월간 정보보호21c 2007. 7 별책

Unified Threat Management

선택! 우리 회사에 맞는 UTM 솔루션

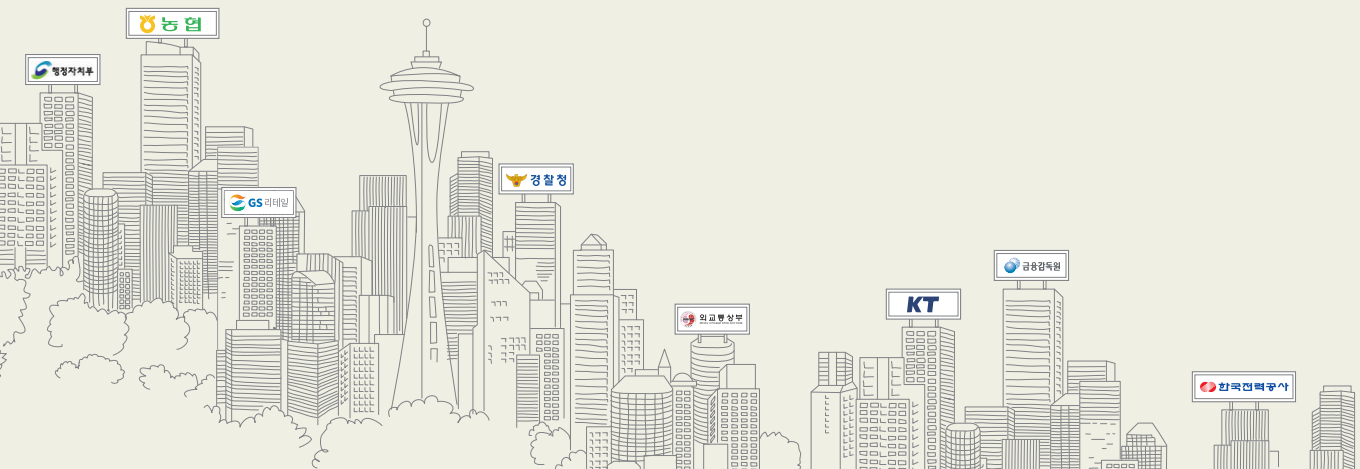
www.future.co.kr

20

대한민국의 네트워크 보안을 지켜온 20년 - 언제나 퓨쳐시스템이 있습니다

1987년 창립 이래 대한민국의 네트워크 보안을 지켜온 20년 –
퓨쳐시스템은 대한민국 곳곳의 동사무소, 은행, 경찰서, 편의점에 이르기까지

우리의 가까운 곳에서 언제나 정보 보호에 앞장서고 있습니다.
끊임없이 일어나는 보안 위험에 앞서 대응하는 최고의 기술력으로 고객의 마음을 먼저 읽으며
쉼없이 노력해 온 퓨쳐시스템. 업계 유일한 20년 역사의 노하우는 아무나 만들 수 없습니다.
고객의 정보, "FutureUTM" 시리즈가 소중하게 지켜드리겠습니다.




FutureUTM 100


FutureUTM 1500


FutureUTM 3000


FutureUTM 6000

Future, Beyond the Security
Future Systems
(주)퓨쳐시스템 문의전화 : 02-6220-7777 www.future.co.kr

Life in Peace
누구나 안심하고 e-비즈니스를 영위할 수 있는 정보화 사회 구현

이 분은 방금 SSL VPN과 웹방화벽의 경쟁력을 갖춘 최적화된 성능의 혁신적인 시큐어웍스 트루인을 선택하셨습니다

SECUREWORKS TRUiN
시큐어웍스 트루인
SSL VPN WEB F/W

■시큐어웍스 트루인이란?

*SSL VPN과 웹방화벽 통합제품
*국내 최초 국가정보원 CCRA(EAL4)인증 계약(2007년 4월 6일)

철저한 접근 권한의 관리와 제어 기능

- 파일레벨까지 관리되는 유연한 엑세스 컨트롤
- 사용자와 그룹, 서버별로 접근을 제어(EAM)
- 인증서를 이용한 강력한 사용자 인증 (공인인증서, 사설인증서 연동 등)
- Firewall 내장으로 자체 보호 기능

웹방화벽 기능

- Web 해킹에 대한 탐지/차단
- 개인 정보 불법 유출 방지
- Web 사이트 위 / 변조 방지
- 악성코드 유포 경로의 사용 차단
- 취약점 분석을 통한 내부 정보의 유출 방지

Web과 Non-web 환경에 베이스 암호화 지원

- SSL을 이용한 VPN 환경 지원
- FTP, Telnet 등의 Non-web환경 암호화 지원

편리한 장비관리와 정확한 통계정보 제공

- 장비의 리소스 사용 현황을 실시간 확인
- 서비스 제어의 손쉬운 컨트롤 환경을 제공
- 운영 중인 어플리케이션 서버에 대한 관리 및 루팅 기능
- 어플리케이션 서버, 그룹, 사용자별 시스템의 접근과 사용 현황
- 시스템과 에러 발생의 현황
- LAN WAN Consol 포트 설정 기능 지원

어울림정보기술(주)
서울특별시 송파구 가락동 78번지 정보통신벤처타워 A동(서관) 10층
Tel : 02-2142-0500~0506 Fax : 02-2142-0507
Tech Center:1588-9575
www.oullim.co.kr

iSEC™ UTM Series

VPN 기반의 WAN 성능 개선 - WAN가속!
핵심 보안기능의 통합 - UTM구축!
이제 iSEC X시리즈로 한번에 가능해집니다.

통합보안 기능	
	Firewall
	VPN
	IDS / IPS
	Content-Filtering
	Anti-Spam
	Anti-Virus

WANㅏ속 기능	
	다중 WAN회선
	다중 터널링
	TCP 성능가속
	WAN 속도증속
	대역폭 관리
	트래픽 통계

* iSEC X 시리즈는 국내외 2000여 개 기업들이 선택한 VPN전문벤더 ㈜액텔라가 [구, ㈜시그엔] 새롭게 선보이는 기업용 통합보안솔루션입니다.

* AWOT (Actela's WAN Optimization Technology), 액텔라가 독자개발한 WAN가속 특허기술

WAN가속 | **AWOT***

actela
㈜액텔라 Actela Co., Ltd

■ 경기도 성남시 중원구 상대원동 190-1 SKn 테크노파크 테크동 1202호
■ Tel : 031-776-2070 ■ Call Center : 1566-3616 ■ Fax : 031-777-2071
■ **영업문의** sales@actela.com ■ **기술문의** support@actela.com

www.fortinet.com

무려 5,000여 고객께서 이미 사용하고 계십니다.

포티넷의 명성이 그냥 만들어진 것이 아닙니다.

저명한 시장 조사 기관인 IDC로부터 2006년 전세계 UTM 시장 1위 제품으로 선정된 포티넷의 포티게이트 시리즈.
업계 최초로 UTM의 개념을 도입했던 포티넷의 제품은 그 누구도 쉽게 따라올 수 없는 다양한 기능과 최고의 성능으로 고객들의 만족을 이끌어 내고 있습니다. 점점 더 지능화되어 가고 있는 다양한 형태의 혼합 공격(Blended Threat)을 최적의 성능으로 막아낼 수 있는 장비가 바로 포티게이트입니다. 업계에서 유일하게 콘텐츠 매칭을 위한 전용 프로세서와 네트워크 전용 프로세서를 채용하여 성능을 혁신적으로 개선하였습니다.

UTM의 미래는 포티넷이 만들어 가겠습니다.

FortiGate 5000 Series

서울시 강남구 삼성동 159-1 한국종합무역센터 27층 Tel | 02-6007-2007 Fax | 02-6007-2703 www.fortinet.com

FORTINET
REAL TIME NETWORK PROTECTION

CLEAN NETWORK PROVIDER ON THE WORLD

"세계 최고의 보안을 만드는 기술"
세계가 인정한 "시큐아이닷컴"의 자산 입니다.

이제 국내 NO1의 자리보다는
미래의 세계 차세대 IT보안을 리드하는 최고의 기업으로
세계 IT보안의 미래를 지켜 나아갈 것입니다.

SECUI

Leader of Business Network Security

www.secui.com

SECUI
NXG 2000 F

고성능 통합 네트워크 보안 솔루션

SECUI
SCAN

취약점 진단 솔루션

- 국내 전체 정보보호업계 1위로서, 세계 1위를 도전하고 있는 기업입니다.
  2002년부터 3년 연속 정보보안업계 매출실적 1위 달성
- 우수한 기술인력과 고급 정보보호 기반기술을 보유하고 있습니다.
  국제적인 성능평가기관 미국의 Tolly Group 인증 (외산 기가비트 방화벽보다 성능 비교 우위)
- 글로벌 마케팅의 선두주자로 나서고 있습니다.
  중국,대만,일본,싱가폴 등에 진출하여 정보보안업계 수출실적 1위 달성

SECUI 시큐아이닷컴주식회사 135-847 서울특별시 강남구 대치3동 949-11 포르쉐 타워 3층
TEL.02)3783-6600 FAX.02)3783-6499 제품지원고객센터.080-331-6600

네트워크 보안도 안철수연구소입니다

안 철수하면 다 잡는다!

PC 통합 보안은 **V3**, 네트워크 통합 보안은 **트러스가드 UTM**

AhnLab TrusGuard UTM

- 복합 공격에 대비한 네트워크 통합 보안 (방화벽, IPS, VPN, 안티바이러스, 안티스팸 등)
- 최신 보안 위협에 대한 24 × 365 실시간 대응 서비스
- 세계적 수준의 바이러스/웜/스파이웨어/해킹/스팸 차단 등의 보안 콘텐츠 기술
- 클라이언트 보안 제품과 결합된 SSL VPN 및 뛰어난 DDoS 공격 차단 기능

AhnLab Absolute IPS

NP 기반의 고성능 IPS
(최고 8Gbps Wire Speed 보장)

AhnLab TrusGuard SCM

웜/스파이웨어 차단 전문 보안장비

AhnLab Suhoshin Absolute

3,000여개 사이트에서 안정성이 검증된
방화벽+VPN+IDS 통합 보안 장비

안철수연구소 | • 기업고객 전용 핫라인 : 02-2186-3082 • 고객만족센터 : 02-2186-3000 • 팩스 : 02-2186-3001
• 홈페이지 : www.ahnlab.com • 주소 : 서울특별시 영등포구 여의도동 12번지 CCMM빌딩 6층

NO.1

네트워크 보안
이젠 하나로 갈 때입니다

STN-UTM 이 안전하게 보호해 드립니다 .

No.1 **L7 트래픽 제어** 기반으로 **QoS 와 보안 기능**을 지원합니다 .
No.1 **고성능 DPI** 기반으로 비정상 패킷을 분석 / 차단 / 제어합니다 .
No.1 빠른 속도와 안정된 품질의 **Speed VPN** 을 지원합니다 .
No.1 애플리케이션 레벨 게이트웨이 구현으로 안티 바이러스 / 안티 스팸 / 스파이웨어를 원천차단합니다 .
No.1 웹애플리케이션 보안을 통해 자산을 보호합니다 .

(주)STN 기술 138-070 서울시 송파구 송파동 43 번지 송광빌딩 2 층 , 대표번호 : 02-421-7191/Fax: 02-412-7194
구입문의 : ㈜에스씨앤티 (T)042-484-1841, 대신네트웍스㈜ (T)051-466-8282, 그리드시스템㈜ (T)051-621-0565,
싸이버테크㈜ (T)062-676-2100, 신야시스템㈜ (T)055-256-5125, ㈜미다스시스템 (T)02-501-9218, ㈜엔에이치넷 (T)02-2058-2280

(주)STN 기술
www.stntech.co.kr

정보보호 컨설팅 〉 네트워크 시큐리티 솔루션 〉 NISP 통합보안 서비스 〉 취약점 정보시스템 구축

Juniper Your Net.

완·전·격·리!

주니퍼 네트웍스 차세대 스마트 방화벽 –

완벽한 네트워크 보호의 시작입니다

귀사의 WAN네트워크의 성능에 아무 지장 없이 바이러스 및 치명적인 보안위협을 차단하고 싶으세요?
그렇다면 주니퍼 네트웍스 차세대 스마트 방화벽으로 업그레이드 하세요.
주니퍼 네트웍스의 SSG는 보안기능을 추가하면 네트워크의 성능이 크게 떨어지는 기존제품들과 달리 WAN 접속기능에 고속 LAN 보호기능까지 갖춘 혁신적 신기술입니다.

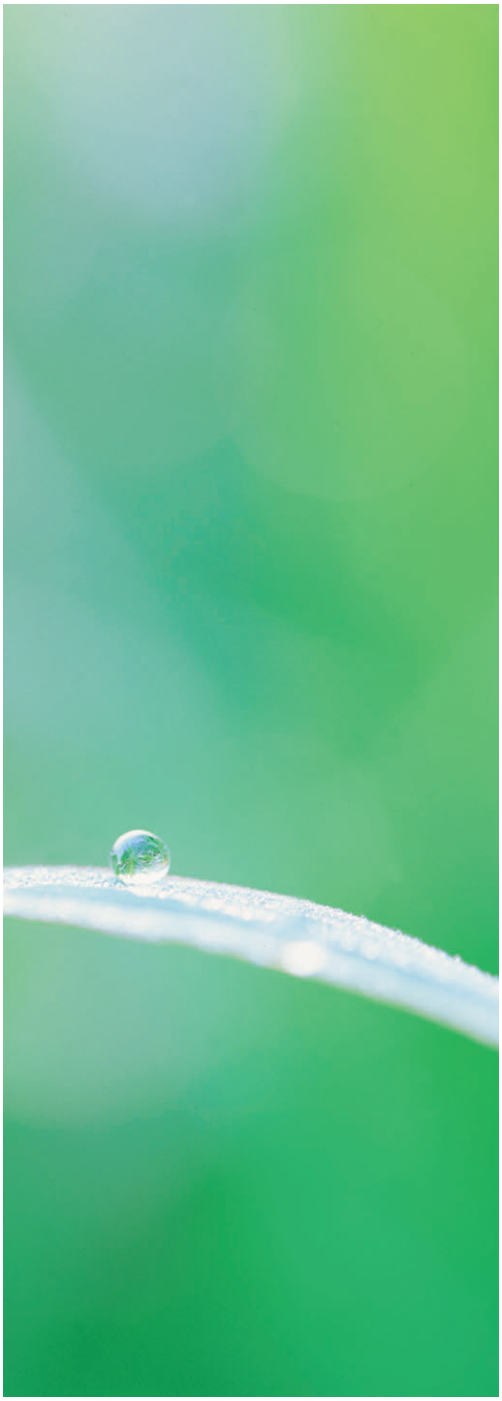
■차별화된 고성능

멀티레이어 네트워크 및 응용 프로그램 수준의 보호기능을 제공할 뿐만 아니라, 보안 솔루션으로 인해 발생하는 LAN 또는 WAN의 병목현상까지 확실히 예방하는 고성능 제품입니다.

■완벽한 통합 위협관리

보안전문 하드웨어 및 방화벽, IPSec VPN, IPS, 바이러스 차단(스파이웨어, 애드웨어 및 피싱 차단기능 포함), 스팸 차단 및 웹 필터링 기능을 모두 갖춘 완벽한 United Threat Managemant(UTM) 차세대 방화벽입니다.

Juniper NETWORKS | **한국주니퍼네트웍스(주)** 서울시 서초구 서초동 1303-22 교보타워 A동 4층
대표전화 : 02-3483-3400 팩스 : 02-3483-3488



월간 정보보호21c 2007년 7월호 별책
발행일 2007년 7월 1일
발행처 (주)인포더 (121-600) 서울 마포우체국 사서함 2호
디자인 이지현(ggaerook@hanmail.net)
출력 웨스턴 그래픽스 인쇄 씨엔씨 미디어

CONTENTS

안전한 세상을 위한 뉴스

보안뉴스

지금 **보안뉴스**에 접속하면
당신의 보안이 **업그레이드**됩니다!!

안전하고 편리한 인터넷과 PC 사용을 위한 최신 정보
안전한 기업경영과 산업보안을 위한 해경방안과 예방책
일상생활 속에서 개인의 안전을 위한 정보와 노하우

www.boannews.com

미디어그룹 인포더 Tel. (02)719-6931 Fax. (02)715-8245 E-mail : ad@boannews.com

UTM A부터 Z까지 알아보자

I

UTM 개념정립부터 해보자!

UTM History 태동부터 현재까지 짚어보자!

UTM이 급부상하는 이유는 무엇일까?

UTM 솔루션 도입시 기대할 수 있는 효과는?

국내 UTM 시장 현황과 전망 및 문제점

효율적인 UTM 도입을 위한 체크리스트, 'UTM 이것만은 확인하고 구입하자'

UTM 개념정립부터 해보자!

Unified Threat Management

통합위협관리 (UTM:Unified Threat Management)는 안티바이러스 · 방화벽 · 가상사설망(VPN) · 침입탐지시스템(IDS) · 침입방지시스템(IPS) · 트래픽 쉐이핑 · 콘텐츠 필터링 · 웹 필터링 · 이메일 필터링 등 이런 보안기능 중 적어도 2개, 많게는 7~8가지 기능을 하나의 박스에 넣어 사용하는 통합보안장비를 말한다.

하지만 UTM에 대한 정의는 각 회사별로 제각각이다. 이는 UTM 솔루션을 제공하는 국내외 벤더의 태생에 따라 다르기 때문이다.

방화벽 제품으로부터 출발하여 이 기능을 기반으로 다른 주요 보안기능들이 포함되면서 발전된 유형이 있고, IDS 제품으로 출발하여 다른 주요 보안기능들이 포함되면서 UTM으로 발전된 유형, 네트워크 장비로부터 출발하여 보안기능들이 추가되면서 UTM으로 진화된 유형들이 있다.

국내외 벤더 태생에 따른 UTM 솔루션 유형

김형률 어울림정보기술 기술연구소 소장은 이런 유형들에 대해 다음과 같이 설명했다.

방화벽이나 IDS 제품으로부터 출발한 UTM 솔루션은 기존의 보안전문회사들의 제품들로 처음부터 보안 기능성을 기반으로 발전되어온 제품이라는 것. 성능을 기반으로 발전된 네트워크 장비 기반의 제품은 네트워크 장비회사의 제품으로 보안전문회사의 제품에 비해서 성능은 우월한 편이나 보안 측면의 기능성은 다양하지 않다는 것이다.

보안전문회사의 UTM 솔루션은 다양하고 강력하며 기본에 충실한 보안기능을 탑재하고 있는 반면, 네트워크 장비회사들의 UTM 솔루션은 보안기능의 다양성 측면보다는 L2~L4 스위치 기능이 포함된 고성능 UTM 솔루션에 초점이 맞추어져 있다.

네트워크 장비의 보안시장 전이 추세에 따라 보안전문회사의 UTM 솔루션도 영향을 받아 이미 Load Balancing 기능이 내장된 제품이 제공되고 있다. 성

통합위협관리 (UTM:Unified Threat Management)은 안티바이러스 · 방화벽 · 가상사설망(VPN) · 침입탐지 시스템(IDS) · 침입방지시스템(IPS) · 트래픽 쉐이핑 · 콘텐츠 필터링 · 웹 필터링 · 이메일 필터링 등 이런 보안기능 중 적어도 2개, 많게는 7~8가지 기능을 하나의 박스에 넣어 사용하는 통합보안장비를 말한다.

능 측면에서도 고성능 플랫폼이 채택된 제품이 출시되고 있으며, 스위치와 같은 기능도 UTM 솔루션에서 지원하는 기능 중 하나가 되고 있어 네트워크 장비 기반의 UTM 장비가 제공하고 있는 특화된 우위 요소도 점차 반감되고 있다.

김 소장은 이런 설명을 기초로 각 유형에 따른 벤더들을 분류했다.

방화벽 기반의 UTM 솔루션을 제공하는 회사는 어울림정보기술, 시큐아이닷컴, 퓨쳐시스템이 있다. 전형적인 방화벽/VPN 전문회사들로 여기에 다른 보안기능과 모듈이 추가 탑재되어 양질의 고기능 고성능 제품화를 추구한다.

IDS/IPS 기반 UTM 솔루션을 제공하는 회사는 윈스테크넷, 포티넷이 있으며 IDS/IPS의 탐지능력에 초점을 두고 용이한 사용성 측면에서 다른 보안기능들을 추가 탑재하여 제공하는 측면의 제품이 출시되고 있다.

네트워크 장비 기반의 UTM 솔루션을 제공하는 회사는 삼성 네트웍스, 시스코 시스템즈, 주니퍼 네트웍스 등이 있으며 고성능 스위치 기반에 탑재되는 보안모듈이 점차 다양화하고 있다.

각 벤더사들이 말하는 UTM 정의

앞서 벤더사들의 태생에 따른 UTM 솔루션 유형을 정리해 보았는데 이번에는 각 벤더사들이 직접 설명하는 UTM의 정의를 들어보겠다.

넥스지는 "보통 각 제조업체마다 본래의 기능에 부가기능을 첨가하는 형태를 많이 선택하는데 예를 들어, 방화벽업체인 경우 본래의 제품군에 IPS 기능을 IPS 업체의 경우 방화벽/VPN을 첨가하여 UTM을 판매하고 있다"며 "보통 방화벽, VPN, IPS, 안티바이러스, 안티스팸, URL 필터링 등의 멀티 보안기능을 수행하는 것"이라고 정의했다.

안철수연구소는 "네트워크 보안에 관련된 기술 플랫폼과 위협을 일으키는 보안콘텐츠에 대응하는 엔진의 결합"이라고 설명했다.

STN기술은 "UTM은 네트워크 통합보안시스템"이라며 "간편한 고객관리, 최소한의 통합비용 절감, 능률과 생산성의 향상, 향후 업그레이드 편의성, 하나의 벤더로 통일, 언제 어디서나 접속가능한 통합모듈 구성 서비스이어야 한다"고 정의했다.

포티넷은 "Deep Contents Inspection 개념을 바탕으로 패킷 데이터 수준부터 애플리케이션 수준까지 일련의 검사기준에 의해 네트워크상의 원 포인트에서 보안성 검토를 하는 기능을 갖고 있는 보안장비"라고 설명했다.

글로벌 독립 보안 테스트 기관인 NSS 그룹의 정의

이처럼 각 벤더사별로 대동소이하면서도 그 벤더사의 특성에 따라 조금씩 다른 UTM의 개념 정의를 처음한 곳은 IDC다.

IDC는 UTM을 "방화벽과 침입방지(IPS), 바이러스 차단 등 여러 가지 보안기능을 포함하는 네트워크 어플라이언스 장비"로 정의했다. 그러나 현재의 UTM 장비들은 처음에 정의되었던 보안기능 이외에 새로운 위협에 대처할 수 있는 다양한 보안기능들을 추가함으로써 그 제공범위를 확대하고 있다. 따라서 현재의 UTM은 여러 가지 보안기능들을 제공하는 네트워크 통합보안장비의 통칭으로 이해해야 한다.

이에 글로벌 독립 보안 테스트 기관인 NSS 그룹이 정의하는 UTM을 개념을 보면 보다 명확해질 수 있다.

"방화벽, VPN, IDS, IPS, 안티바이러스, 안티스팸, 안티스파이웨어 등 기본적인 7가지 기능을 갖추고 있어야 UTM이라고 규정한다."

UTM History
태동부터 현재까지 짚어보자!

3~4년 전만해도 보안이라고 하면 방화벽을 먼저 떠올렸다. 말 그대로 진입장벽을 만들어 필요로 하지 않는 내용에 대해 막자는 의미가 컸던 보안서비스다. 하지만 최근 들어 이러한 개념이 일반적인 인식 변화를 가져오면서 이제 '보안 = UTM' 이라는 등식이 성립되는 과정에 까지 이르렀다. 그렇다면 UTM의 시작은 언제부터일까.

방화벽의 진화에서 UTM까지

김형률 어울림정보기술 기술연구소 소장은 보안시장의 태동기부터 거슬러 올라가 설명했다.

1990년대 말부터 여러 보안회사들은 네트워크 보안을 위해 방화벽, 가상사설망(VPN), 침입탐지 시스템(IDS), 침입방지 시스템(IPS), 안티바이러스, 안티스팸, 메일보안 및 웹보안 등 다양한 보안솔루션을 선보였다. 보안시스템들은 시간이 지나면서 다양한 솔루션으로 늘어나게 되었으며 네트워크의 변화와 증가로 인해 운용해야 하는 보안시스템들의 양적 증가로 이어졌다. 이 때문에 운용 · 관리하는 업무가 증가되고 보안관리 인력이 늘어나며 더 많은 비용이 소요됐다. 이에 많은 기업과 기관이 이 문제를 해결하고 더 효율적으로 운용할 수 있는 통합보안솔루션을 요구하게 되었다.

기술적인 측면에서도 초기 보안시장은 세부적인 단위의 보안제품으로 분화하는 과정을 거치면서 다양한 보안솔루션이 나타났다. 최근 몇 년간 출시된 보안솔루션은 통합운영되었을 때 다양한 위협으로부터 종합적인 보호가 가능하다는 개념이 나오면서 통합위협관리(UTM) 솔루션이 등장했다.

새 보안위협에 맞선 네트워크 보안장비?

나형택 시큐아이닷컴 기술기획팀 팀장은 UTM의 출발을 기존 네트워크 보안장비의 한계에서부터 지적했다. 기존 네트워크 보안장비는 그 동작범위가 협의적이었기 때문에 이슈의 변화에 제대로 대처할 수 없었다. 1999년 네트워크 보안이 처음으로 주목받기 시작하면서부터 이슈의 전환이 있었던 지점들을 기준으로 분류하면 크게 삼분화가 가능하다.

첫째 시기는 야후와 이베이 등 인터넷 사업의 효시였던 네트워크들에 대한 무차별적인 DDoS공격으로 특징 지워진다. 이 시기에는 무엇보다, 성능이 좋은 기가바이트형 방화벽 장비가 얼마나 빠르게 유해 트래픽을 차단할 수 있는가가 이슈였다. 이 시기의 유해 트래픽은 그 정체가 표지에 다 드러나 있었기 때문에 표지 정보의 빠른 검사와 판단이 필수적이었다. 판별의 근거는 오로지 'Default Deny'. 즉, 허용한 트래픽 이외의 모든 트래픽은 기본적으로 차단한다.

둘째 시기에는 웜 트래픽의 엄청난 확산이 제일 큰 문제였으며 공격대상이 특정에서 불특정 무차별로 옮겨가게 된다. 2003년 1월 전 세계를 강타하였던 SLAMMER 공격이 가장 전형적인 형태였고 이 사고를 계기로 IPS란 네트워크 보안장비에 대한 수요가 급증하게 된다. 페이로드를 검사해야만 했던 것이다. 이 시기의 방화벽들은 페이로드에 대해서는 장님이나 다름없었

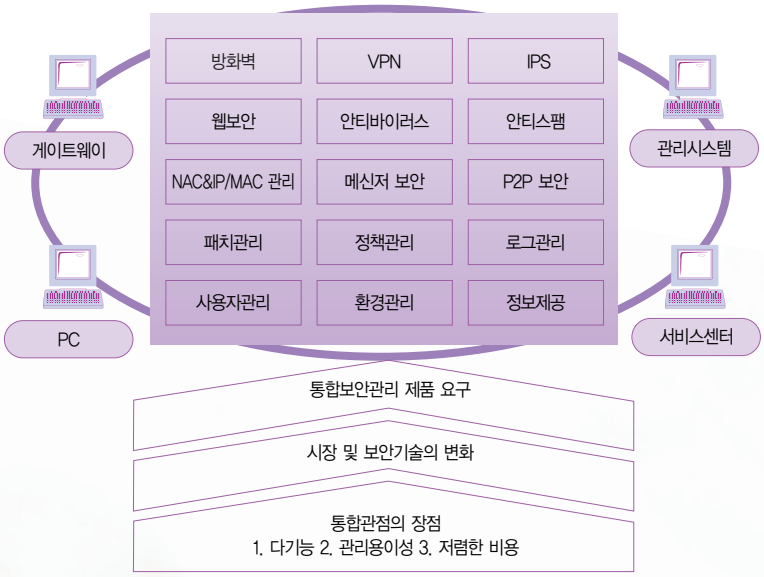


그림. UTM 개요

다. 유해성 여부의 주된 판단기준은 페이로드에 의심가는 패턴이 있느냐 없느냐였다.

셋째 시기는 현재이며 이슈의 다변화가 가속화된 시기다. 특정 유해 트랙픽에 대한 차단 여부뿐만 아니라 악의가 없는 내부자에 의한 공격, 웹 서비스 상에 존재하는 다양한 형태의 취약점들, 내부기밀의 다양한 유출경로, P2P 등의 창궐, 인터넷에 따른 생산성 방해, 각종 고소 고발건에 대한 네트워크 트래픽 내역 증빙, 개인정보보호, VoIP의 확산과 VoIP 영역의 취약점 등이 주요 이슈들이다. 이제는 단순한 유해 트래픽 판단여부가 중요하지 않고 각 네트워크 단위가 지켜야 할 주요 보안정책들을 네트워크 보안장비가 얼마나 충실하게 관철시켜 주는가가 관건이 되었다.

이런 시대에 필요한 네트워크 보안장비가 UTM이고, 이 UTM은 기존 보안 요구사항에서 영역이 확장된 형태의 보안요구들을 만족할 수 있는 보안정책을 수행해야 한다. UTM이 집행해야 할 확장된 보안정책이란 기존의 보안정책을 당연히 포함해야 한다.

김홍선 안철수연구소 기술고문은 네트워크 보안장비의 역사를 3단계로 설명했다.

1세대 제품은 초기 방화벽, IDS 등으로 소프트웨어 제품으로서 범용 서버나 워크스테이션에서 운용되었다. 2세대 제품은 고장이 날 원인을 줄이기 위해서, 즉 POS(Points Of Failure)를 줄이고 가격대비 성능을 높이기 위해서 어플라이언스와 하드웨어 전용장비로 방화벽, VPN, IPS가 변화했다. UTM은 2세대 개념의 기술들을 통합하고 보안콘텐츠와 단단히 결합된 서비스 기반의 네트워크 어플라이언스 제품이라고 규정할 수가 있다. 콘텐츠 관리와 서비스가 네트워크 보안제품의 중요한 축으로 참여한다는 점에서 네트워크 보안의 3세대 제품이라 할 수 있다.

차세대 UTM 보안솔루션

앞서 UTM 솔루션의 역사를 잠시 살펴보았듯이 UTM의 출발은 네트워크 보안을 위한 방화벽 설치에서부터 시작한다. 그렇다면 이런 UTM이 향후에는 어떻게 진화될 수 있을까.

리처드 스티에논(Richard Stiennon) 포티넷 CMO는 차세대 UTM 솔루션이 전적으로 스위치 기반의 네트워크 구조를 기본으로 한다고 밝혔다. 일반적으로 이 솔루션은 스위치에 대한 접속뿐만 아니라 코어 스위치들까지 포함하며 가상 LAN은 필요한 장비에 대한 개별적인 차단을 제공하기 위해 사용된다. 또한 스위치는 L2 및 L3 정보에 기반해 정책강화와 정상으로 허가된 데이터 스트림은 부가적인 IPS 기능에 의해 필터링된다.

UTM이 급부상하는 이유는 무엇일까?

최근 들어 UTM이 화두가 되는 이유는 무엇일까. 다양한 보안솔루션의 도입에 따른 비용과다 문제, 각각의 보안솔루션 운용방법을 익히기 위한 시간비용 그리고 운용을 위한 물리적 공간과 인력 확보가 요구되면서 이에 대한 효과적인 관리대안이 필요하기 때문이다.

그 해법은 다양한 보안솔루션을 하나로 묶어 비용을 절감하고 각각의 보안기능 사이의 시너지를 내면서 보다 쉽게 운영관리가 가능할 수 있도록 하는 방안이 강구되기 시작했고 그게 바로 'UTM' 이다.

사용자로서는 각종 보안기능을 통합하면서도 설치 및 관리가 쉽고 비용까지 절감할 수 있는 UTM에 대한 관심이 높을 수밖에 없고, 사업자로서도 단품 판매와 바이러스 등 다양한 패턴을 제공하는 서비스 결합, 비즈니스 모델의 다양화가 가능한 UTM이 구미가 당긴다.

정병선 LG 엔시스 전략사업부문장은 "무엇보다 UTM 보안 어플라이언스는 단일 제품식 접근법으로 제품선택, 통합, 지원 서비스가 단순해져 복잡성을 완화했다는 것"이라며 "게다가 플러그 앤 플레이 방식으로 설치가 용이할 뿐 아니라 블랙박스식 접근법을 통해 사용자로 인한 피해를 줄일 수 있으며 경비를 줄이고 보안성을 높여준다"고 설명했다. 또한 정 부문장은 "특히 보안 어플라이언스에 보안위협이 발생했을 때 이를 신속히 차단한 후 대응할 수 있다"며 "UTM은 개별 보안솔루션을 무력하게 만들 수 있는 혼합공격에 효과적으로 대처할 수 있다"고 밝혔다. 이외에도 개별적으로 각각의 장비를 도입할 때와 비교해 설치가 매우 쉽고 관리 역시 상대적으로 용이해 투입인력 및 TCO를 최소화할 수 있다는 장점이 있다.

날로 진화하는 보안위협 대응에 '적합'

김홍선 안철수연구소 기술고문은 UTM 개념이 대두되게 된 배경을 최근 위협동향의 변화에서 찾기도 한다. 먼저 보안위협의 행위 형태가 복잡하게 바뀌었다. 대

표적인 현상이 바이러스나 웜, 해킹을 조합한 복합공격, 즉 Blended Threat가 증대하고 있다. 공격이 발생하는 계층도 패킷 레벨부터 애플리케이션에 이르기까지 다양한 계층에 이르고 있다.

또한 BotNet과 같이 PC에 백도어 형태로 설치되어 스팸메일이나 네트워크 스캔 공격을 하는 PC/네트워크 연동공격이 증대하고 있다.

이런 공격에 효율적으로 대응하기 위해서는 위협을 종합적으로 판단해서 네트워크 상의 여러 계층에서 중심을 갖고 대응할 수 있는 UTM이 절실하다.

다음으로는 공격의 루트가 다양하다. 외부에서 게이트웨이를 통해 들어오는 위협부터, 내부 네트워크 접속단인 엔드 포인트 그리고 각종 서버들이 위협을 일으키는 근원이 된다. 공격이 이루어지는 경로도 외부 해커로부터의 직접적인 인바운드 공격뿐만 아니라 내부 PC로부터 웜이나 스파이웨어를 네트워크로 뿌리는 아웃바운드 위협이 있다. 또한 위협 활동에 이용되는 도구도 패킷, 메일 등 다양하게 이용되고 있다. 이렇게 전방위에서 벌어지는 위협을 탐지하기 위해서는 모든 패킷을 지능적으로 판단할 수 있어야 한다.

마지막으로 위협의 특성이다. 바이러스나 웜과 같은 위협 콘텐츠는 특정 목적을 가지고 끊임없이 생성된다. 어떤 위협은 기업이나 개인에게 중대한 위험이 따르지만 어떤 경우는 트래픽 발생과 시간낭비를 일으키기도 한다. 따라서 위협을 막기 위한 정책도 단일정책보다 각 기업과 기관의 특성에 따라 우선순위와 실행 의지에 따라 결정된다. 문제는 이러한 다양한 위협 콘텐츠에 대해 파악하고 준비되어 있어야 한다는 점이다.

최근 제품동향과 기술동향

이처럼 급부상하고 있는 UTM은 국내뿐 아니라 외국 시장에서도 보안시장의 화두로 떠오르고 있다. 이미 지난해 상반기를 기점으로 전 세계 주요 보안전시회에서도 단독 솔루션보다는 주로 UTM과 같은 복합기능의 제품이 주를 이루고 있어 단일 솔루션의 퇴조현상이 뚜렷해지고 있는 게 현실이다.

국내에서는 시장 초기였던 2004년까지는 포티넷 · 시만텍 · 시큐어컴퓨팅 등 외산제품들이 높은 관심을 끌었으나 최근에는 토종기업들이 고성능 · 고기능 제품의 출시를 활발하게 진행하고 있어 양측의 경쟁 속에서 UTM 솔루션이 지속적으로 진화할 전망이다.

이에 따른 최근의 제품동향이나 기술동향을 살펴보면, 제품 및 기술에 대한 큰 트렌드가 존재하기보다는 네트워크의 각 솔루션별 업체 혹은 애플리케이션 업체가 자사가 강점을 보이는 부분으로부터 기술을 발전시키고 있는 상황이다.

포티넷은 제품동향에 대해 "High-End 급의 장비가 출시되고 있다"고 밝혔다. 또한 기술동향은 다기능을 제공함으로써 발생하는 성능상의 제약을 해소하기 위해 하드웨어 구성상 콘텐츠 프로세스 ASIC와 네트워크 프로세스 ASIC 그리고 일반 CPU 등을 채택하는 구조를 택하고 있다.

이외 일반적인 흐름을 보면 요즘 출시되는 UTM 솔루션은 다양한 보안서비스를 제공함과 동시에 VLAN, LB, QoS, HA와 같은 고급 네트워크 기능까지 지원하는 추세다. 이와 함께 VoIP 관련 프로토콜을 지원하며 기존의 IPSec 기반의 VPN 이외에도 SSL 기반의 VPN 서비스까지 UTM 장비에 탑재될 예정이다.

UTM 솔루션 도입시 기대할 수 있는 효과는?

UTM은 하나의 보안 어플라이언스에 여러 가지 보안 기능을 통합한 보안플랫폼으로 2005년경부터 본격적으로 UTM이라는 말이 사용되기 시작했고 많은 사람들이 관심을 모으고 있는 초기 단계의 솔루션 개념이다.

일반적으로 UTM은 네트워크 보안의 기본 구성인 방화벽 · VPN · IPS · 바이러스월 · 안티스팸 · 안티스파이웨어 기능의 전부, 혹은 일부를 통합 구현하는 것을 기본으로 하고 있다. 하지만 UTM의 개념이 아직 확실히 정립되지 않았기 때문에 저마다 서로 다른 정의를 적용하는 경우도 많다. 그러나 UTM이라는 보안장비의 화두는 인터넷 웜 등에 대한 새로운 네트워크에 부하를 주는 공격에 대비, 네트워크에서 공통 적용이 가능한 보안기능의 통합, 하드웨어 기반의 어플라이언스 적용을 통한 비용대비 효과상승이라 할 수 있다.

UTM 도입시 기대할 수 있는 효과

이에 기업들이 UTM 솔루션을 도입했을 때 기대할 수 있는 효과에는 무엇이 있는지 알아보았다.

- 지능화되는 공격에 방어 : 외부공격이 점차 지능화 · 복잡화되어 가고 있다. 따라서 과거 단일 보안제품으로 보호할 수 없는 영역이 생기게 된다. 예를

들어 과거에는 사용하지 않는 포트는 방화벽에서 차단시키면 되었다. 하지만 현재는 많은 P2P, 메신저, 웜, 바이러스가 HTTP 같은 일반적인 포트를 사용하기 때문에 탐지 및 차단이 더욱 어려워지게 되었다.

- 통합관리의 용이함 : 관리 포인트 감소로 효율적인 보안관리 기능이 가능하며 비용절감 효과도 누릴 수 있다.
- 설치 및 유지보수의 총비용 절감을 통한 경제적인 가격효과
- 각 고객정책에 맞는 보안정책의 선택적 적용과 변경이 가능해 보안정책 적용이 편리
- 다수의 보안기능들에 대해 일관적 운영 · 관리가능
- 불필요한 트래픽의 자원 독점 방지와 중요한 트래픽에 대한 우선처리
- P2P 트래픽 사용량 축소에 따른 월 백본 회선 및 장비 증설 비용절감
- 트래픽 과부하로 인한 병목방지와 업무와 관련된 트래픽에 대한 최소한의 대역폭 보장으로 업무 효율성 증대
- P2P 또는 메신저 등과 같이 업무에 불필요한 프로그램에 대한 접근 차단
- 외부로부터 내부 네트워크 보호와 웜 및 바이러스 차단
- 각각의 개별기능을 하는 장비의 수비범위가 한정되어 있어 장비 간 수비범위의 차이로 인한 Security Hole이 발생할 수 있으나 UTM의 다양한 보안기능은 서로 오버랩되면서 보안성 강화
- 장비 간 Latency 문제 해결 : 패킷이 복수의 보안장비를 거침으로써 발생하는 지연을 해결

UTM에 대한 잘못된 편견을 버리자!

※ UTM이 새로운 패러다임으로 자리잡다 보니 일부 잘못된 편견이 회자되고 있어 바로 잡고자 한다.

Q UTM은 기존 네트워크 보안제품의 기능을 합쳐 놓은데 불과하다. 이미 대부분 방화벽에는 AV가 탑재되었고 일부 IPS 기능도 구현되어 있다. 무엇이 다른가?

A 단순한 물리적 결합은 최적화된 성능을 낼 수가 없다. 진정한 UTM은 멀티 계층에서 각 위협에 대해 적응하게 대응하고 탐지하는 것이기 때문에 UTM을 위한 전용 설계가 필요하다. 다시 말해서 방화벽, IPS, 보안콘텐츠 기술이 단단하게 묶인 유기적 결합이 필수적이다. 따라서 UTM은 하이 레벨부터 하드웨어까지 각 위협에 대해 최적의 경로를 통해 차단하는 아키텍처를 가져야 하는 새로운 패러다임의 제품인 것이다.

Q UTM 기능을 모두 사용할 경우 성능이 크게 떨어진다?

A 현재의 제품들에서 어느 정도 한계가 있는 것은 사실이다. 트래픽이 많거나 바이러스, 웜이 많이 발생하는 구간에서는 눈에 띄게 발견할 수 있다. 그러나 얼마나 기술통합이 최적화로 이뤄졌느냐에 따라, 또한 보안콘텐츠가 얼마나 이런 기술과 결합되느냐에 따라 성능 이슈는 상당히 해소된다. 아울러 이미 보안콘텐츠를 가속하기 위한 하드웨어 기술들이 나오고 있고 효율적인 가격으로 이 문제를 접근할 수 있는 방향을 보여준다.

Q UTM 만으로 모든 보안문제가 해결된다?

A 이미 완벽한 보안보다는 효율적인 보안이 중요한 원칙이 되고 있다. 물론 UTM은 게이트웨이에서 많은 문제를 필터링할 수 있다. 그러나 사이트 특성에 따라 위협의 근원지가 다양하고 복잡하기 때문에 '완전'이라는 표현은 사용하기 어렵다. 그러나 보통 발견할 수 있는 많은 문제들이 UTM을 통해 해결될 수 있는 플랫폼임은 명약관화하다. 앞서 언급했듯이 UTM의 정책을 어떻게 우선순위를 갖고 실행하는가는 전적으로 사용자의 몫이다. 완전 보안보다 중요한 것은 자신들의 IT 생산성과 적절한 보안정책을 접목시키는 노력이 중요하다.

국내 UTM 시장 현황과 전망 및 문제점

그동안 국내 UTM 시장은 소수 외산사업자의 텃밭이나 다름없었다.

하지만 향후 국내 UTM 시장은 본격적인 경쟁체제로 돌아선다. 제품 도입에 비용 부담을 안고 있고 대기업과 달리 거대 용량의 트래픽이 필요치 않은 SMB 시장의 UTM 요구가 점점 높아지고 있어 이에 따른 시장 신규진입이 이어지고 있기 때문이다. 국내에서는 기존의 STN기술, LG엔시스 외에도 최근 안철수연구소가 합류했고, 넥스지 · 시큐아이닷컴 · 하우리 등이 가세할 예정이다.

올해 국내 UTM 시장 600억원 예측

한국 IDC가 최근 발간한 〈한국 보안 어플라이언스 시장분석 및 전망 보고서〉에 따르면, 2004년 국내 보안 어플라이언스 장비시장은 1154억원 규모로 추산되며 2003년부터 향후 5년간 연평균성장률 17.9%를 기록, 오는 2008년에는 2177억원으로 증가할 전망이다.

장비별 유형을 보면, 단독 방화벽/VPN 보다는 하나의 박스에서 방화벽/VPN, IDS/IPS, 안티바이러스, 웹 필터링 등의 복합기능을 제공하는 통합위협관리(UTM) 어플라이언스가 큰 폭으로 성장할 것으로 기대되며 단독 IDS/IPS도 견고한 성장을 기록할 것으로 전망한다. IDC에서 분류하는 보안 어플라이언스는 방화벽/VPN, IDS/IPS(침입탐지 및 예방), 통합위협관리, SCM, 일부 L4~7 스위치 등이 있다.

제품 유형별로 2004년 보안 어플라이언스 시장을 살

펴보면, 방화벽/VPN이 637억원으로 전체시장의 55.2%를 차지할 것으로 추산되며, UTM이 26.4%인 305억원, IDS/IPS가 18.4%인 212억원을 기록할 것으로 보인다. 2004년 시장의 26.4%를 차지한 UTM은 2003년부터 2008년까지 향후 5년간 연평균 40.8%의 성장률을 보이며 2008년에는 방화벽/VPN을 제치고 가장 큰 시장규모를 형성할 것으로 예상된다.

박예리 한국IDC 연구원은 "국내 보안장비시장은 과거 범용 서버에 소프트웨어를 탑재하는 방식에서 벗어나 소프트웨어를 최적화시킨 전용 어플라이언스로 추세가 변하고 있다"며 "이는 속도나 성능면에서 전용 어플라이언스가 이점을 지니고 있기 때문"이라고 설명했다. 또한 그는 "이는 국내뿐 아니라 전 세계적 추세"라며 "IDC에서는 전 세계적으로 2007년 경이 되면 보안제품의 약 80%가 보안 어플라이언스 형태로 공급될 것으로 보고 있다"고 밝혔다. 특히 보안 어플라이언스 가운데 UTM의 성장이 두드러질 것으로 예상했다.

이에 대해 넥스지측은 "한국IDC에서는 2007년 국내 UTM 시장규모를 600억원 정도로 예측했고 전 세계적으로 2007년 1억 2000달러의 시장규모가 될 것으로 추측한다"며 "기존 방화벽/VPN 시장이 급속하게 UTM 시장으로 대체될 것이다"고 설명했다. 또한 "비단 보고서뿐만 아니라 지금은 디지털 컨버전스(융합) 시대"라며 "보안관리자는 핸드폰을 구매할 때처럼 여러 보안기능을 비교한 후 네트워크 장비를 구매하게 될 것"이라는 전망을 내놓았다.

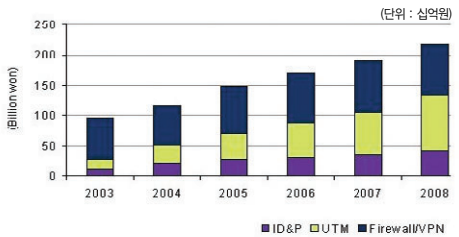


그림. 국내 보안 어플라이언스 시장 전망, 2003~2008년

UTM, 기술전문화 노력 필요

하지만 UTM과 관련해 이같은 장밋빛 전망만 있는 것은 아니다.

임채호 NHN 보안실 실장은 UTM과 관련해 세 가지 문제점을 지적했다. 먼저 보안기능을 모두 적용하기에는 성능상 문제가 있다는 것. 국내에 소개되고 있는 각 제품들을 보면 외산은 주로 방화벽 · 안티바이러스 · VPN · IDS/IPS 등 네트워크에 관련된 기능이 주된 반면, 국산제품은 방화벽 · VPN · IDS/IPS 등에 초점이 맞춰져 있다. 그렇기 때문에 이를 도입하는 기업이 자신의 네트워크 환경에 잘 적용할 수 있도록 2~3개의 기능에만 만족하는 것이 올바른 선택이 될 것이다. 두 번째 이들을 선택하면 업무처리에는 훨씬 효과적이나 알려지지 않은 새로운 공격을 다 막아내기가 어려울 것이라는 점이다. 특히 제로데이 공격, 사회공학 공격 등은 네트워크가 아닌 애플리케이션 등을 공격하므로 이러한 공격에 대해서는 전문적인 감시체계 및 프로세스를 갖춘 대응을 해야 한다. 물론 UTM도 공격이 아닌데 공격으로 판단하는 False Positive, 공격인데 탐지를 못하는 False Negative가 꽤 있을 수 있다는 사실을 알아야 한다. 마지막으로 UTM은 각각의 보안기능이 중요한 선택기준이 되며, 물론 못지 않게 도입기관이 납득할 수준의 성능이 중요하다. 하지만 더 중요한 것은 탐지된 보안사건, 즉 보안이벤트가 각각의 탐지결과 등과 제대로 된 상관관계 분석이 이루어지고, 관리자가 쉽게 판단할 수 있는 사용자 인터페이스를 제공하는지 여부가 문제다.

이외에도 각 벤더사들이 지적하는 문제점을 살펴보면, 어느 한 기능이 문제가 발생할 때 보안장비 전체를 점검해야 하는 불편함이 있다는 것이다. 또한 많은 업체들이 통합보안장비를 발표하고 있지만 완벽하게 각 기능을 통합적으로 지원하기에는 아직 미흡한 점이 많다.

특히 2004년과 2005년에 성장하던 UTM 시장이 2006년에는 정체되어 있는 분위기인데 이는 엔터프라이드급 시장공략 결과가 그다지 좋지 않았기 때문이며, SMB 시장에서 ISP 사업자들과의 협업을 통한 임대사업 모델이 포화에 이른 탓이라는 분석도 있다. 이는 SMB 시장에서 그동안 유효했던 임대사업 모델을 벗어나 독자적인 솔루션 시장을 형성하는 힘이 부족해 시장성장의 걸림돌이 되고 있다는 지적이다.

효율적인 UTM 도입을 위한 체크리스트, UTM 이것만은 확인하고 구입하자

보안에 있어 UTM이 대세라고 하지만 각 기업의 보안실무자들이 가장 혼란스러워 하는 부분이 무엇을 기준으로 UTM을 도입할 것인가 하는 문제다. 컨설팅 회사 코어 콤퍼턴스 부사장인 리자 피퍼는 UTM을 설치하기 전에, 제품이 아닌 설계 방법으로 생각을 전환할 때 고려해야 할 몇 가지 문제점을 제안했다.

- ☑ 교체하고 싶은 기존의 보안시스템이 무엇인가? 너무 비용이 많이 들거나, 더 이상 신뢰할만큼 당신의 필요를 충족시키지 못하는 플랫폼이 후보 1순위다.
- ☑ 어떤 BOB 제품을 남기고 싶은가? UTM이 다른 서비스들을 대체할 수 있지만 당신의 필요를 충족하는 솔루션을 바꿀 것을 요구해서는 안된다.
- ☑ UTM 어플라이언스가 BOB와 스위치 같은 인접 시스템과 어떻게 조화되어야 하는가? 모든 제품들이 망이나 가상 LAN을 지원하는 것은 아니다.
- ☑ 당신은 어떤 종류의 인증을 사용하는가? 많은 UTM 제품들이 RADIUS와 인터페이스 할 수 있지만 싱글 사인온, 액티브 디렉터리, 802.1x의 지원에서 다양할 수 있다.
- ☑ UTM이 당신의 관리 모니터링 프레임워크에 어떻게 맞춰져야 하는가? 멀티 유니트 또는 다계층 정책행정과 SNMP 같은 역량들은 보편적인 것과 거리가 멀다.
- ☑ 현재와 미래의 성능 요구사항을 설정하는가? 공급업체의 설명서는 단지 지침일 뿐이다. 실제 성능을 시험하고 그에 따라 조절할 계획을 세운다.
- ☑ 성장을 어떻게 조절할 것인가? 하나의 CPU에 모든 것을 통합하는 것이 비현실적이라면 어플라이언스나 블레이드에 서비스들을 분배하고, 부하의 균형이나 암호 가속 옵션을 찾는다.

대기업의 UTM 선택시 고려사항

- ☑ 한두 가지 기능에 집중 (기가비트 백본망을 보유한 곳에서의 성능저하를 예방하고 기능별로 전문적이고 목적에 맞는 전용 보안장비를 필수적으로 쓸 수 밖에 없는 환경일 가능성이 높다)
- ☑ UTM 제공 기능과 사용중인 전용 제품들 사이에 겹치는 부분 확인
- ☑ VPN 교체용으로 도입시 기존 VPN 시스템들과 호환이 가능한지 확인
- ☑ 사후 서비스 대응력이 얼마나 빠르며 이를 위한 인프라를 갖췄는지 확인
- ☑ 중앙 집중관리의 편의성 확인

중소기업의 UTM 선택시 고려사항

- ☑ 스팸과 안티바이러스가 잘 탐지되고 차단되는지 확인 (중소기업은 외부공격보다 업무에 장애를 초래하는 수많은 스팸과 애드웨어가 더 절실할 수 있다)
- ☑ 설치 및 유지보수, 통합관리가 쉽고, 장애처리가 잘 되는지 확인
- ☑ 연간 패턴 업데이트 서비스나 유지보수 서비스의 가격 비교
- ☑ 장비에 대한 관리 대행을 비롯한 기술지원 서비스를 원활하게 받을 수 있는 인력 및 시스템 노하우를 갖췄는지 확인

공공기관의 UTM 선택시 고려사항

- ☑ 국가정보원의 인증제품임을 확인
- ☑ 한국 고유의 알고리즘(예를 들어 SEED)을 지원하는지 확인
- ☑ 대형망에 대한 장비설치 및 유지보수 경험 여부

국내에 출시되어 있는 각 사별 UTM 솔루션의 주요 기능 및 특징

II

퓨쳐시스템 / 안철수연구소 / 어울림정보기술 /
현대HDS[워치가드] / 주니퍼네트웍스 / 액텔라 /
포티넷 / 시큐아이닷컴 / STN 기술 /
시스코시스템즈코리아 / 한국쓰리콤 / 체크포인트 /
모젠소프트 / 넥스지

시장에서 검증된 독자적 하드웨어 기술, 퓨쳐시스템

Future UTM 시리즈

'FutureUTM'은 지난해 퓨쳐시스템에서 출시한 통합보안솔루션으로 기존 방화벽, VPN은 물론 IPS, 바이러스월 등의 기능을 한대의 장비에서 제공하여 네트워크를 통한 다양한 보안위협에 능동적으로 대응이 가능하도록 한 제품이다.

'FutureUTM'은 통합보안에 대한 시장의 니즈에 부합하는 다양한 보안기능을 제공하는 한편 기존 통합보안솔루션에서 문제점으로 지적되어 왔던 성능 및 복잡한 관리기능을 대폭 개선한 것이 특징이다.

'FutureUTM'은 기존 방화벽, VPN은 물론 IPS, 바이러스월 등의 기능을 한대의 장비에서 제공하여 네트워크를 통한 다양한 보안위협에 능동적으로 대응이 가능하도록 한 제품

방화벽/VPN + IPS 기능의 하드웨어 기반

'FutureUTM'은 수년간 시장에서 검증된 독자적인 하드웨어 기술을 기반으로 속도 및 성능에 영향을 주지 않으면서 위협에 대한 효과적인 차단기능을 수행하는 통합보안엔진을 탑재하여 빠르고 정확한 네트워크 보안기능을 수행하는 것이 특징이다.

또한 사용자 편의성을 대폭 향상한 관리 툴은 실시간 네트워크 분석, 감시, 차단 기능 등 세분화된 모니터링 및 컨트롤을 할 수 있을 뿐만 아니라 도킹 윈도(Docking Window) 기능을 적용하여 자신이 원하는 형태로 화면을 설정하여 사용 가능하다.

현재 'FutureUTM'은 고객의 네트워크 환경에 따라 적정한 제품을 선택하여 구축할 수 있도록 기가네트워크를 지원하는 중대형사이트용 FutureUTM 6000, FutureUTM 3000과 10/100M 급의 중소형 제품인 FutureUTM 1500, FutureUTM 100의 제품 라인업을 갖추고 있다.

'Future UTM' 제품은 기존의 방화벽/VPN 제품에 IPS기능을 더한 하드웨어 기반의 통합 네트워크보안 게이트웨이다. 시장에서 검증된 빠르고 안정된 처리 속도를 자랑하는 퓨쳐 방화벽/VPN 통합솔루션에 IPS의 기능을 추가함으로써 고객의 니즈에 부합하는 빠른 처리 속도와 강력한 보안 두 가지를 동시에 만족한다.

하드웨어 기반의 방화벽

'FutureUTM'의 주요한 특징이라고 한다면 VPN/방화벽을 통해 수년간 시장에서 검증된 독자적인 하드웨어 기술을 기반으로 했다는 점이다. 이에 퓨쳐 VPN/방화벽의 특징을 살펴보기로 하겠다.

퓨쳐 VPN/방화벽은 16년간 쌓아온 퓨쳐시스템의 노하우로 네트워크 및 시스템 부하를 최소화하도록 설계, 개발된 하드웨어 기반이다. 수백 Mbps, 그 이상의 Gbps 범위까지 네트워크 속도의 발전과 고도로 지능화되는 각종 해킹 또는 웜 공격에도 안전하다.

일관된 처리능력과 뛰어난 안정성으로 호평받고 있다. 각종 룰 설정과 검사해야 할 네트워크 패킷이 증가할수록 소프트웨어 형태의 제품은 그 성능이 저하되나 하드웨어 기반의 제품은 일관된 처리성능을 유지한다. 또한 빠른 속도를 위해 탐지해야 할 패킷에 대해 일정 크기 이상에 대한 처리를 제한하는 소프트웨어 형태의 제품에 비해 하드웨어 기반의 제품은 모든 패킷에 대해 빠른 속도로 처리한다.

전용 OS로 보안위협을 최소화한다. 우리나라 인터넷을 마비시킨 슬래머 웜을 비롯해 블래스터 웜, 사세르 웜, 베이글 웜, 아고보트 웜 등 상용 OS의 보안취약점을 노리는 웜이 급증하면서 그 피해사례도 늘어가고 있는 추세이다. 특히 최근에는 보안취약점이 발견되고 이를 공격하는 웜의 출현 주기가 점점 빨라져 보안 패치파일 및 백신 프로그램으로 막는데 한계가 있다. 퓨쳐 방화벽/VPN은 ASIC 기반의 독자적으로 개발한 전용 OS를 사용하여 윈도, 유닉스 등 상용 OS에서 발생한 보안문제에 영향을 받지 않는다.

또한 소프트웨어 대비 짧은 부팅시간으로 경제적 손실을 최소화한다. 퓨쳐 방화벽/VPN은 네트워크 장애발생 등으로 인한 재부팅시 별도 서버를 이용하는 소프

솔루션명 : FutureUTM
특징/장점 : 하드웨어 기반의 고성능 통합보안 제품
최신의 다양한 유해 트래픽을 효과적으로 차단하는 IPS 탑재
사용자 중심의 GUI와 다양한 모니터링 및 리포팅 기능
각 기능별 취사선택이 가능한 고객 맞춤형 제품 구현

VPN/방화벽을 통해 수년간 시장에서 검증된 독자적인 하드웨어 기술을 기반으로 속도 및 성능에 영향을 주지 않으면서 위협에 대한 효과적인 차단기능을 수행하는 통합보안엔진을 탑재

트웨어 방식의 보안장비 보다 월등히 짧은 시간에 복구가 가능하다. 이를 통해 혹시라도 발생할 수 있는 장애로 인한 유 · 무형의 자산 손실까지도 최소화한다.

국내 유일의 보안장비 자체 생산시설을 보유했다. 퓨쳐시스템은 자체 생산시설을 보유하고 설계에서 생산을 모두 도맡아 완성도 높은 보안제품을 생산하고 있다. 외국기업과 기술제휴 또는 생산을 아웃소싱하고 있는 기업들과 달리 ISO 9001:2000 인증을 획득한 자체 생산라인에서 자체 기술력을 바탕으로 제품개발과 원가를 절감한다.

퓨쳐 방화벽/VPN은 손쉽고 다양한 관리가 가능하다. 국내뿐만 아니라 해외 여러 지역에 분산되어 설치 운용되더라도 중앙에서 통합집중관리가 가능하다. 퓨쳐 방화벽인 'SecuwayCenter 2000'을 통해 소속된 모든 장비 및 사용자 관리(등록, 변경, 삭제), 인증서 관리, 정책관리 및 전송, 집중적인 로그관리 등의 모든 작업을 통제할 수 있다.

또한 'SecuwayCenter 2000'은 한글을 지원할 뿐만 아니라 사용자 중심의 웹 기반 사용자 인터페이스를 제공함으로써 관리자가 보다 손쉽게 설치운용중인 다수의 퓨쳐 방화벽/VPN을 관리할 수 있다.

'FutureUTM 시리즈'의 주요 특징

하드웨어 기반의 고성능 통합보안 제품 하드웨어 기반의 고성능 통합보안 엔진을 탑재하여 빠르고 정확한 네트워크 보안기능을 수행한다. 이미 시장에서 검증된 퓨쳐시스템의 하드웨어 개발 노하우로 최고의 속도와 안정성을 제공한다.

최신의 다양한 유해 트래픽을 효과적으로 차단하는 IPS 탑재 하드웨어에 최적화된 고성능의 IPS 엔진을 통해 네트워크를 통해 들어오는 웜, 바이러스 등 유해 트래픽에 대한 차단기능을 제공한다. 전문화된 자체 CERT를 통해 새로운 공격에 대한 침입방지 패턴을 신속하게 제공하여 보다 안전한 네트워크 환경을 보장한다. 사용자 중심의 관리기능을 통해 차단 상세 제어는 물론 손쉽게 차단 세션에 대한 확인 및 해제를 한다.

사용자 중심의 GUI와 다양한 모니터링 및 리포팅 기능 사용자가 쉽게 실시간으로 상태를 이해하고 관리할 수 있도록 사용자가 원하는 형태로 구성할 수 있는 관리 툴을 제공한다. 실시간으로 파악된 데이터를 사용자가 원하는 형태로 표현할 수 있는 다양한 보고서 및 패턴 상세 정보의 포맷을 제공한다.

각 기능별 취사선택이 가능한 고객 맞춤형 제품 구현 방화벽을 중심으로 VPN, Viruswall, IPS 등의 기능을 제공하는 통합보안제품으로 고객의 환경에

www.future.co.kr

따라 필요한 기능만 선택할 수 있어 TCO 절감과 관리부담을 감소한다.

기업 규모에 따라 선택할 수 있는 다양한 라인업

퓨쳐시스템 'FutureUTM 시리즈'의 차별성이라고 한다면 먼저 속도와 성능을 꼽을 수 있다. VPN/방화벽을 통해 수년간 시장에서 검증된 독자적인 하드웨어 기술을 기반으로 속도 및 성능에 영향을 주지 않으면서 위협에 대한 효과적인 차단기능을 수행하는 통합보안엔진을 탑재하여 빠르고 정확한 네트워크 보안 기능을 수행한다.

또한 사용자 편리성이다. 그동안 쌓아온 노하우를 통해 개발한 UTM 관리 툴은 실시간 네트워크 분석, 감시, 차단기능 등 세분화된 모니터링 및 컨트롤을 제공할 뿐만 아니라 도킹 윈도(Docking Window) 기능을 통해 자신이 원하는 형태로 화면을 설정하여 사용 가능하도록 함으로써 사용자 편의성을 강화했다.

기타 경쟁력으로는 기업의 규모에 따라 선택할 수 있는 다양한 라인업 구축, 그동안 시장에서 검증받은 제품의 안정성, 고객의 요구에 대응할 수 있는 제품에 대한 커스터마이징(customizing) 능력과 신속한 기술 지원 서비스이다.

타깃시장으로는 VPN/방화벽 선도업체로서 그동안 확보하고 있는 두터운 고객망을 기반으로 대형망부터 중소형망에 이르기까지 기존 고객의 교체 및 추가 수요를 UTM으로 적극 유도할 계획이다.

퓨쳐시스템

퓨쳐시스템(김광태 대표)은 명실상부한 우리나라를 대표하는 네트워크 보안전문기업이다. 올해로 창사 20주년을 맞이하는 퓨쳐시스템은 인터넷이 낯설 당시인 1990년대 초반 TCP/IP 솔루션을 통해 네트워크 사업에 진출하였으며 1997년 국내 최초로 VPN 제품을 자체 개발하면서 본격적인 네트워크 보안사업을 시작하였다. 국내 최초 VPN 제품 상용화, 국내 최초 네트워크 보안용 SoC 개발, 국내 최다수, 최대규모의 VPN 고객 보유 등 우리나라의 네트워크 보안분야의 역사에서 퓨쳐시스템은 누구도 따라올 수 없는 위상을 쌓아왔다.

퓨쳐시스템의 가장 큰 자산은 그동안 쌓아온 위상과 브랜드 파워 이외에도 무엇보다 탄탄하게 유지하고 있는 기존 고객층이다. 국내 최대 규모의 네트워크 망을 자랑하는 행정자치부와 농협을 중심으로 우리나라 공공과 금융권에서 가장 두터운 고객층을 확보하고 있다.

20년간 쌓아온 네트워크 및 네트워크 보안에 대한 기술력과 노하우, 브랜드 파워, 탄탄한 고객층을 기반으로 UTM을 필두로 펼쳐지는 향후의 네트워크 보안시장에서 지속적인 성장과 가치 창조를 통해 국내를 넘어 세계적인 네트워크 보안전문기업으로 거듭날 것이다.

www.future.co.kr / Tel. 02-6220-7760

UTM의 진검 승부사, 안철수연구소 트러스가드 UTM 시리즈

안철수연구소가 UTM 솔루션을 준비한 것은 2006년 초이며, (구)시큐어소프트의 네트워크시큐리티 기술과 안철수연구소의 컨텐츠시큐리티 기술이 결합된 전방위 네트워크 보안제품인 '트러스가드 UTM'은 2007년 5월 7일 출시했다.

안철수연구소는 '트러스가드 UTM'을 출시함에 따라 자체 핵심 원천기술로 세계 수준의 네트워크 보안 경쟁력을 확보하는 한편, 외산 위주의 네트워크 보안 시장을 재편할 리더로 역량을 갖추었다는 게 자체 평가다. 또한 PC 단위부터 모바일 기기 및 온라인 게임보안은 물론 네트워크 단위까지 전방위 통합보안솔루션을 갖춰 보안업계의 리더로 급부상했다.

안철수연구소는 '트러스가드 UTM'을 출시함에 따라 자체 핵심 원천기술로 세계 수준의 네트워크 보안 경쟁력을 확보하는 한편, 외산 위주의 네트워크 보안시장을 재편할 리더로 역량을 갖춰

3세대 네트워크 보안 패러다임 변화 주도

안철수연구소는 보안 패러다임 상에서 UTM을 3세대 네트워크 보안솔루션으로서 '통합보안 플랫폼'이라고 정의했다. 즉, 소프트웨어 기반의 방화벽과 IDS(침입탐지 시스템) 중심의 1세대와 하드웨어 어플라이언스 기반의 방화벽과 IPS(침입방지 시스템) 중심의 2세대를 거쳐 3세대는 바이러스, 웜, 트로이목마 등의 악성코드와 네트워크 공격을 종합적으로 처리해주는 UTM이 주도할 것으로 전망한 것이다. 또한 네트워크 보안의 패러다임이 보안콘텐츠와 실시간 서비스 중심으로 바뀌고 있다고 진단했다. 안철수연구소는 이런 보안의 패러다임 변화를 자사의 '트러스가드 UTM'으로 주도해나가겠다는 전략이다. 하지만 2007년 UTM 관련 예상 매출규모에 대해서는 올해 5월에 출시했기 때문에 비중이 크지 않다고 밝혔다.

트러스가드 UTM은 최신 보안위협 대처 '탁월'

안철수연구소는 기존의 개별 보안제품들은 각각의 한계가 있기 때문에 한 장비로 다종다양한 보안위협을 막고자 하는 기업에게 '트러스가드 UTM' 도입을 제안한다. 최근 가장 심각한 보안위협 요소는 복합적 공격과 제로데이 공격, DDoS(분산서비스 거부) 공격, 특정 IRC 서버에 접속해 수시로 악의적 프로그램을 내려받는 악성코드 등으로 '트러스가드 UTM'이 이런 최신 위협에 가장 잘 대처할 수 있는 제품이라는 설명이다. 또한 보안관리와 운영의 통합으로 관리부담이나 비용을 절감해준다.

'트러스가드 UTM'에는 19년 동안 축적된 안티바이러스/스파이웨어/스팸 등의 보안콘텐츠 기술이 구현돼 있다. 따라서 그동안 네트워크 수준에서 대응할 수 없었던 바이러스, 웜, 스파이웨어 등의 악성코드와 이를 기반으로 이루어지는 공격을 높은 기술력으로 차단해준다. 또한 3000여 개의 고객사에서 검증되고 10년 이상의 지속적인 기술개발로 발전을 거듭한 최신 방화벽 엔진과 IPS 엔진이 장착돼 있어 안정적인 네트워크 보안기능을 제공한다. 방화벽과 VPN은 '수호신 앱솔루트 방화벽'의 고성능 패킷 처리기술과 검증된 안정성을, IPS는 '앱솔루트 IPS'의 지능형 방어기술을 기반으로 한다. 아울러 24시간 365일 쉬지 않고 운영되는 시큐리티대응센터(ASEC)에서 각종 보안위협을 모니터링하며 긴급 대응 정책을 제공한다. 네트워크 장비로는 최초로 CDN(Content Delivery Network)을 통해 보안콘텐츠 엔진을 최단 시간 내에 업데이트 해준다.

'트러스가드 UTM'은 이 밖에도 PC 보안솔루션과 연동하여 더 완벽한 보안체제를 제공한다. 위협의 진원지가 되는 감염 시스템을 발견하여 차단/격리해주며 검증되지 않은 PC에 대해 안철수연구소의 키보드 보안솔루션인 '마이키디펜스(MyKeyDefense)', 실시간 해킹차단 솔루션인 '마이파이어월(MyFirewall)'과 연동해 완벽한 보안환경을 구현한다. 또한 네트워크의 전반적 상황을 지능적으로 판단함으로써 위협에 대한 종합적 처리와 사후관리를 수행하는 것도 강점이다.

네트워크 보안, 실시간 긴급 대응기술의 완벽한 결합

'트러스가드 UTM'의 강점은 보안콘텐츠 기술과 네트워크 보안기술 그리고 실

솔루션명 : 트러스가드 UTM
특징/장점 : 탁월한 보안콘텐츠 기술에 기반한 높은 보안위협 탐지율
철저히 검증된 네트워크 보안기술
24시간 365일 실시간 예방/대응 및 업데이트 서비스
독보적인 엔드포인트 보안관리

'트러스가드 UTM'의 강점은 보안콘텐츠 기술과 네트워크 보안기술 그리고 실시간 긴급 대응 체계의 3요소가 긴밀하게 결합돼 탁월한 시너지 효과를 낸다는 것

시간 긴급 대응 체계의 3요소가 긴밀하게 결합돼 탁월한 시너지 효과를 낸다는 것이다. 즉, 안티바이러스/스파이웨어/스팸 등의 보안콘텐츠 기술과 방화벽, IPS, VPN 등의 네트워크 보안기술, 24시간 365일 실시간 예방/대응 서비스가 화학적으로 결합돼 동종제품 가운데 가장 빠른 속도와 효율성을 제공한다.

더욱이 국내외 보안업계에서 유일하게 핵심적인 원천기술을 안철수연구소가 자체 보유해 높은 신뢰도와 기술력을 갖추고 있다. 보안콘텐츠 기술은 '트러스가드 SCM'의 IPS와 웜/스파이웨어 탐지기술을, 방화벽과 VPN은 '수호신 앱솔루트 방화벽'의 고성능 패킷 처리기술, 네트워크 환경 운용경험, 애플리케이션 처리기술, 검증된 안정성 그리고 IPS는 '앱솔루트 IPS'의 지능형 방어기술을 기반으로 한다.

한편 '트러스가드 UTM'은 SSL VPN 기능이 포함되어 있다. SSL VPN은 자신의 PC가 아닌 이동 환경에서도 쉽게 사용할 수 있다는 관점에서 IPSec VPN과 함께 쌍벽을 이룰 VPN의 신규시장이라고 할 수 있다. 안철수연구소는 기존 '수호신 앱솔루트'에서 지원되던 IPSec VPN과 함께 '트러스가드 UTM'에서 SSL VPN을 갖춤으로써 전체 VPN 라인업을 갖추게 되었다. 특히 안철수연구소의 SSL VPN은 PC 단위 보안솔루션과 완전히 연동함으로써 SSL VPN 연결 사전/사후에 PC를 관리해 주는 특성을 갖추었다.

트러스가드 UTM의 주요 특징

탁월한 보안콘텐츠 기술에 기반한 높은 보안위협 탐지율 '트러스가드 UTM'의 보안위협 탐지율은 19년 간 최고의 자리를 지켜 온 콘텐츠 보안기술을 기반으로 한다. 보안장비의 가장 중요한 속성은 '성능'과 '탐지율'이다. 기존 업체들이 성능을 강조하고 있지만 고객들이 진정 원하는 것은 복합공격에 대한 높은 방어능력이다. 특히 최근의 보안위협을 보면 해커에 의한 공격보다는 바이러스나 웜 등의 콘텐츠 기반의 공격이 대부분이다. 복합된 공격들 또한 그 파괴력은 웜, 바이러스, 유해 스크립트 등 콘텐츠에 의한 것이다.

철저히 검증된 네트워크 보안기술 3000여 개의 고객사에서 검증되고 10년 이상의 지속적인 기술개발로 발전을 거듭한 최신 방화벽 엔진과 IPS 엔진이 장착돼 있어 안정적인 네트워크 보안기능을 제공한다. 방화벽과 VPN은 '앱솔루트 방화벽'의 고성능 패킷 처리기술과 검증된 안정성을, IPS는 '앱솔루트 IPS'의 지능형 방어기술을 기반으로 한다. 커널 기반의 IPS 엔진과 완벽하게 동작하도록 아키텍처가 설계되었기 때문에 다양한 보안모듈들이 안정적인 네트워크 보안기술 기반 위에서 작동한다.

24시간 365일 실시간 예방/대응 및 업데이트 서비스 그런가하면 공격이 감지될 때 보안관리자들은 1분 1초를 다투는데, 이때 담당 보안업체가 신속히 대응할 수 있는 체계를 갖추고 있느냐는 고객에게 매우 중요한 문제이다. 안철수연구소는 24시간 365일 각종 보안위협을 모니터링하고 실시간 응급 대응하는 전문 조직인 시큐리티대응센터(ASEC)를 보유하고 있으며, 공격 이전 단계인 취약점 발표 단계에서부터 예측 차단 룰(Proactive Defense Rule)을 배포한다.

독보적인 엔드포인트 보안관리 SSL VPN은 자신의 PC가 아닌 이동 환경에서도 쉽게 사용할 수 있다는 관점에서 IPSec VPN과 함께 쌍벽을 이룰 VPN의 신규시장이다. 안철수연구소는 기존 '수호신 앱솔루트'에서 지원되던 IPSec VPN과 함께 '트러스가드 UTM'에서 SSL VPN을 갖춤으로써 전체 VPN 라인업을 갖추게 되었다. 특히 안철수연구소의 SSL VPN은 PC 단위 보안솔루션과 완전히 연동함으로써, SSL VPN 연결 사전/사후에 엔드포인트를 관리해준다.

높은 성능과 가용성 독자 개발한 네트워크 OS인 ANOS(AhnLab Network OS) 엔진으로 최적의 IPS 성능을 실현하였으며 부하 분산기법을 이용한 프록시 설계로 애플리케이션 처리 성능이 매우 우수하다. 또한 HA 구성 시 세션의 끊김없이 빠른 속도의 절체가 가능하다. 별도의 스위치 장비 없이 풀메쉬(Full Mesh) 네트워크를 지원하며 자동화된 물리적 바이패스(bypass)도 가능하다.

안철수연구소

안철수연구소(오석주 대표)는 1995년 3월 창립된 글로벌 통합보안 솔루션/서비스 기업이다. 국내 최장수 소프트웨어 브랜드인 V3 제품군을 비롯해 온라인 보안서비스 '빛자루', 네트워크 통합보안 장비 트러스가드 시리즈, 모바일 보안솔루션, 온라인 게임 보안솔루션 등 첨단 인터넷/네트워크 환경에 적합한 보안솔루션을 개발 공급하고 있으며, 정보통신부 지정 정보보호컨설팅 전문업체로서 보안컨설팅도 제공하고 있다. 안철수연구소는 세계적 기술력을 보유한, 국내 보안업계에서 가장 오랜 역사와 가장 큰 규모를 가진 업체이다.

세계적으로 정보보안 시장이 형성되기 시작한 1988년부터 쌓은 정보보안 노하우를 기반으로 시장을 개척해왔으며, 설립 이래 꾸준한 매출성장을 보여 국내 보안업계 선두를 유지하는 한편, 역동적으로 글로벌시장에 진출해 성공사례를 만들어가고 있다.

안철수연구소는 급변하는 IT 환경과 그에 따른 사용자의 요구를 제품과 서비스를 통해 충족함으로써 2010년 세계 10대 보안전문 기업으로 도약한다는 비전을 목표로 한다. 장기적으로는 구성원 모두 핵심 가치를 진심으로 믿고 지속적으로 견지해나가는 '영혼이 있는 기업'이 목표다.

www.ahnlab.com / Tel. 02-2186-6000

하드웨어 기반 고성능, 어울림정보기술 SECUREWORKS 시리즈

어울림정보기술의 SECUREWORKS ezWall 200 제품은 네트워크에서 발생하는 모든 위험요소들을 완벽하게 진단/차단/방어할 수 있는 능동형 통합보안제품이다. SMB와 SOHO급 네트워크 환경에 알맞은 일체형 장비로 강력한 보안성을 유지시켜주는 고기능성 제품으로 쉽고 편리한 운용성을 제공한다. 제공되는 뛰어난 성능의 IPS와 방화벽, VPN, 내부 사용자 제어를 위한 NAC 기능 등은 다양한 침입과 불법적 접근에 대해서 효과적으로 탐지/차단/방어하는 효율적인 구조를 채택하고 있기 때문에 안심하고 각종 네트워크 및 인터넷 사용을 가능하게 하는 안전한 환경을 제공한다.

어울림정보기술의 SECUREWORKS ezWall 200 제품은 네트워크에서 발생하는 모든 위험요소들을 완벽하게 진단/차단/방어할 수 있는 능동형 통합보안제품

VPN의 암호화 속도 개선

어울림정보기술의 UTM 제품은 하드웨어의 특성을 효과적으로 이용하고 각 모듈간의 인터페이스를 독립적으로 구성한 장비로 이를 통하여 성능 및 기능에서 탁월한 장점을 제공한다.

하드웨어의 경우 멀티 코어를 이용하여 각 코어별 독립 프로세스를 할당하여 패킷과 스트림의 전처리 및 후처리를 나누어 처리하는 개념을 도입했다. 예전의 포트나 서비스별 또는 기능별로 처리하는 제품들과는 다르게 동작하는데, 각 코어에서 먼저 발견된 잘못된 결과를 처리하기 때문에 보다 빠른 판단을 이끌어 낼 수 있어 하드웨어의 자원 확보 및 성능을 대폭 개선할 수 있다.

또한 코어에 내장된 가속기 기능을 이용하여 VPN의 암호화 속도 개선을 이루었고, IPS나 기타 콘텐츠 필터링에서의 Regular Expression의 성능도 대폭 향

상시킴으로써 방화벽, VPN, IPS의 인프라 기능 및 성능 개선으로 인해 후반부의 콘텐츠 필터링의 성능 개선도 뒷받침 되고 있다.

또한 메인 프로세서를 N개를 사용하여 안티바이러스, 안티스팸, 콘텐츠 필터링을 Primary Core와 Secondary Core로 구분하여 처리하며, 그 결과를 프로세서 간의 Fast-Path를 통해 공유함으로써 마치 하나의 프로세서에서 처리되는 것과 같은 효과를 볼 수 있다.

이처럼 하드웨어를 마치 소프트웨어의 멀티 쓰레드와 같이 사용할 수 있도록 하여 보다 효과적인 UTM 구성이 가능하며, 또한 동적으로 각 프로세서와 각 기능 간의 매칭을 변경할 수 있는 장점을 제공하고 있다.

이같은 어울림정보기술의 VPN 기술은 둘째가라면 서러울 정도다. 이는 레퍼런스 확보에도 단단히 한몫하고 있다. 어울림정보기술은 최근 LIG 손해보험, 삼육재단의 기가급 방화벽과 가상사설망(VPN)사업 프로젝트를 수주했다.

이번에 LIG손해보험에 공급한 장비는 어울림정보기술이 개발한 통합보안장비로 암호화를 통해 인터넷을 사설망처럼 안전하게 통신할 수 있게 했다. 기존 방화벽과 VPN을 기가 장비로 업그레이드, 전국 1천여 개의 지점 및 대리점에서 고속 인터넷 서비스가 가능하도록 했다. 또한 최근 삼육어학원의 전국 40여 개 지점을 연결하는 총 3억3천만원 규모의 VPN 프로젝트를 수주하기도 했다.

어울림정보기술은 공격적인 레퍼런스 확보뿐만 아니라 시큐어웍스 시리즈인 '아이피에스월 1000 V4.0' 제품에 대해 국제공통평가기준 상호인정협정(이하 CCRA) EAL4(Evaluation Assurance Level 4) 등급 인증을 획득했다.

2006년 12월 국정원으로부터 동일 제품에 대한 CC인증을 획득하였으나, 우리나라가 지난 5월 CCRA에 가입함에 따라 국제적으로 통용 가능한 CC인증을 재획득하게 되었다. CCRA는 정보보호제품의 안정성을 회원국간 상호 인정해 활용을 증진시키는 국제 협약이다.

기존의 CC인증이 국내에서만 영향력을 발휘할 수 있었던 것과는 달리 금번에 획득한 인증은 CCRA 가입국가 24개 국에서 공통적으로 효력을 인정받게 된다는 점에서 상당한 의미가 있다는 것이 어울림 측의 설명이다.

금번에 인증을 획득한 '시큐어웍스 아이피에스월 1000' 제품은 방화벽, VPN, IPS, 안티바이러스 등의 기능을 모두 지원하는 통합관리솔루션 장비이다.

솔루션명 : SECUREWORKS 시리즈
특징/장점 : 동급 중에서 고성능 제공
다양한 보안기능 제공
다양한 속도의 제품
클라이언트 보안과의 결합
통합관리도구

자체 개발한 하드웨어 일체형 장비로써 멀티코어 네트워크 프로세서와 이더넷 컨트롤러가 탑재되어 높은 쓰루풋을 제공하고 네트워크 병목현상을 최소화해 최고의 성능을 보장

다이내믹 하드웨어 스케줄링으로 트래픽 자체 분석

어울림정보기술의 UTM 솔루션은 다이내믹 하드웨어 스케줄링으로 네트워크 트래픽을 자체적으로 분석 및 판단하여 요구되는 기능의 우선순위별로 하드웨어 프로세서를 할당하는 기능을 가지고 있다. 이러한 기능을 사용할 경우 단위 시간당 요청되는 서비스의 변화에 유동적으로 대처가 가능하므로 고품질의 서비스를 유지할 수 있다.

또한 패킷을 선분석하면서 트래픽 미터링 기능을 이용하여 전체 시스템의 트래픽 조절이 가능하다. 따라서 IPS 기능의 트래픽 Anomaly 기능을 단순한 임계치를 이용한 방법을 사용하는 것 보다 훨씬 강화된 자체적인 통계방법을 통해 지속적인 셀프 러닝을 수행하고, 이를 통한 결과를 제시할 수 있는 강점을 제공한다.

새롭게 개발된 고성능 장비는 기업시장과 통신시장을 겨냥하여 출시하였으며, CC인증을 취득한 후에는 공공, 금융 시장에 본격적인 진입을 할 계획이다. 따라서 하드웨어의 특성을 극대화한 고성능을 기반으로 네트워크와 사용자 단까지 모든 보안을 일괄적으로 제공 가능한 시스템으로 기존의 보안장비의 한계점을 뛰어 넘을 수 있으며, 통합관리 도구도 준비되어 있기 때문에 사용자의 관리 편의성도 극대화 가능하다.

하드웨어 기반 고성능 통합보안솔루션

어울림정보기술의 UTM 솔루션은 네트워크에서 발생하는 모든 위험요소들을 완벽하게 진단, 차단, 방어할 수 있는 능동형 통합보안제품으로 가상사설망 기능을 갖추고 있어 데이터 전송시 안전하게 데이터를 전달한다. 또한 VPN 트래픽에 대해서도 IPS 기능이 동작하여 VPN 터널을 통한 바이러스나 웜 확산 방지를 지원한다. 특히 자체 개발한 하드웨어 일체형 장비로써 멀티코어 네트워크 프로세서와 이더넷 컨트롤러가 탑재되어 높은 쓰루풋을 제공하고 네트워크 병목현상을 최소화해 최고의 성능을 보장한다. 로드 쉐링구조와 병렬처리 구조를 지원함으로써 어떤 네트워크 환경에서도 최상의 성능을 제공한다.

최첨단 패킷 필터링 방식인 상태검사 기법과 애플리케이션 프록시를 결합한 강력한 하이브리드 형태의 침입차단 시스템과 IPSec 표준기반의 VPN 기능을 탑재했다. 자체 OS를 탑재함으로써 일반 운영체제에서 발생할 수 있는 보안상의 취약성을 제거했다. 또한 시간대별, 사용자별, 네트워크별, 서비스별로 차등 보안설정이 가능하기 때문에 정교한 보안정책 설정으로 내부 네트워크를 더욱 견고히 지켜준다. 인텔리전트 침입대응 모듈을 장착하여 주요 네트워크 해킹 공격 발생시에 효율적으로 침입을 탐지하고 차단, 경고함으로써 외부에서의 공격발생에 ego 최전방에서 방어가 가능하다.

www.oulim.co.kr

‘SECUREWORKS 시리즈’의 주요 특징

동급 중에서 고성능 제공 멀티 코어의 프로세서를 사용함으로써 기존의 동급 네트워크 보안제품들과 비교하여 월등히 뛰어난 성능을 제공한다.

다양한 보안기능 제공 방화벽, VPN, IPS, 콘텐츠 필터링의 각 보안기능들은 기존의 단독형 네트워크 보안장비 기능에 준하는 기능을 다양하게 제공한다.

다양한 속도의 제품 하드웨어의 특성을 효과적으로 이용하고 각 모듈간의 인터페이스를 독립적으로 구성한 장비로, 10G급의 대형 장비부터 SOHO용 장비까지 모든 구성을 대응할 수 있는 다양한 속도의 제품들이 있다.

클라이언트 보안과의 결합 자체 클라이언트인 CLA(Client Local Agent)를 이용하여 네트워크 보안에서부터 사용자 보안까지 일괄적 제공되기 때문에 보다 완벽한 보안이 가능하다.

통합관리 도구 독립적인 CS 환경을 기반으로 통합 관리툴, 로그 서버, 모니터링, 분석/보고툴을 모두 갖춘 통합관리 도구가 준비되어 있어 All-In-On 보안이 가능한 네트워크 보안시스템이다.

어울림정보기술

어울림정보기술(박동혁 대표)은 K4E 인증 및 CC 기반의 정보보안 전문업체로 자체 기술로 개발한 SECUREWORKS를 통해 K4E, ICSA 그리고 CC 등 다양한 인증을 획득하여 국내는 물론 해외에서도 널리 기술의 우수성을 인정받고 있다. 어울림정보기술의 SECUREWORKS는 국내 주요 공공기관, 금융기관 뿐 아니라 일반 기업 대형 포털 사이트에 이르기까지 수많은 기관에 설치되어 안전한 네트워크 환경을 지켜주고 있다.

국내 최고 수준의 자체기술로 개발한 SECUREWORKS 시리즈로 기존의 네트워크 보안제품인 방화벽, 침입방지시스템 (IPSWall), 가상사설망(VPN)을 위주로 사업을 펼쳐온 것에서 더 나아가 통합보안관리(ESM), 패치관리솔루션(PMS)과 통합보안서비스를 전략 사업으로 중점 육성하고 있다. 이를 위해 관련 부분의 투자를 확대하고 대대적으로 사업을 강화하여 통합보안관리를 제공하는 종합 정보보안 솔루션 전문업체로의 기반을 마련하였고, 최근에는 M&A 등의 공격적인 사업다각화 전략으로 뜨거운 관심을 받으며 새롭게 도약하고 있다.

www.oulim.co.kr / Tel. 02-2142-0500

기업 정보보호 위한 최적 통합보안솔루션, 현대HDS[워치가드] Firebox X

현대HDS[워치가드]의 'Firebox X' 시리즈는 통합된 단일 장비에 네트워크 규모 확장에 따라 성능 및 기능 향상을 라이선스 키만으로 간편하게 업그레이드 할 수 있도록 설계된 확장형 플랫폼 기반의 통합보안솔루션이다.

'Firebox X' 시리즈는 바이러스월, QoS, 방화벽, VPN, SSL VPN, IPS, 애플리케이션 보안, 스팸차단, 웹 컨텐츠 필터링, 취약점분석 및 인증기능을 지능 계층형 보안 아키텍처 내에 하나로 통합한 보안 어플라이언스로 고객의 보안요구에 따른 확장을 지원하도록 설계된 능동형 보안시스템이다.

이런 UTM 솔루션은 1997년부터 최초로 전용보안 OS를 기반으로 시작하여 2000년 통합보안 제품으로서 면모를 준비하고 있었다. 2006년부터 본격적으로 버전 업그레이드에 나서 전용 OS인 파이어웨어 9.0으로 명실공히 준비된 UTM으로 거듭나고 있다.

현대HDS[워치가드]의 'Firebox X' 시리즈는 통합된 단일 장비에 네트워크 규모 확장에 따라 성능 및 기능 향상을 라이선스 키만으로 간편하게 업그레이드 할 수 있도록 설계된 확장형 플랫폼 기반의 통합보안솔루션

기업 정보보호를 위한 최적 통합보안솔루션

Peak 'Firebox X Peak'는 워치가드의 통합위협관리 장비 중 가장 성능이 뛰어난 제품으로서 제로데이 방어기능을 제공하며 초당 멀티 기가비트의 방화벽 성능을 발휘한다. 고급 네트워크 기능과 강력한 보안성능을 통합한 'Firebox X Peak'는 엔터프라이즈 네트워크 환경의 요건마저 충족시킬 수 있는 탁월한 통합보안솔루션이다.

멀티 기가비트 방화벽과 최대 600Mbps VPN 성능을 제공하는 'Firebox X Peak'는 워치가드의 제품 라인에 있는 다른 UTM 솔루션보다 뛰어난 최고의

성능을 발휘한다. 'Firebox X Peak'는 기가비트 WAN 연결뿐만 아니라 고속의 LAN 백본 인프라를 지원하기 위해 전 모델에서 8개의 10/100/1000 기가비트 이더넷 포트를 갖추고 있다. 또한 포트 활용도를 극대화하기 위해 트러스트, 익스터널 또는 DMZ 등의 다양한 방식으로 8개의 포트를 자유롭게 구성할 수 있다.

'Firebox X Peak'의 고급 네트워킹 기능은 지능적으로 자원을 관리하고 트래픽을 최적화하며 네트워크 가동시간을 늘려준다. VLAN 기능은 하드웨어 추가 구입을 줄여주고 뛰어난 상호 운용성을 보장한다. 멀티 WAN 로드 밸런싱, 고가용성, WAN/VPN 페일오버를 통해 성능 및 안정성을 향상하였다. 동적 라우팅 및 트래픽 쉐이핑을 통해 네트워크 유연성 및 효율성 극대화하였고 정책 기반 라우팅으로 서비스별로 전송 인터페이스를 지정하여 대역폭 관리가 가능하다.

Core 'Firebox X Core' 통합위협관리 솔루션은 각 보안계층마다 완벽한 보안서비스를 제공하여 프록시 기반의 철저한 애플리케이션 프로토콜 검사 방화벽, VPN, 제로데이 공격방지, 스파이웨어 방지, 스팸 방지, 바이러스 방지, 침입방지 및 URL 필터링 등 다양한 보안서비스들을 단일 플랫폼에 통합함으로써 운영 및 관리에 소요되는 시간과 비용을 줄여주고 복합적인 네트워크 공격으로부터 완벽한 제로데이 프로텍션 기능을 제공한다.

'Firebox X Core'에는 사전 차단 방식의 방어기능이 내장되어 있어서 소프트웨어 보안취약성으로 인한 새로운 유형의 네트워크 공격으로부터 안전하게 보호한다. 제로데이 방어기능은 정교한 프록시 기술을 기반으로 새로운 위협을 즉시 식별하여 차단한다.

각각의 워치가드 보안서비스는 보안성능의 탁월한 조합을 위해 'Firebox X Core'의 내장형 제로데이 공격방지 기능과 원활하게 작동한다. 게이트웨이 AV/IPS는 강력한 서명기반 보호기능을 통해 스파이웨어, 트로이 목마, 바이러스 및 웹 기반 공격을 차단하고 스팸블록은 업계 최고의 스팸 차단 서비스로서 원치않는 이메일을 최대 97%까지 실시간으로 차단한다. 웹블록은 악성 웹 콘텐츠로의 접근을 차단하고 사용자의 웹 서핑을 관리함으로써 직원들의 생산성을 늘리고 보안위험을 최소화한다.

솔루션명 : Firebox X시리즈
특징/장점 : 프록시 기반의 애플리케이션 레벨의 프로토콜로 강력한 제로데이 프로텍션 방어기능
탑재된 모든 보안계층들이 서로 트래픽 관련 정보 공유
여러 가지 기법이 혼합된 해커의 공격에도 높은 수준의 보안서비스 제공

제로데이 공격을 완전히 차단하고 복잡한 네트워크를 위한 고급 보안 및 네트워크 운영 시스템인 'Firebox X' 시리즈는 '파이어웨어 프로'를 운영시스템으로 사용

www.hyundaihds.co.kr

Edge 'Firebox X Edge' 보안장비는 소규모 업체 및 원격/지점 사무실을 위한 강력한 네트워크 보안을 제공한다. 단일 통합형 보안장비 또는 VPN 엔드포인트 솔루션으로써 사용되는 'Firebox X Edge'는 상태관리 방화벽, VPN, URL 필터링 및 고급 네트워킹 기능 및 대역폭 가용성을 최대화하기 위해 트래픽 관리 기능을 제공한다. 직관적인 웹 기반의 사용자 인터페이스는 빠르고 간편한 컨피그 설정을 제공하는 반면 워치가드 시스템 관리자는 멀티 박스 환경을 위한 중앙 집중형 관리를 제공한다. 따라서 고객이 'Firebox X Edge'을 사이트별로 관리하던지 중앙 집중식으로 관리하던지 시간과 관리비용이 크게 줄어든다.

'Firebox X Edge'는 단순하고 간편한 직관형의 웹기반 인터페이스로 관리된다. 손쉬운 설치 및 간단한 사용법으로 인해 IT 전문가가 보안정책을 설정하는데 소요되는 시간을 줄여주면서 보안장비에 대해 경험이 많지 않은 관리자들도 쉽게 설치할 수 있다.

프록시 기반으로 강력한 제로데이 프로텍션 방어기능

현대HDS[워치가드] 'Firebox X'의 차별점은 프록시 기반의 애플리케이션 레벨의 프로토콜로 강력한 제로데이 프로텍션 방어기능이다. 타사의 일반 UTM 솔루션은 네트워크 프로토콜의 준수 여부를 체크하고 바로 시그니처 기반의 서비스로 유해 트래픽을 탐지한다. 시그니처 기반의 보안서비스는 잘 알려진 공격에 대해서는 잘 막아내는 반면 알려지지 않은 새로운 공격에 대해서는 대부분 막아내지 못하는 단점이 있다. 실제로 대부분의 새로운 공격기법들은 기존의 공격기법들에서 조금씩 변형되어 제작된 공격기법들이다.

현존하는 수많은 공격기법들을 모두 이해하면 이를 몇 개의 그룹으로 나누는 것이 가능하기 때문에 이를 잘 활용하면 기존 시그니처 솔루션을 보완하여 모든 공격의 유형을 차단할 수 있는 보안시스템 개발이 가능하다. 알려지지 않은 새로운 공격에 대한 제로데이 프로텍션 기능을 구현하기 위해서는 HTTP, FTP, DNS, SMTP와 같은 애플리케이션 프로토콜에 대한 철저한 검사가 필요하다. 그 이유는 많은 보안공격들이 애플리케이션 레벨의 프로토콜을 변조하여 내부 네트워크로 침입하기 때문이다. 워치가드는 네트워크 프로토콜 준수여부를 확인할 뿐만 아니라 애플리케이션 프로토콜 준수여부를 시그니처 기반의 서비스 앞단에서 한번 더 확인하고 탑재된 모든 보안계층들이 서로 트래픽 관련 정보를 공유하며 유기적으로 동작하므로 여러 가지 기법이 혼합된 해커의 공격에도 높은 수준의 보안서비스를 제공한다.

확장형 플랫폼 기반 통합보안시스템

'Firebox X' 시리즈는 기업의 정보보호를 위한 최적의 통합보안솔루션으로 기

업의 네트워크 규모 확장에 따른 성능 및 기능 향상 요구를 라이선스 키만으로 간편하게 업그레이드할 수 있도록 설계된 확장형 플랫폼 기반 통합보안시스템이다.

'파이어웨어 프로'의 지능형 계층 보안(ILS)으로 제로데이 공격을 완전히 차단하고 복잡한 네트워크를 위한 고급 보안 및 네트워크 운영 시스템인 'Firebox X' 시리즈는 '파이어웨어 프로'를 운영시스템으로 사용한다.

스테이트풀 패킷 방화벽, VPN, 지능형 계층 보안, 게이트웨이 안티바이러스, 침입방지 서비스, 스팸차단과 웹 컨텐츠 필터링을 단일 시스템으로 통합하여 포괄적인 통합보안을 수행하기 때문에 멀티 포인트 솔루션에 비해 시간과 비용이 크게 절약된다.

현대HDS[워치가드]

현대HDS[워치가드](이종혁 대표)는 미국 워싱턴주 시애틀에 위치하였으며 1996년에 설립된 회사이다. 소프트웨어 기반의 보안솔루션이 주도할 당시 최초로 네트워크 보안장비를 출시한 선도기업이다. Deep Application Inspection 개념을 네트워크 보안시장에서 최초로 선보인 회사이며 출시하고 있는 모든 제품 모델에 UTM 기능을 탑재한 UTM 전문기업이다. 현재까지 35만 개의 장비를 판매하였으며 전 세계 150여 개 국 고객들에게 네트워크 보안장비를 판매하고 있다. 2006년 인포네틱스 발표에 의하면 SMB를 위한 네트워크 보안장비 솔루션 업체에서 1위를 차지하였으며 특히 VPN 솔루션 업체로서 시장점유율 1위를 차지하였다. 워치가드의 목표는 중소규모 기업고객 뿐만 아니라 엔터프라이즈 영역에서까지 네트워크 통합보안 솔루션 1위 업체로서 확고한 위치를 자리매김하는 것이다. 최근 워치가드의 경영진이 새롭게 바뀌면서 해외 기술연구소 설립 및 기존 업무프로세스 개선 등 다양한 활동을 추진하고 있다. 가까운 시일내에 기존의 애플리케이션 레이어에서 유해 트래픽을 차단하는 프록시 기반의 통합보안솔루션을 한층 더 업그레이드 한 새로운 엔터프라이즈 제품군이 출시될 예정이다.

www.hyundaihds.co.kr / Tel. 02-724-0700

강력한 라우팅 엔진 장착, 주니퍼 네트웍스 SSG 시리즈

주니퍼 UTM 솔루션 'SSG 시리즈'는 방화벽과 IPSec VPN, IPS, AV, 스팸차단, 웹필터링 기능 포함한 UTM 보안기능 세트로 성능에 따라 SSG 5/ 20/ 140/520/ 550/550M으로 구성되었다. 또한 소규모부터 중견규모의 기업을 위한 제품이다.

비즈니스 환경이 점차 분산되면서 기업들은 보안과제에 직면하게 되었고, 이를 효과적으로 해결하기 위해 통합보안솔루션을 요구하고 있다. 'SSG 시리즈'를 통해 주니퍼는 가격 대비 성능을 높이는 등 분산된 엔터프라이즈 환경에서 보안시장 리더로서의 입지를 다시 한번 입증하고 보안에 대한 업계 표준지표를 세우는 것은 물론, 지사 방화벽시장에 광범위한 WAN 연결 옵션을 제공하고 있다.

'SSG 시리즈'를 통해 주니퍼는 가격 대비 성능을 높이는 등 분산된 엔터프라이즈 환경에서 보안시장 리더로서의 입지를 다시 한번 입증

새로운 유형의 맞춤형 보안장비

주니퍼네트웍스 'SSG(Secure Services Gateway) 시리즈'는 지역 사무소 및 지사 사이트 구축을 위해 고성능, 보안 및 LAN/WAN 접속기능을 제공하는 새로운 유형의 맞춤형 보안장비이다.

방화벽, IPSec VPN, IPS, 바이러스 차단(스파이웨어/애드웨어/피싱 차단 포함), 스팸 차단 및 웹 필터링을 포함한 포괄적인 UTM 보안기능 세트가 포함되어 있어 지사에서 수행되는 트랜잭션을 웜, 스파이웨어, 트로이 목마 및 악성코드로부터 보호할 수 있다.

이 제품을 통해 주니퍼는 원격지 직원 및 비즈니스 파트너, 브랜치 오피스 등에 안전하고 안정적인 네트워크를 제공하는 '브랜치 솔루션(Branch Solution)'에

주력하고 있다. 고성능 방화벽/VPN 플랫폼에 근거리통신망(LAN)과 광역통신망(WAN) 인터페이스를 통합함으로써 기업들에게 점점 그 필요성이 대두되고 있는 지사나 중간 규모 오피스에 맞는 브랜치 솔루션을 제공하게 되어 기업의 장비 구입에 있어 경제성을 높였다.

'SSG 시리즈'의 주요 특징

SSG 5 SSG 5는 160 Mbps의 Stateful 방화벽 트래픽과 40 Mbps의 IPSec VPN 처리성능을 제공하는 6개의 고정 폼 팩터 플랫폼 시리즈로 이루어져 있다. 각각 7개의 고속 이더넷 포트와 1개의 공장 구성된(Factory Configured) WAN I/O 옵션(ISDN BRI S/T 또는 V.92 또는 RS232 Serial/Aux)을 보유하고 있다. 802.11 a/b/g에 대한 지원 옵션은 단일 박스를 통해 완벽한 네트워크를 제공한다.

SSG 5는 기업, 서비스 사업자, 독립 사업부 등을 비롯해 비교적 직원 수가 적은 소규모 조직이지만, WAN 및 고속 내부 네트워크를 통해 전달되는 비즈니스 크리티컬 트래픽을 보호하기 위해 고급 보안 및 라우팅 기능을 필요로 하는 사이트에 가장 적합하다. 일반적으로 소기업, 분산 지사, 소매점 및 고정 재택근무자 환경에서 널리 사용되고 있다.

SSG 20 SSG 20은 160 Mbps의 Stateful 방화벽 트래픽과 40 Mbps의 IPSec VPN 처리성능을 제공하는 모듈식 보안 및 네트워킹 장비다. 5개의 온보드 10/100 인터페이스가 장착되어 있으며 추가 WAN 접속을 위해 ADSL2+, T1, E1, ISDN BRI S/T 및 V.92 연결 옵션을 지원하는 2개의 확장 슬롯을 비롯해 5개의 고속 이더넷 포트를 제공한다. 또한 SSG 5와 마찬가지로 802.11 a/b/g 연결 옵션을 지원하기 때문에 보안, 라우팅 및 무선 액세스 지점을 단일 장비에 통합할 수 있다.

SSG 140 SSG 140은 8개의 고속 이더넷 포트와 2개의 구리 Gb 포트를 갖춘 모듈식 제품으로서, 가장 저렴한 구리 Gb 플랫폼과 함께 저렴한 비용으로 최고의 인터페이스 밀도를 자랑하는 플랫폼이다. I/O 유연성 향상을 위해 SSG

솔루션명 : SSG 시리즈
특징/장점 : 각 모듈별 업계 최고의 전문적인 업체제품을 선정해 통합
성능이 입증된 Stateful 방화벽 및 IPSec VPN, IPS, 바이러스 차단, 스팸 차단기능
LAN/WAN 접속 옵션과 지원 프로토콜을 갖추고 있어 TOC 절감

주니퍼네트웍스 'SSG 시리즈'의 고객이 UTM 통합장비에 가지고 있는 각 모듈별 전문성 부족 부분에 대해 각 모듈별로 업계 최고의 전문적인 업체제품을 선정해 통합했다는 점

140은 T1, E1, ISDN BRI S/T 및 Serial 연결 옵션을 지원하는 4개의 WAN I/O 확장 슬롯을 가지고 있다.

SSG 140은 대기업, 서비스 사업자, 독립 사업부 등에서 사용된다. WAN 및 고속 LAN을 통해 전달되는 비즈니스 크리티컬 트래픽을 보호할 수 있는 고급 보안 및 라우팅 기능을 필요로 하는 중견 기업에서 가장 이상적이다.

SSG 520 SSG 520은 맞춤형 고성능 플랫폼을 통해 지역 사무실/지사 및 중기업에 첨단 보안 및 혁신적인 LAN/WAN 라우팅을 제공한다. 600Mbps의 방화벽(IMIX 트래픽) 및 300Mbps의 VPN 성능을 발휘하는 SSG 520은 내부 공격과 애플리케이션 수준 공격을 차단할 수 있기 때문에 기업들은 라우팅 및 보안장비를 통합하고 IT 비용을 절감할 수 있다.

SSG 550 SSG 550은 맞춤형 고성능 플랫폼으로 지역 사무실/지사 및 중기업에 첨단 보안 및 혁신적인 LAN/WAN 라우팅 성능을 제공한다. 1Gbps의 방화벽(IMIX 트래픽)과 500Mbps의 VPN 성능을 지원하는 SSG 550은 내부 공격 및 애플리케이션 수준의 공격도 차단할 수 있기 때문에 기업들은 라우팅 및 보안 장비를 하나로 통합하고 IT 비용을 절감할 수 있다.

전문적 업체제품 선정 통합

주니퍼네트웍스 'SSG 시리즈'의 차별점이라고 한다면 고객이 UTM 통합장비에 가지고 있는 각 모듈별 전문성 부족 부분에 대해 각 모듈별로 업계 최고의 전문적인 업체제품을 선정해 통합했다는 점이다. 시만텍의 안티스팸, 서프컨트롤의 웹필터링, 카스퍼스키의 안티바이러스, 넷스크린 방화벽, 주니퍼 라우터로 최상의 상태로 통합한 장비라고 할 수 있다.

보안에서는 성능이 입증된 Stateful 방화벽 및 IPSec VPN이 IPS, 바이러스 차단, 스팸 차단 및 웹 필터링 등을 포함한 동급 최강의 UTM 보안기능에 통합되어 있기 때문에 웜, 스파이웨어, 트로이 목마, 악성코드 및 기타 신종 공격으로부터 LAN 및 WAN 트래픽을 보호할 수 있다.

LAN/WAN 접속은 LAN/WAN 접속 옵션과 지원 프로토콜을 모두 갖추고 있기 때문에 TCO를 절감할 수 있다.

네트워크 세그먼트 분할 기능을 제공하기 때문에 관리자는 네트워크를 별도의 보안 도메인으로 분할하고 고유 보안정책을 구현함으로써 사용자 그룹에 따라 서로 다른 수준의 보안기능을 구축할 수 있다.

로컬 사이트에 단 몇 대의 SSG를 구축하든 아니면 세계 전역에 수천 대를 구축하든 관계없이 주니퍼네트웍스 프로페셔널 서비스를 유용하게 활용할 수 있다.

www.kr.juniper.net

간단한 랩 테스트에서 대규모 네트워크 구현에 이르기까지 주니퍼의 전문가들이 목표 규명, 구축 프로세스의 정의, 네트워크 설계의 개발/검증, 구축 시스템 관리 등 모든 단계에서 지원할 것이다.

독립형 네트워크 보호장비 구축

주니퍼네트웍스 'SSG 시리즈'는 Stateful 방화벽, IPSec VPN, IPS, 바이러스 차단, 스팸 차단 및 웹 필터링을 포함한 포괄적인 UTM 보안기능 세트가 포함되어 있어 독립형 네트워크 보호장비로 구축할 수 있다.

또한 강력한 라우팅 엔진을 장착하고 있기 때문에 기존 지사 라우터 또는 보안/라우팅 통합장비로서 구축해 IT 투자비용 및 운영경비를 줄일 수 있다.

주니퍼네트웍스 'SSG 시리즈'는 탁월한 보안기능을 토대로 고정 LAN 접속과 함께 WAN I/O 옵션을 제공함으로써 비용절감 및 한층 강력한 투자보호의 이점을 제공하는 확장형 I/O아키텍처다. 동급 최강의 보안 파트너의 지원을 바탕으로 모든 형태의 공격으로부터 네트워크를 보호하는 UTM 보안기능이 있다.

또한 관리자가 게스트, 무선 네트워크 및 지역 서버/데이터베이스를 구분해 보안정책을 구축함으로써 인증받지 않은 액세스를 차단하고 발생가능한 모든 공격을 억제할 수 있도록 보장하는 네트워크 세그먼트 분할 등을 비롯한 고급 보안기능이 있다. 고속 LAN을 비롯해 저속 WAN 접속을 보호하기 위해 필요한 성능을 제공하는 보안 전용 프로세싱 하드웨어 및 소프트웨어 플랫폼이다.

주니퍼네트웍스

주니퍼네트웍스(강익춘 지사장)는 높은 퍼포먼스 네트워킹을 지향하는 네트워크 업체로써 단일 네트워크 상에서 서비스와 애플리케이션 운용을 가속화 시킬 수 있는 신뢰성 있는 네트워크 환경 구축을 위해 높은 퍼포먼스 네트워킹 인프라를 제공하는데 주력하고 있다. 이러한 높은 퍼포먼스 네트워킹은 곧 고객에게 높은 퍼포먼스 비즈니스가 가능하게 하는 원동력이 되고 있다.

주니퍼의 높은 퍼포먼스 네트워킹이란 네트워크 성능을 통해 업무처리 속도를 향상시키고 업무의 보안을 위한 위협을 관리하며 비즈니스의 유연성을 위해 개방형 표준을 따르고 파트너십을 활성화 한다는 것이다. 주니퍼는 이렇게 비즈니스 환경 개선을 위해 올해 '위협 관리' '애플리케이션 성능향상' '접근 제어' 3대 캠페인을 벌이면서 높은 퍼포먼스 네트워킹을 가능하게 할 것이다.

또한 주니퍼네트웍스는 전 세계 정보교환의 경제성을 혁신하고 있다. 고객들은 주니퍼의 맞춤형 고성능 IP 플랫폼을 통해 여러 다양한 서비스와 애플리케이션을 지원하고 있다. 전 세계 서비스 사업자, 기업, 정부 기관, 연구 및 교육 기관들은 주니퍼네트웍스를 활용해 사용자, 서비스 및 애플리케이션의 특정 요구에 부합하는 네트워크를 구축하고 있다.

www.kr.juniper.net / Tel. 02-3483-3400

바이러스 · IPS에 오픈소스 엔진과 패턴 적용, 액텔라 isec UTM 시리즈

액텔라의 UTM 제품 라인업을 소개하면 다음과 같다.

isec X1100/isec X1600는 방화벽/VPN/WAN가속 기능을 사용하려는 고객을 위한 최소형 장비로 스위치가 내장되어 있으며, PC 대수가 5대 미만인 소규모 점포나 무인 PC가 있는 매장에 적합하다. isec X2100/isec X3100는 방화벽/VPN/WAN가속/IDP 기능을 사용하고자하는 SMB에 적합하다.

isec X6100는 방화벽/VPN/WAN가속/IDP/AV/AS 기능을 사용하고자 하면서 사내 100Mbps 이상의 대용량 네트워크 사용량을 가진 중규모 기업에 적합하다. isec X7100는 방화벽/VPN/WAN가속/IDP/AV/AS 기능을 사용하고자 하는 대규모 기업이나 이중화 구성이 필요한 센터용으로 적합하다.

'isec X3100'은 멀티 시큐리티 게이트웨이

isec X3100은 SMB를 위한 Cost-Effective 플랫폼의 멀티 시큐리티 게이트웨이이다.

보안성능 가속을 위한 하드웨어 가속기를 옵션으로 장착할 수 있으며 전원 공급 중단에도 네트워크 기능을 사용하도록 하는 하드웨어 Bypass 기능을 기본으로 탑재

isecOS V5.5 Security OS를 기반으로 전용 하드웨어 어플라이언스를 채용하였다. 또한 보안성능 가속을 위한 하드웨어 가속기를 옵션으로 장착할 수 있으며 전원 공급 중단에도 네트워크 기능을 사용하도록 하는 하드웨어 Bypass 기능을 기본으로 탑재하였다.

장비관리와 모니터링 및 보고서 기능은 웹 인터페이스를 통해 개별적으로도 가능하며 secuManager에 등록하여 ESM을 통해 원격으로도 가능하도록 ESM Agent가 기본적으로 제공된다.

isec X3100은 중소규모 기업을 위한 본지사간 VPN과 기본적인 방화벽 정책을 수립하고, 내부 사용자들에 대한 유해 웹사이트 차단과 P2P나 비업무 트래픽 사용을 억제시키고, 사내로 유입되는 공격과 바이러스 및 스팸 메일을 차단할 수 있는 매우 유용한 올인원 시큐리티 솔루션이다.

하드웨어 사양은 Pentium Mobile CEL 600MHz으로 6x10/100 Fast Ether net, 512M memory, 80G HDD, Bypass 1 pair이다.

소프트웨어 기능은 다음과 같다.

방화벽 기능은 L3~L7 Layer 패킷 필터링. P2P, 메신저 차단기능. Stateful Packet Inspection Pre-configured 보안정책, 사용자 · 네트워크별 차단기능. 패킷 사이즈, 시간대별 차단기능, 세션 최대 수 제한 기능이 있다.

콘텐츠 필터링은 URL 카테고리 customization, 카테고리별 Permission/Deny configuration, 속도저하가 없는 Non-Proxy 방식의 콘텐츠 필터링, 키워드 블로킹이 있다.

커널레벨 필터링 통한 고성능 URL 필터링

IP와 포트뿐만 아니라 애플리케이션 별 세션제어를 할 수 있는 L7 기반의 방화벽기능, 프록시 기반의 URL 필터링이 아닌 커널레벨 필터링을 통한 고성능 URL필터링 성능, WAN가속과 최적화를 통한 본 · 지사 업무 최적화를 지원할 수 있는 특허 기술인 AWOT(Actela's WAN Optimization Technology)를 통한 본 · 지사 성능의 최적화 지원가능, 프로토콜에 상관없이 확장이 가능한 범용 TCP 프록시 기반의 안티바이러스 기능, Basian 필터, Gray Listing, RBL 등의 핵심 필터링 기능을 탑재한 안티스팸 기능이다.

IPS 기능의 경우 Agentless NAC 기능을 Embedded시켜서 허용 · 차단 · 탐지 · 드롭뿐만 아니라 네트워크로부터의 격리를 통해 감염 PC의 내부 네트워크에 미치는 영향을 최소화할 수 있다. 트래픽 분석과 제어기능을 통한 비정상적인 네트워크 사용에 대한 사전 차단을 통해 네트워크 가용성을 최대한 보장할 수 있다. 이 외에 ESM이 자체적으로 개발되어져 있어서 다수의 UTM을 통합관리하고 운영하기 쉬운 점도 차별점이라고 할 수 있다.

타사 UTM 제품과의 경쟁력이라고 한다면 바이러스와 IPS 등에 오픈소스 엔진

솔루션명 : isec UTM시리즈
특징/장점 : 통합보안기능을 제공하며 전용 하드웨어를 채용해 안정성과 성능 향상
애플리케이션 계층에서의 보안기능 한층 강화
커널 기반의 패킷 처리기능과 VPN 패킷 가속화 기능을 통해 최상의 네트워크 성능 보장
AWOT 기반의 회선 다중화 및 가속화 기능 활용

WAN가속과 최적화를 통한 본·지사 업무 최적화를 지원할 수 있는 특허 기술인 AWOT를 통한 본·지사 성능의 최적화 지원가능

과 패턴을 최대한 기본적으로 활용하여 SMB를 위한 원가 부담을 최소화하였으면서도, 향후 상용 엔진을 선택적으로 추가 가능한 확장성을 유지하였다는 점이 경쟁력 요소이자 단점이기도 하다.

여기에 그동안 VPN 벤더로서의 노하우를 살린 본·지사간의 업무 속도 개선을 적용할 수 있는 장점을 UTM에서 함께 활용할 수 있다는 점도 타사에서는 볼 수 없는 경쟁력이다.

또한 자체적으로 패턴 업데이트와 관제서비스를 운영하고 있어 24시간 기술지원과 모니터링이 가능해서 판매 후 사후 관리능력에서도 서비스 경쟁력 우위를 가지고 있다.

액텔라 'isec UTM 시리즈'의 주 타깃시장은 SMB 마켓이다. 장비 도입비용이 비교적 저렴하고 보안정책의 수립과 적용을 자체적으로 하기 힘든 전산 인력이 부족한 기업을 대상으로 임대 및 관제를 통한 보안관제서비스 형태로 시장에 진입한다는 전략이다. 이미 보유하고 있는 VPN기업들에 대한 UTM으로의 Migration도 하나의 목표시장이기도 하다.

이 외에 ISP와 호스팅 및 보안관제 사업자들에 서비스용 장비를 공급하는 전략을 통해 장비의 단품 판매보다는 서비스형 공급사업을 강화할 예정이다.

'isec UTM 시리즈'의 주요 특징

All-in-One Security Box Solution VPN, 방화벽, IDS, IPS, 콘텐츠 필터, 안티스팸, 안티바이러스 기능 등의 통합 보안기능을 제공하며 전용 하드웨어와 Hardened Security OS를 채용해 안정성과 성능을 향상시켰다.

Enhanced 애플리케이션 보안솔루션 애플리케이션 계층에서의 보안기능이 한층 강화되어 안티바이러스, 안티스팸, 콘텐츠 필터 게이트웨이 기능 등 메일, 웹 등에 대한 애플리케이션 통합 보안기능들과 주기적인 패턴업데이트 서비스가 제공된다.

High Performance 보안 성능 커널 기반의 패킷 처리기능과 VPN 패킷 가속화 기능을 통해 최상의 네트워크 성능을 보장하며 보안전용 가속 하드웨어를 채용해 고성능의 보안기능을 제공한다.

WAN Acceleration & Optimization Solution AWOT(Actela's WAN Optimization Technology)기반의 회선 다중화 및 가속화 기능을 활용하여 기존의 WAN회선을 가속화해서 사용할 수 있는 기능과 본·지사간의 트래픽을 압축하고 우선순위에 따른 처리가 가능하도록 하는 트래픽 압축 기능과 TCP가속

www.actela.com

기능을 제공한다.

Tunnel/Device High availability 터널에 대한 자동 Failover와 로드 밸런싱 기능과 장비의 이중화 작업도 L4/L2 스위치를 활용한 Active/active 혹은 Active/Standby 구성이 가능하므로 고 가용성의 네트워크 인프라를 운영하는 기업에 적합하다.

24X7 시큐리티 센터 24시간 365일 운영되고 있는 보안관제 센터를 통해 장비의 기능 업그레이드 및 각종 보안 모듈의 패턴 자동 업데이트를 제공하며 콜센터를 통해 기술 지원 및 장애시 실시간 대응체제를 운영하고 있다.

엔터프라이즈 보안 메니저 – secuManger 다수의 isec UTM 장비들을 용이하게 관리해주는 secuManager를 활용하면 장비 구성관리, 네트워크 관리, 장애관리, 보안관리, 보안정책과 업그레이드 일괄 적용 및 각종 보고서 생성 등과 같은 종합적인 전사적 보안관리가 가능하다.

액텔라

액텔라(최일연 대표)는 1999년 11월 시그엔 시절의 정보보안 사업부로 출발했다. 2001년 isec 방화벽을 개발하기 시작하였고, 2002년부터 isec V4.0 VPN시리즈로 수많은 기업들의 VPN망 구축용으로 장비를 납품하기 시작하였다. 액텔라는 국내 ADSL VPN 역사의 산 증인이라 할 만큼 지금까지 수많은 기업에 안정적으로 VPN 네트워크를 구축해 왔으며 2005년 1월 이후 보안사업부만 따로 분사하여 현재의 액텔라라는 사명으로 바꾸고 UTM 개발을 2년간 진행한 결과 isec X시리즈인 V5.5 UTM을 개발완료하게 되었다.

연혁으로만 봐도 보안장비개발에만 약 7년 여의 경험과 노하우를 가지고 있는 보안전문개발회사인 액텔라는 보안장비 임대 관제서비스를 2년째 새로운 사업분야로 육성하고 있는 보안분야의 터주대감이다. 액텔라의 올해 목표는 시그엔 시절의 VPN시장의 리더 역할을 하였던 그 때의 명성을 다시 찾는 것이다. 현재에도 약 7000여 대 가량 전국에 설치되어서 운영 중인 isec 장비에 대한 신뢰도와 우수성은 이미 현대기아차, 현대오일뱅크, 쌍용자동차, 대우전자서비스, 경기버스조합 등 굴지의 대기업들을 통해 검증된 바 있다.

www.actela.com / Tel. 031-776-2070

세계 최초 UTM, 포티넷 FortiGate5000

2004년 시장조사기관인 IDC가 UTM을 정의하기 시작하면서 네트워크 보안업체들이 UTM 시장에 본격적으로 진입하기 시작했다. 하지만 포티넷은 2001년부터 UTM 컨셉으로 100% 솔루션 아키텍처를 디자인해왔다.

세계 최초, 현재 세계 시장점유율 1위

포티넷의 'FortiGate'는 세계최초의 UTM 이며 현재 세계 시장점유율 1위의 통합보안장비로 전용 ASIC을 탑재하여 뛰어난 성능을 자랑한다. 사실상의 UTM 표준을 제공하는 어플라이언스다. 20여 종류의 제품 라인업은 고객의 네트워크 사용량에 가장 적합한 장비를 선택 할 수 있도록 한다.

'FortiAnalyzer'는 FortiGate로부터 로그를 전송받아 리포트 작성, Data mining 작업을 통해 포렌식 수행, 사용자의 사용 콘텐츠들을 기록하고 감시한다. 부가기능으로 취약점 분석 엔진을 내장하고 있어 서버나 PC의 취약점 분석 보고를 통해 보안을 강화토록 한다.

'FortiManager'는 원격지에 떨어져 있는 다수의 FortiGate를 중앙에서 관리/모니터링할 수 있도록 돕는 어플라이언스다. 이를 통해 고객은 보안관제 시스템을 간단하게 구축할 수 있으며 원격 장비의 상태나 보안정책, 보안 위반 사항들을 실시간으로 검토할 수 있도록 한다. 아울러 대형 사이트의 FortiGate 장비들이나 FortiClient들에 대한 패턴이나 시그니처 업데이트 기능을 수행한다.

'FortiClient'는 개인 PC에 설치하여 UTM 기능(개인방화벽, IPS, VPN, 안티스팸, URL 필터링, 스파이웨어 차단 등)을 사용할 수 있도록 제공되는 소프트웨어

포티넷의 'FortiGate'는 세계 최초의 UTM 이며 현재 세계 시장점유율 1위의 통합보안장비로 전용 ASIC을 탑재하여 뛰어난 성능을 자랑

이다. 자체 바이러스 탐지 엔진을 기본으로 포함하고 있으며 VB 100% 인증을 받았다.

'FortiMail' 은 FortiGate에 기존 탑재되어 있는 스팸메일/바이러스 메일 차단 기능을 더욱 정교하고 치밀하게 업그레이드 한 어플라이언스이다. 탐지/차단율은 세계 최고를 자랑하며 2byte 언어도 완벽하게 지원한다.

'FortiGate 5000' 의 주요 특징

자체 기술력으로 개발한 AV, IPS, 웹 필터링, 콘텐츠 프로세싱 ASIC, ATCA 기반의 보안솔루션을 제공하는 등 광범위한 기술 플랫폼을 가진 UTM 솔루션이다. 포티게이트는 콘텐츠 검사 및 처리 성능 향상과 동시에 50% 이상의 방화벽 쓰루풋을 제공하며 안티바이러스, 방화벽, VPN, IPS, 안티스팸, 웹 필터링 및 트래픽 쉐이핑 등과 같은 통합된 8가지 필수 보안 애플리케이션 및 서비스를 통해 포괄적인 네트워크 및 콘텐츠 보호를 제공한다.

특히 포티가드 배포 서비스를 통해 포티게이트 전 시스템에 업데이트된 바이러스, 웜, 트로이목마를 비롯한 보안위협에 대한 데이터베이스를 전 세계에서 24시간 포티게이트 플랫폼으로 자동전송 받을 수 있다.

다양한 제품라인과 범세계적인 기술지원 채널 고객의 규모에 맞는 다양한 성능의 제품군을 제공하고 통합관리/분석을 할 수 있는 어플라이언스까지도 제공한다. 전 세계적인 기술지원조직과 영업조직을 구축했다.

광범위한 보안 분석/지원/서비스 조직 세계 7개 국에 100명의 보안 분석/지원/서비스 조직 구축으로 24시간 보안 업데이트 및 기술지원을 한다.

콘텐츠를 전문으로 분석하기 위한 ASIC 탑재

패킷처리 및 세션 유지를 전문적으로 수행하기 위한 NPU 탑재

24 X 7 보안 업데이트 및 기술지원 (FortiGuard & FortiCare service)

솔루션명 : FortiGate 5000
특징/장점 : 보안기반 ATAC 플랫폼
확장성(최대 112Gbps 인터페이스)이 가장 뛰어난 다기능 보안 플랫폼
사용자가 원하는 대로 보안 네트워크 구성이 가능한 구조
ASIC 가속기능을 제공하는 다기능 보안장비
스테이트풀 방화벽, 바이러스/웜 차단, 스파이웨어 차단, P2P 트래픽 제어, 침입탐지 및 차단, VPN, 스팸차단, 웹 콘텐츠 차단, 대역폭 조절기능(QoS) 등을 통합적으로 제공

자체 기술력으로 개발한 AV, IPS, 웹 필터링, 콘텐츠 프로세싱 ASIC, ATCA 기반의 보안솔루션을 제공하는 등 광범위한 기술 플랫폼을 가진 UTM 솔루션

고객의 네트워크 규모에 꼭 맞는 다양한 규모의 제품 라인업

자체 개발한 보안기능(방화벽, IPS, AV, AS, 웹 필터링, VPN, P2P, QoS) 탑재

Push/Pull 패턴 업데이트 기능

하이엔드 시장 타깃, 성능 · 유연성 · 보안성 강화

'FortiGate 5000'은 하이엔드 시장을 타깃으로 성능, 유연성, 보안성 등을 강화한 것으로 기존의 방화벽, VPN, IPS 등을 자체 제공하거나 이런 기능을 지원하는 장비와 연동해 실시간으로 바이러스 방역, 스파이웨어 차단, P2P 트래픽 차단 및 제어, 스팸메일 차단, 유해사이트 차단 기능을 제공한다.

대표적인 레퍼런스로는 경남도청, 울산케이블방송을 비롯해 아산병원, 을지병원, 피자헛, 현대상선, 온미디어, SK C&C 등 중소기업에서 대기업에 이르기까지 다양한 산업별 고객을 확보하고 있다.

네트워크 보안 시스템업체이자 UTM 마켓리더로 알려진 포티넷코리아는 2007년 포티게이트의 차별화된 기능과 성능으로 경쟁우위를 점하며, 중소기업 시장을 넘어 엔터프라이즈 시장까지 선점할 계획이다.

포티게이트 시리즈는 무엇보다 IPS, 안티바이러스, IPSec/SSL VPN, 방화벽, 콘텐츠 필터링을 포함한 8가지 보안기능을 ASIC화 했다는 것이 강점이다.

제품 설계 때부터 통합보안을 목적으로 했기 때문에 각각의 기능으로 완성된 제품을 통합한 제품들보다 성능에서 뛰어나다.

또한 기존의 방화벽 · VPN · IPS 등과 연동, 실시간으로 바이러스 방역, 스파이웨어 차단, P2P 트래픽 차단 및 제어, 스팸메일차단, 유해사이트 차단기능을 제공한다. 그리고 간단한 설정 변경을 통해 전체 네트워크 보호서비스를 위한 설치가 가능하다. 그뿐만 아니라 중단없는 서비스를 가능하게 하고 대용량, 신뢰성과 제품의 손쉬운 관리기능도 장점이다.

www.fortinet.co.kr

딥 패킷 인스펙션의 한계 극복한 '컴플릿 콘텐츠 인스펙션(CCI)' 기술

'FortiGate 5000'의 가장 큰 특징은 IPS 장비들이 채택하고 있는 딥 패킷 인스펙션의 한계를 극복한 컴플릿 콘텐츠 인스펙션(CCI) 기술이다. 모든 포티게이트 제품군은 이 기술을 통해 기존 IPS 장비들이 놓치는 웜 · 바이러스 · 스파이웨어 뿐만 아니라 압축된 공격 프로그램들까지도 콘텐츠 분석에 근거해 차단한다. 따라서 웜 · 바이러스 · 스파이웨어 등의 공격 프로그램을 압축파일 이름이나 확장자 등을 이용해 차단하는 타 업체들의 보안장비들과는 차원이 다른 보안레벨을

통합적으로 제공한다.

초기에 포티넷은 SMB 시장의 보안전담 인원 및 예산의 부족이란 문제점을 해결하기 위해 통합보안의 특장점과 KT비즈메카의 시큐어넷이나 데이콤의 시큐어박스와 같은 임대 서비스를 통해 SMB 시장에서 괄목한 만한 성장을 거두는 등 성공적으로 시장에 안착했다.

올해 포티넷은 이러한 SMB 시장에서의 성과를 바탕으로 엔터프라이즈 시장 진출을 꾀한다는 계획이다. 이미 포티넷은 통신사업자, MSSP, 대기업을 위한 ACTA 준수 시스템인 포티게이트5000 시리즈를 위한 새로운 로드밸런싱 스위치 및 고성능 보안 블레이드를 보강함으로써 하이엔드 솔루션 포트폴리오를 구축했으며, 속속 대형 레퍼런스를 확보하고 있다.

포티넷

포티넷(이상준 지사장)은 2000년 넷스크린(현재 주니퍼회사에 35억 달러로 매각됨)의 CEO 겸 창립자인 Ken Xie에 의해 설립되었으며, 네트워크 보안과 안전에 경험이 많은 관리팀에 의해 관리되고 있다. 포티넷은 산업 주요 벤처 자본 기관들로부터 1억 달러 이상의 투자를 받음으로써 시장 주도형 비공개 네트워크 보안회사로서의 확고한 위치를 인정받았다. 본사는 미국 캘리포니아의 Sunnyvale에 위치하고 있으며, 고객의 성공을 꾸준히 보호하고 지키기 위해 북아메리카, 유럽 및 아시아 등에 지사를 두고 고객 지원 및 개발 판매를 하고 있다.

UTM 분야 전 세계 마켓쉐어 1위이며 콘텐츠 프로세싱 ASIC을 제공하는 유일한 회사이다. 총 900명의 직원 중 600여명이 개발인력으로 UTM 컨셉을 최초로 만들었고, 사실상 그 표준을 선도하는 기업이다. 포티넷의 목표는 전 세계 UTM 분야의 리더를 계속 유지하며 진정한 의미의 하이엔드 급 UTM 장비의 계속적인 공급이다.

www.fortinet.co.kr / Tel. 02-6007-2007

방화벽 시장점유 독보적, 시큐아이닷컴 리얼UTM SECUINXG U시리즈

시큐아이닷컴이 UTM 솔루션을 준비한 것은 2004년부터다. 하이엔드 시장용인 기가비트 급으로 UTM 제품을 준비해왔고 시장에 NXG 시리즈로 널리 알려져 있는 통합보안제품이 그것이다.

시큐아이닷컴의 NXG 시리즈는 이미 IDC자료를 통해 2005년 세계 UTM 시장 8위로 기록되고 세계시장에서 입증되었다.

NXG 시리즈, IDC에 세계 UTM 시장 8위 기록

시큐아이닷컴의 '리얼UTM SECUINXG U시리즈'는 SMB, 중견기업, 엔터프라이즈 별 라인업을 확보하고 이들 각각이 요구하는 다양한 포인트를 가지고 접근할 계획이다. 현재 기존 장비를 대체할 수 있는 지 여부가 필수 관건으로 예상된다. 이를 위해 신규 브랜드 아이덴티티를 수립, 기존에 보유하고 있는 NXG 기능을 재정비하여 전 라인업에서 UTM 기능을 가능케 함은 물론, 변화된 고객의 입맛에 맞추어 신규 라인업을 제시하고 있다. 또한 소프트웨어적인 업그레이드를 통해 유지보수 부담을 감소시키고 하드웨어적인 업그레이드를 통한 국제적인 경쟁력을 제공할 예정이다.

'리얼UTM SECUINXG U시리즈'는 신규 브랜드 아이덴티티를 수립, 기존에 보유하고 있는 NXG 기능을 재정비하여 전 라인업에서 UTM 기능을 가능케 함은 물론, 변화된 고객의입맛에 맞추어 신규 라인업을 제시

방화벽 시장에서 약 40% 시장점유율의 독보적인 위치를 차지하고 있고, 7년간 시장을 통해 검증된 솔루션을 공급해온 시큐아이닷컴은 기존 NXG에서 새로운 모습으로 업그레이드된 U시리즈를 시장에 공급할 예정이다. 예를 들어, 대기업 중심의 관문 네트워크는 인터넷과 관계사 등 외부망과 연계되어 트래픽량이 많고 보안이슈도 다양하여 성능적인 뒷받침이 필수적인 시장이라고 할 수 있다.

NXG 시리즈 독자적인 등급별 알고리즘 적용

시큐아이닷컴의 '리얼UTM SECUINXG U 시리즈'의 성능이나 제품특성을 이해하기 위해서는 'NXG 시리즈'를 아는 것이 수월하다.

'NXG 시리즈' 가운데 특히 NXG 2000은 하드웨어 일체형이다. 공공/금융기관이 보안에 필수적인 기가비트 방화벽에 대해 국가정보원 K4 인증을 업계 최초로 획득했다. 독자적인 등급별 알고리즘을 적용해 초고속 패킷처리를 했다. 美 Tolly Group 테스트에서 입증된 Rule과 세션 수에 관계없이 기가비트 N/W 성능을 유지한다. 세계 최초의 Active-Active High Availability로 안정성 향상 이중화와 동시에 로드 밸런싱으로 네트워크를 안정적이며 효과적으로 운영이 가능하다.

방화벽, VPN 기능이 효과적으로 결합된 통합네트워크 보안솔루션이며 분산된 보안 요구사항을 하나의 장비에서 구현 가능함으로 관리 및 운영이 용이하다. 암호 가속칩 탑재로 IPSec 통신의 고성능 처리보안이 가능하며 프로토콜의 성능 향상을 위한 전용 암호화 가속칩 탑재로 VPN 모듈 성능이 향상되었다.

또한 모든 패킷의 유입, 분류, 전송을 커널 레벨에서 처리하여 트래픽 병목현상을 최소화했다. 스테플 인스펙션의 확장으로 애플리케이션 영역까지의 정보검색 및 보안성이 보장되며 폴링 방식으로 변환하여 안정된 성능이 보장된다. 부하분산과 이중화를 동시에 지원하며 커널 레벨에서 세션 정보를 동기화하여 분산된 패킷의 세션유지 관리 및 장애 발생시 세션 유지가 가능하다. 다양한 이중화 구성으로 뛰어난 성능을 유지한다. 고가의 L4장비 없이 L2, L3 스위치만으로 로드 밸런싱을 구현한다.

서비스 프로토콜별 대역폭 제한을 통해 한정된 대역폭에 대해 효율적이다. 업무용 트래픽과 비업무용 트래픽을 구분하여 우선순위에 따른 대역폭을 할당했고 비업무용 트래픽의 대역폭 과다 점유 문제를 해결했다.

다양한 네트워크를 구성했는데 '라우팅 모드 HA'는 특정 인터페이스 장애 발생시, 해당 인터페이스의 가상 IP 주소를 정상동작중인 인터페이스가 사용한다. 'Bridge 모드 HA'는 네트워크 변경 및 별도 IP 설정없이 설치되어 라우팅 모드보다 뛰어난 성능을 유지한다.

솔루션명 : UTM SECUINXG U 시리즈
특징/장점 : 방화벽 기반의 통합보안
다양한 콘텐츠 기반의 보안 기능

리얼UTM SECUINXG U시리즈'의 주요 타깃 시장은 엔터프라이즈에서 지점망까지 전체 시장을 타깃으로 하며 제품은 성능에 따라 다양하게 개발할 계획

SecuiMSS 통합관제 서비스

시큐아이닷컴은 특히 실시간 전산시스템의 침해현황을 파악하고 위험요소에 신속히 대처하기 위해 'SecuiMSS 통합관제 서비스'를 실시하고 있다.

월 1회 자동화된 취약점 분석도구를 이용한 취약점 분석, 조치사항 권고, 분석결과 리포팅, 중요한 신규 취약점 발생시 해당 취약점 점검 및 리포팅, 반기 1회 대상 시스템 선정후 모의해킹 실시 및 결과 리포팅까지 관리한다.

또한 방화벽 로그 모니터링, 이상 로그 발생시 통보 및 조치사항 권고, 방화벽 룰 감사 및 정책권고를 한다. 물론 IDS 로그 모니터링도 하고 있다.

와이어 스피드의 엔터프라이즈급 성능 보장

시큐아이닷컴의 '리얼UTM SECUINXG U시리즈'는 엔터프라이즈급 하이엔드 시장을 주요 타깃으로 삼고 있다. 하이엔드급 시장은 성능의 우수성이 뒷받침되어야만 공략 가능한 시장이다. 이미 7년의 시장검증을 거치고 중추적인 보안장비인 방화벽을 공급해온 시큐아이닷컴이 엔터프라이즈 시장에서도 기존 네트워크 자원을 대체할 수 있는 UTM 솔루션을 제공할 것이다.

특히 대기업 등 미션 크리티컬한 업무를 처리하는 엔터프라이즈급 고객의 경우 기존 장비를 대체할 수 있도록 본원적인 네트워크 기능을 얼마나 충실히 제공할 수 있는가가 중요 선택기준이 되며, 보안 애플리케이션 기능은 그 이후의 주요 요소이다. 이를 위해서는 성능의 우수성이 필수적으로 뒷받침되어야 한다.

전체시장 타깃으로 다양한 개발

'리얼UTM SECUINXG U시리즈'는 와이어 스피드의 엔터프라이즈급 성능을 보장한 통합 보안장비다. 또한 다양한 콘텐츠 기반의 요구사항을 수용한 다기능형 복합 방어장비로 High Speed & Flexibility, Multi-Layered Single Point Protection 이다.

주요 타깃 시장은 엔터프라이즈에서 지점망까지 전체 시장을 타깃으로 하며 제품은 성능에 따라 다양하게 개발할 계획이다. 하지만 중점 타깃 시장은 SMB 시장으로 단일 장비로 보안할 예정이다.

- 엔터프라이즈 시장 (통신 시장) : 10기가급 장비
- SMB 시장 : secuinxg 400 ~ 2000 장비
- 지점, 영업소 등 : secuinxg 100, 200 장비

'리얼UTM SECUINXG U시리즈'의 주요 특징

방화벽 기반의 통합보안(UTM) 정책에 의한 트래픽 통과, 차단, 조절(Shaping)하는 역할이다. 다양한 트래픽의 정의와 구별이 가능케 하는 역할

www.secui.com

(Classification)이다. 유해트래픽 차단의 정책은 융통성있는 정책조합이 가능해야 하며 콘트롤이 가능해야 한다.
방화벽 기반 UTM의 주요 특징으로는 장비 자체를 스스로 보호할 수 있는 장치와 보안성 필요하며 다양한 네트워크 적용이 가능해야 한다. 예를 들어 라우팅, Bridge, VLAN, H-A 기능 등이다. 또한 멀티 기가급의 고성능 플랫폼이 가능해야 한다. 보안정책, 보안기능의 유연한 적용이 가능해야 하며 본사 · 지점 · 영업소 등의 각 사이트별로 최적화해서 활용이 가능해야 한다.

다양한 콘텐츠 기반의 보안기능 웹 애플리케이션 방화벽은 보다 안전한 웹 트래픽을 위하여, 검사/모니터링/은폐/방어를 실시한다. 안티바이러스 기능은 안티바이러스 엔진을 자체 내장하여 바이러스/웜 등을 차단 방어한다. 안티스팸 기능은 안티스팸 엔진을 자체 내장하여 불필요한 메일(스팸) 등을 차단 방어한다.
비정상트래픽의 공격 차단기능(IPS Behavior Based Detection - Scan/White List)은 트래픽 분석, WhiteList 기법을 통한 유해트래픽 차단 방어한다. QOS 기능(Session 및 트래픽 Shaping)은 각 서비스별 트래픽 제어를 통해 네트워크 QOS를 보장하며, Unknown Port 트래픽 감시를 통해 알려지지 않은 공격에 대비 방어한다.
Session/트래픽 폭주 탐지 및 차단 기능은 세션 제한으로 웜/DDOS 공격에 따른 피해 확산 방지한다.

시큐아이닷컴

시큐아이닷컴(김종선 대표)은 2000년 3월 삼성의 네트워크 전문 인력들이 모여 세계 1위를 지향하며 창립했다. 시큐아이닷컴은 초고속 네트워크 보안제품을 창립 3년만에 출시함으로써 그간 외산제품에게 내주었던 국내 기가비트 보안제품 시장을 탈환해 국내 정보보호업계 1위를 달성하기도 했다.
시큐아이닷컴의 목표는 UTM, 10기가급 개발 장비와 관리 및 스케닝 등의 소프트웨어 솔루션과 축적된 노하우를 기반으로 차별화된 진단 및 컨설팅 서비스 및 부수되는 유지보수는 물론 고객이 필요로 하는 보안의 모든 것을 공급하는 종합 보안회사로 부상하는 것이다. 이는 고객이 보안에 대한 모든 것을 의뢰한 후 보안에 대해 믿고 맡기며, 본연의 사업기회를 극대화 할 수 있도록 기업에게 비즈니스적인 여유를 제공하겠다는 것이다.
2007년은 정량적으로 500억 매출, 50억 영업이익을 목표로 하고 있으며 대한민국 정보보안 대표기업 이미지와 세계 UTM 시장 8위 기업을 넘어 2010년 글로벌 톱 10으로의 도약을 위해 매진하고자 계획하고 있다.
www.secui.com / Tel. 02-3783-6600

QoS기반의 통합보안, STN기술

STN UTM

처음 시장에 선보였던 UTM 장비들은 하나의 장비에 여러 가지 기능을 통합해 시스템의 성능저하 및 기존 네트워크 장비와의 호환에 많은 문제를 발생시켰다. 이로 인해 기존 기업들의 보안솔루션 구입에 적지않은 부담을 주었던 것이 사실이다.

하지만 전 세계 UTM 시장이 약 4년간 24억 달러 규모의 성장이 예상되며 국내 SMB 시장은 물론 IPTV 시장의 본격 개막을 앞두고 QoS 기반의 통합 보안장비는 기업의 이익 창출 및 고품질 서비스에 큰 기여를 할 것으로 기대된다.

이런 모든 조건들을 충족하기 위해 만든 장비가 STN기술의 'STN UTM 엔터프라이즈 솔루션'이다. 이 시스템은 기존의 UTM이 갖고 있는 통합기능에 STN기술이 독자개발한 QoS 엔진기반의 QTM&I 알고리즘을 적용한 애플리케이션 레이어 트래픽 컨트롤과 딥 패킷 인스펙션을 수행하는 네트워크 통합보안시스템이다.

'STN UTM 엔터프라이즈 솔루션'은 기존의 UTM이 갖고 있는 통합기능에 STN기술이 독자개발한 QoS 엔진기반의 QTM&I 알고리즘을 적용한 애플리케이션 레이어 트래픽 컨트롤과 딥 패킷 인스펙션을 수행하는 네트워크 통합보안시스템

독자 개발한 QoS 엔진 기반의 QTM&I 알고리즘 기반

'STN UTM'은 독자 개발한 QoS 엔진 기반의 QTM&I(Quality of service Traffic Managemetn & Intereption) 알고리즘을 기반으로 통합모듈 설계 전반에 적용하며, L3/L4/L7 패킷 필터링기능을 제공함으로써 각 모듈별 네트워크 보안관리 기능을 한층 더 강화, 네트워크 통합보안 기능을 제공한다.

QTM&I 알고리즘은 DB에 저장되어 있는 패턴 및 목록을 스트링 검색기반 구조에 의해 OSI7 계층에서 패턴매칭에 의한 패킷 분석 및 탐지가 이루어지며 패킷을 분류하고 필터링 하여 접근제어가 이루어진다.

'STN UTM'은 QTM&I 알고리즘 기반으로 QoS, 방화벽, VPN, Web-Secure, 안티바이러스 기능을 제공한다.

QoS는 프로토콜(HTTP, FTP, VoIP, eDonkey, 소리바다)을 IP 주소 또는 포트 번호에 상관없이 식별이 가능하며, 해당 패킷에 대한 세션을 지속적으로 추적하여 세션 전체에 대한 트래픽을 제어함으로써 트래픽 분석, 트래픽 차단, 대역폭 제한 및 보장, 패킷제어에 대한 우선순위 설정, 별도의 경로 설정 기능을 제공한다.

방화벽은 애플리케이션 레이어 패킷 필터링 구현으로 방화벽을 우회하는 침해성 접근을 차단한다. 또 Rate Limit는 source IP, destination IP, source Port, destination Port 별로 해시 테이블에 저장되어 라우트 계산을 하여 단위 시간(초)당 포워딩할 패킷을 제어함으로써 Dos/DDos공격, Flooding 공격 또는 내부 호스트의 웜 감염으로 인한 과다 트래픽 발생시 효과적으로 대응할 수 있다.

VPN은 IPSec과 Ether IP를 같이 사용함으로써 라우팅 처리를 할 수 있어 복잡한 네트워크 구조에 효과적이다.

이더넷 터널은 IP 데이터그램내에 이더넷 프레임을 Encapsulating하여 전송하며, 시스템 내부적으로 가상 이더넷 채널을 생성한다.

Web-Secure는 HTTP(80 port)와 HTTPS(443 port) 프로토콜 등 방화벽이나 침입탐지 시스템(IDS) 등 네트워크 장비로서는 탐지 및 해킹방지가 어려운 웹 트래픽에 대한 해킹을 차단해주며, 특정 포트의 네트워크 접근 제어/차단 및 위조/변조된 웹 프로토콜의 접근 제어/차단 기능을 제공한다.

안티바이러스는 오픈소스 기반의 안티바이러스 스캐너를 적용하고 있으며, 바이러스 패턴 DB는 6만 5000 바이러스 시그니처를 가지고 있으며, 정확하고 빠른 Live 업데이트를 지원하고 있다.

패턴매칭 통한 성능과 안전성 보장

'STN UTM'은 기존 통합보안 솔루션의 성능과 안전성이 떨어지는 문제점을 패턴매칭을 통해 극복함으로써 정밀한 탐지와 방어, 패킷 통신의 무결성 및 안전성을 높이고 고품질 서비스를 제공한다. 또 네트워크와 각각의 보안모듈이 하나로 통합돼 3단계 방어 시스템(1단계 : 감염차단, 2단계 : 감지 후 차단, 3단계 : 발생차단)으로 보안위협을 손쉽게 차단할 수 있다.

솔루션명 : STN UTM
특징/장점 : 한정된 인프라에서 중요업무와 서비스 대역폭 보장
전체 네트워크의 강력한 보안기능 구현
Web-Shield의 강력한 80 포트 제어기능
내부 접근제어 시스템의 새로운 패러다임인 NAC 개념 수용

'STN UTM'은 QoS에 기반해 방화벽, VPN, Web Contents, 안티바이러스 등 모듈식 구조로 구성되어 있어 효과적으로 트래픽 관리

1단계 '감염차단'은 내부로 흘러들어오는 바이러스를 정확한 시그니처를 통해 바이러스가 감염되기 전에 예방해 네트워크 성능보장과 오탐을 최소화한다.

2단계 '감지 후 차단'은 일시적인 내부 트래픽이 폭주했을 때 스케닝 탐지와 세션 제안 정책을 통해 공격 등에 대해 트래픽 통계 분석을 함으로써 정책을 세워 비정상 패킷을 차단한다.

3단계 '발생차단'은 클라이언트의 격리기능으로 발생하는 아웃바운드 이상 트래픽을 임계치 설정을 통해 비정상 트래픽을 발신지를 확인, 이상 징후에 따라 제어한다.

주요 타깃 시장으로 제1 및 2금융권(신규시장인 웹 방화벽 및 NAC 시장 공략)/ KT, 하나로통신, 온세통신, 데이콤(기존 방화벽 업그레이드 및 신규시장 진입)/ 대기업, 제조, 유통 (통합보안 솔루션 UTM 시장 진입)/ 시 · 군 · 구(웹 방화벽 시장 및 QoS 시장 진입)/ 4년제 및 2년제 대학(QoS 시장 진입 및 웹 방화벽 시장진출)/ 시 · 도 교육청 및 초 · 중 · 고 학내망 (방화벽 및 QoS 시장 진출)

'STN UTM'의 주요 특징

'STN UTM'은 QoS에 기반해 방화벽, VPN, Web Contents, 안티바이러스 등 모듈식 구조로 구성되어 있어 효과적으로 트래픽 관리를 할 수 있으며, 애플리케이션 계층의 패턴을 식별하여 패킷에 대한 세션을 지속적으로 추적함으로써 세션 전체에 대한 트래픽 차단, 트래픽 분석, 대역폭 제한, 우선순위 처리, 별도 경로 설정 등의 동작이 가능하다.

한정된 인프라에서 중요업무와 서비스 대역폭을 보장하며 전체 네트워크의 강력한 보안기능을 구현한다. 또한 웹 쉐일드의 강력한 80포트 제어기능과 내부 접근제어 시스템의 새로운 패러다임인 NAC 개념을 수용했다. 이로 인해 네트워크 상에 존재하는 모든 위협요소에 대한 감사 및 격리 차단정책의 일원화를 지원한다.

'STN UTM'은 보안기능과 패킷 콘트롤 기능 전반에 대한 기능수행이 가능함으로 중복투자를 줄여준다. QoS, 웹 애플리케이션 보안, 안티바이러스, 방화벽/VPN, 유해사이트 차단에 대한 강력한 통제기능들의 유기적 결합이 가능하다. 또한 강력한 패킷 컨트롤 기능으로 무결한 네트워크 환경을 구축할 수 있다.

STN UTM QoS는 한정된 인프라에서 중요업무와 서비스 보장 및 보안솔루션 연동이 가능한 네트워크 품질 최적화 솔루션이다. 전체 대역폭에서 절대적인 점유를 차지하는 P2P, 메신저 등의 트래픽에 대한 대역폭 제한 및 접근제어까지 동시에 수행하며 강력한 분석 모니터링 기능까지 제공한다.

또한 유연한 Class 기반제어, 합리적인 트래픽 관리, 7-Layer 기반 QoS, 1.5G Throughput, 포트 차단없이 특정 세션 선별제어 가능, WAN 대역폭에 대한 효

www.stntech.co.kr

율적인 관리성능 극대화, 내부 접근제어 및 DPI 방식 보안모듈 탑재 네트워크 보안향상, 내부 사용자의 불필요한 인터넷 사용제한 등이 있다.

STN UTM 방화벽/VPN은 애플리케이션 레이어 패킷 필터링 구현으로 방화벽을 우회하는 침해성 접근을 완전차단하고 고속처리 능력을 극대화하며 실시간으로 자동 필터링된다. 80 포트에 대한 정밀 제어차단이 가능하고 리미트 정책구현으로 내외부 공격성 접속을 원천 차단한다. STN UTM VPN은 IPSec, L2TP, Ether IP를 지원하며 다중 회선 로드 밸런싱과 회선간 Failover와 Dead Time이 1초 미만이다.

STN UTM WebSecure는 HPPT 게이트웨이에서 안티바이러스, 악성코드 차단, 사이트 및 URL 차단, 유해 사이트 차단, 피싱 사이트 차단, Transparent 모드 지원, 이벤트 발생시 관리자 경고화면 제공 및 메일을 발송한다.

STN기술

STN기술(윤재영 대표)은 웹 2.0과 다양한 정보보호기술 시대의 새로운 비전 그리고 전문화된 보안사업 아이템으로 지난해 1월 설립했다.

STN기술은 네트워크 통합보안 개발업체로 진정한 보안구현을 위한 고객의 편이를 목표로 하고 있다. 네트워크 통합보안 제품인 'STN-UTM'은 자체 개발한 QTM&I 엔진을 바탕으로 데이터의 흐름을 빠르게 검색할 수 있으며 QoS, 방화벽, VPN, 바이러스 월, Web-Secure 등 다양한 보안기능을 지원한다.

또한 STN기술은 부단한 연구개발을 통하여 정보보안 기술을 주도하고 세계시장을 선도하는 네트워크 통합보안 전문기업으로 성장하고자 최선을 다하고 있다.

동시에 고객과 최고의 IT파트너로서 고객의 비즈니스 환경을 철저히 분석하여 고객이 필요로 하는 정보보안 기술에 관한 기획 및 전략 수립을 통해 최적의 업무 프로세스를 제안함으로써 성공 비즈니스를 위한 전략을 제시할 것이다.

www.stntech.co.kr / Tel. 02-412-7194

시스코 적응형 보안 어플라이언스, 시스코 ASA 5500 시리즈

시스코는 자가방어 네트워크(SDN) 구현을 위한 핵심 구성요소로 방화벽, 침입방지시스템(IPS), VPN 등 다양한 보안기술을 한데 결집시킨 통합보안솔루션을 다양한 형태로 선보이고 있다. 실제로 시스코는 하드웨어 일체형의 'ASA 5500 시리즈'와 ISR 보안번들인 'ISR SEC/HSEC 시리즈' 그리고 카탈리스트 6500 서비스 모듈형태로 통합보안솔루션을 공급함으로써 고객들의 다양한 요구에 부응하고 있다.

네트워크 보안 보장

2005년 5월에 발표한 시스코 'ASA 5500 시리즈'는 고성능 방화벽, IPS, 안티엑스(Anti-X), IPsec/SSL(IP Security/Secure Sockets Layer) VPN 기술을 하나의 통합보안솔루션 장비로 구현, 고객들의 비용 및 관리 부담은 줄여 주면서 동시에 네트워크 보안을 보장해 준다. 즉, 고객들은 방화벽 투자비용 정도로 다양한 보안서비스를 제공 받을 수 있을 뿐 아니라 보안성능도 크게 개선할 수 있다. 특히 시스코 'ASA 5500 시리즈'는 서로 다른 기업의 네트워크 환경에 맞게 적절한 통합보안서비스를 제공할 수 있는 것이 큰 장점이다. 일례의 중소기업들의 경우 시스코 'ASA 5500 시리즈' 비즈니스 에디션을 사용하여 업계 최고의 방화벽, VPN, 선택적 안티엑스 기능 등을 결합한 포괄적인 기업 보안시스템을 완비할 수 있다. 이밖에도 'ASA 5500 시리즈'는 지능형 위협 방어 기술을 기반으로 새로운 위협에도 고객의 귀중한 데이터와 자산을 보호

해 주며 IPSec VPN과 SSL VPN을 동시에 지원해 주기도 한다.

시스코 'ASA 5500 시리즈'의 주요 특징

시장에서 검증된 보안 및 VPN 기능 완벽한 기능의 고성능 방화벽, IPS (Intrusion Prevention System), 네트워크 바이러스 차단 및 IPSec/SSL (IP Security/Secure Sockets Layer) VPN 기술은 강력한 애플리케이션 보안, 사용자 및 애플리케이션기반 액세스 제어, 웜 및 바이러스 경감 및 악성코드 보호 기능, 원격 사용자/사이트 연결 등을 제공한다.

확장형 AIM (Adaptive Identification and Mitigation) 서비스 아키텍처 AIM은 모듈형 서비스 처리 및 정책 프레임워크를 활용하여 개별 트래픽 플로우 단위로 특정 보안 또는 네트워크 서비스를 적용하므로 체계적인 트래픽 처리를 통한 고도로 세분화된 정책제어 및 안티-X 보호가 가능하다. 사용자가 설치 가능한 SSM(Security Services Module)을 통한 소프트웨어 및 하드웨어 확장성과 시스코 'ASA 5500 시리즈' AIM 아키텍처의 효율성을 활용하면 기존의 서비스를 개선하여 발전시킬 수 있을 뿐만 아니라 플랫폼을 교체하거나 성능에 손상을 주지 않고 새로운 서비스를 배치할 수 있다. 시스코 'ASA 5500 시리즈'의 아키텍처 기반으로서 AIM을 사용하면 보안정책을 고도로 커스터마이즈하고 최상의 서비스 확장성을 제공한다.

시스코시스템즈 코리아

시스코시스템즈(손영진 대표)는 1984년 말에 스탠포드대학 전산과 출신 몇몇에 의해 설립되었다. 1986년 첫 제품을 선적한 이후, 시스코는 현재 참여하고 있는 네트워크 전반에 걸친 모든 영역에서 시장 점유율 1~ 2위를 차지하는 명실상부한 글로벌 시장 리더로 성장했다. 현재 시스코는 전 세계 75개 국, 225여 개의 사무소에 5만 4563명(2007년 5월 기준)의 직원을 고용하고 있는 세계적인 기업으로 성장했다.

시스코의 연간 매출액은 1990년 상장한 당시 6900만 달러에서 2006 회계연도에 284억 8000만 달러를 기록, 16년 만에 거의 410배 이상의 성장을 보였으며 2007 회계연도 역시 매 분기마다 높은 매출 성장세를 이어가고 있다. 시스코는 세계적인 네트워킹 솔루션 제공업체로 정보망을 구축하거나 다른 네트워크와의 연결에 사용되는 엔드-투-엔드(End-to-End) 네트워킹 솔루션부터 가정에서 사용되는 전자제품들 간의 네트워킹을 위한 솔루션까지 토털 네트워킹 솔루션을 공급하고 있다. 실제로 시스코는 정보망을 구축하거나 정보망 액세스에 필요한 광범위한 하드웨어 제품군과 네트워크 서비스를 모두 제공하며 네트워크화된 애플리케이션을 가능하게 해주는 시스코 IOS 소프트웨어가 있다.

www.cisco.com/kr / Tel. 02-3429-8000

IPS 기반의 통합보안솔루션, 한국쓰리콤

X-패밀리

한국쓰리콤이 최근 출시한 '쓰리콤 X-패밀리 통합보안 플랫폼(3Com X-Family Unified Security Platforms)'은 일반적인 UTM 제품과는 차별화되는데, 그것은 단순히 보안기능을 묶는 형태에서 벗어나 쓰리콤이 강점을 보유하고 있는 네트워크 기반 IPS에 VPN과 방화벽, 웹 컨텐츠 필터링, 트래픽 쉐이핑 기능을 긴밀하게 결합시킨 최초의 네트워크 통합보안 솔루션이기 때문이다.

IPS 분야를 선도해온 티핑포인트의 강력한 네트워크 보안기술 위에 기업들이 필요로 하는 핵심적인 보안 기능들을 통합해 차별화한 '쓰리콤 X-패밀리'는 보안 침해로 야기되는 기업 명성의 훼손이나 매출 손실을 일으키는 보안위협에 대해 이전에 볼 수 없었던 탁월한 보안대응 기능을 제공한다. 이 제품은 또한 비즈니스 연속성을 보장하고 시스템 중단을 방지하는 것과 함께 여러 보안장비의 도입에 따른 구축 및 관리 운영의 부담을 덜고, 상당한 비용 절감 효과까지 제공하는 것이 특징이다. 특히 '쓰리콤 X-패밀리 통합보안 플랫폼'은 트래픽 쉐이핑, 애플리케이션 우선순위 지정과 같은 최근의 시장 요구를 반영해 설계된 'X5'와 'X506' 제품군으로 구성되며, 대기업은 물론 대기업 수준의 강력한 보안기능을 필요로 하는 중소 및 중견기업에 특화된 관리 기능과 함께 경쟁력 있는 가격, 간편한 구축 및 운영 환경을 제공한다.

보안관리시스템과 연동, 중앙집중화 된 관리 환경 제공

쓰리콤의 'X-패밀리'는 최강의 IPS 기술 위에 기업들이 필요로

하는 핵심 보안기능을 긴밀하게 통합시킨 솔루션으로 네트워크 보안수준을 강력하게 업그레이드할 수 있게 해준다. 이를 통해 사용자들은 한층 안전한 통합 네트워크 보안환경을 갖추는 것은 물론, 통합 솔루션이 제공하는 구축과 운영, 관리의 이점과 비용 지출에 대한 부담 경감 등 다양한 효과를 만끽할 수 있다.

쓰리콤은 특히 X5와 X506으로 구성된 통합 보안솔루션과 함께 '보안관리시스템(SMS, Security Management System)'을 별도로 공급해 중앙집중화된 관리 운영기능을 제공한다.

쓰리콤의 SMS를 이용하면 관리자는 IPS와 방화벽의 사용 범위 지정, VPN 구축, 대역폭 관리 등을 간편하게 할 수 있으며, 본사나 중앙에서 콘텐츠 필터링과 작업 실행 환경의 설정 업무를 수행하면서 동시에 원격 지사나 본사와 떨어진 곳에서 근무하는 사용자를 위한 안전한 보안환경을 유지하도록 할 수 있다.

분산된 네트워크 환경에 이상적인 제품

'쓰리콤 X-패밀리'는 분산된 네트워크 환경에 이상적인 제품군으로 VoIP와 미션 크리티컬한 트래픽에 대한 QoS 요구를 충족시키며, 통합된 대역폭 관리 기능을 이용해 음성이나 비디오 트래픽에 대한 우선 수위를 부여할 수 있고, 동시에 필요없는 트래픽을 제압할 수 있다. 이 기능을 이용하면 최대치의 네트워크 자원을 필요로 하는 P2P 파일 공유 애플리케이션의 작동을 안전하게 제어할 수 있으며 불법적이거나 개인적인 목적으로 사용되는 네트워크의 흐름을 차단해 항

쓰리콤

한국쓰리콤(이수현 대표)은 쓰리콤의 한국지사이며, 쓰리콤은 인터넷 발전의 근간이 되는 이더넷을 발명한 로버트 멧카프(Robert Metcalfe) 박사가 1979년 설립한 정통 네트워크 기업이다. 쓰리콤의 3C는 컴퓨터(Computer), 커뮤니케이션(Communication), 호환(Compatibility)을 의미한다.

쓰리콤은 30년 전 업계 최초로 이더넷 네트워크 인터페이스 카드(NIC)를 출시했으며 이후 쓰리콤의 퍼베이시브 네트워크 비전은 세계의 인정을 받아왔다. 쓰리콤은 또한 모든 규모의 기업들을 위한 음성, 데이터, 보안을 통합한 네트워킹 솔루션을 공급하는 선도적인 시큐어 컨버지드 네트워크 솔루션 업체로도 높은 평가를 받고 있다.

쓰리콤은 세계적인 영업과 서비스, 지원과 함께 광범위하고도 혁신적인 제품들을 제공함으로써 고객을 위한 비즈니스 가치 극대화에 주력하고 있다. 쓰리콤은 교육기관, 정부기관, 금융기관 등을 위해 맞춤형 솔루션을 제공함으로써 고객에게 차별화된 선택의 기회를 제공한다.

2003년 11월 쓰리콤과 중국의 화웨이가 공동 출자해 설립한 '화웨이-쓰리콤(Huawei-3Com Co. Ltd)'은 쓰리콤의 라우팅 및 스위칭 제품군을 생산하여, 쓰리콤의 중대형 제품 라인을 확장시켜왔다.

www.3com.co.kr / Tel. 02-3455-6300

중소기업 인터넷 위협 다중보안 제공, 체크포인트 UTM-1

체크포인트 'UTM-1'은 중소기업이나 대기업의 지사 및 지점을 타깃으로 하는 제품이다. 스파이웨어, 바이러스, 네트워크 공격 같은 인터넷 위협들로부터 다중의 보안을 제공하는 통합보안솔루션이다.

보안기능, 하드웨어 어플라이언스에서 모두 구현 가능

체크포인트의 'UTM-1'은 모두 8가지의 Security Function들이 UTM-1이라는 하나의 하드웨어 어플라이언스에서 모두 구현 가능하다는 장점을 가지고 있다. 심지어 타사 UTM 솔루션에서는 많이 포함되어 있지 않은 웹 방화벽 기능까지 적용할 수 있어 웹을 이용한 취약성 공격이 날로 늘어나는 현 추세에서 능동적으로 대처가 가능하다.

또한 탑재된 모든 보안솔루션들은 하나의 통합관리 콘솔을 통해 설정, 모니터링, 리포팅, 업데이트 등의 손쉬운 관리가 이루어진다. 이는 솔루션별로 각각의 사용자 인터페이스를 가지고 있던 이전의 UTM 솔루션들과 차별화되는 점으로 '관리를 위한 관리'가 되는 것을 지양한다.

이 외에 장애처리나 트래픽 'Troubleshooting'에 있어서도 발 빠른 대처를 보일 수 있다는 장점이 있지만, 가장 중요한 장점은 이런 보안기능들이 상호 유기적으로 연동 및 보완되는 Correlation 알고리즘이 있다는 것이다.

각각의 보안기능에서 나오는 로그들은 체크포인트 스마트디펜스라는 관리 툴에 저장되고 Correlation 알고리즘이라는 상호연관관계에 의거 분석되어, 신속한 위험 경고 및 각각의 솔루

션에서 미처 발견되지 못한 부분을 감지해낼 수 있다.

한편 각각의 보안솔루션들은 체크포인트에서 개별로 출시되던 지능적이고 최첨단의 보안솔루션이 그대로 적용된 것으로써 가령 방화벽 부분에서 지원되는 애플리케이션 및 프로토콜이 수백 가지에 달한다. 개별 보안솔루션의 애플리케이션에 대한 이해능력 또한 뛰어나다고 할 수 있다. 그리고 VPN 은 CA서버기능이 UTM-1에 기본 포함되어 있어서 IPSec VPN이나 SSL VPN 구성 시 간편하고 시큐어한 VPN을 구성할 수 있다.

'UTM-1' 의 주 타깃은 450Mbps에서 2Gbps 급의 Middle Enterprise이다. 그러나 다음 달에 발표될 후속 모델(일명 M Series)은 4G이상 12Gbps급까지 커버가 가능하다. 대형 엔터프라이즈 및 서비스 프로바이더 데이터 센터까지 타깃이 확장될 예정이다.

'UTM-1' 의 주요 특징

- 수백 개의 애플리케이션과 프로토콜을 보호하는 업계에서 가장 검증된 방화벽
- 안전한 site-to-site 접속과 원격접근을 가능케 하는 강력한 IPSec VPN
- 별도의 하드웨어가 필요 없는 탄력적인 SSL 원격 접근
- FTP, HTTP, POP3, SMTP와 같은 중요 프로토콜에 대한 게이트웨이 안티바이러스
- 웹 어플리케이션 방화벽 및 게이트웨이 안티스파이웨어 보호

체크포인트

체크포인트 소프트웨어 테크놀로지(조현제 지사장)는 1993년 설립되어 전 세계 기업용 방화벽, 개인용 방화벽과 가상사설망(VPN) 시장 선두기업으로 널리 인정돼 왔으며 세계 88개 국, 2200여 기업과 협력관계를 맺고 솔루션과 서비스를 제공하고 있다.

체크포인트는 350개 이상의 각 분야 상위기업들이 제공하는 최고의 솔루션과 통합 및 상호 연동을 실현하는 프레임워크인 OPSEC(Open Platform for Security)을 통해 자사 솔루션의 능력을 더욱 확대하고 있으며, 1999년부터 4년 동안 그리고 2002년과 2004~2005년 가트너의 '방화벽 매직 쿼더런트' 에서 기업 방화벽 시장 리더로 선정, 여러 차례 IPSec VPN 시장 리더로도 선정된 바 있다. 또한 2005년 전 세계 방화벽 · VPN 소프트웨어 시장의 94%를 점유하고 있는 것으로 조사되었다.

한편 지난 2004년, 통합 보안 아키텍처를 바탕으로 경계 보안뿐만 아니라 내부 웹 보안과 엔드포인트 보안관리로 영역을 확장한 체크포인트는 2007년 들어 데이터 보안시장까지 포괄한 PURE(Protected Unified Reliable Extensible) 보안솔루션 제공에 박차를 가하고 있다.

www.checkpoint.com / Tel. 02-565-4222

사용자 인증기반, 모젠소프트 사이버롬 UTM

모젠소프트가 독점 계약한 사이버롬 UTM은 위협요소에 대해 즉각적인 탐지와 통합된 제어를 제공하며 사용자 인증에 기반을 두고 있다. 특히 전통적인 방화벽과 다르게 사이버롬의 사용자 인증기반 방화벽은 사용자를 확인하기 위해 IP주소를 요구하지 않기 때문에 IP주소 로그인에 상관없이 사용자의 접근을 제어해준다.

노철희 모젠소프트 대표는 "국내에서 유통되고 있는 다양한 보안제품들을 다뤄오면서 기술적이고 가격적인 한계점을 극복하기 위해 좀더 근본적인 방식으로 네트워크 보안에 접근하는 보안제품들을 수년간 모색해 온 결과"라고 밝혔다.

사이버롬 UTM의 주요 특징

강력한 통합보안은 물론 뛰어난 네트워크 관리 툴 제공 사이버롬은 강력한 네트워크 통합보안은 물론 세부적인 관리지원을 통해 최적의 네트워크 관리 환경을 제공한다.

고성능 대비 경제적인 비용 국내외 일반적인 UTM 장비들은 방화벽/IDS/AV/콘텐츠 필터링 등 각각의 기존 장비들을 더해 복합적인 UI(사용자 환경)를 구성하는 구조로써 전체적인 성능이 저하될 수 있다. 사이버롬 UTM은 연구개발 단계부터 통합보안을 위한 구조로 설계된 UTM 전문장비로써 해외 여러 국가의 공개적인 성능 테스트에서 이미 수차례 그 성능을 인증받았다.

사이버롬의 본사인 엘리트코어는 전 세계 IT 기업의 엔지니어들이 집결해 있는 인도에서 첫 번째 그리고 최고의 통신기업이며 대부분의 엔지니어들이 해외 석사학위를 보유한 우수인재들이다. 앞서가는 기술과 경쟁력 있는 가격은 사이버롬의 특징 가운데 하나이다.

편리한 관리자 환경(UI) 사이버롬 UTM은 관리자가 정책설정을 위해 각각의 기능별로 페이지를 이동해야 하는 타 UTM과 달리, 하나의 방화벽 화면 내에서 모든 기능의 정책구성 및 관리가 가능하다. 이를 통해 안티바이러스, 안티스팸, IDP, 웹과 애플리케이션 필터링, 대역폭 관리, 복합적인 링크관리 등에 대한 정책을 사용자에게 즉각적이며 효과적으로 적용시킬 수 있는 멀티 정책관리가 가능하다. 관리자에게 최적의 관리환경은 물론, 문제해결에서도 신속함과 편리함을 제공한다.

유동적인 IP환경에서 완벽한 보안 사이버롬의 사용자 인증기반 방화벽은 사용자를 확인하고 통제하기 위한 중간 요소로 IP 주소를 필요로 하지 않는다. IP 주소기반의 솔루션들과는 다른 방식으로 네트워크 내부에 정체불명의 사용자들을 확인하고 제거함으로써 IP 주소를 통해 사용자 인증이 될 수 없는 DHCP나 Wi-Fi 같은 유동적인 IP 환경에 완벽한 보안을 제공한다.

모젠소프트

모젠소프트(노철희 대표)는 우수 엔지니어들이 모여 설립한 기술과 고객을 중심으로 하는 기업 정보보호업체이다. 2005년 설립한 당시, 뛰어난 컨설턴트와 함께 국내 제품들을 취급해 오면서 1년 만에 130% 성장을 이루었다. 오랜 시간에 걸쳐 글로벌 우수제품들을 검토해 오면서 2006년 12월 인도시장 점유율 1위인 사이버롬(Cyberoam) UTM에 대한 국내시장 총판계약, 2007년 3월 Nevis 총판계약을 맺고 국내시장에 출시하였다.

5월 현재, 두 제품의 기술력과 우수 엔지니어들의 친절한 컨설팅을 바탕으로 전국적인 채널망과 우수 고객사를 확보한 상태이다. 향후 계획으로 2007년도는 사이버롬 UTM 사업을 함께 꾸려갈 소수의 우수한 채널망 구축을 확보하여 사업을 확장해 갈 것이며, 추진중인 자체 연구개발도 함께 진행하여 향후, 기업에게 보다 뛰어난 보안서비스를 제공하는 선두 기업으로의 도약을 위해 노력해갈 것이다.

www.mozensoft.com / Tel. 02-3409-3770

SMB 시장 대비, 넥스지 VForce UTM

넥스지 UTM 장비는 2007년에 출시될 예정이며 VPN, 방화벽, IPS 등이 통합된 형태다. NPU를 활용한 고성능 UTM 장비를 출시할 계획으로 개발에 매진하고 있는데 하이엔드 고객보다는 SMB 고객을 타깃으로 영업할 방침이라고 한다.

SMB 시장 대비 UTM 장비 출시 예정

출시 예정인 UTM 장비는 VPN은 물론, 방화벽, IPS 등이 통합된 형태이며 SMB 시장을 타깃으로 한 기가급 고성능 UTM 장비이다. 현재 대부분 UTM 장비는 하이엔드 고객을 대상으로 하는 장비로 넥스지는 SMB 시장을 대상으로 하는 기가급 UTM 장비 개발로 타 경쟁사와 차별화 할 계획이다. 주갑수 넥스지 사장은 "앞으로 사용자들의 인프라 환경이 FTTH로 이행될 것이고 이는 기존 보안장비로 업그레이드된 망을 지원하기 힘들다"며 "넥스지는 SMB용 기가급 UTM으로 저렴한 가격에 고품질의 장비, 서비스를 제공하는 보안업체로 자리 매김할 계획이다"고 밝혔다.

소프트웨어 방식처리 최대한 배제, 하드웨어 모듈 활용

넥스지 UTM 장비는 2005년 10월부터 개발을 진행했으며 현재 80% 정도 개발이 완료되었다. 넥스지의 UTM 신제품은 소프트웨어 방식처리를 최대한 배제하고, IPS/방화벽/VPN 등 각 기능에 최적화된 하드웨어 모듈을 활용함으로써 다양한 기능 활용에도 성능 저하가 발생하지 않도록 개발 진행 중이다. 또한 10 기가급 고성능 UTM 장비로 SMB 시장을 공략할 계획이다.

NexG

넥스지가 출시할 UTM 장비의 장점과 타사 제품과 비교한 차별성을 살펴보면 다음과 같다.

HW 기반의 고성능 인터넷의 속도가 점차 고속화됨에 따라 보안장비 역시 고속의 패킷 연산 필요성이 높아져 고속 패킷 연산을 위해 멀티 코어 기반의 네트워크 프로세서를 사용했다. 네트워크 프로세서는 패킷 연산, 암호화/복호화, 패턴 매칭, 압축 등 다양한 보안기능을 넣어 최대 16개의 코어를 지원하며 각 코어 당 개별 보안기능을 할당하여 사용한다.

VAAN 서비스를 통해 습득한 최적의 고객 만족 솔루션 수년간 고객에게 서비스를 제공하면서 요청받은 고객의 요구사항을 제품에 반영했다. 서비스를 통한 IPS의 패턴/스팸 튜닝 및 오탐을 최소화했다.

보안 컴포넌트간의 유기적 연동 각각의 보안 컴포넌트를 통합하는 수준이 아니라 이들 개별 보안 컴포넌트를 유기적으로 연동시킨다. 예를 들어 IPS가 비정상인 패킷을 탐지하면 이 IP주소를 방화벽 룰에 자동추가하거나, IPsec 패킷의 경우 데이터가 암호화되어 있어 유해여부를 판단할 수 없을 때 디코딩 후 IPS 엔진을 한 번 더 통과하여 공격을 탐지하는 기능을 말한다.

넥스지

넥스지(주갑수 대표)는 지난 2001년 설립되어 가상사설망(VPN) 솔루션과 통합보안관제서비스로 꾸준한 상승 가도를 달리며 주목 받고 있는 유망기업이다. 넥스지의 '인터넷 보안관제서비스(VAAN)'는 2001년 설립될 당시부터 지금까지 줄곧 유지되고 있는 주력 사업분야 중 하나로 현재 1500개 고객사에 서비스를 제공하고 있다. 넥스지는 상대적으로 많은 개발비용이 들지만 엔진부터 모든 솔루션을 자립기술 개발하고 있는 것을 경영모토로 하고 있다.

또한 장기적으로 하드웨어 기술개발과 원천기술 확보에 역점을 두고 있다. 넥스지는 매년 총 매출액 중 높은 비중을 연구개발(R&D)에 투자하고 있다. 현재 총 인원 70명 중 연구개발 인력이 20명으로 R&D부문에 집중하고 있으며 올해 연구인력 보강을 위해 인재를 물색 중에 있다. 사업 확대를 위해 보안 등 다양한 분야에서 새로운 아이템도 준비하고 있는 넥스지는 시장 상황에 휘둘리지 않는 탄탄한 사업기반을 다지기 위해 개발 분야는 기본적으로 투자에 제한을 두고 있지 않은 가운데 인력, 장비개발 등에 과감한 투자를 단행하고 있다.

www.nexg.net / Tel. 02-577-8426

Ⅲ. Comparison Chart

각 사별 UTM 솔루션 주요 기능 비교표

고성능 UTM 제품의 비교표는 각 회사들의 이용가능한 보안서비스와 네트워크 인터페이스 역량을 보여준다.

구성 \ 회사	퓨쳐시스템 FutureUTM	안철수연구소 트러스가드 UTM	어울림정보기술 SECUREWORKS	현대HDS [워치가드] Firebox X	주니퍼네트웍스 SSG 시리즈	액텔라 isec UTM	
이더넷 포트	O (8)	O(10/100/1000)	O(12)	O	O(10/100/1000)	O(4~6)	
안티바이러스 스캔용 최대 첨부 크기	16M	사용자 설정 가능	10M	·	사용자 설정 가능	메일첨부 100M, 웹 첨부 무제한	
안티바이러스 공급업체	안철수연구소 & 하우리 (예정)	안철수연구소	안철수연구소	Clam AV	카스퍼스키	Clam AV (상용엔진 추가 예정)	
방화벽	O	O	O	O	O	O	
가상사설망(VPN)	O	O	O	O	O	O	
침입탐지 시스템(IDS)	IPS 기능에 포함	X	O	O	O	O	
침입방지 시스템(IPS)	O	O	O	O	·	O	
트래픽 쉐이핑	O	O	O	O	·	O	
콘텐츠 필터링	O	O	O	O	O	O	
콘텐츠 필터링 공급업체	·	·	자체 개발	워치가드	서프컨트롤	자체 개발	
웹 필터링	O	O	O	O	O	O	
스팸 필터링	X	O	O	O	O	O	

	포티넷 FortiGate 5000	시큐아이닷컴 리얼UTM SECUINXG U	STN 기술 STN UTM	시스코시스템즈 ASA 5500	한국쓰리콤 X-패밀리	체크포인트 UTM-1	모젠소프트 사이버롬 UTM	넥스지 VForce UTM
	O(4~80)	O	O(10/100/ 1000)	O	O	O(8)	O(8)	O(8)
	547M	·	512M	·	·	사용자 설정 가능	50M	·
	자체 개발	·	카스퍼스키	트렌드마이크로	·	CA사	카스퍼스키	카스퍼스키, 오픈소스 (고객선택 가능)
	O	O	O	O	O	O	O	O
	O	O	O	O	O	O	O	O
	O	O	X	O	O	O	O	O
	O	O	O	O	O	O	O	O
	O	O	O	·	O	O	O	△ (일부 지원)
	O	O	O	·	O	O	O	O
	자체 개발	자체 개발	카스퍼스키, 자체 개발	·	서프 컨트롤	자체 개발	사이버롬	정통부
	O	O	O	·	O	O	O	O
	O	O	O	·	X	O	O	O

산업보안 실무 매거진

월간 시큐리티월드

보안시장 황금알 낳는 방법이 궁금하시다고요?

보안기술과 시장동향, 산업보안 노하우!
보안종합전문지 시큐리티월드가
그 방법을 제시하겠습니다.

미디어그룹 인포더 Tel. (02)719-6931 Fax. (02)715-8245 E-mail : ad@infothe.com

10

편안하고 따뜻한

디지털 세상만들기

한국정보보호진흥원

묵묵히 걸어온 정보보호의 외길 10년!

안전한 디지털 세상을 지키는 파수꾼, KISA가 함께 합니다

WatchGuard Firebox X

Common Criteria 국제CC인증계약 (등급:EAL4)

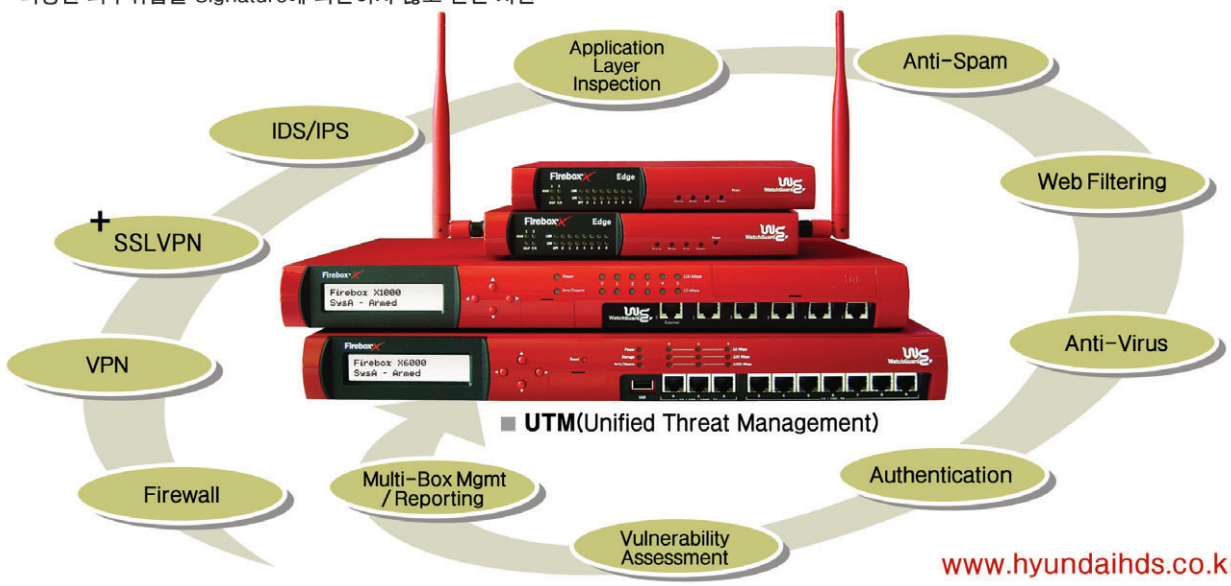
150여개국, 35만개 이상의 기업에서 사용하고 있는 검증된 보안 솔루션

세계 최초 확장 플랫폼 기반 통합 보안 시스템

네트워크 보안의 미래!
최강의 통합 보안 솔루션!

STRONGER SECURITY, SIMPLY DONE™

■ **지능계층형 차세대 보안 아키텍처**
ILS(Intelligent Layered Security)기반의 Zero Day Protection
다양한 외부위협을 Signature에 의존하지 않고 원천 차단



■ **UTM**(Unified Threat Management)

www.hyundaihds.co.kr

현대HDS와 함께 미래의 네트워크와 보안 키워드를 만나 보십시오

검색엔진에서 "UTM 워치가드 VPN SSL-VPN 세이프넷 무선랜스위치 트라페즈 MESH 스트릭스" 를 쳐보세요

WatchGuard

■ 전 세계 통합보안솔루션(UTM)의 리더
■ SMB에서 엔터프라이즈까지 지원 가능한 고가용성 솔루션 (방화벽,VPN, IPS)
www.watchguard.co.kr

TRAPEZE smart mobile

■ 무선랜스위치의 새로운 리더 트라페즈
■ 802.11n Ready WLAN 솔루션
www.trapeze.co.kr

네트워크·보안 솔루션 프론티어
현대 HDS

SafeNet
The Foundation of Information Security

■ 정보보호의 선구자 세이프넷 SSL-VPN
■ 2 Factor 인증이 가능한 SSL-VPN 원격접속 솔루션
www.ssl-vpn.co.kr

StrixSYSTEMS
NETWORKS WITHOUT WIRES™

■ 차세대 무선네트워크 스트릭스 메쉬
■ 세계시장 점유율 1위 메쉬네트워크 솔루션
www.strix.co.kr

• 서울특별시 종로구 당주동 5번지 로얄B/D 5층 520호 110-721
• 솔루션/영업문의: handpsys@hyundaihds.co.kr

고객지원 콜센터 1644-0895
지역대리점 및 리셀러 모집