

PCRE를 완벽하게 지원하는 유일한 솔루션

SOLIGATE™ UTM

고객의 네트워크 안정성을 보장하는
통합보안 솔루션



INFNIS

㈜인프니스네트웍스

2009년 7.7 DDoS 대란이나 최근 3.3 DDoS 공격에서 알 수 있듯이 대규모 공격은 네트워크 환경에서 이루어 집니다. 이와 같은 보안사고에 대하여 PC 보안, 침해대응 분야에서는 사후 대응이 최선의 방법이었지만, 네트워크 보안은 사전 예방과 실시간 방어를 우선으로 합니다.



네트워크 보안
(Firewall, IPS, DDoS, UTM)

〈 네트워크 보안의 중요성 〉

- ✓ 대규모 공격의 대부분이 네트워크 기반
- ✓ 좀비 PC 감염 경로: 파일 다운로드
- ✓ PC 감염 확산 경로: 인터넷
- ✓ PC 보안, 침해대응 → 사후 대응
네트워크 보안 → 사전 예방과 실시간 방어
- ✓ 네트워크 보안은 업데이트, 관리, 통제 용이

네트워크 보안 기술 중 가장 어려워면서도 중요한 분야는 침입 탐지 및 방어입니다. 이 기술의 핵심은 실시간 탐지와 방어의 정확도입니다. 지금까지는 누구도 혁신적인 기술을 제시하지 못했습니다.

기존의 보안 제품은 알려진 공격에 대해서는 문자열 시그니처(Signature) 기반 IPS 기능으로 방어가 가능하지만, 알려지지 않은 공격에 대해서는 방어가 어렵습니다. 또한, 보안 사고가 발생하더라도 보안 관제 등을 통한 빠른 대응이 최선이었습니다.

문제는 변형된 공격, 즉 변종 공격입니다. 문자열 시그니처는 공격 패턴을 약간만 변형하여도 탐지할 수 없습니다. 정규표현식(Regular Expression) 기반의 PCRE 패턴은 공격 패턴을 유형별로 일괄 표현하여 다양한 변종 공격들을 능동적으로 탐지할 수 있습니다. PCRE는 기술적 어려움이 있어 기존에는 완벽하게 구현된 제품이 없었습니다.

PCRE(Perl Compatible Regular Expression)는 널리 사용되는 정규표현식의 확장으로, 복수의 문자열을 전산 기호를 사용하여 수학적으로 일괄 표현합니다. 문자열 시그니처는 하나의 패턴으로 하나의 공격을 탐지하는데 반해 하나의 PCRE 패턴은 하나의 패턴으로 다수의 변형된 공격을 탐지합니다. PCRE 기능을 제대로 지원하려면 성능을 유지하면서 미탐지가 없도록 구현하는 것이 무엇보다 중요합니다.

종류	해결 방안	타제품 대응 수준
알려진 공격	문자열 시그니처 기반 방어	○
알려지지 않은 공격	보안 관제로 침해 대응, 네트워크 점유 형태 제한(DDoS)	△
변종 공격	정규표현식(PCRE 등) 적용	X

표 1. 침입 탐지 및 방어의 구분과 대응

PCRE 지원 요건

PCRE 패턴을 변형하지 않고 사용 (미탐지 Zero)

다량 패턴에서 충분한 성능 유지 (최소 500개 이상 적용)

합리적인 가격 (소프트웨어 기반)

인프니스네트웍스의 Soligate UTM은 PCRE의 세 가지 요건을 만족하는 최초의 제품입니다.

소프트웨어 기반으로 비용을 최소화하였으며, 성능 저하 없이 변형하거나 축약하지 않은 PCRE 패턴을 1,000개 이상 지원합니다.



- 알려진 공격 : 완벽한 방어
- 알려지지 않은 공격 : 네트워크 점유 형태는 제한
침해대응센터를 통한 신속한 대응
- 변종 공격 : 정규표현식 (PCRE)을 이용한 최대한의 방어

지금껏 PCRE를 제대로 지원하는 제품이 없었던 이유 ?

첫째, 패턴 개수가 100개 초과할 경우 성능 저하 발생

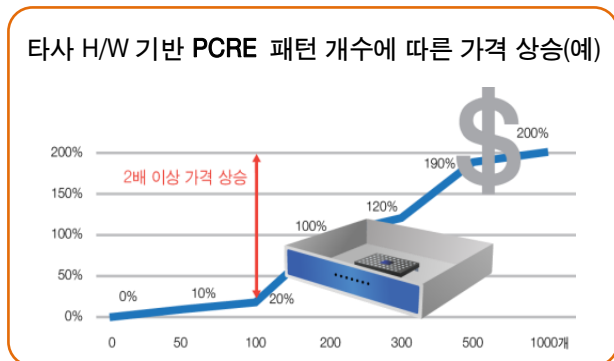
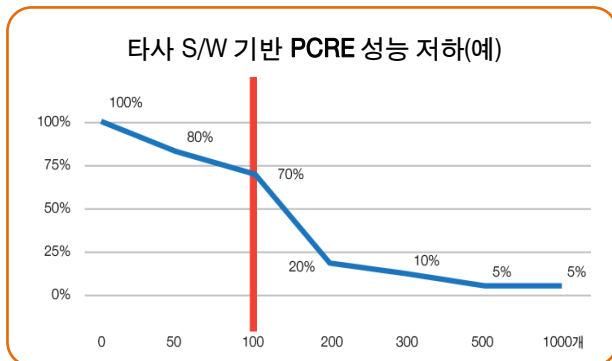
PCRE 패턴은 다양한 변종 공격을 방어할 수 있지만, 적은 개수의 패턴으로 모든 공격을 막을 수는 없습니다. 최소 500개 이상의 패턴이 지원되어야 다양한 공격을 방어할 수 있습니다. 하지만 기존 소프트웨어 제품의 기술로는 패턴의 개수가 100개를 넘으면 성능 부하로 트래픽 용량을 감당하지 못합니다. 이는 PCRE로 표현된 다량의 패턴을 빠른 시간 안에 탐색하는 기술이 개발되지 않았기 때문입니다. 많은 패턴을 동시에 비교하지 못하고 하나씩 비교하는 방식을 쓰면, 패턴의 개수 증가에 따라 탐색 시간도 비례하여 증가하므로 실제 망에서는 운영할 수 없습니다.

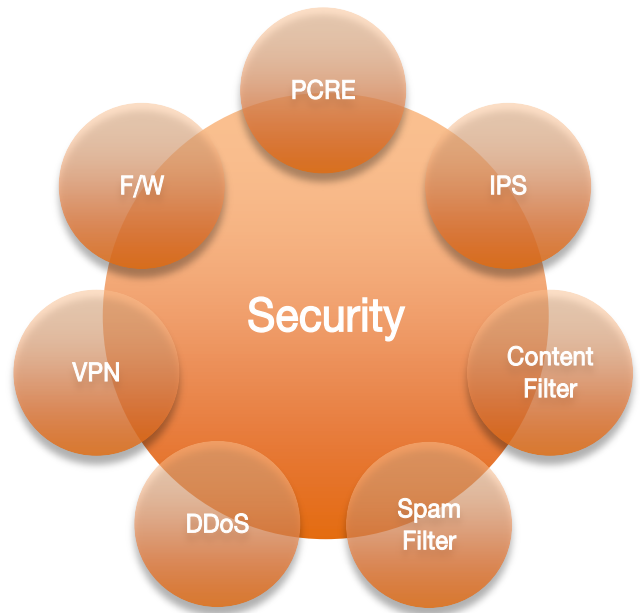
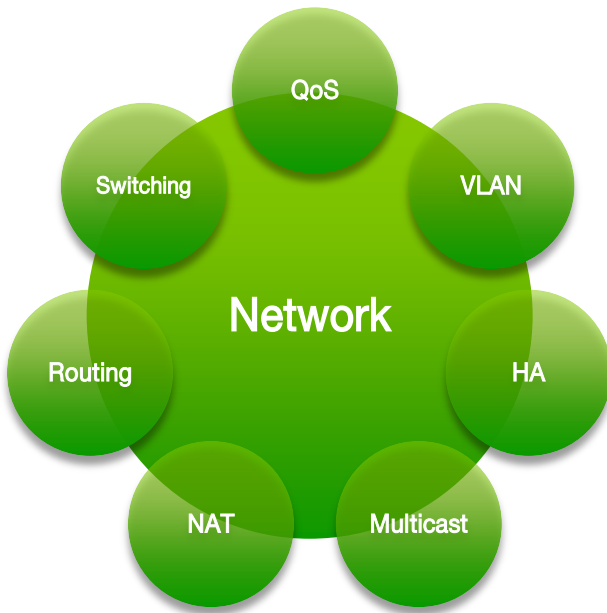
둘째, 성능 저하를 막기 위해 패턴을 변형하거나 축약하여 미탐지 발생

타 제품들은 속도를 높이기 위해 PCRE 패턴으로부터 문자열을 추출하여 검출하는 부분 검사 방식을 이용합니다. 이 방식은 성능 저하를 줄일 수 있지만 미탐지 발생률이 높아지므로 PCRE 기술을 지원한다고 볼 수 없습니다.

셋째, 하드웨어 기반 기술 사용으로 비용 증가

타 제품의 일부는 성능을 향상시키기 위하여 하드웨어 가속칩을 이용합니다. 가속칩을 사용하면 패턴의 개수 증가에 따라 메모리 사용도 동시에 늘어나기 때문에 결국 제품의 가격이 상승합니다. 또한, 별도 하드웨어를 장착하는 것은 제품 전체의 안정성을 침해하고 대용량 트래픽 처리 시 성능 저하를 야기하므로 운영의 신뢰성을 보장하기 어렵습니다.





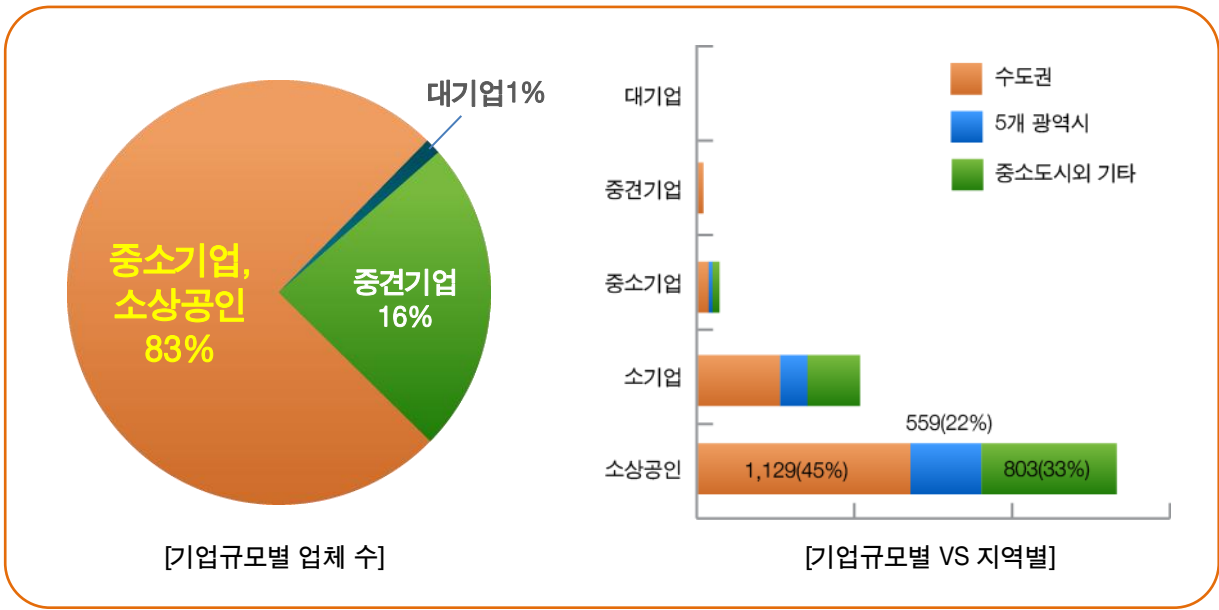
PCRE 패턴 기반 SOLIGATE™ UTM (Unified Threat Management)

인프니스네트웍스 Soligate UTM은 네트워크 기능과 보안 기능을 함께 갖추었습니다. 스위칭, 라우팅, NAT, 멀티캐스트, VLAN, QoS가 대표적인 네트워크 기능입니다. 보안 기능으로는 방화벽, DDoS, PCRE 패턴 기반의 IPS, 유해 사이트 차단(Web filter), 스팸 차단(Spam filter), VPN 등을 망라하고 있습니다. Soligate UTM은 Unified 라는 말에 가장 어울리는 제품입니다.

데이터 암호화 (VPN)	표준 IPSec 지원 및 다양한 고객 환경에 적합한 네트워크 구성 지원
네트워크 통제 (Firewall)	Stateful Inspection 기반의 고성능 방화벽
사용자 제한	유해 사이트 차단, 스팸 차단, NAC 연동 등으로 사용과 접근 제어
침입 탐지 및 방어 (IPS : Intrusion Prevention System)	3,000여 개 시그니처를 이용한 알려진 공격 완벽 탐지 PCRE (Perl 호환 정규표현식) 패턴을 이용한 변종 공격 적극 대응 Collaborative Defense Scheme 기반의 DDoS 방어(출시 예정) 침해 대응 서비스(출시 예정)

인프니스네트웍스 Soligate 시리즈는 **PCRE 기술을 완벽하게 지원**하는 유일한 제품입니다.

인프니스네트웍스는 이미 수많은 고객으로부터 VPN, 방화벽, IPS, 유해사이트 차단, 스팸 차단 등의 기술을 검증 받았습니다. 각종 기업용 응용프로그램의 제어가 가능한 NAC 기능을 보유하고 있습니다. 가장 어려운 기술인 IPS 기능은 혁신적인 기술 진보를 이루었습니다. 알려진 공격은 문자열 시그니처로, 변종 공격은 PCRE 패턴으로 탐지 및 방어하며, 이는 타 업체와 비교할 수 없는 수준으로 월등한 성능과 정확도를 자랑합니다.

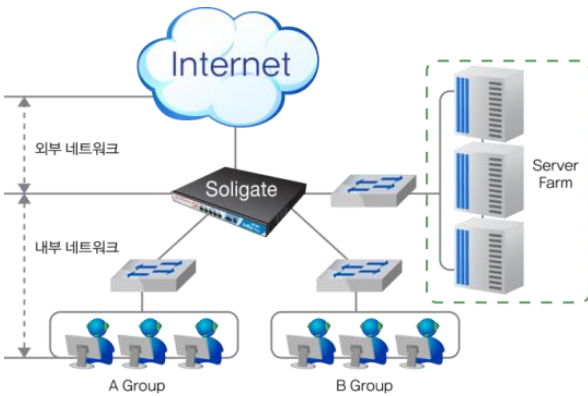


전체 기업에서 17%를 차지하는 대기업, 중견기업, 국가기관, 공공기관, 학교 등은 대부분 보안 제품을 보유하고 있으므로 신규 구매에 대한 수요가 많은 것은 아닙니다. 그러나, 이 고객으로부터는 고도화에 따라 기존 보안 제품에 대한 대체 수요가 꾸준합니다. 대체 수요는 3-5년 사이에 항상 발생하므로 여전히 매력적인 고객군입니다.

전체 기업에서 83%를 차지하는 중소기업과 소상공인은 보다 더 매력적인 고객군입니다. 이 고객들은 보안 사고의 경험과 보안에 대한 법률 강화로 인해 점차 보안 의식이 높아지고 있지만, 기 보유한 보안 제품은 없는 경우가 대부분입니다. 이 고객군은 보안 제품이 필요한 신규 시장이며, 병원과 같이 보안에 민감한 분야를 시작으로 기업군을 단계적, 선택적으로 분리하여 개척할 수 있습니다.

규모	모델	권장 속도(bps)	권장 사용자수(명)
소규모	1000	~ 250M	5 - 10
	1500		10 - 30
중규모	3700	~ 500M	30 - 100
	5000	1G ~	100 - 200
대규모	7000	~ 2G	200 이상
	10000	2G ~	200 이상

표 2. Soligate UTM 라인업



기본 구성

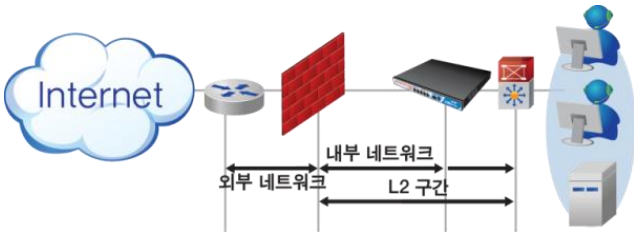
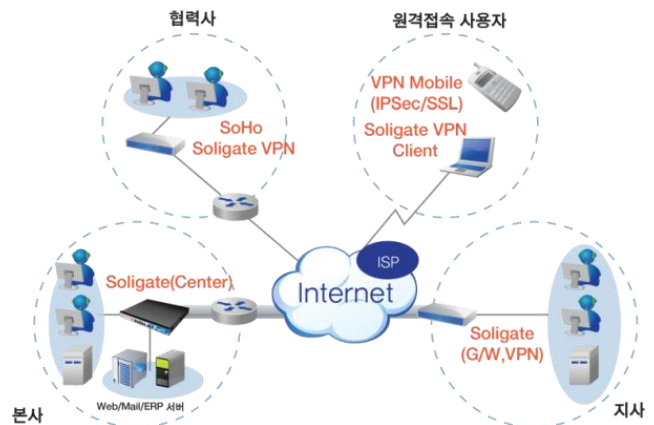
별도의 라우터나 L3 스위치 없이 라우팅 기능을 수행합니다.

- ✓ 특징
 - 외부와 내부를 연결해주는 게이트웨이 역할 (L3 스위치 기능)
- ✓ 장점
 - 다수의 LAN 포트를 이용하여 사용자 그룹 및 Server Farm의 물리적 구분

VPN

본/지사 형태의 고객은 VPN 구성이 적합합니다.

- ✓ 특징
 - IPSec을 통한 본/지사 암호화 통신
 - 별도의 WAN 장비 없이 구성 가능 (라우팅 기능 수행)
 - 외부 협력사 및 원격 접속 사용자 적용 가능
- ✓ 장점
 - 회선 비용 절감
 - 모바일 용 VPN 클라이언트 소프트웨어를 이용한 재택 근무 지원
 - 보안 강화로 대외 신뢰도 향상



Bridge

기존 네트워크 구성 변경을 원하지 않으시는 고객에게는 Bridge 구성이 적합합니다.

- ✓ 특징
 - 기존 네트워크 변경 없이 구성 가능
- ✓ 장점
 - IPS, 유해사이트차단, 스팸 필터 등의 보안 기능 적용

HA(High Availability)

중단 없는 네트워크를 위해 이중화 구성이 가능합니다.

- ✓ 특징
 - Active-Active, Active-Standby 구성 가능
 - 장비 간 설정 및 상태 정보 공유
 - 별도의 L4 장비 없이 로드밸런싱 수행
- ✓ 장점
 - 장비 장애 시 자동 전환
 - 서비스 가용성 보장



침입 차단 시스템(Firewall)

외부와 내부의 접점에서 보안 게이트웨이 역할을 수행합니다. 안전한 환경(DMZ)을 구성할 수 있습니다.

상태기반 감시(Stateful Inspection)

Soligate UTM은 일정 시간 동안 통신 패킷을 추적함으로써 강화된 보안 기능을 제공합니다. 송수신 패킷을 모두 검사하며, 특정한 형태의 수신 패킷을 요청하는 송신 패킷들도 추적하여 오직 적절한 응답이라고 판단되는 수신 패킷에 대해서만 통과를 허용합니다. 즉, 관리자가 정의한 보안 정책에 적합하도록 패킷의 상태 정보를 이용하여 좀더 빠르고 높은 보안성을 제공합니다.

L2기반 차단 기능 제공

ARP 프로토콜의 취약점을 이용하는 ARP Spoofing 공격, IP 프로토콜의 인증 취약점을 이용하는 IP Spoofing 공격 등의 차단 기능을 제공합니다.

NAT

1:1, N:1, M:N 등 다양한 NAT 환경을 지원합니다.



침입 탐지 및 방어 시스템(IPS : Intrusion Prevention System)

인프니스네트웍스 Soligate UTM은 네트워크와 시스템에 대한 비정상적인 패킷과 세션을 차단하는 기능은 물론, 다양한 형태의 침입 행위에 대해 즉각적으로 탐지하고 분석하여 능동적으로 대응합니다.

Deep Packet Inspection

Soligate UTM의 IPS 엔진은 강력한 침입 탐지 및 방어 기능을 수행합니다. 3,000여 개의 알려진 공격에 대한 최신 시그니처로 웜, 바이러스, 악성 코드를 차단합니다. 또한 SQL Injection, Web Shell Upload, 애플리케이션 취약점을 이용한 Exploit 코드와 같은 다양한 형태의 공격을 방어합니다.

변종 공격 차단(PCRE 기반)

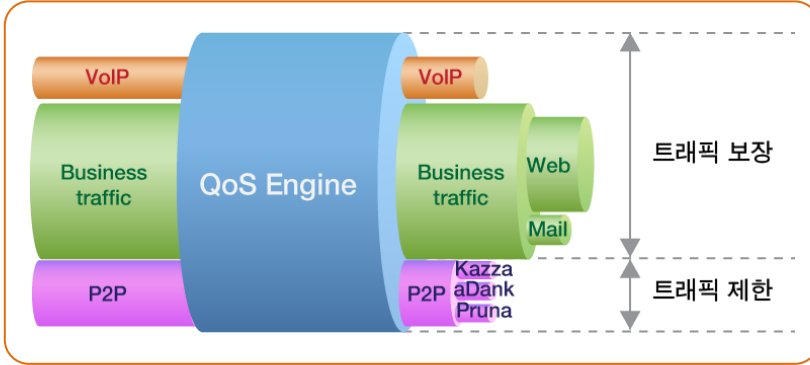
Soligate UTM은 정규표현식 기반의 PCRE 기술을 지원하여 변형된 공격을 차단합니다. 관리자가 PCRE 패턴을 변형하지 않고 직접 입력이 가능하며, 1,000개 이상의 패턴을 적용하여도 성능 저하가 미미합니다.

DDoS(Distributed Denial Of Service) 방어

Soligate UTM은 Ping of Death, LAND Attack과 같은 DoS 공격을 차단합니다. 또한 다양한 형태의 Flooding 공격을 차단하는 기능을 제공합니다. SYN, ACK, RST, URG 등의 TCP flooding 공격을 방어하고, UDP, ICMP flooding 및 DNS query 공격 등도 차단합니다.

품질 보장 서비스(QoS : Quality of Service)

QoS 기능은 트래픽 관리를 위한 기능입니다. 대용량 대역폭의 회선을 사용한다고 해도 P2P와 같은 하나의 프로그램이 전체 대역폭을 점유할 수 있습니다. Soligate UTM은 트래픽을 보장 또는 제한합니다.



- ✓ 업무용 또는 중요 트래픽 보장
- ✓ P2P와 같은 비업무 트래픽 제한
- ✓ IP, 포트별 제어
- ✓ 사용 그룹별, 시간별 적용 가능
- ✓ Shaping 방식으로 데이터 무손실

유해 콘텐츠 차단

유해 사이트 차단

Soligate UTM은 관리자가 정의한 정책에 따라 업무와 연관성이 없는 웹 사이트 접근을 차단합니다. 방송통신심의 위원회에서 제공하는 DB와 연동하여 유해사이트 차단 정책의 설정이 가능합니다. 또한 내용등급(PICS label) 표시에 따른 차단 기능을 제공합니다. P2P, 웹하드, 게임 사이트 등의 유해 사이트 목록을 항목별로 분류하여 제공합니다. 사용자 정의 URL filter 기능은 관리자의 판단에 따라 특정 웹 사이트를 차단할 수 있도록 합니다.

웹 메일 차단

Web Mail Filter 기능은 내부 정보가 외부로 허락없이 유출되거나, 외부의 감염 데이터가 분별없이 내부망으로 침입하는 경로를 차단하는 것이 목적입니다. 관리자가 정의한 정책에 따라 지정된 웹 메일 서비스의 읽기, 쓰기, 파일 첨부 등의 기능을 제한할 수 있습니다.

스팸 차단

스팸 차단 기능은 내부망으로 전송되는 메일의 내용과 첨부 파일을 검사하여 스팸 메일인 경우 격리 처리합니다. 격리된 메일은 운용 방식에 따라 파기하거나 임시로 저장해 둘 수 있습니다. 더불어 2,381,093개의 바이러스 시그니처와 비교하여 메일과 첨부 파일의 바이러스 감염 여부를 판단하고 감염된 메일은 차단합니다. 또한, 메일 크기를 제한할 수 있는 기능을 제공합니다.

관리 기능

관리자는 직관적인 사용자 인터페이스를 사용하여 다양한 보안 정책을 설정할 수 있습니다.

모니터링 및 로그 검색

장비 상태, 보안 이벤트의 실시간 모니터링 및 로그 검색 기능을 제공하여 각종 보안 사고를 예방할 수 있습니다.

- ✓ CPU 부하량 모니터링
- ✓ 메모리/디스크 사용량
- ✓ 실시간 보안 로그 모니터링 및 로그 검색 기능



INFNIS

(주)인프니스네트웍스

서울시 강남구 논현동 130-29 (논현로 653) 3층

<http://www.infnis.com>

TEL 02-3443-3456(代)

FAX 02-3443-6060

E-mail sales@infnis.com