윈스
솔루션 소개

contents

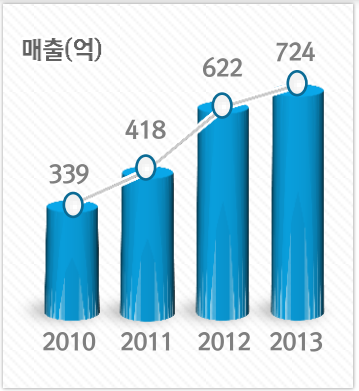
- 통합보안솔루션 (Sniper UTM)
- Anti-DDoS (Sniper DDX)
- 침입방지시스템 (Sniper IPS)
- 위협관리시스템 (Sniper iTMS)
- 방화벽_AF (Sniper AF)

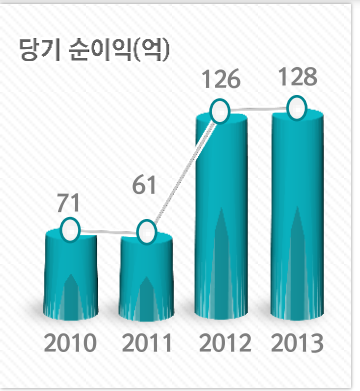
회사소개

㈜윈스

대표자	김대연
해당부문종사 기간	1996년 4월 ~ 현재 (약 18년)
자본금	57억
종업원수	320명
기업신용평가 등급	E-3- (회사채등급 : A-)

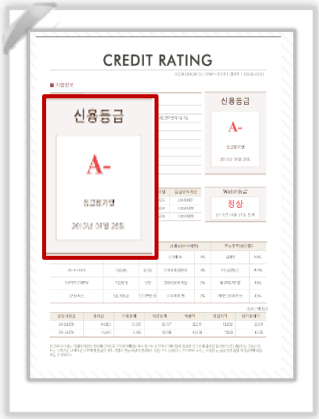
경영상태 성장





대외인지도

신용평가등급(A-)



World Class 300

컨설팅 전문업체

보안관제 전문업체

1000만불 수출탑

윈스 사업영역(보안솔루션)

“시장점유율 1위”

Sniper IPS 84%

Sniper DDX 47%

Sniper iTMS 55%

네트워크 보안

Sniper IPS 침입방지

Sniper FW 침입차단

Sniper UTM 통합보안

DDoS 대응

DDoS방어 Sniper DDX

APT 방어 Sniper APTX

통합 보안

Sniper iTMS 위협관리

Sniper TSMA 통합보안관제

VoIP 보안

VoIP방화벽 Sniper VF

VoIP IPS Sniper IPS-V

웹 보안

Sniper WAF 웹방화벽

윈스 사업영역(보안서비스)

보안 관제

파견관제

원격관제

정보보안 컨설팅

통합보안 컨설팅

인증취득 컨설팅

기반시설 컨설팅

진단 및 모의해킹

보안 SI/NI

사업설계 및 컨설팅

제안 및 시스템 구축

위협 예/경보

취약점 /악성코드 DB

글로벌 위협정보

웹 보안

예방 및 점검

네트워크 보안 리더, 윈스

Global Network Security Leader

글로벌 네트워크 정보보안 리더

"기업 환경의 전방위적 네트워크 보안 체계 제공"

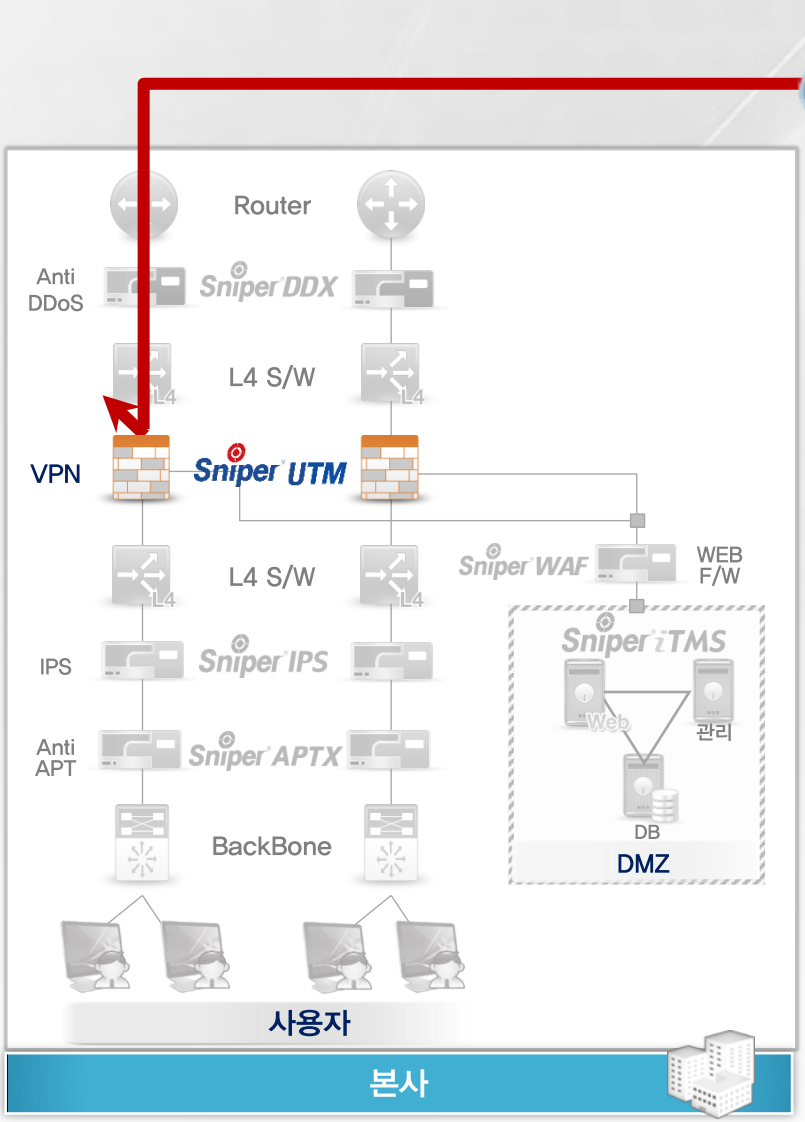
I 통합보안솔루션 (Sniper UTM)

가. UTM 개요

나. 주요 기능

다. Line-Up

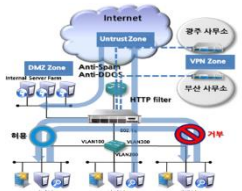
가. UTM 개요



Sniper UTM 개요

다양한 보안 기능 통합 솔루션

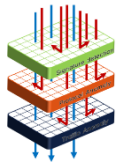
F/W기능 (정책기반제어)



VPN 기능

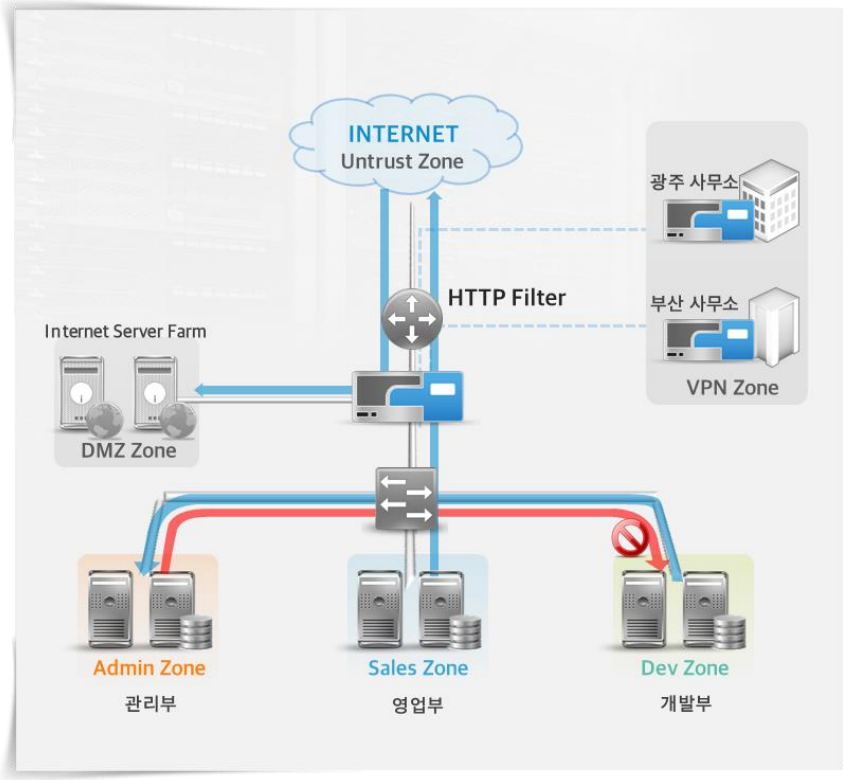
컨텐츠 필터링

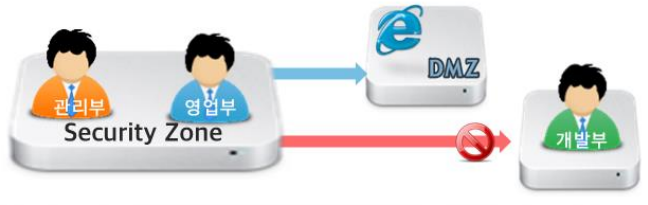
IPS/DDoS 기능



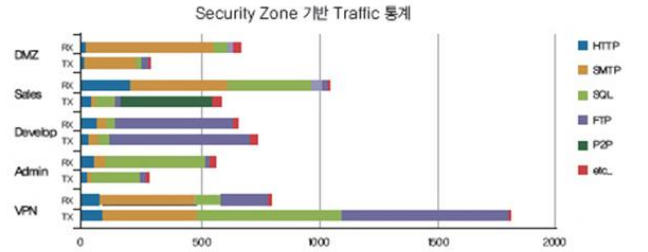
나. 주요기능

Zone 별 개별 정책/ 로그/ 통계





- 그룹으로 나누어 정책관리 및 모니터링
- 가상 방화벽 기능으로 존별로 객체 및 정책 설정 지원



다. Line-Up

	UTM 1000	UTM 2000	UTM 4000	UTM 5000
Throughput	2Gbps	4Gbps	8Gbps	40Gbps
Hardware				
CPU	Intel PineView D525 1.8Ghz	Intel Core2Duo 3.0GHz	Intel QuadCore 3.4GHz	Intel QuadCore 2.53GHz*2
Memory / HDD	1GB / 500GB	4GB / 500GB	8GB/1TB	24GB/2TB
Interface	1G Copper * 6	1G Copper *4+1G Fiber *4	1G Copper *8 or 1G Copper *4+1G Fiber *4	10G Fiber*2 1G Fiber*4 1G Copper*4
대상고객	← 중소규모 네트워크 →		← 대규모 네트워크/ 서비스팜 →	

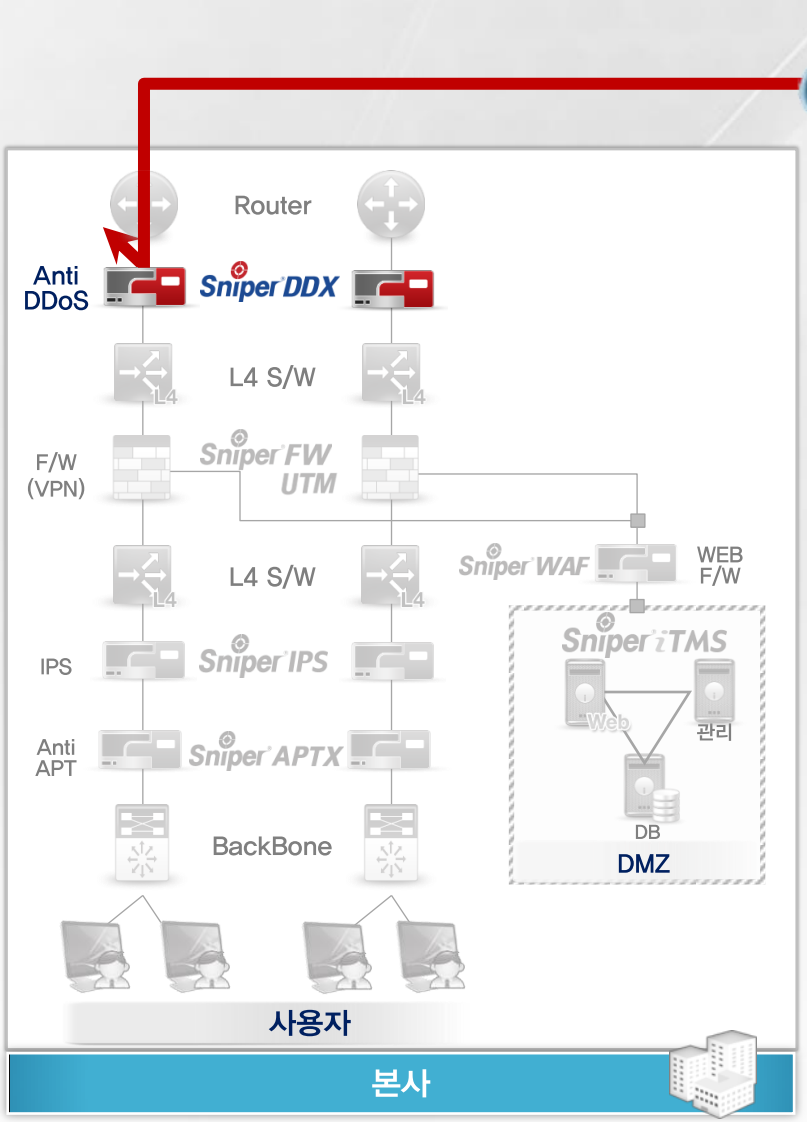
Ⅱ Anti-DDoS (Sniper DDX)

가. Anti-DDoS 개요

나. 시장점유율

다. Line-Up

가. Anti-DDoS 개요

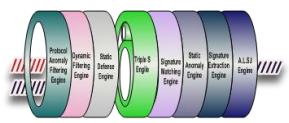


Sniper DDX 개요

DDoS 공격 탐지/방어 제품

실시간 트래픽 모니터링

DDoS 공격 탐지



DDoS 공격 방어(특허엔진)

국/내외 탐지 패턴 업데이트

나. 시장점유율

인터넷서비스제공자 Anti-DDoS 구축

주요 ISP에서도
Sniper DDX로 DDoS 방어

kt
SK telecom
SK broadband
LG U+
SEJONG TELECOM
CJ 헬로비전
t-broad
HYUNDAI 현대HCN
SeAH Dreamline Co.,Ltd.

Anti-DDoS 시장 점유율

국내 공공부분 시장 점유율 47%

✓조달 구매 통계 ('11~'13년)

국내 최초 Anti-DDoS 제품 출시, DDoS에 민감한 ISP에서 검증된 제품

다. Line-Up

	ND1000	ND2000	ND4000	ND5000	10G
Throughput	400Mbps	2Gbps	4Gbps	10Gbps	20Gbps
Hardware					
CPU	Quad Core 2.4Ghz	Quad Core 2.4Ghz * 2	Quad Core 2.4Ghz * 2	Quad Core 2.4Ghz * 2	IQuad Core 2.66Ghz * 2
Memory / HDD	6GB / 500GB	8GB / 500GB	12GB / 1TB*2	12GB / 1TB*2	12GB / 1TB*2
Interface	10/100/1000*2	10/100/1000(TX)*4 or 1000(SX/LX)*4	1000BaseSX(LX) *4	10G BaseSR(LR)*4	10G BaseSR(LR)*4
Power	Dual 2중화	Dual 2중화	Dual 2중화	Dual 2중화	Dual 2중화

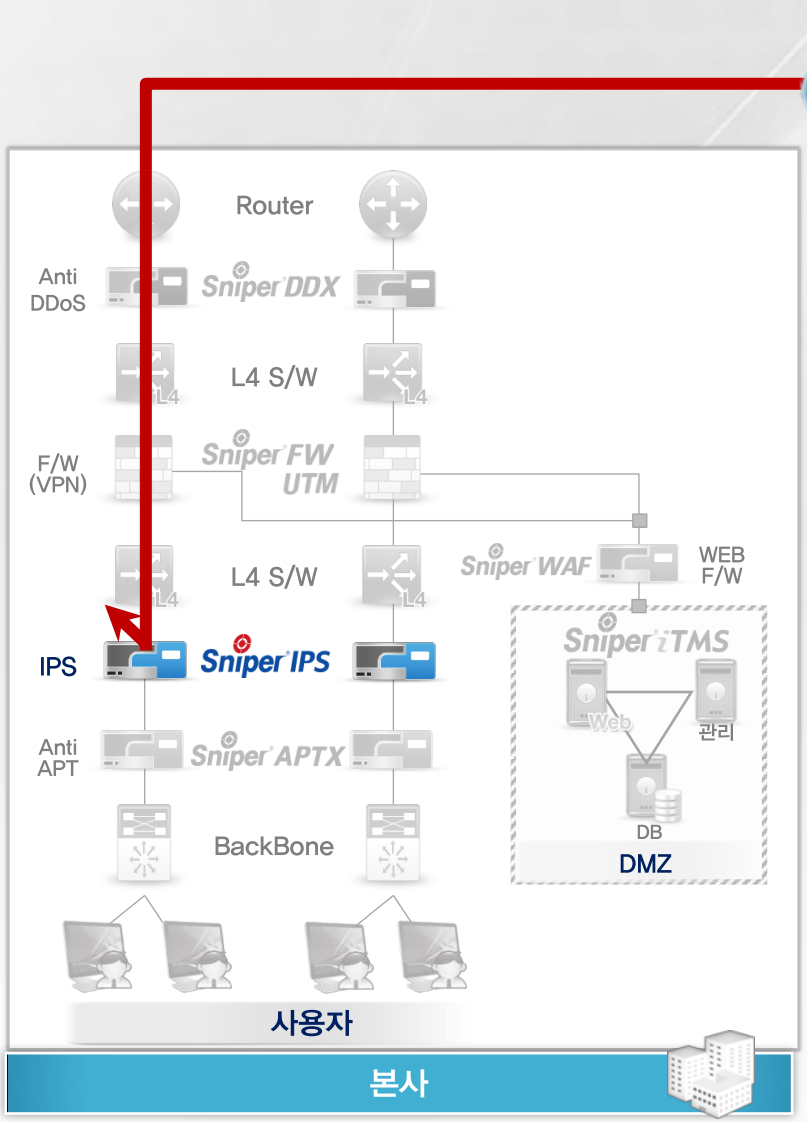
Ⅲ 침입방지시스템 (Sniper IPS)

가. IPS 개요

나. IPS 특장점

다. Line-Up

가. IPS 개요



Sniper IPS 개요

해킹 및 침해사고 탐지/차단 솔루션

- 어플리케이션 취약성
- 정보수집의 위협
- Injection, XSS
- 악성 Bot
- 중국발 해커
- Web Shell 위협
- DHCP 공격
- Worm 위협

L7 Semantics Analysis

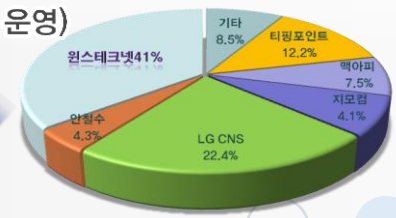
Protocol Anomaly	Layer 7까지	Signature 축약
Signature 분석	정밀한탐지및분석가능	오탐지 최소화

나. IPS 특장점(1/2)

IPS/IDS 10년 연속 시장점유율 1위

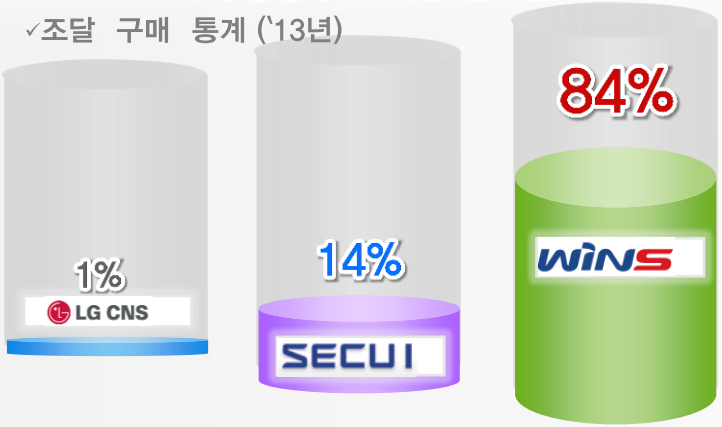
시장 점유율 1위

(3,000여 고객/12,800대 운영)



' 13 국내 공공부분 시장 점유율 84%

✓조달 구매 통계 ('13년)



일본에서 인정받은 기술력

윈스테크넷, 전년동기대비 45% 성장 달성

2012년 07월 26일 (목) 15:32:12 오현식 기자 hyun@datanet.co.kr

윈스테크넷의 상반기 실적발표에 따르면, 매출 261억원, 영업이익 58억원을 달성했다. 전년동기와 비교할 때 매출은 45% 증가한 수치며 영업이익은 90% 증가한 것. 이같은 실적 호조에 대해 윈스테크넷은 일본 비즈니스의 매출증가와 10Gbps 제품의 공급호조, 그리고 보안관제, 유지관리 매출증가가 주요 원인으로 설명했다.

특히 일본 수출이 본격화에 접었들었다는 점이 눈에 띈다. 윈스테크넷은 상반기 일본시장에서 60억원 가량의 매출을 올린 것으로 전해진다. 이는 전체 매출의 23% 수준에 달하며, 당초 해외사업 연간목표로 설정했던 규모다. 또한 캐시카우 역할을 하고 있는 IPS와 침입탐지시스템(IDS)의 10Gbps 고성능 모델의 수요가 증가하고, 서비스 부문도 전년 매출을 상반기에 초과하며 새로운 성장축이 되고 있다는 분석이다.

NTT docomo

구분	내용
납품 현황 ('11~13년)	• IPS 10G x 500 EA • IPS 2G x 1EA • IPS 1G x 9EA
시사점	• IPS 기술력 해외에서 인정 • 까다로운 일본시장에서 검증된 제품 • 단일 품목 1000만불 수출

나. IPS 특장점(2/2)

지속적인 IPS 탐지 패턴 업데이트

패턴코드	패턴명	월	No
1586	DDoS.Agent.	4월	64
1587	DDoS.Agent.	4월	65
1588	DDoS.Agent.	4월	66
1589	DDoS.Agent.	4월	67
1590	DDoS.Agent.	4월	68
1591	DDoS.Agent.	4월	69
1592	DDoS.Agent.	4월	70
1593	DDoS.Agent.65024.D.C&C	4월	71
1594	MS Common Controls MSCOMCTL.OCX Remote Code EXE.A	4월	72
1595	MS Common Controls MSCOMCTL.OCX Remote Code EXE.A(SMTP)	4월	73
1596	MS Common Controls MSCOMCTL.OCX Remote Code EXE.B	4월	74
1597	MS Common Controls MSCOMCTL.OCX Remote Code EXE.B(SMTP)	4월	75
1598	Obfuscated Script Detection(nb224=)	5월	76
1599	Unicode Extionsion Bypass Vul.A(SMTP)	5월	77
1600	Unicode Extionsion Bypass Vul.B(SMTP)	5월	78
1601	Unicode Extionsion Bypass Vul.C(SMTP)	5월	79
1602	Unicode Extionsion Bypass Vul.D(SMTP)	5월	80
1603	Unicode Extionsion Bypass Vul.E(SMTP)	5월	81
1604	Unicode Extionsion Bypass Vul.F(SMTP)	5월	82
1605	Unicode Extionsion Bypass Vul.G(SMTP)	5월	83
1606	Unicode Extionsion Bypass Vul.H(SMTP)	5월	84
1607	Unicode Extionsion Bypass Vul.I(SMTP)	5월	85
1608	Unicode Extionsion Bypass Vul.J(SMTP)	5월	86
1609	Adobe Multiple Product Type Confusion Code Execution Vul	5월	87
1610	Malware File Donwload(MZ_XOR)	5월	88
1611	User-Agent Field PHP Code Execution	6월	89
1612	Obfuscated Script Detection(Yszz)	6월	90
1613	MS Office RTF Mismatch Memory Corruption	6월	91
1614	MS Digital Certificates Spoofing Vul	6월	92
1615	MS Digital Certificates Spoofing Vul.A	6월	93
1616	MS XML Core Services Remote Code Execution Vul	7월	94
1617	MS XML Core Services Remote Code Execution Vul.A	7월	95
1618	Obfuscated Script Detection(Dadong)-4	7월	96
1619	Obfuscated Script Detection(TCP-5920)	7월	97
1620	Oracle Java Runtime Bytecode Verifier Cache Code Exe	7월	98
1621	Adobe Photoshop Asset Elements Stack BoF	7월	99
1622	Apple Quicktime Plugin SetLanguage BoF	7월	100
1623	Apple iTunes '.m3u' Playlist File Heap BoF	7월	101
1624	Oracle GlassFish Enterprise Server REST Interface CSRF	7월	102

13년 상반기

패턴 블록 102건 +Web CGI 13건

윈스 침해사고대응센터

13년 상반기 **115건**

(월 평균 16건)

지속적 공격 분석으로

신/변종 탐지 패턴 제공

다. Line-Up

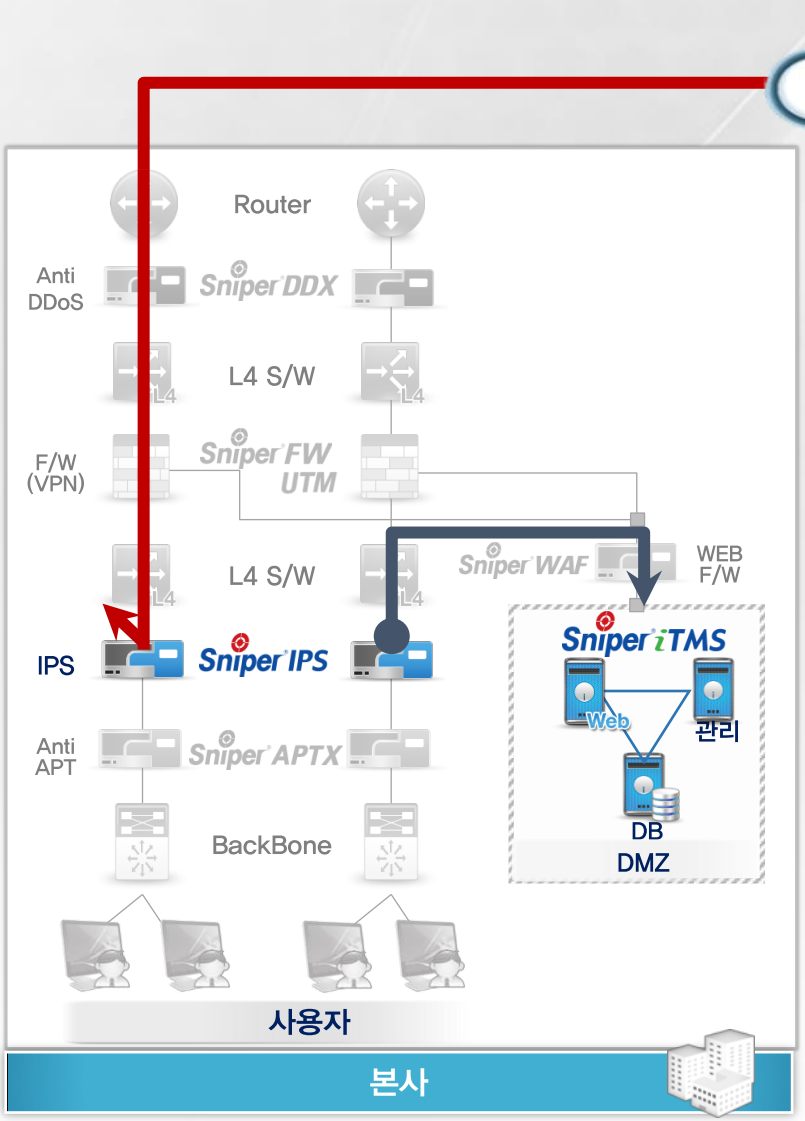
	NE1000	NE2000	NE4000	NE5000	IPS 10G
Throughput	400Mbps	2Gbps	4Gbps	10Gbps	20Gbps
Hardware					
CPU	Quad Core 2.4Ghz	Quad Core 2.4Ghz * 2	Quad Core 2.4Ghz * 2	Quad Core 2.4Ghz * 2	Quad Core 2.66Ghz * 2
Memory / HDD	6GB / 500GB	8GB / 500GB	12GB / 1TB*2	12GB / 1TB*2	12GB / 1TB*2
Interface	10/100/1000*2	10/100/1000(TX)*4 or 1000(SX/LX)*4	1000BaseSX(LX)*4	10G BaseSR(LR)*4	10G BaseSR(LR)*4
Power	Dual 2중화	Dual 2중화	Dual 2중화	Dual 2중화	Dual 2중화

Ⅳ 위협관리시스템 (Sniper iTMS)

가. TMS 개요

나. TMS 필요성

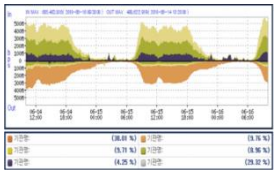
가. TMS 개요



Sniper iTMS 개요

사이버 위협의 **통합 분석/대응**솔루션

위협 관리 및 트랜드 분석



국정원 최신 탐지 정책

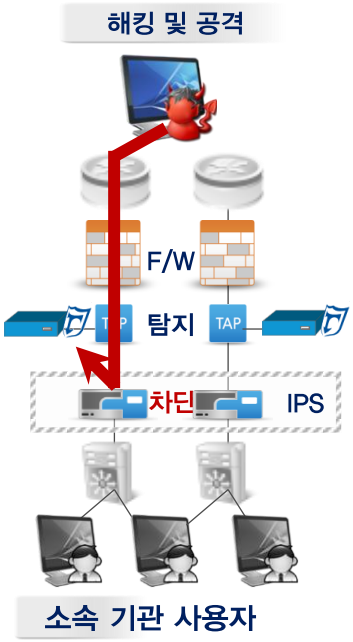
NIS 국가정보원

국내/외 최신 취약성 정보

Sniper IDS
Sniper DDX
Sniper IPS
Sniper WAF

보안장비 이벤트 통합

나. TMS 필요성



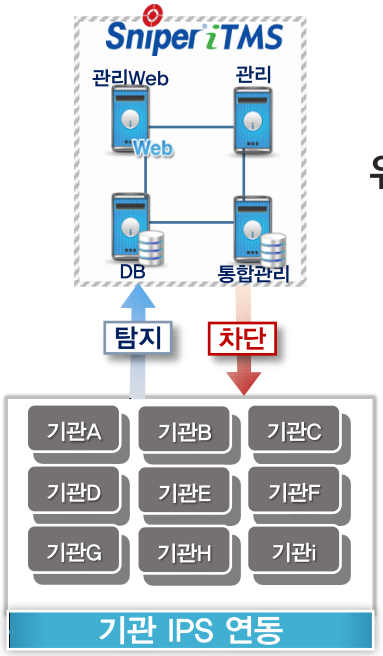
개별 정책 운영

위협정보 **공유 불가**

- 개별 모니터링 수행
- 개별 차단 정책 운영
- 야간 모니터링 불가
- → 각 조직 역량에 의존

침해사고 발생시

중앙 통제 어려움



통합 정책 운영

위협트래픽 **제어 및 관리**

- 통합 모니터링
- 표준 차단 정책 운영
- → 시스템화된 보안 수준

침해사고 발생시

중앙 통제

"**표준화된 보안 정책** 운영과 **중앙집중적 통제**로 기관 전체 보안성 향상"

V

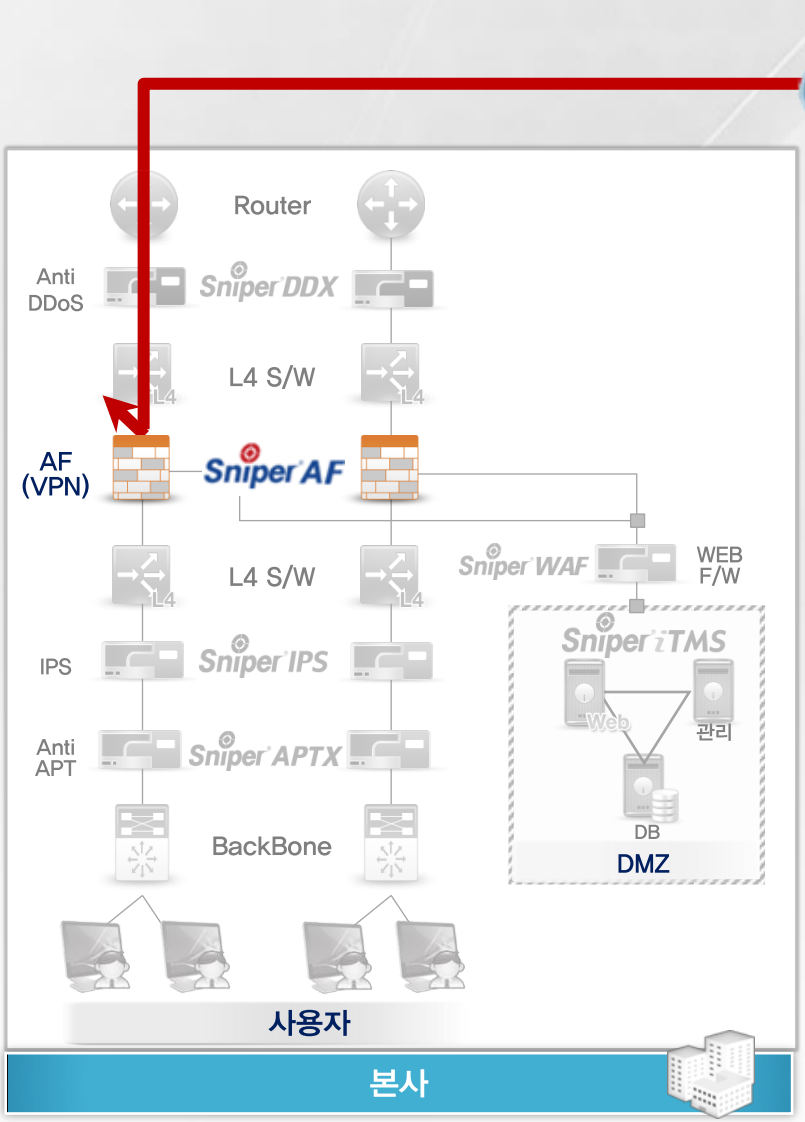
차세대방화벽
(Sniper AF)

가. AF개요

나. 주요기능

다. Line-Up

가. AF 개요



Sniper AF (F/W) 개요

다양한 보안 기능 통합 솔루션

- 어플리케이션제어
- 컨텐츠필터링
- SSLVPN
- Anti-Spam

나. 주요기능

단순 차단이 아닌 세부제어를 통한 보안성 강화

1400개 이상 애플리케이션 차단

웹 애플리케이션 차단

P2P, IM, 웹하드

애플리케이션별 User ID 로 행위 제어

사용자 부서 이동/IP변경에 상관없음

프로파일 별 해당 정책 자동 변경

다. Line-Up

	AF 100	AF 500	AF 1000	AF 2000	AF 4000	AF 20G	AF 40G
Throughput	500 Mbps	1Gbps	2Gbps	4Gbps	8Gbps	40Gbps	50Gbps
Hardware							
CPU	Octeon Single Core 500Mhz	Octeon Dual Core 700Mhz	Intel Dual Core 1.8Ghz	Intel Dual Core 3.0GHz	Intel Quad Core 3.4GHz	Intel Quad Core 2.53GHz * 2	Intel Hexa Core 3.06Ghz * 2
Memory / HDD	1GB / N.A	1GB / N.A	1GB / 500G	4GB / 1TB	16GB / 2TB	24GB / 4TB	24GB /4TB
Interface	10/100/1000 Base-T * 6 (Ethernet * 2, Switch *4)	10/100/1000 Base-T * 6 (Ethernet * 2, Switch *4)	10/100/1000 Base-T * 6	10/100/1000 Base-T * 4 1G Base-F * 4	10/100/1000 Base-T * 8 or 10/100/1000 Base-T * 4 + 1G Base-F * 4 (opt. 10G Base-R * 2 or 1G Base-F *4)	10/100/1000 Base-T * 8(Max28) 1G Base-F * 8(Max28) 10G Base-R * 2(Max6)	10/100/1000 Base-T * 8(Max24) 1G Base-F * 8(Max24) 10G Base-R * 2(Max6)
Power	Single	Single	Single	Single	Dual	Dual	Dual
대상고객	← 지점/SMB →		← 중소규모 네트워크 →		← 대규모 네트워크/ 서비스팜 →		

감사합니다.