

기본상품 규격서

TESS TAS V7.5

(대표기능 : 유해트래픽 수집 소프트웨어)

1. 상품개요 및 구매조건

1.1 상품개요

TESS TAS V7.5는 네트워크 환경에서의 모든 패킷을 실시간 수집하고, 다양한 알려진 공격에 대한 침입 탐지 패턴 적용 및 처리를 수행합니다. 신종 사이버 위협의 유연한 대처를 위한 정규표현식(PCRE)과 YARA 기반 사용자 정의 시그니처를 처리하는 보안 시스템입니다.

1.2 규격별 적용대상 및 범위, 사용기간

구분	물품분류번호	모델명	구매 단위	라이선스 (적용대상)	SW라이선스 (사용기간)	인도 조건	비고
	물품식별번호	제품규격		라이선스 (적용범위)			
1	43233205	TESS TAS V7.5	조 (copy)	사이트	제한 없음	현장 설치도	
	26047203	유해트래픽수집, 500Mbps		Server			
2	43233205	TESS TAS V7.5	조 (copy)	사이트	제한 없음	현장 설치도	1000SC
	25199877	유해트래픽수집, 1Gbps		Server			
3	43233205	TESS TAS V7.5	조 (copy)	사이트	제한 없음	현장 설치도	2000SC
	25199878	유해트래픽수집, 2Gbps		Server			

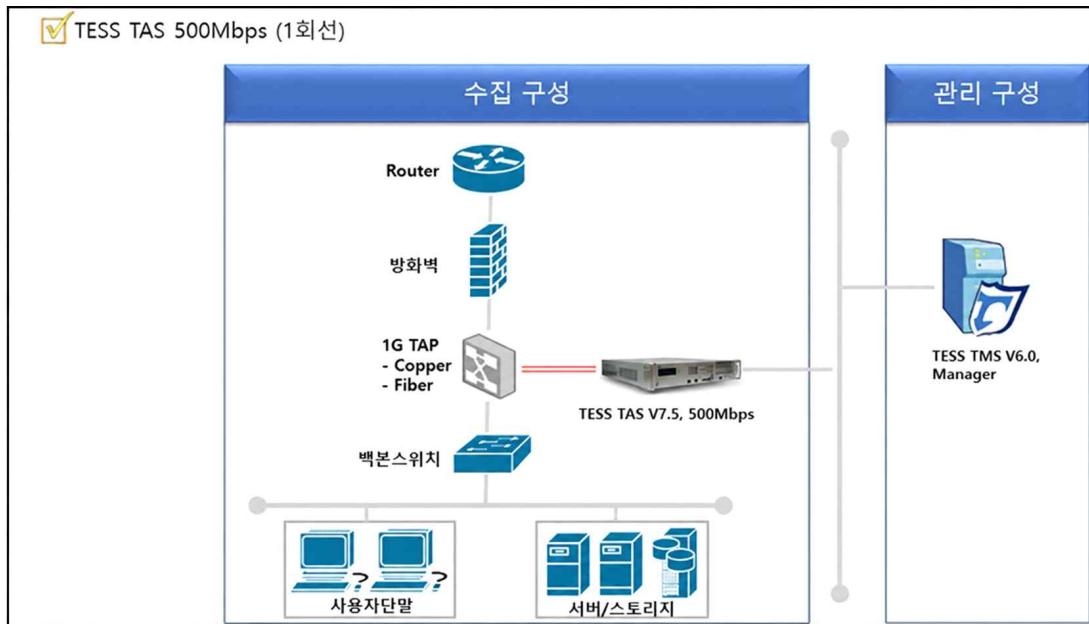
1.3 규격별 1조(copy)구매시 SW라이선스 사용권리 및 사용기간

구분	물품식별 번호	모델명 및 제품규격	라이선스 적용대상 및 범위, 정책 등 (1조(copy)구매시)	
1	26047203	TESS TAS V7.5, 유해트래픽수집, 500Mbps	라이선스 범위	해당 제품은 1조 구매 시 SW라이선스 사용(Server단위)로 구매가 가능합니다.
			규격의 역할	서버에 설치하여 유해트래픽을 수집하는 역할을 합니다. 1회선 구간 탐지 가능합니다.
			사용기간	구매 시 사용기간에 제한이 없습니다
2	25199877	TESS TAS V7.5, 유해트래픽수집, 1Gbps	라이선스 범위	해당 제품은 1조 구매 시 SW라이선스 사용(Server단위)로 구매가 가능합니다.
			규격의 역할	서버에 설치하여 유해트래픽을 수집하는 역할을 합니다. 1회선 구간 탐지 가능합니다.
			사용기간	구매 시 사용기간에 제한이 없습니다

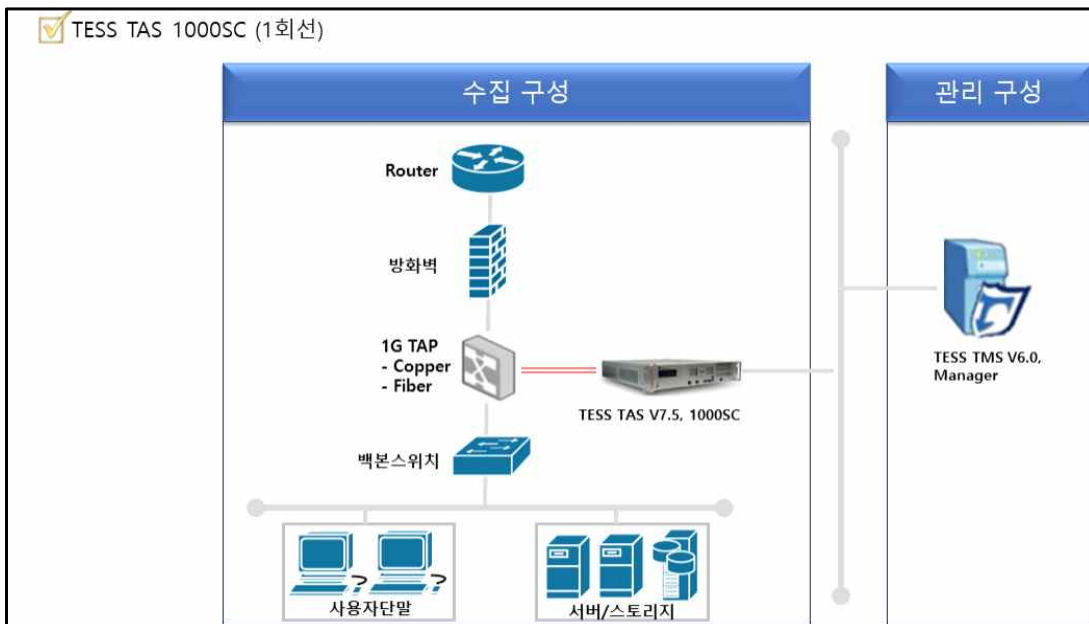
3	25199878	TESS TAS V7.5, 유해트래픽수집, 2Gbps	라이선스 범위	해당 제품은 1조 구매 시 SW라이선스 사용(Server단위)로 구매가 가능합니다.
			규격의 역할	서버에 설치하여 유해트래픽을 수집하는 역할을 합니다. 2회선 구간 탐지 가능합니다.
			사용기간	구매 시 사용기간에 제한이 없습니다

1.4 구매예시

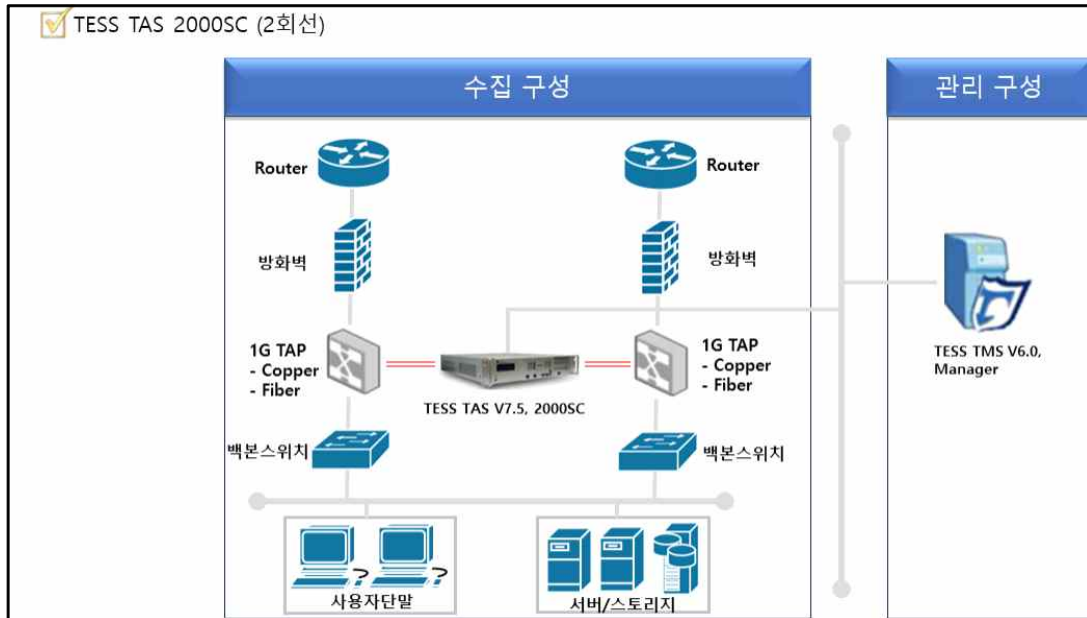
1) 탐지구간이 1회선(500Mbps*2Port)인 경우 -> 500Mbps 규격 1조 구매



2) 탐지구간이 1회선(1G*2Port)인 경우 -> 1Gbps 규격 1조 구매



3) 탐지구간이 2회선(1G*4Port)인 경우 -> 2Gbps 규격 1조 구매



- 하드웨어(서버) 및 TAP 장비는 고객과의 협의를 통하여 수의계약 또는 별도 구매 진행함

1.5 해당 규격별 제품은 기본 커스터마이징이 포함된 상품입니다.

※ 기본 커스터마이징 범위는 수요기관과 납품업체가 상호협의

2. 제품 인증내역

분 류	인증 번호	인증 명칭	만료일자
GS인증(1등급)	22-0580	TESS TAS V7.5	해당없음

3. 제품 권장사양

3.1 구매한 S/W가 설치될 H/W제품 권장사양

NO	물품 식별번호	모델명 및 제품규격	권장사양(H/W)	운영환경 (서버, 사용자)
1	26047203	TESS TAS V7.5, 유해트래픽수집, 500Mbps	1.CPU: 3.30GHz (6Core) 이상 2.Memory: 16GB 이상 3.HDD: 1TB 이상	1.지원플랫폼 -Server : Embedded OS -Client : PUTTY, SecureCRT

2	25199877	TESS TAS V7.5, 유해트래픽수집 ,1Gbps	1.CPU: 3.30GHz (6Core) 이상 2.Memory: 16GB 이상 3.HDD: 1TB 이상	1.지원플랫폼 -Server : Embedded OS -Client : PUTTY, SecureCRT
3	25199878	TESS TAS V7.5, 유해트래픽수집 ,2Gbps	1.CPU: 2.10GHz (8Core) 이상 2.Memory: 16GB 이상 3.HDD: 2TB 이상	1.지원플랫폼 -Server : Embedded OS -Client : PUTTY, SecureCRT

4. SW구매시 제공되는 기능

- 네트워크에서의 모든 패킷을 실시간 수집, 탐지
- 기관/사용자별(네트워크 구간별) 트래픽 분류·수집
- 다양한 유해트래픽 탐지
- PCRE 정규 표현식 및 YARA룰을 이용한 사용자 정의 시그니처 적용 및 탐지
- NCSC 등에서 배포하는 PCRE, YARA 문법으로 배포한 사용자 탐지 정책을 변경 없이 적용
- 탐지된 패킷으로부터 분석에 필요한 통계정보 추출, DB시스템에 선택적 전달
- 수집된 네트워크 패킷에 대하여 실시간 데이터베이스에 저장
- 인터페이스, 프로토콜, 서비스, IP등에 따라 Raw패킷을 수집·저장
- 시스템 장애 시에도 네트워크 서비스 보장
- 침해위협정보 관리 시스템과 암호화 통신을 통한 정보 교환
- 트래픽 미러링 전용 장비 이용, 미러링 구성으로 N/W안정성 및 성능 보장
- 네트워크 인입 구간의 모든 트래픽에 대한 시그니처 기반 탐지 규칙에 의한 유해 패킷 탐지
- 내·외부를 구분하여 세분화된 모니터링 기능 및 최신 공격기법 관련 시그니처 순차적 제공
- 암호화는 SSL, X.509등 표준 보안 인터페이스 지원
- 관리 서버로부터 수신한 탐지 규칙 실시간 적용
- 악성코드 탐지 엔진 및 정책 적용을 통해 파일을 수집하며 악성코드 감염 여부 탐지

5. 서비스 구성 개념도

TESS TAS V7.5는 유해트래픽을 탐지할 구간에 설치되는 제품으로, 미러링장치 (TAP)로부터 전송된 트래픽을 통해 이용기관별 트래픽 분류 수집, 유해트래픽 탐지, 트래픽 분석, 트래픽 정보 수집(트래픽/세션 로깅)을 하여 수집된 정보를 위협관리및 분석솔루션(TESS TMS V6.0)으로 시스템 정보와 함께 전달하는 기능을 수행합니다.

각 구성도는 '1.4 구매예시' 참조 (2p)

6. 공급 및 설치, 타시스템과의 연계 지원방안

적용하려는 기관의 구성 확인 및 설치 위치 협의 후 설치를 진행합니다. 본 제품 설치 시 탐지구간은 백본, L3, L2 장비의 포트 미러링 기능을 사용하는 방법 또는 네트워크 TAP장비를 사용하는 방법을 통하여 트래픽 미러링을 제공해주어야 합니다. 설치 이후 TESS TMS V6.0과 연동하여 수집된 트래픽에 대한 정보 확인이 가능합니다.

7. 제품 구성 및 납품 방법

7.1 제품 구성

구분	종류	수량	비고
S/W	설치용 프로그램	1조	
제품인증서	소프트웨어 사용인증서	1부	
문서	매뉴얼	1부	

7.2 납품 방법

○ 납품 일정 및 장소, 방법 등은 구매 기관과 협의하여 진행합니다.

8. 검사 및 시험

- 구매 기관 담당자의 입회하에 기관이 지정하는 방법에 따라 검수를 실시합니다.
- 설치완료 후에는 소프트웨어 기능별 작동유무, 연계 등을 검사받습니다.
- 규격서상의 구입내역과 동일한 사양이 충족되고, 테스트 후 이상이 없을 때를 설치가 완료되는 시점으로 합니다.

9. 하자보수 서비스

○ 구매 후 1년간 아래와 같이 무상하자보수 서비스를 제공합니다.

무상하자보수 내용			설 명
항목	세부항목	지원범위	
기술 지원	장애발생 후 복구(응답시간)	4시간 이내 (상호협의를 후 정함)	- 시스템 장애 시 대응 시간, 장애 처리 절차 등
	정기점검	방문 (월, 분기 또는 반기) ※구매자↔공급자 간 상호협의를 후 정함	- 시스템의 장애를 사전에 예방하기 위하여 정기적으로 지원하는 정기점검, 정기성능 조율 서비스 - 제품의 점검 및 유지관리 이력관리, 시스템 사용자 관리지원 - 유지관리 작업 보고서 작성, 시스템 운영 보고서 작성
	일상지원	전화,e-mail	- 콜센터 운영, 사이트 운영, 전화/e-mail 등을 통한 장애접수, 질의응답
	이전 설치	이전 1회	- 제품의 이전설치 지원
제품 지원	업데이트 및 패치	원격지원	- 기존 SW제품의 기능 보완 및 새로운 기술의 적용이나 운영체제의 변화 등으로 발생하는 불일치 조정
	마이너 업그레이드	방문지원	- 기존 SW 제품을 향상시키기 위하여 새로운 버전으로 교체하는 서비스(예시: 2.0→2.1, 버전의 소수점 변화)
교육 지원	운영자 교육	1회	- 제품 운영을 위한 운영자 교육
	사용자 교육	1회	- 제품 사용을 위한 사용자 교육

10. 보안 준수

○ 제품 설치 등을 위해 구매 기관 방문 시에는 구매 기관의 보안 규정을 준수합니다.

11. 저작권 및 사용권

○ 공급된 소프트웨어의 저작권은 기본적으로 공급사에 있으며 구매 기관은 해당 소프트웨어에 대한 사용권만을 가집니다.

12. 담당자 연락처

홈페이지	http://www.kornicglory.co.kr/
이메일 상담	sales@kglory.co.kr
고객센터	Tel.02-3479-7498
팩스	Fax.02-3476-4215
주소	서울특별시 강남구 학동로 155, 3~4층 (논현동, 원영빌딩)