ePati

antikor v2
Unified Cyber Security System

Antikor Integrated Cyber Security System EPA-CTNM-K3 Series, SD-WAN Central Management System (CTNM), is a product that provides central management with advanced management functions. Centrally monitors and manages all Dual Layer SD-WAN products with flexible configuration, live dashboard, and advanced profile capabilities.

Profile Support

Central Management System manages multiple security policies under the name "Profile". Managed SD-WAN products can be subscribed to more than one profile. In this way, all managed systems can be included in the general security profile, and regional settings can be applied with specialized security profiles.

Batch Policy Management

Antikor Dual Layer SD-WAN Central Management System (CTNM) collectively applies your corporate security policy to the Antikor Dual Layer SD-WAN products you manage. It displays the accessibility status and notifications of the nodes you manage centrally on the map.

Performance

Operates your network with maximum performance while executing security functions. Provides enterprise networks security and network requirements easily and highly efficiently by its powerful network stack.

Management

Antikor CTNM can provide Update Server Service to Antikor SD-WANs connected to it from the Central Management, Configuration Template Management, Individual Management and Bulk Update Management.

Product Specifications

Central Management Features

For Managed Antikor NGFW Systems;

- Configuration Management
- Configuration Template Management
- Update Server Service
- Security Policy and Object Management
- Periodic Configuration Backup
- Access Monitoring the Map
- Tracking Alerts and Notifications
- Communications Encrypted with IPsec Tunnel
- Ability to Manage Singularly
- Profile / Global Configuration Management
- Batch Update Management

Detailed Audit Logs

Notification Management

Authority Management

Network Interface Specifications

Loopback Interface, IEEE 802.1Q VLAN support

Link Aggregation:

- LACP, Failover, Load Balance, Round Robin

Bridging / STP / Ethernet Bypass

Virtual Extensible LAN (VXLAN)

IPv4 / IPv6 Static Routing

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

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	32
Number of Managable Antikor SD-WAN	3000
Number of IPsec VPN Tunnels	3000
Maximum Number of Profiles	300

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

Virtual Switch Features

Assigning Layer2 Tunnels as Virtual Ports

IPsec Encryption for Layer2 Tunnels

Physical Port Assignment

IEEE 802.1Q VLAN for both Virtual and Physical Ports:

- - Untag Port Assignment
- - Tagged Port Assignment
- - Hybrid Port Assignment

VLAN Enabled MAC Table

IEEE 802.3ad Link Aggregation Control Protocol (LACP)

Spanning Tree Protocol

Rapid Spanning Tree Protocol

Link Layer Discovery Protocol

NetFlow Export Service

MAC Learning

Minimum Requirements for Physical Platforms

Min 32 Core Processor

Min 48 GB Ram

2 TB Solid State Disk

MultiQueue Server Ethernet Card

Minimum Requirements for Virtual Platforms

VMware ESXi 6.7 or higher Hypervisor

Min 32 Core AESNI Enabled CPU

Min 48 GB Reserved Ram

At Least 2 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.