

EPA-CLM-20K Series NGFW Central Logging System



Antikor v2 Integrated Cyber Security System EPA-CLM-20K Series Next Generation Firewall (NGFW) Central Logging System (CLM), advanced features ile providing centralized logging product. With flexible configuration, live dashboard, and statistical capabilities ile it allows you to centrally collect the logs of all your security firewalls, enabling searchability across these logs from a single center.

Logging Support

The Central Logging System aggregates and consolidates the logs of multiple endpoint NGFWs into a single center. In the generated graphics from the collected logs, clicking on the relevant log provides the option to 'Search Logs' retrospectively, enabling searches for past entries.

Performance

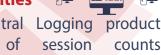
The Central Logging product retains historical hourly/daily/monthly and yearly data for all displayed statistics. Graphs are updated with new data added within seconds, replacing the previous data.

The Antikor Central Logging product draws graphs of session (passed/dropped) in the statistics of logs coming from endpoint NGFWs. categorizes and draws graphs based on the highest Source IP, Destination IP, Services, and Protocols.

Authorization

Antikor® Central Logging provides authorization services for data coming from affiliated Antikor NGFWs. Authorized users can search their own logs based on their authorization.

Statistical Capabilities









Mersin Universitesi Ciftlikkoy Kampusu Teknopark Idari Binasi Kat: 4 No: 411 Zip Code: 33343 Yenisehir / MERSIN / TURKIYE



EPA-CLM-20K Series

Product Specifications



Central Logging Features
For Managed Antikor NGFW Systems;
Logging Management
Logging Template Management
Real-time Logs
Daily Session Count Statistics
Hourly Session Count Statistics
Statistics of Top 10 Destination IPs
Statistics of Top 10 Source IPs
Statistics of Top 10 Services
Encrypted Communication with IPsec Tunnels
Tracking Alerts and Notifications
Protocol Distribution Statistics
Detailed Audit Logs
Notification Management
Authorization Management
Network Interface Specifications

Network	Interface	Specific	tations
Loopback Inte	rface_IFFF.80	2 10 VI AN	support

Link Aggregation:

Link Aggregation:

LACP, Failover, Load Balance, Round Robin

Bridging / STP / Ethernet Bypass

Virtual Extensible LAN (VXLAN)

NAT64, IPv6 6to4 Tunneling

Static ARP

IPsec VPN

Encryption:

AES, CAMELIA, NULL_ENC, SERPENT, TWOFISH

Authentication:

MD5, SHA1, SHA256, SHA384, SHA512, AES

WildCard ID Support

NAT Traversal Support

PKI - Public Key Infrastructure Support

PSK - Pre Shared Key Support

Services

Live Dashboard

Automated Update System

Online Update

Automatic Configuration Backup

Antikor® Shared Management - Virtual System

SNMP v2/v3 Service

Log Timestamping

TUBITAK Kamu SM - Timestamp Integration

Syslog - supported formats;

RAW, CEF, EWMM, GELF, JSON, WELF, CIM

LLDP Service

Licensing	
High Availability (HA) - Cluster Support	Active-Passive
Number of Addressable CPU Threads	28
The number of Antikor NGFWs it can log	100
Number of IPsec VPN Tunnels	100
Maximum Logging Performance (Logs/Second)	20K

Management Interface Features

HTML5 Responsive Web Interface

SSL Certificate based authentication

2FA - Two-Factor Authentication

Customizing the Service Port

SSH Console

Physical Console (Monitor, Keyboard)

Serial Console (If exists on hardware)

Incident Notification Service

SMS, Email, Brower Notification

Authentication Methods

Mernis

SMS

Local User

HTTP(API)

LDAP / Active Directory

RADIUS

POP3 / IMAP

TACACS+

Product Certifications

Commom Criteria EAL4+

TRtest Product Conformity Certificate

%100 Turkish Made

Routing

IPv4 / IPv6 Static Routing

Routing Monitor

Minimum Requirements for Physical Platforms

Min 28 Core Processor

Min 96 GB Ram

14 TB Solid State Disk

MultiQueue Server Ethernet Card

Minimum Requirements for Virtual Platforms

VMware ESXi 6.7 or higher Hypervisor

Min 28 Core AESNI Enabled CPU

Min 96 GB Reserved Ram

At Least 14 TB Storage Area (At Least 10000 IOPS with 4KB Blocks)

Ethernet Cards must be Configured as PassThrough

* Minimum requirements may vary based on system configuration and hardware.

eP-FR-79 Rev.02 / Release date: 01.04.2019 / Rev.date: 02.05.2021



Mersin Universitesi Ciftlikkoy Kampusu Teknopark Idari Binasi Kat: 4 No: 411 Zip Code: 33343 Yenisehir / MERSIN / TURKIYE



