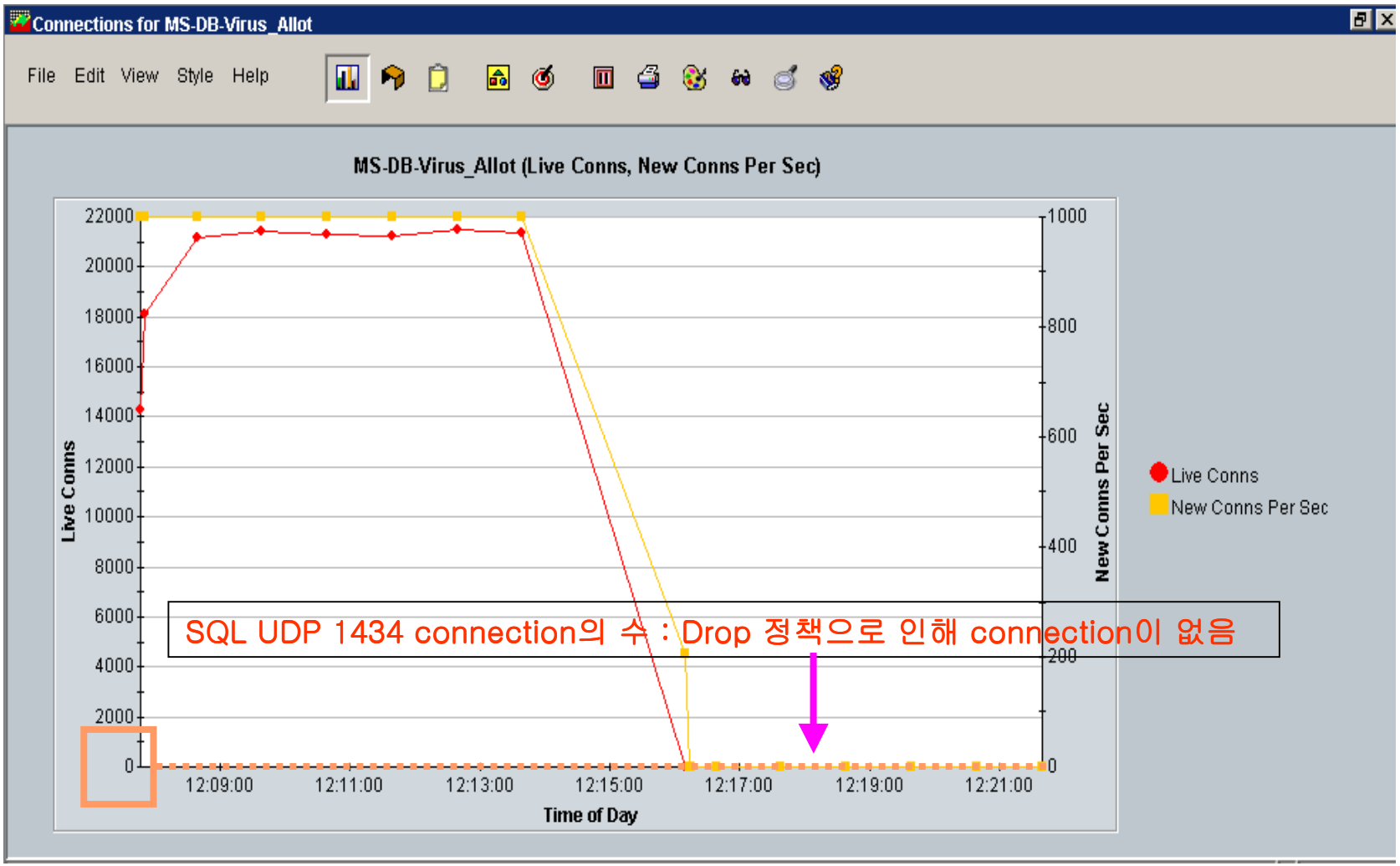
- Max Session 제어를 통한 문제접근



Name	In Use	Connection Source	Dir	Connection Destination	Service	Time		Access	Quality of Service	Connection Control
Allot	✓	**Any**	⇔	**Any**	**All IP**	**Anytime**	→	**Accept**	**Normal Priority...**	**Pass As Is**
MS-DB-Virus	✓	MS-DB	⇔	Any	UDP1434	Anytime	→	Accept	MAX Connection	Pass As Is
pc1	✓	pc1	⇔	Any	All IP	Anytime	→	Accept	Normal Priority ...	Pass As Is
pc2	✓	pc2	⇔	Any	All IP	Anytime	→	Accept	Normal Priority ...	Pass As Is
pc3	✓	pc3	⇔	Any	All IP	Anytime	→	Accept	Normal Priority ...	Pass As Is
pc4	✓	pc4	⇔	Any	All IP	Anytime	→	Accept	Normal Priority ...	Pass As Is
Fallback	✓	Any	⇔	Any	All Service	Anytime	→	Accept	Normal Priority ...	Pass As Is

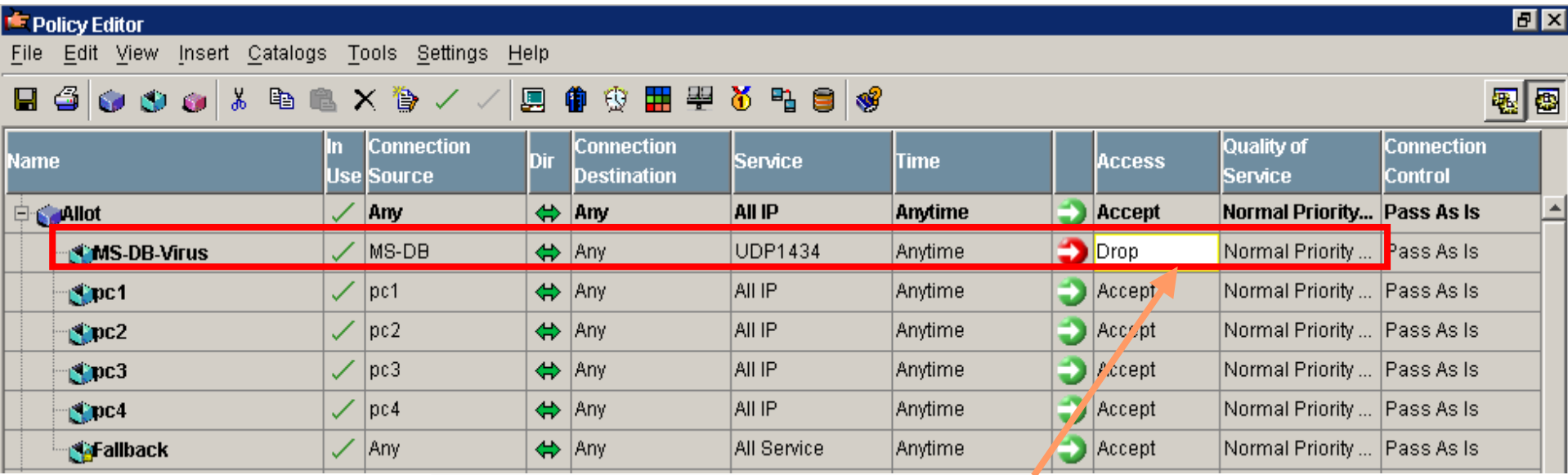
1.25대란 대응사례

- Session 제어 결과



1.25대란 대응사례

- Access Control을 통한 Virus 통제



SQL UDP 1434 connection을 Drop 시킴

1.25대란 대응사례

- ACL Log를 통한 Virus 감염자 추적

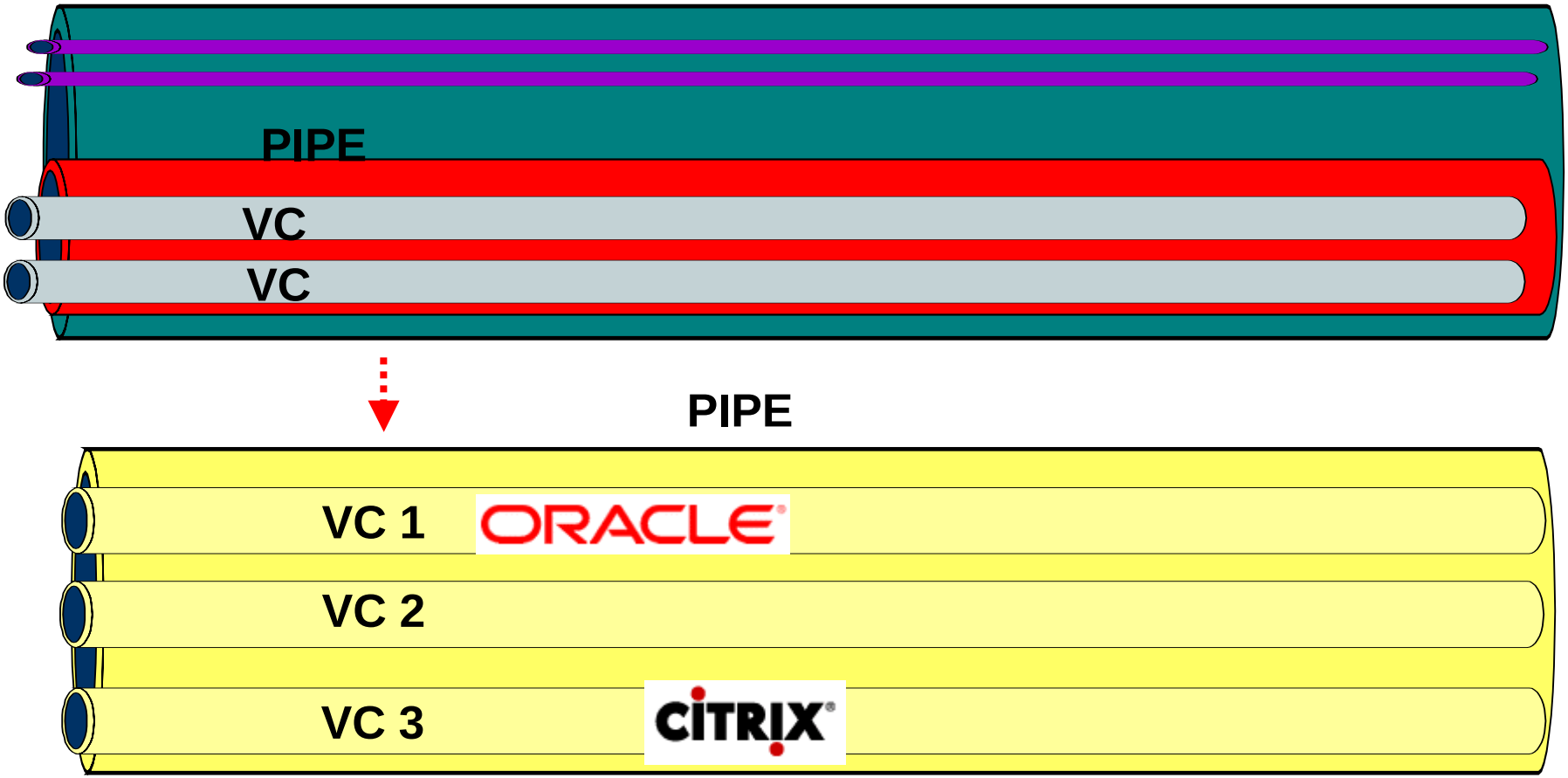
```
AC401:/usr/local/SWG/logs# tail -f log.SWG |more
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,54.92.72.42:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,72.132.104.86:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,18.212.226.212:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,180.140.3.198:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,206.106.146.205:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,128.184.50.68:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,106.23.11.94:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,172.34.118.166:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,230.136.248.93:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:30 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,56.190.70.13:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:31 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,38.12.224.244:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:31 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,120.52.45.81:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:31 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,130.131.241.51:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:31 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,100.62.193.157:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:31 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,190.21.156.190:1434> Access Denied
 Allot,MS-DB-Virusn 26 12:15:31 2003 Fatal   AcC    <IP,UDP,210.205.    :2348,176.119.77.3:1434> Access Denied
```

UDP 14340l Access Deny되고 있는 상황

Connection Limitation

T1 Connection

Total guaranteed throughput = 1.5Mbps

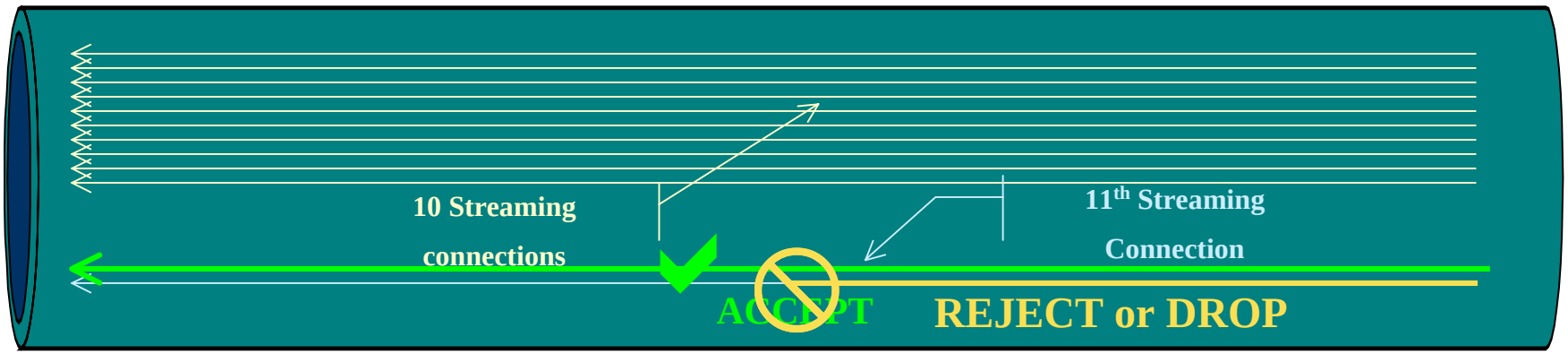


VC Maximum = 150Kbps, Minimum per Connection = 45Kbps

Quality of Service Options

- Minimum
- Maximum
- Maximum no. connections
- Priority
- Per Pipe
  - Min/Max, Priority, max no. connections
- Per VC
  - Min/max, priority, max no. connections
- Per connection
  - CBR + delay
  - Gurantee + burst
  - CIR/EIR
- Direction Specific
    - Inbound / Outbound
    - Both direction

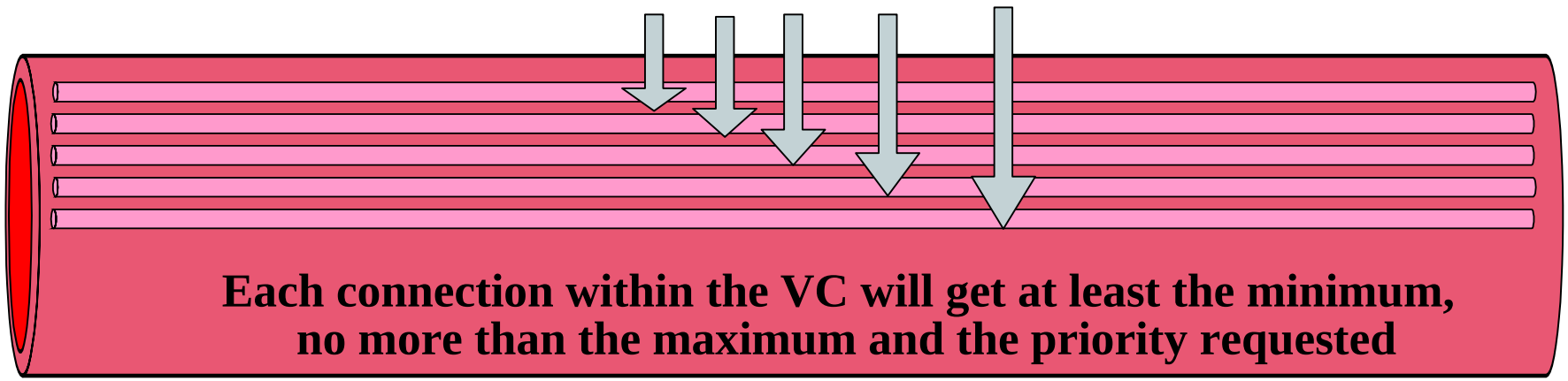
Traffic Control Per Connection



Minimum, Maximum and Priority

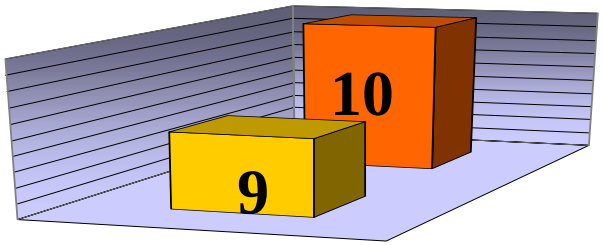
UDP Protocol

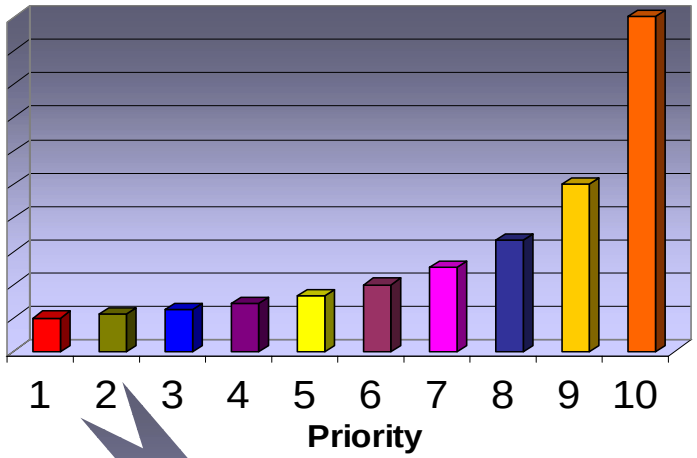
Min, Max and Priority for each connection



Each connection within the VC will get at least the minimum, no more than the maximum and the priority requested

Priority Matrix (10 Level)





Priority									
2	1.1								
3	1.2	1.1							
4	1.4	1.2	1.1						
5	1.6	1.5	1.3	1.1					
6	2.0	1.8	1.6	1.4	1.2				
7	2.5	2.2	2.0	1.7	1.5	1.2			
8	3.3	3.0	2.7	2.4	2.0	1.7	1.4		
9	5.0	4.5	4.0	3.5	3.0	2.5	2.0	1.5	2.0
10	10.0	9.0	8.0	7.0	6.0	5.0	4.0	3.0	2.0
Priority	1	2	3	4	5	6	7	8	9

QoS 메커니즘 비교표

	PFQ	CBQ	TCP Rate Limiting
QoS Policy Guarantee	**Per flow queuing** **Individual session/connection** **Packet adaptation**	**Tosses packets** **Packet loss** **Retransmissions**	**Packet loss** **Retransmission**
Priority Level	**10 Levels** **Hierarchical**	**7 Levels**	**7 Levels** **Hierarchical**
Directional	**In-bound and/or out-bound**	**Out-bound**	**In-bound and/or out-bound**
QoS Assurance	**Minimum, maximum, burst, CIR, connection, fairness of access**	**Minimum, maximum, burst, CIR, point-to-point only**	**Minimum, maximum, burst, reject packets when congested**
QoS Policy Delay Bound	**Traffic classification** **Bits-per-second control** **Connection-based for TCP packets** **Flow-by-flow for UDP packets**	**Traffic Classification** **Bits-per-second control** **Flow-by-flow control**	**Traffic classification** **Bits-per-second control** **No flow control, Rate-based**
Control method	**Dynamic**	**Static**	**Dynamic**

통합보안 서비스의 구축

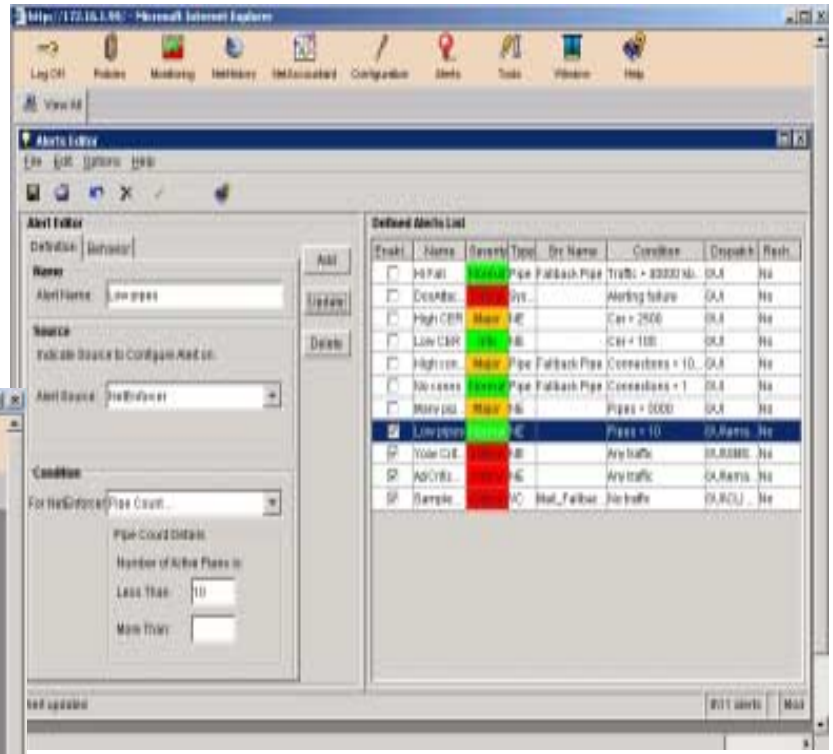
- 서비스 내역
  - 24X365 무정지 전담요원 모니터링
  - 특수 애플리케이션 모니터링 지원
  - 장애발생 및 내역 실시간 인적 통보
  - 인프라 운영현황 온/오프라인 정기리포
  - 전문 요원 기술 자문 위원

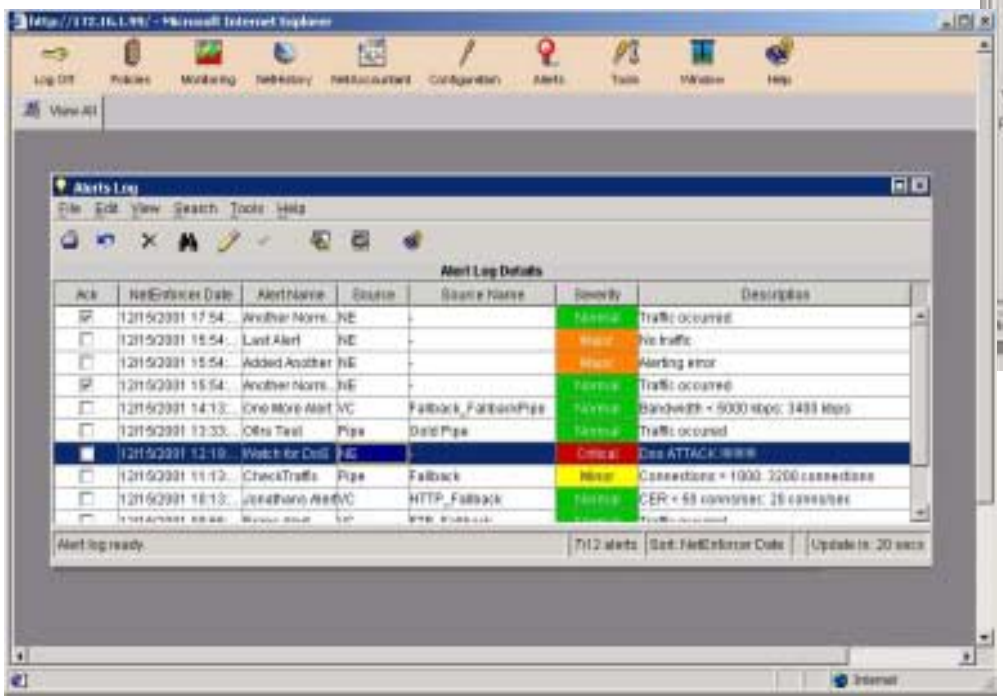
- 서비스 특징
  - 전담 요원 지정 모니터링 책임 관리
  - 장애 발생 예후 즉시 고객사 전화통보
  - 다양한 리포팅 프리젠테이션 결과물
  - 전문 기술진 노하우 전수, 문제관리
  - on-site 장애해결 지원 연계

실시간 경보 자동화 시스템
-Alert Module

NetEnforcer Alert Module

- **maximum** 임계치 초과시 **Alert** 발생
- 정책의 변동요인 발생시
  Email 또는 **SMS message** 송신



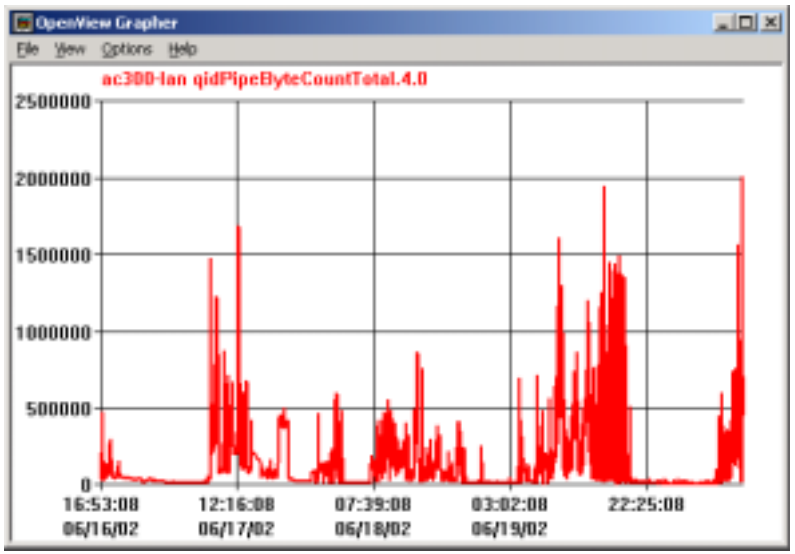


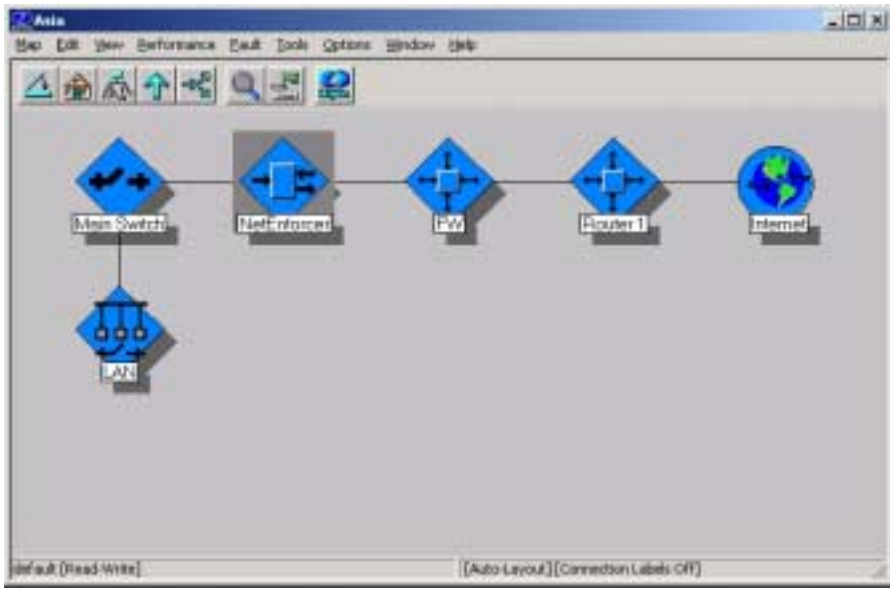
NMS 연동서비스

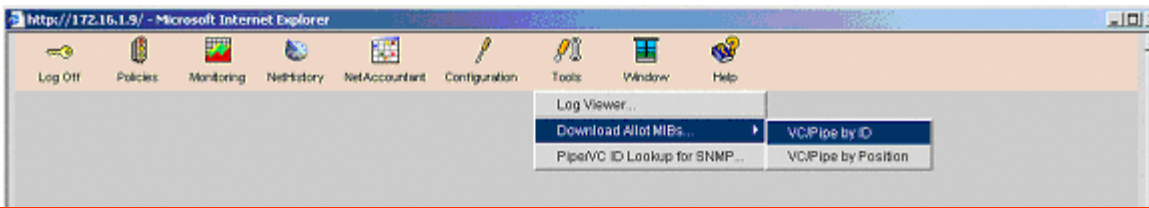
- NMS 연동 서비스

 - NetEnforcer의 Mib을 다운로드하여 NMS상에 NetEnforcer를 등록함

 - NMS상에서 QoS장비가 제공하는 Pipe/VC 레벨의 트래픽 사용 현황을 모니터링 할 수 있음.

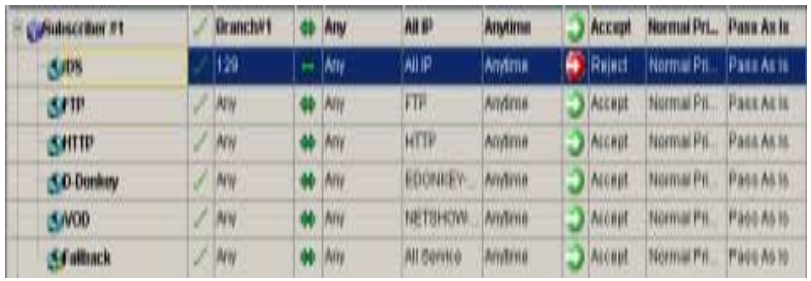




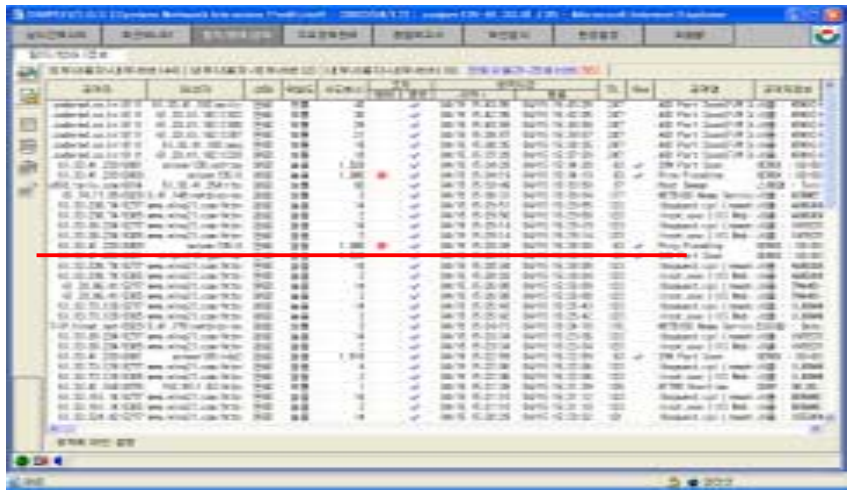


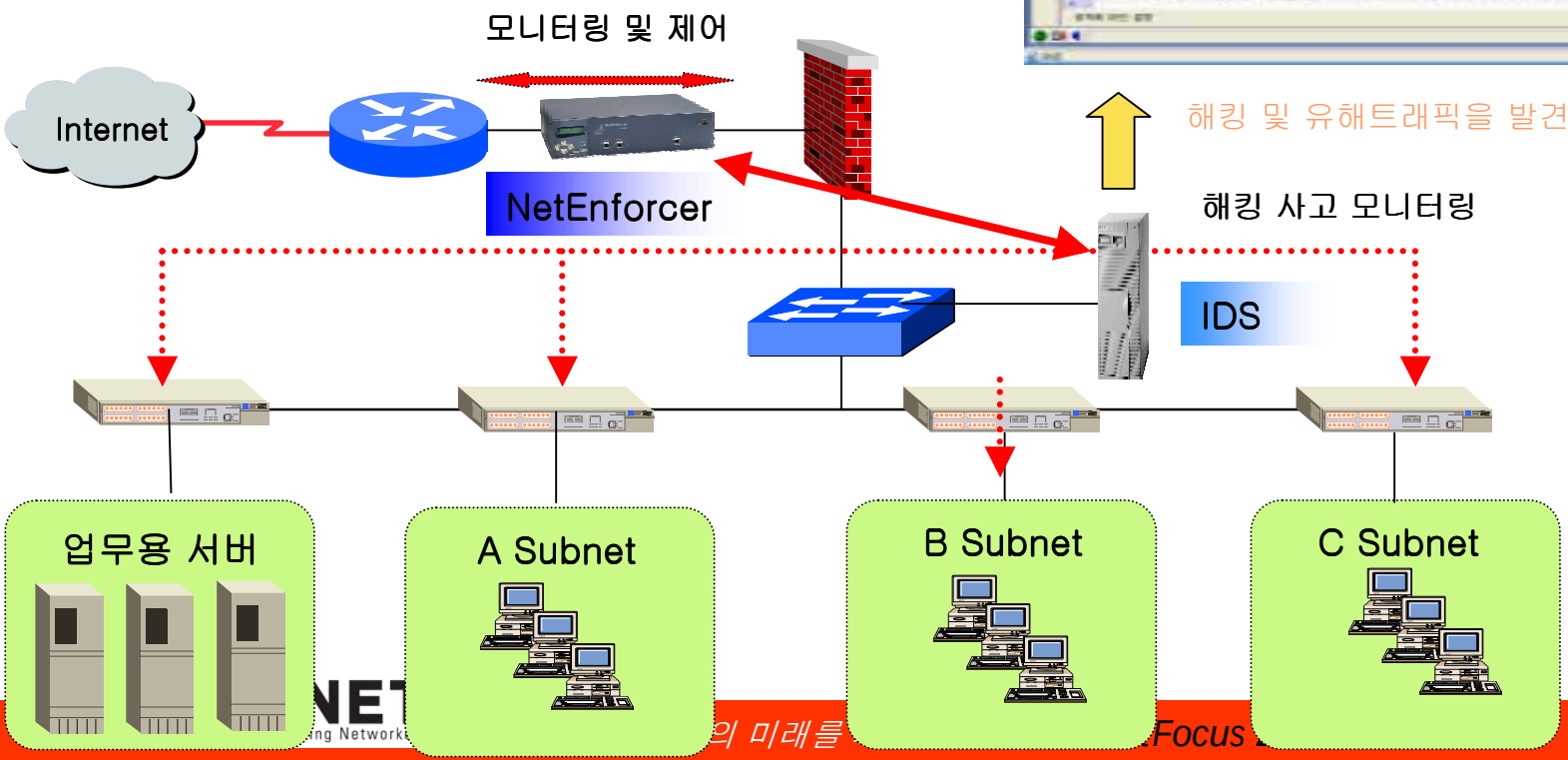
IDS/Firewall과의 연동

해당 트래픽에 대한 제어



Alarm





Proactive Network Enforcement 장점

- 사내 네트워크 트래픽을 **Business Application** 중심으로 운영이 가능
- 정책기반의 네트워크 구축이 가능**(LDAP**과 연동**)**
- 현재 네트워크 장애 유발 요인에 대한 진단과 실시간 대응이 가능함
- **Session Base Management**를 통한 비업무용 애플리케이션에 대한 제어가 가능
- **LAN/WAN Edge**구간을 **Worm Virus**에 대해서 안전한 구성이 가능함
- 다양한 솔루션과의 통합을 통해 통합관리의 지표 제시

Q & A