Detailed Info

www.novacybersecurity.com

NETAS TELEKOMUNIKASYON A.Ş.
Yenişehir Mah. Osmanlı Bulvarı No:11 34912 Kurtköy - Pendik/İstanbul/Turkey
www.netas.com.tr/en
E-mail: info@novacybersecurity.com
Tel: +90 216 522 20 00
Fax: +90 216 522 22 22

/NetasTR
/NetasTR
/NetasTR
/company/netas
/NetasTR

NETAS

Netas provides innovative end-to-end value added systems integration and technology services in information and communications technologies (ICT). Its customers range from telco providers to public and private enterprises in domestic and international markets. Netas's constant focus on productivity is based on its next generation competencies around technology skillset and expertise. The company holds a track-record of 50 years and continues its foray in the next generation technologies, supported with its experienced, best of breed research and development teams.

The company, provides its customer with solutions in various domains such as networking, cyber security, unified communications, virtualization, cloud computing, broadband mobility, optical and carrier Ethernet, GSM-R. Netas is a leader in IT integration services, managed services and software development solut¬ions. Netas also plays an important role in the modernization of the Turkish Armed Forces' communication networks. Also, the company serves armed forces of some other countries in North Africa, Asia-Pacific and the CIS.

NOVA
Cyber Security Solutions by NETAS

Are you aware that you are vulnerable to many threats on the Internet?

With increasing voice and video transmission over IP and emerging new technologies such as 4G LTE and 5G, data vulnerabilities and lack of security are the main concerns due to the nature of IP infrastructure systems. Reports show that most of attacks occur in the application layer. Therefore our products and services focus on the application layer security. Discover vulnerabilities, detect and prevent attacks, enable secure media communication with our solution.

Find out your vulnerabilities and protect your network with NOVA!

Create and operate a secure VoIP infrastructure with comprehensive VoIP Penetration Test relies on, NOVA PENTEST Services via NOVA V-SPY Vulnerability Scanning and Analysis Tool.

V-SPY is an automated enriched VoIP penetration test suite including rich variety of VoIP attack modules, detailed reports of security measures via expert system.

Detect and prevent VoIP threats using VoIP Application Firewall, NOVA V-GATE.

V-GATE is ready to guard your VoIP infrastructure by performing deep packet inspection, statistical and behavioral analysis, detecting anomalies and preventing VoIP attacks, VoIP monitoring and operational management.

Detect telecommunication frauds using Fraud Management System, NOVA FMS.

FMS offers an intelligent, agile and economical solution that can perform security analysis on massive data volume with machine-learning techniques in real-time to detect frauds and threats.

Make a secure multimedia communication via Secure Media Communication Platform, NOVA S/COM.

S/COM can achieve secure media transfer with its support for various security methods and flexible crypto algorithm, enabling secure voice and video communication, whiteboard usage, file and message transfer.

Maintain a secure operation in UC network, VoIP ad Web applications with NOVA Product Family.

NOVA is a product name of NETAS Cyber Security Technology Development Group developments. VoIP, Web, IoT, Mobile security are the main areas with real time data analysis, artificial intelligence, big data analytics methods usage.

NOVA V-GATE

NEXT GENERATION VoIP/UC SECURITY & MANAGEMENT

NETAS

www.novacybersecurity.com

Secure VoIP/UC Communications and Collaborations

NOVA V-GATE is a modular, transparent and high-performance VoIP security and management product aiming to protect VoIP systems from high costly, damaging attacks by preventing known and unknown application-layer attacks such as toll fraud, premium rate services, TDoS, brute force, fuzzing.

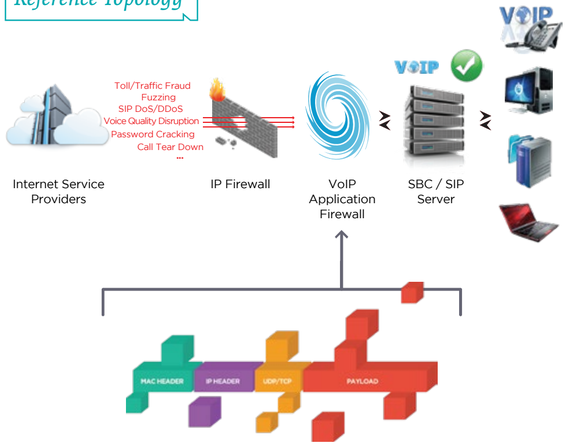
It has Telecom Toll and Traffic Fraud Prevention & Detection via user behavior analysis as well as Operational Management and Monitoring modules.

Most attacks targeting the VoIP infrastructure exploit application layer implementation deficiencies. Therefore, an application level analysis is required to protect the VoIP system. **NOVA V-GATE** was designed to circumvent attacks targeting these vulnerabilities.

NOVA V-GATE not only detect anomalies and prevents attacks, but also detects and prevents VoIP frauds such as toll fraud, premium rate service calls.

NOVA V-GATE is a comprehensive VoIP security solution which provides a combined approach such as stateful inspection, protocol anomaly detection, intrusion detection and prevention, user behavior analysis, CDR generation, traffic analysis.

Reference Topology



Some of the highlights of our solution:

- *Real-time packet monitoring, deep inspection and control management*
- *Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)*
- *Operational Management through the Policy Rule Editor*
- *Measurement of Quality of Services and advance reporting via VoIP Monitoring*
- *Detection and prevention systems against attacks such as toll fraud, traffic fraud, brute force attack, TDoS, active call drop and fuzzing*
- *Anomaly detection with critical parameter control*
- *Automatic fault diagnosis and self-recovery*

Features

IDS/IPS (Intrusion Detection and Prevention System)

- Packet based IDS/IPS
- Call based IDS/IPS
- Call Theft and Toll Fraud Protection
- Behavioral Learning - Anomaly Detection
- Traffic Fraud

VoIP Monitoring

- SIP Signaling Traffic Monitoring
- Call Detail Record (CDR) Generation and CDR Based Reporting
- IDS Reporting
- Security, Attacks and Events Reporting
- Network Performance Reporting
- Call Performance and Ad-hoc Reporting
- SIP Packet Tracking and Recording
- SIP Trunk Monitoring

Firewall / Operational Functionalities

- Stateful Inspection
- SIP Packet Filtering
- Access Control List
- Security Rules and Profiles
- Dynamic Whitelist/Blacklist
- Signaling Control
- Management/Configuration via Web GUI
- VoIP Traffic Classification Rules
- Policy Rule Editor

Features

Threat Protection

- DoS and TDoS Attacks
- Group Based TDoS Attacks
- Buffer Overflow Attacks
- Brute Force Attacks
- Teardown Attacks
- Wangiri Attacks
- User Enumeration Attacks
- Malformed Message and Fuzzing Attacks
- Block Anomalous Behavior

System Level Features

- Detailed Alerts and Notification Mechanism
- SNMP V1, V2C, V3
- Syslog
- By Pass Support
- User and IP Group Definitions
- Automatic Failure Diagnosis and Recovery Process
- High Availability
- Multi-Tenant Support
- UDP & TCP Support
- Proxy, Bridge and Mirror Mode Supports