epati

ePati Cyber Security

antikor

Unified Cyber Security System

www.epati.com.tr

# Founding Partners and Board of Directors

## Ph.D. Lect.  Özkan KIRIK

- ePati Cyber Security Inc. Head of Directors Board
- Mersin Univ. IT Research and Application Center
- T.C. Presidency "Science, Technology and Innovation Policy Board" Cyber Security Advisory Board Member
- Turkish Cyber Security Cluster Firewall Test Criteria Comission Member
- TSE Certified White Hat Hacker
- Cisco Certified Trainer
- FreeBSD Project Contributor

## Lect. Kutluhan KİBRİT

- ePati Cyber Security Inc. Directors Board Member
- Mersin University, IT Department
- TSE Certified White Hat Hacker
- Cisco Certified Trainer

## Lect. N. Can KIRIK

- ePati Cyber Security Inc. Directors Board Member
- Mersin Univ. IT Research and Application Center Assist. Director
- PostgreSQL Contributor
- Cisco Certified Trainer

MEMBER OF TURKISH CYBER SECURITY CLUSTER

# About ePati Cyber Security

MEMBER OF
TURKISH CYBER SECURITY
CLUSTER

- **ePati Cyber Security**
  - Was born in 2006 November in Mersin Technology Development Zone
  - Is the first company in Mersin Technology Development Zone.
  - It has been one of the catalog suppliers of the State Supply Office since 2011.
  - Member of Turkish Cyber Security Cluster.
  - Is focused on developing products about Network Security and Advanced Computer Networking.
- **Founders**
  - All of the founding partners are academic staff at Mersin University. Additionally, they have been appointed to the Technopark by Mersin University in accordance with Law No. 4691.

www.dmo.gov.tr

epati

MEMBER OF
TURKISH CYBER SECURITY
CLUSTER

antikor

# Standards and Certifications

## Enterprise Management Standards

ISO/IEC 27001

ISO 9001

FACILITY SECURITY CLEARANCE CERT.

NATIONAL SECRET
NATO SECRET

## Product Certificates

COMMON CRITERIA
EAL4+

%100 antikor YERLİ MALI

TRtest Test ve Değerlendirme A.Ş.

FIREWALL
PRODUCT COMFORMITY CERTIFICATE

MEMBER OF TURKISH CYBER SECURITY CLUSTER

Common Criteria

HOME | ABOUT THE CC | PUBLICATIONS | TECHNICAL COMMUNITIES | CERTIFIED PRODUCTS | COLLABORATIVE PPS | PROTECTION PROFILES | ICCC | NEWS

# CERTIFIED PRODUCTS

⊞ Access Control Devices and Systems – 21 Certified Products

⊟ Boundary Protection Devices and Systems – 40 Certified Products

| Product | Vendor | Product Certificate | Date Certificate Issued | Certificate Validity Expiration Date | Compliance | Scheme |
|---|---|---|---|---|---|---|
| Antikor Next Generation Firewall Management v2.0.1188<br>Certification Report Security Target | Epati Siber Güvenlik Tek. San. ve Tic. A.S. | CCRA Certificate | 2023-04-17 | 2028-04-17 | EAL4+ ALC_FLR.1 | TR |
| Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect<br>Certification Report Security Target | Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134-1706 USA | CCRA Certificate | 2022-10-07 | 2027-10-07 | EAL4+ ALC_FLR.2 | NL |
| McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x<br>Certification Report Security Target | Trellix | CCRA Certificate | 2022-07-28 | 2027-07-28 | EAL2+ ALC_FLR.2 | CA |
| ST Engineering Data Diode Model 5282, version 2.2.1055 & Model 5283 version 2.2.1055<br>Certification Report Security Target | ST Engineering Electronics | CCRA Certificate | 2022-07-08 | 2027-07-08 | EAL4+ AVA_VAN.5 | SG |
| Trend Micro Deep Security 20<br>Certification Report Security Target | Trend Micro Inc. | CCRA Certificate | 2022-05-31 | 2027-05-31 | EAL2+ ALC_FLR.1 | CA |
| Fortinet FortiGate™ Next Generation Firewalls with FortiOS 6.2.7<br>Certification Report Security Target | Fortinet, Inc. | CCRA Certificate | 2021-10-15 | 2026-10-15 | EAL4+ ADV_FSP.3 | CA |

Certificate Authorizing Members

Certificate Consuming Members

# Türkiye's Only

COMMON CRITERIA
EAL4+
CERTIFIED

# Next Generation Firewall

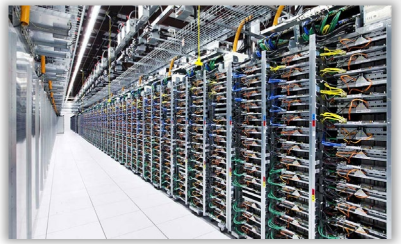
antikor


**Antikor NGFW is approved by “TRtest Inc.” which is founded by Presicency of the Republic of Türkiye Defence Industry Agency**

# antikor - Target Scale

➢ **By Network Size**

| Scale | Min NGFW / FW Thr. | Max NGFW / FW Thr. |
| --- | --- | --- |
| Telco | 60 Gbps / 220 Gbps | 75 Gbps / 280 Gbps |
| Data Center Grade | 20 Gbps / 80 Gbps | 50 Gbps / 200 Gbps |
| Large Enterprise | 10 Gbps / 40 Gbps | 18 Gbps / 72 Gbps |
| Enterprise | 3.0 Gbps / 12 Gbps | 7 Gbps / 28 Gbps |
| Mid. Size Enterprise | 1.0 Gbps / 4.0 Gbps | 2.0 Gbps / 8 Gbps |
| Small Enterprise | 0.5 Gbps / 2.0 Gbps | 0.8 Gbps / 3.2 Gbps |
| Branch Office | 0.3 Gbps / 1.2 Gbps | 0.4 Gbps / 1.6 Gbps |

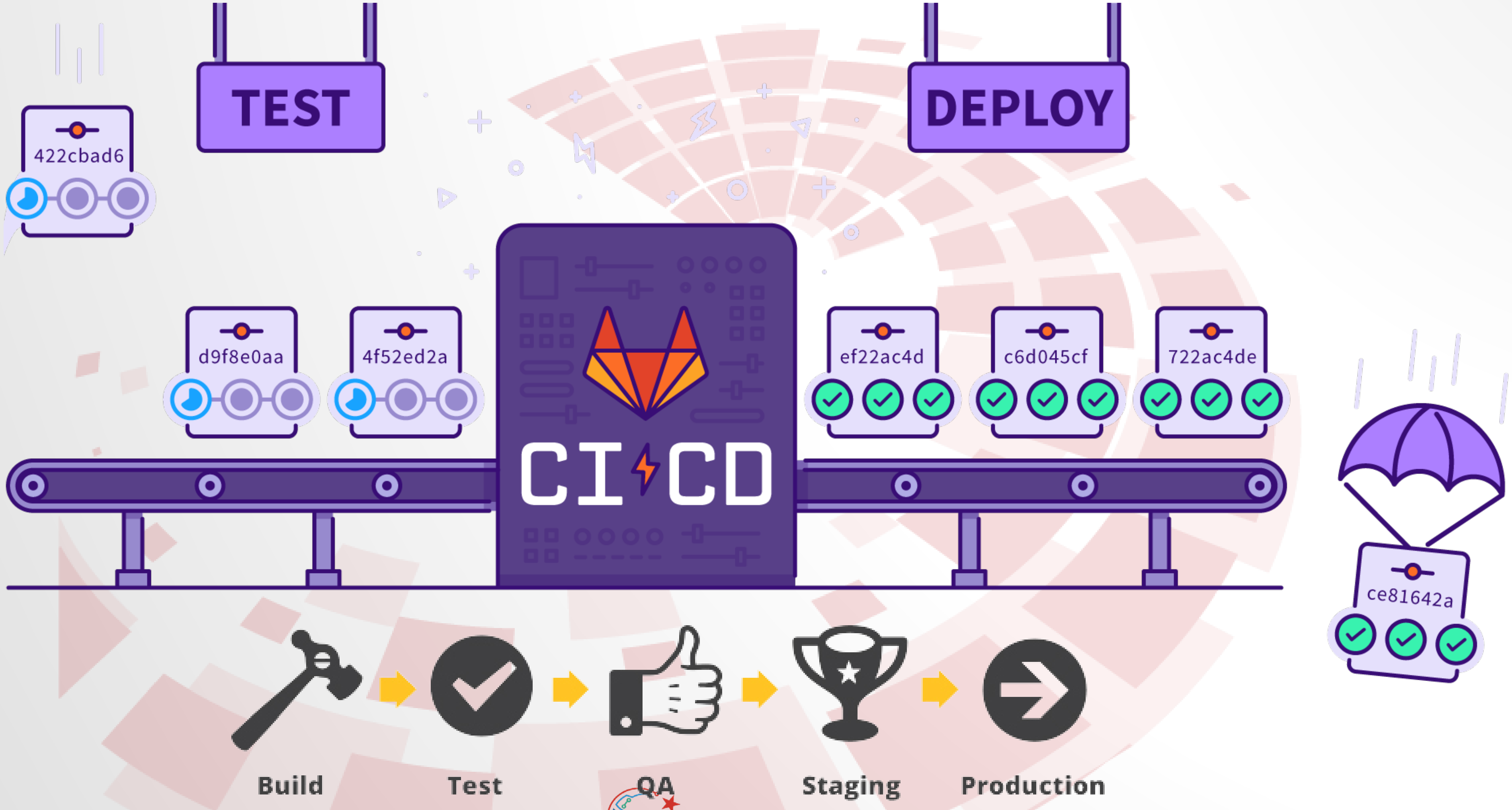


# Product Development and Roadmap

www.epati.com.tr/en

# antikor – Software Quality Control CI / CD

➢ CI / CD – Continuous Integration & Continuous Deployment



# Product Portfolio

Next Generation Firewall

Dual Layer SD-WAN

Central NGFW Management

Central SD-WAN Management

Central Log Management

# Antikor NGFW
# Next Generation Firewall

COMMON CRITERIA
EAL4+

ÜRÜN UYGUNLUK
TRtest
BELGESİ

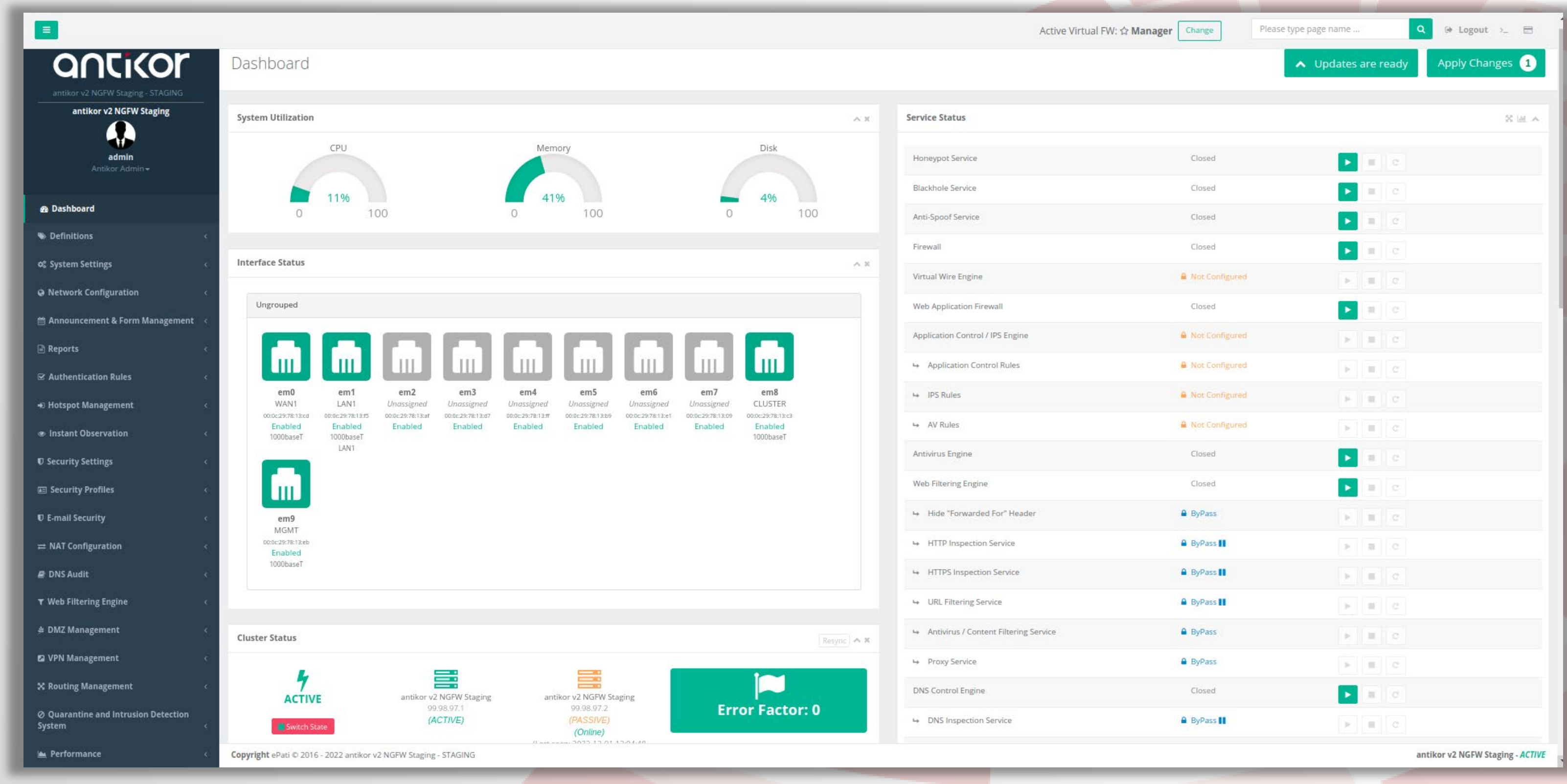
www.epati.com.tr

antikor

# Antikor v2 NGFW
# Next Generation Firewall

TRtest

COMMON CRITERIA
EAL4+





vmware

Microsoft Hyper-V

PROXMOX

epati

MEMBER OF
TURKISH CYBER SECURITY
CLUSTER

antikor

# antikor – Our Major Success Stories

PRESIDENCY OF THE REPUBLIC OF TÜRKİYE
DEFENCE INDUSTRY AGENCY

TURKISH AEROSPACE

TURKISH NAVAL FORCES

roketsan

REPUBLIC OF TÜRKİYE
MINISTRY OF HEALTH

TURKCELL

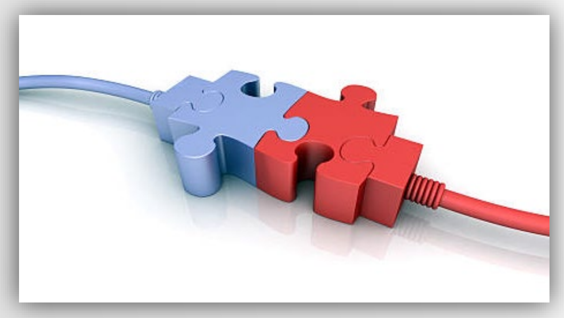
Türk Telekom

BAŞKENT ÜNİVERSİTESİ HASTANESİ

# antikor – Highlights

TRtest
ÜRÜN UYGUNLUK BELGESİ

COMMON CRITERIA
EAL4+



Virtual Wire

IPsec VTI ve TS Mode
Both Route Based and
Enc. Domain

Solarwinds Integration
Backbox Integration

Stealth Mod

Active – Passive
Cluster

Management Plane and For SSL VPN
Local, RADIUS, LDAP, AD, TACACS+,
POP3, SOAP, HTTP API + 2FA support

MEMBER OF
TURKISH CYBER SECURITY
CLUSTER

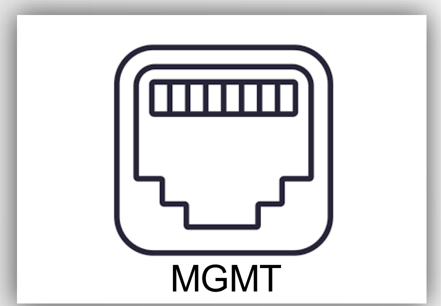
epati

antikor

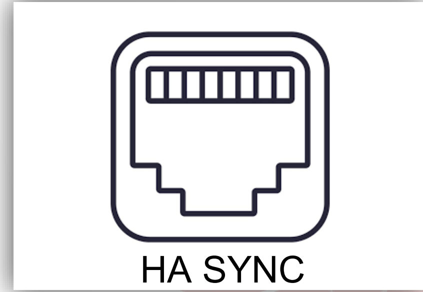
# antikor – Highlights

TRtest

COMMON CRITERIA
EAL4+

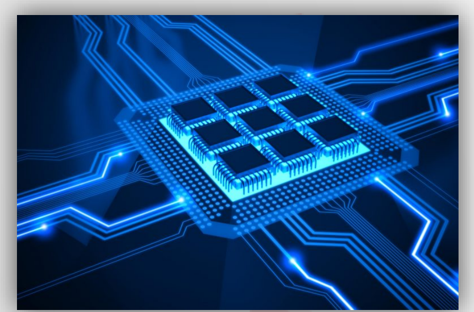



Out of Band Management



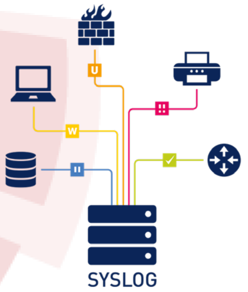

Out of Band Cluster Interface


Detailed Audit Logs with Undo Capability



Reserved Mgmt Processor Managment Interface Always Accessable Although Traffic Saturation

Online and Offline Updates No Traffic Interruption During Update



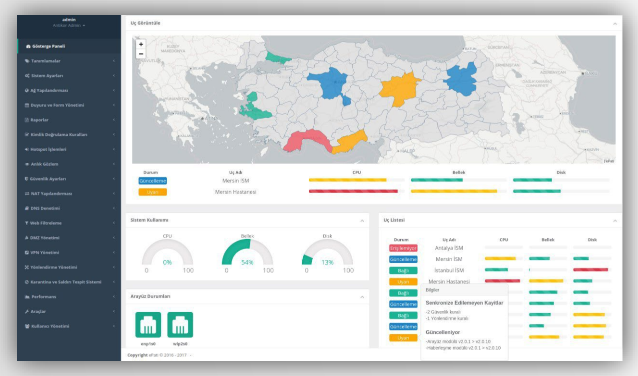

Syslog – SIEM Integration CEF, JSON, EWMM, WELF, CIM

epati

MEMBER OF TURKISH CYBER SECURITY CLUSTER

antikor

# antikor – Highlights



Central Management Support

Approval changes before the Save & Deploy stage

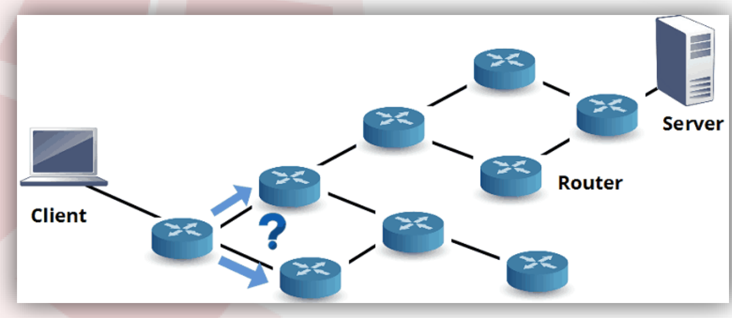
Service Based Timeouts

COMMON CRITERIA

EAL4+

Policy / Section Structure


HTTP API Support




Dynamic Routing

RIP, RIPng, OSPF, OSPFv3, BGP

epati

MEMBER OF TURKISH CYBER SECURITY CLUSTER

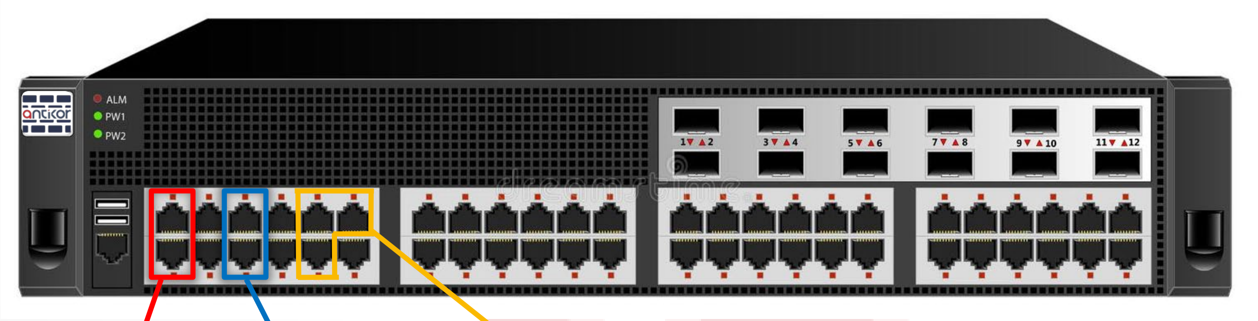
antikor

# antikor – Highlights

## Virtual FW / VDOM / Virtual System

~~To Every Customer or Every Branch~~
~~Separate Firewall Hardware~~

Logical Firewall for each Customer or Branch
in Single Firewall Hardware (Multitenancy)




1st Customer Branch
2 port

2nd Customer Branch
2 port

3rd Customer Branch
3 port

antikor Next Generation Firewall

antikor Next Generation Firewall

antikor Next Generation Firewall

TRtest ÜRÜN UYGUNLUK BELGESİ

COMMON CRITERIA EAL4+

MEMBER OF
TURKISH CYBER SECURITY
CLUSTER

epati

antikor

# antikor - Major Features

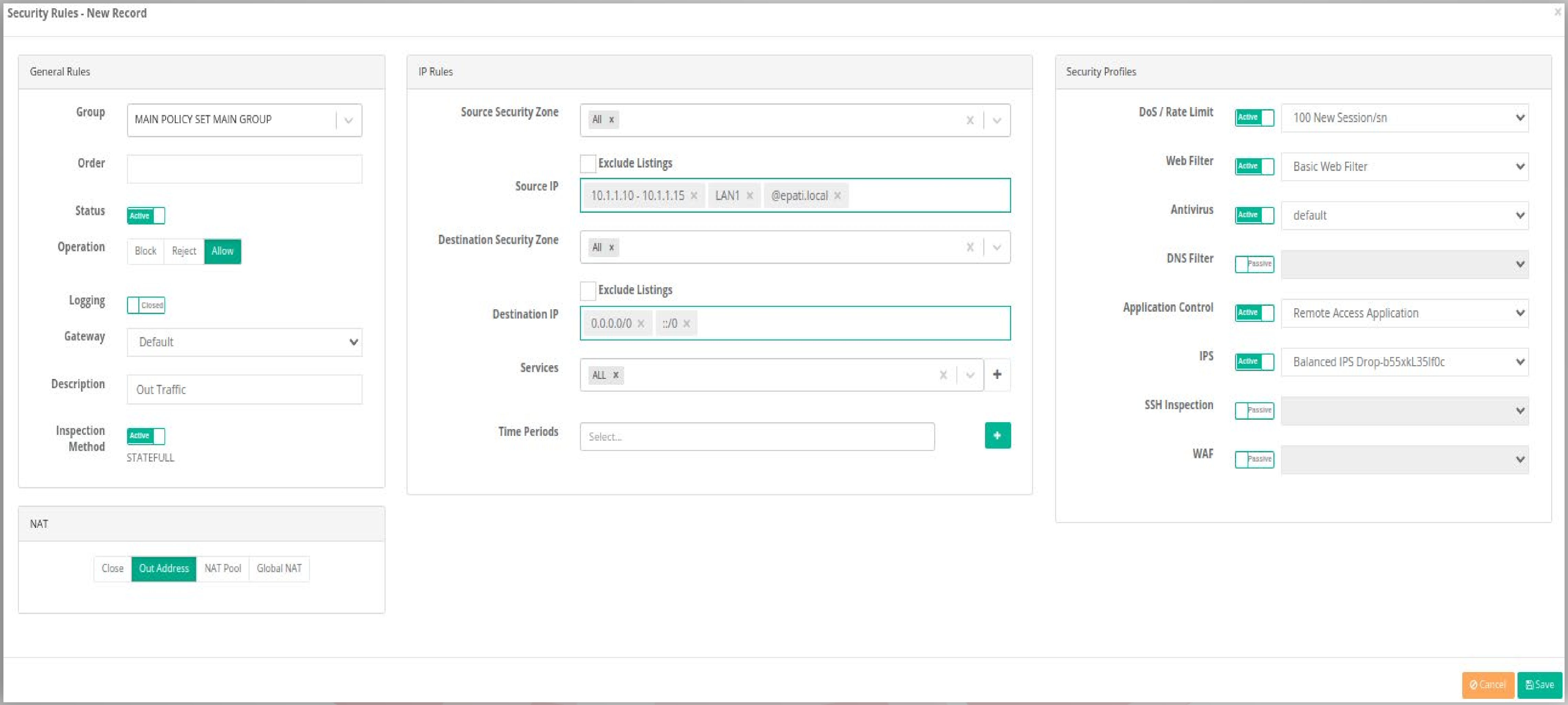
## Security Functions

- Application Security (AppID)
- Honeypot Trapping
- IPS – Intrusion Detection / Prevention System
- SPI – Statefull Package Inspection
- DPI – Deep Packet Inspection
- Deep SSH Inspection
- Deep SSL Inspection
- Web Filtering (http / https)
- DNS Query Filtering
- Flood Intrusion Prevention
- DoS Prevention
- Traffic Rate Limiting
- Anti IP Spoofing
- MAC Based Quarantine
- MAC – IP Matching Control
- ARP Poisoning Protection
- Anti Botnet
- Gateway Antivirus / Antispam

TRtest ÜRÜN UYGUNLUK BELGESİ

COMMON CRITERIA EAL4+

# antikor – Profile Based Security Management




COMMON CRITERIA
EAL4+

MEMBER OF
TURKISH CYBER SECURITY
CLUSTER

# antikor – Major Features

➢ **Services**

- DHCPv4 / v6 Server, Relay and Monitor
- Authenticated http/https Proxy
- QoS - Quality of Service
- Time and Quota based Hotspot - Captive Portal
- Active Directory, Kerberos, Mernis Integration
- LDAP, RADIUS, SMS - OTP, POP3, SOAP, JSON, XML Service Integration
- Bandwidth Monitor
- LLDP Service
- SNMP v2/v3 Service
- 5651 Logging, Syslog Export Service
- Antikor® Registration Service
- Antikor® Announcement Service
- NetFlow Export Service
- RADIUS Server ve Proxy
- Domain Based http/https Forwarding
- https SSL Offload Service
- http/https Caching / Domain Based Bandwidth Limiting
- IPsec VPN and SSL VPN
- L2TP and PPTP VPN Services
- RIP, OSPF, BGP Services
- Policy Based Routing

ÜRÜN UYGUNLUK BELGESİ TRtest

COMMON CRITERIA
EAL4+

# antikor – Rapid Migration

## ➢ Configuration Migration Script from Fortigate

Convertable Sections:

- config firewall address
- config firewall addrgrp
- config firewall ippool
- config firewall policy
- config firewall service custom
- config firewall service group
- config firewall vip
- config firewall vipgrp
- config router static
- config system dns
- config system external-resource
- config system interface
- config system ntp
- config vpn ipsec phase1-interface
- config vpn ipsec phase2-interface

FORTINET → antikor

MEMBER OF
TURKISH CYBER SECURITY
CLUSTER

epati

# Antikor CFWM

## Central NGFW Management System

---

# Antikor CLM

## Central Log Management System

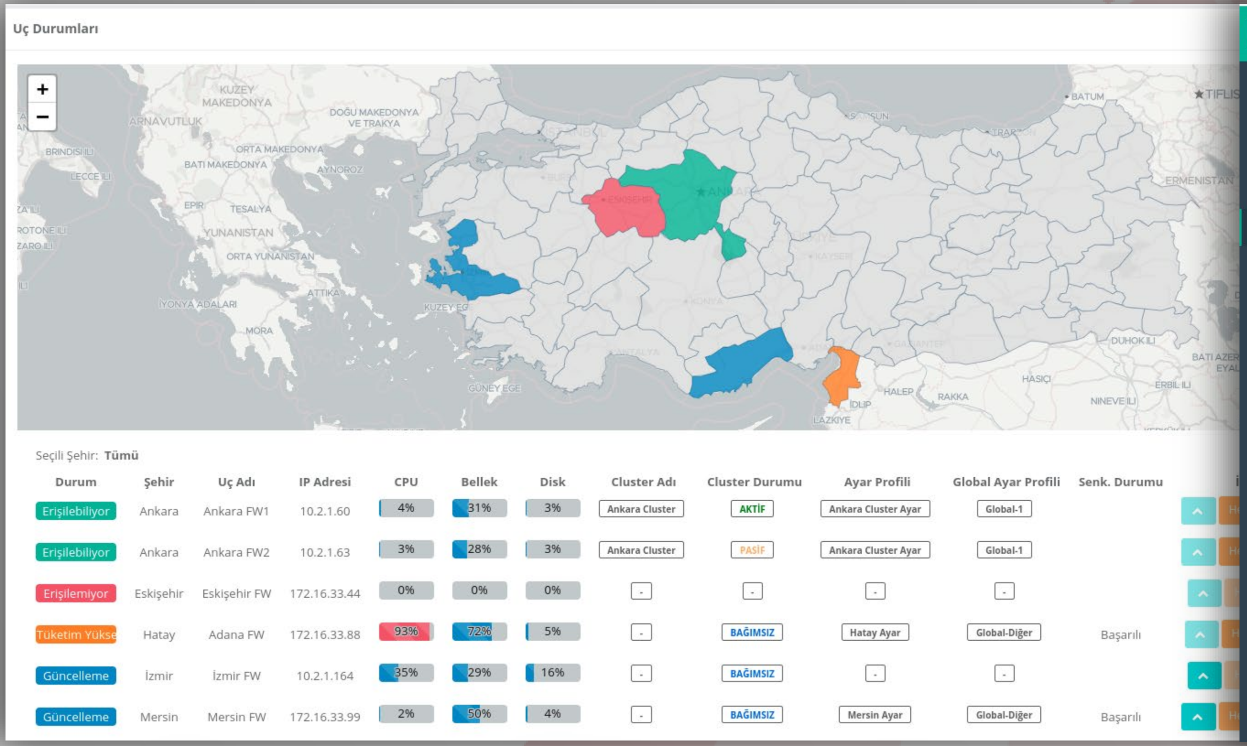

www.epati.com.tr

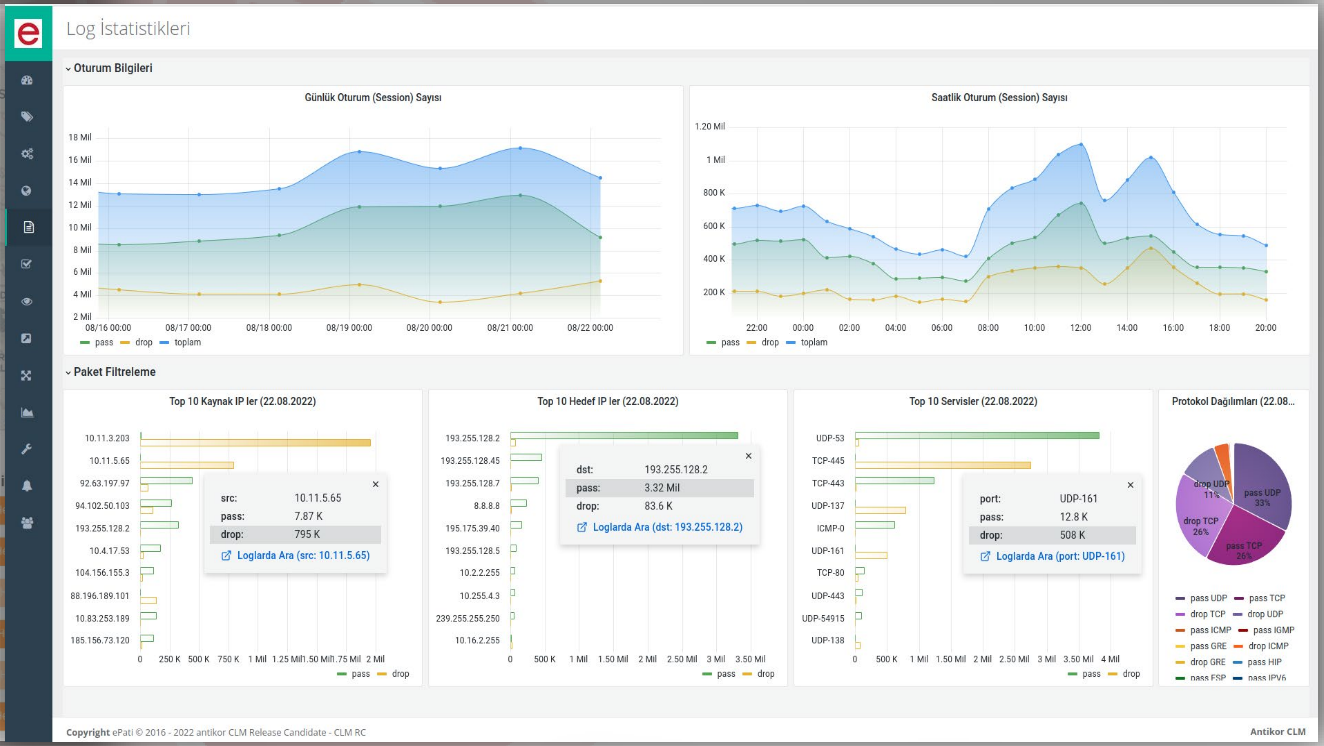
# Antikor CFWM

## Central NGFW Management

# Antikor CLM

## Central Log Management




vmware | Microsoft Hyper-V | PROXMOX | vmware | Microsoft Hyper-V | PROXMOX

epati

MEMBER OF
TURKISH CYBER SECURITY
CLUSTER

antikor

# antikor – Product Family Main Features

## Central NGFW Management (CFWM)

- Batch Policy Management
- Batch Configuration Management
- Configuration Template Management
- Update Server Service
- Detailed Authorization
- Security Policy and Object Mgmt.
- Bulk Update Deployment and Mgmt.
- Read Only Operation Support
- Tracking Alerts and Notifications
- Periodic Configuration Backup

## Central Log Managment (CLM)

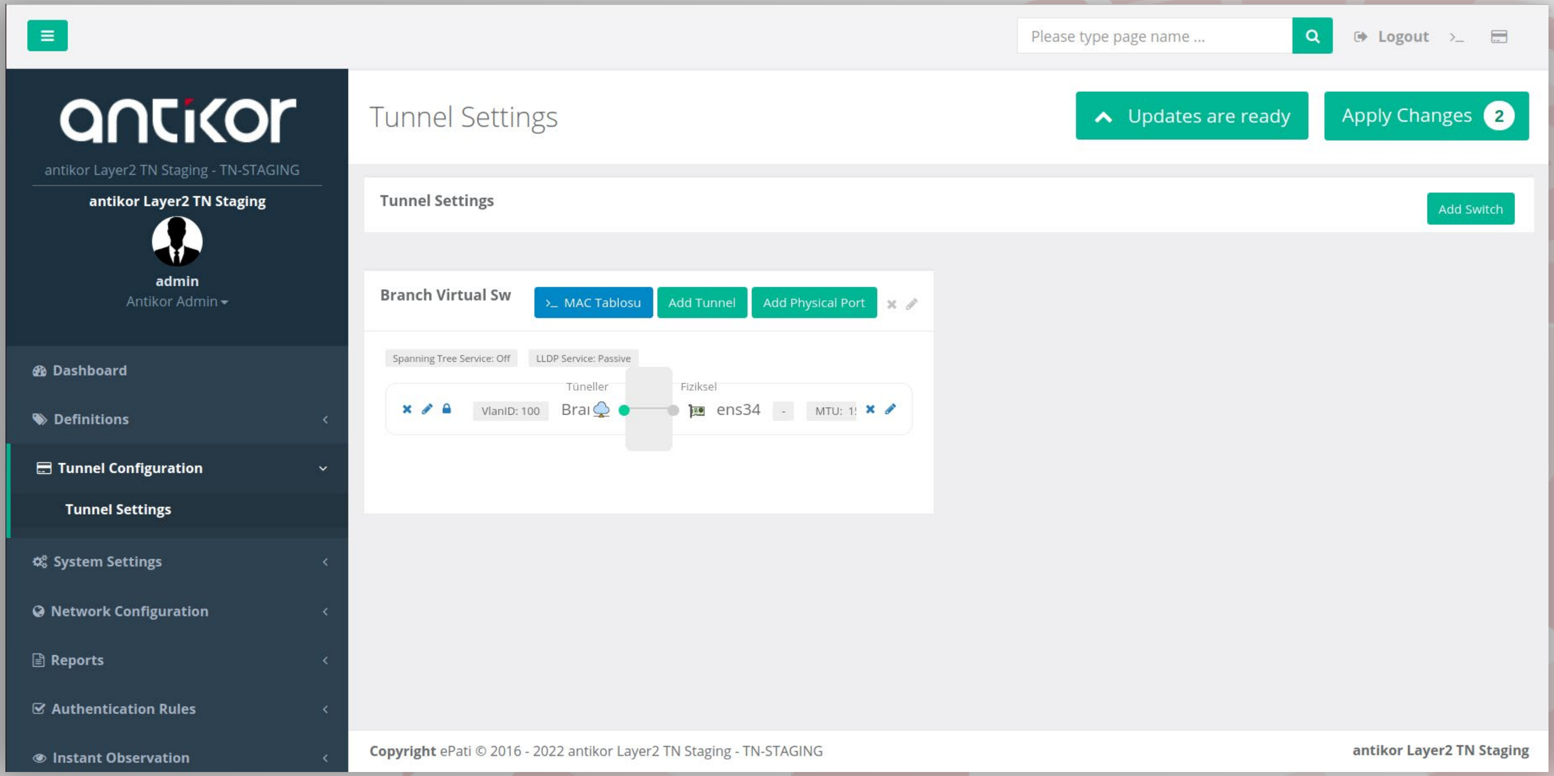
- Logging Management
- Logging Template Management
- Daily Session Count Statistics
- Hourly Session Count Statistics
- Statistics of Top 10 Destination IPs
- Statistics of Top 10 Source IPs
- Statistics of Top 10 Services
- Encrypted Transfers with SSH Tunnels
- Tracking Alerts and Notications
- Protocol Distribution Statistics

# Antikor TN

## Encrypted Dual Layer (L2 & L3) SD-WAN

www.epati.com.tr

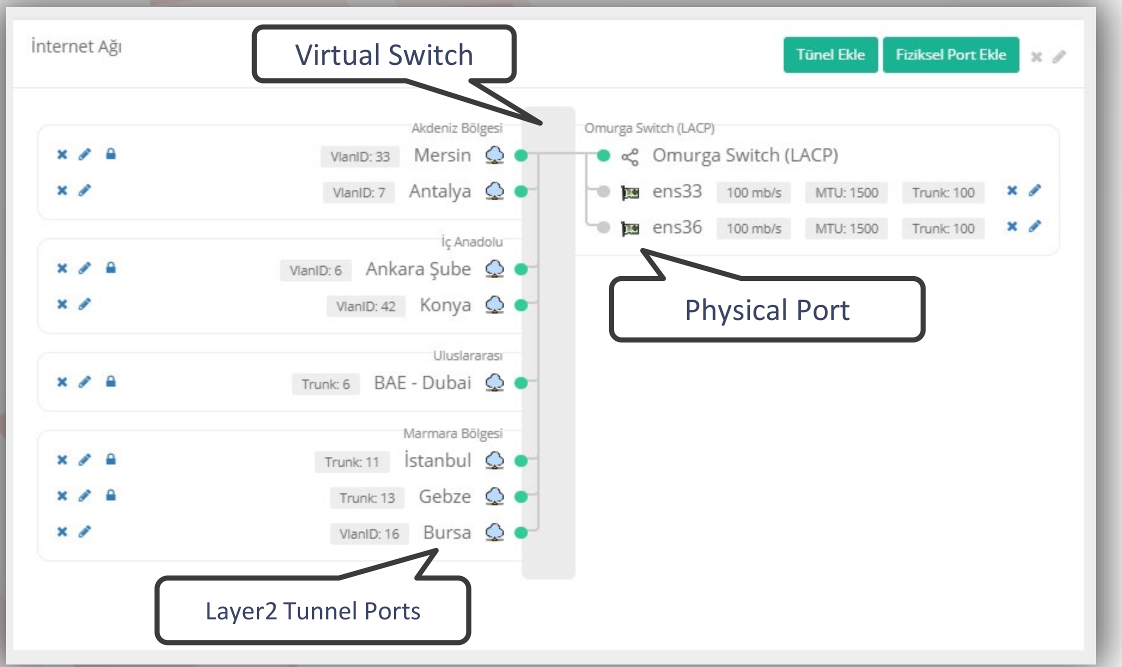
# Antikor TN Dual Layer SD-WAN




MEMBER OF
TURKISH CYBER SECURITY
CLUSTER

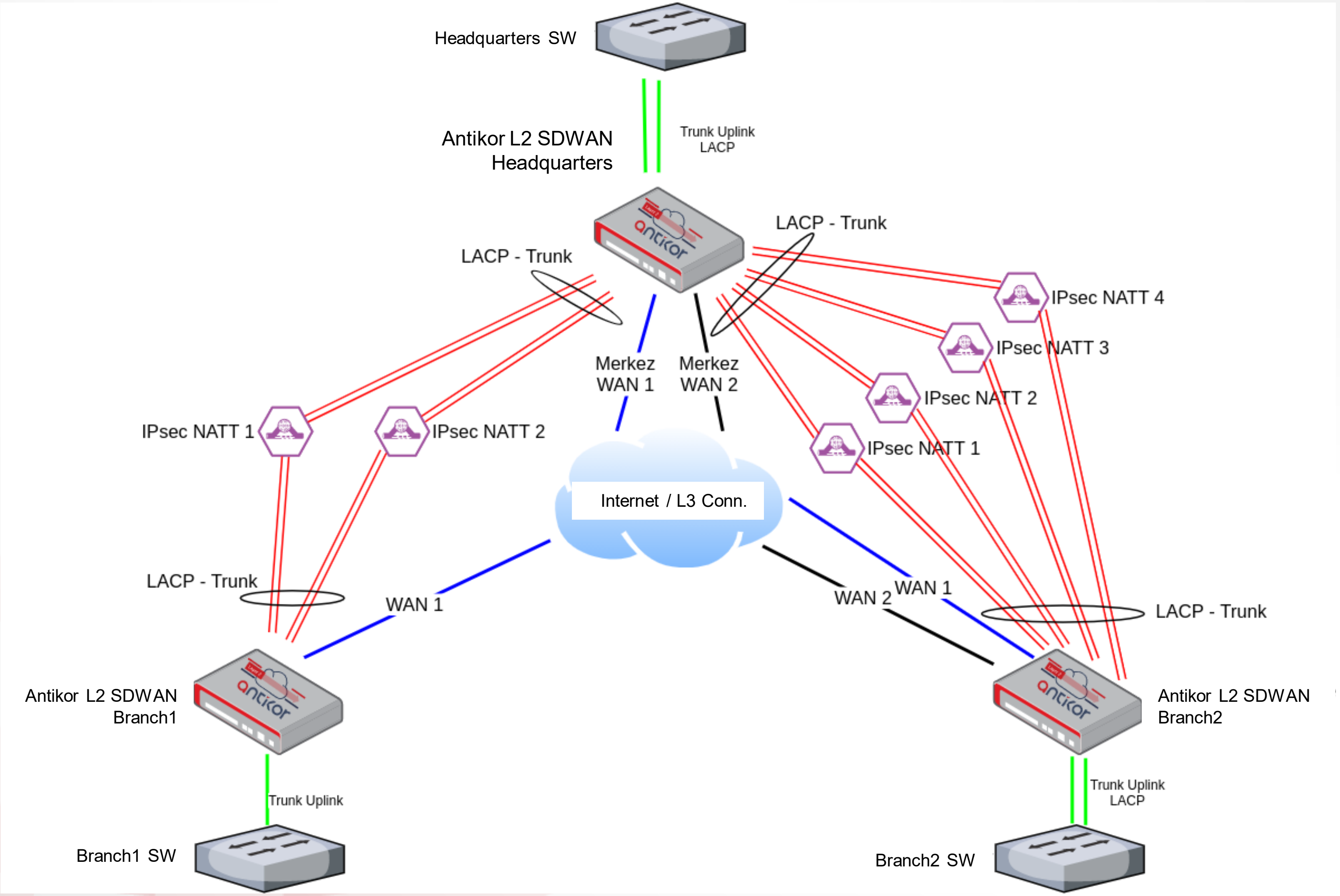
# – Dual Layer SD-WAN

- **It is now very easy to set up an Encrypted Layer2 Network between your locations!**
- **Operator independent:** You can connect all locations over IP (Internet and intranet).
- **Connection Type Freedom:** Metro Ethernet, home Fiber, xDSL, 4.5G etc. It works on all technologies.
- **No Static IP Required:** Even with dynamic IP, your locations join your network seamlessly.
- **Port Forwarding etc. No NAT Required:** You can also set up tunnels behind NAT and include your location in your network, even from shared internet.
- **Manage Wide Area Like Local Area:** You can carry an unlimited number of IEEE 802.1Q tagged VLANs. You can expand the broadcast domain, you can expand your VLANs such as Voice VLAN, LAB network between your locations.
- **Packet Filtering and QoS:** You can ensure that unwanted packets (some broadcasts, multicast, various services, etc.) are not tunneled, and you can make QoS for allowed traffic.



# – Dual Layer SD-WAN

- **WAN Bonding**
  - With WAN Bonding feature, multiple WAN connection can be aggregated.
  - You can aggregate slow links such as 4,5G/LTE and xDSL networks to gain wide bantwidths and fail-over.
  - Layer2 SD-WAN aggregations depends on LACP protocol.



# Dual Layer SD-WAN antikor – Highlights

**Automatic Registration to Controller**

**Managing Behind NAT**

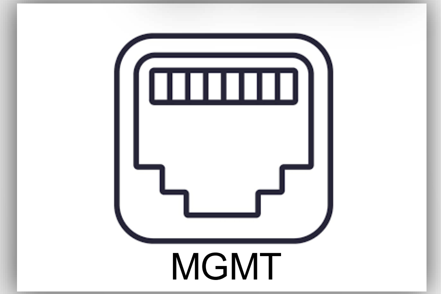
**Multi-Centric Architecture Support for Disaster Recorvery Scenario**

**Support over 1000 CPE in Same Network**

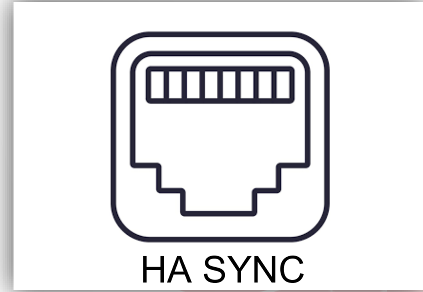
**Full BGP Support**


**4G/LTE Support & MultiWAN**

# Dual Layer SD-WAN antikor – Highlights




Out of Band Management

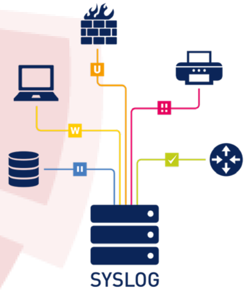



Out of Band Cluster Interface


Detailed Audit Logs with Undo Capability

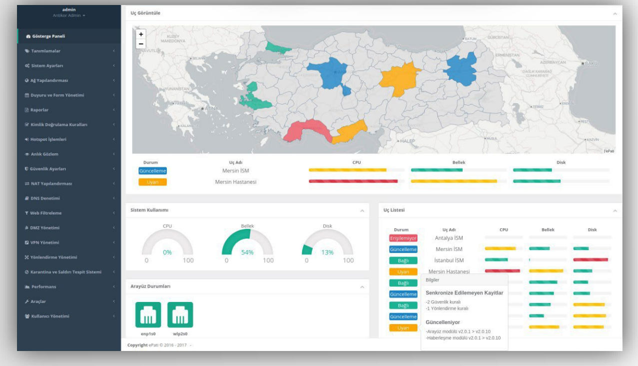
Controller is also Update Server

Online and Offline Updates
No Traffic Interruption During Update




Syslog – SIEM Integration
CEF, JSON, EWMM, WELF, CIM

# Dual Layer SD-WAN antikor – Highlights



Central Management Support

Approval changes before the Save & Deploy stage


HTTP API Support

Layer2-4 Packet Filtering

Layer2-4 QoS

Management Plane Authentication Backends: Local, RADIUS, LDAP, AD, TACACS+, POP3, SOAP, HTTP API + 2FA

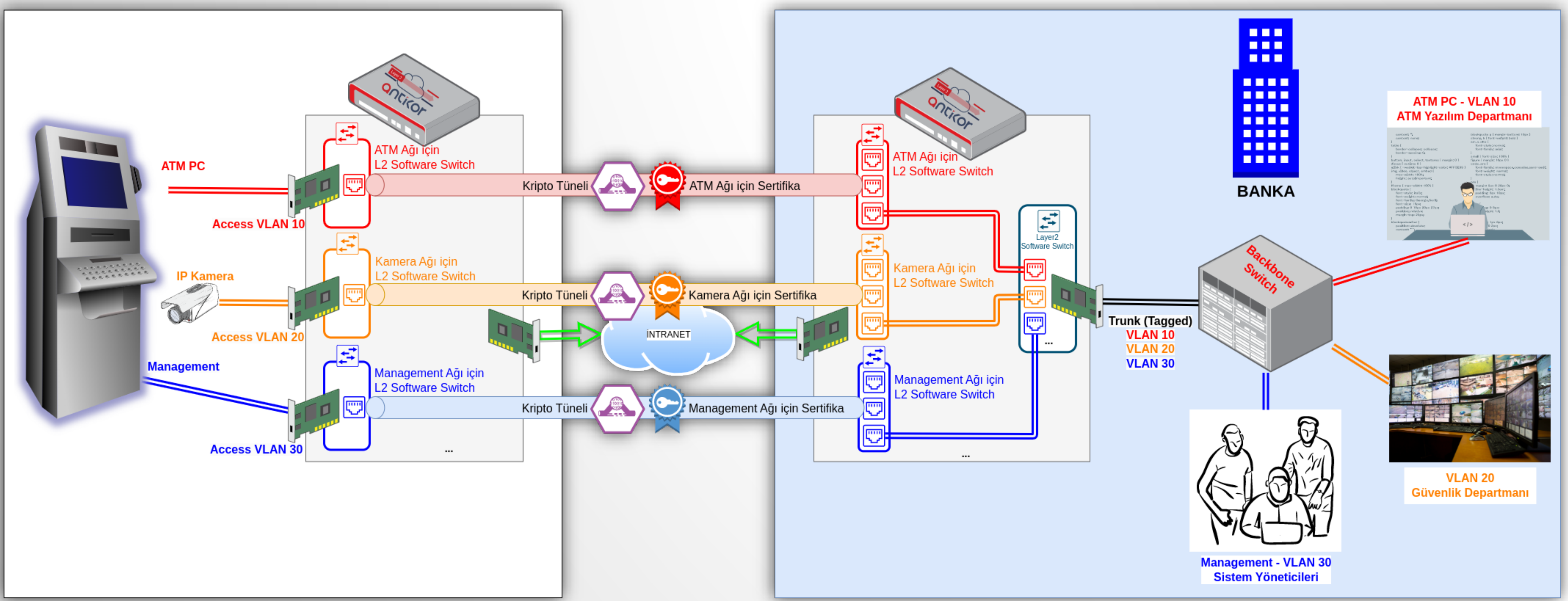
# – Encrypted Dual Layer SDWAN

## Usage Examples

- Installing Layer 2 SD-WAN on mobile vehicles to transport both Voice VLAN and Data VLAN. Applications include ambulances, etc.
- Utilizing Layer 2 SD-WAN over 4.5G for internet sharing compliant with Law No. 5651 in public transportation vehicles, with traffic routed to the central firewall. Establishing a Mernis Integrated Hotspot from the central firewall.
- Establishing a secure intranet network for organizations with international locations
- Setting up a secure intranet network for multi-location organizations requiring services from different operators.
- Connecting to the central office using multiple internet lines with bonding in locations where telecommunication infrastructure is insufficient for high-speed internet.
- Fulfilling the need for utilizing VLANs from the central office in structures like additional service buildings.
- Extending closed networks such as Research and Development labs between locations without using routers.
- Distributing isolated networks like Central Printer VLAN, Voice VLAN, Camera VLAN, etc., to all locations in multi-location setups such as municipalities.
- Securely connecting locations such as power plants, mines to the central office. Additionally, transporting IT and OT networks in isolation when required.
- Providing secure connections between branches of store/market chains.

# – Encrypted Dual Layer SDWAN

➤ **Multi-Channel Encrypted Isolated Security for ATMs**

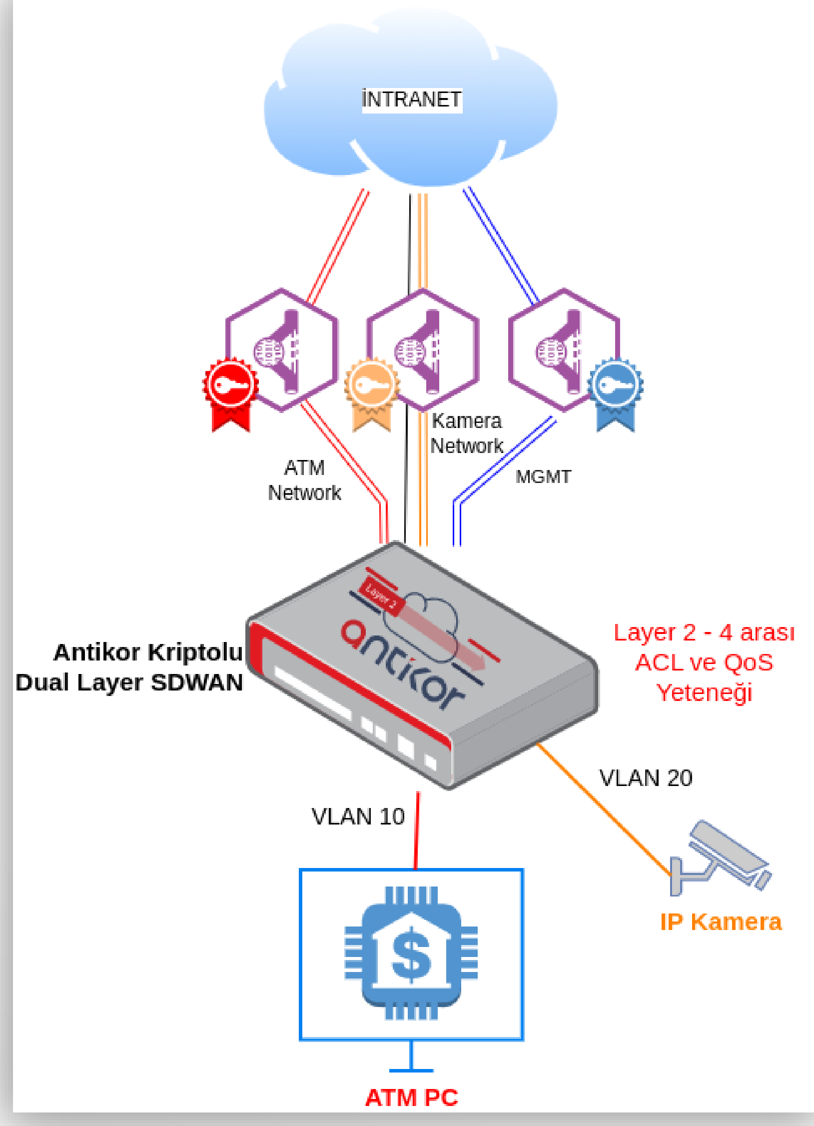


# – Encrypted Dual Layer SDWAN

## ➢ Multilayer Security for ATMs

- ➢ Transporting VLANs with Dual-Layer (Layer 2 + Layer 3) SDWAN
- ➢ Encrypting Each VLAN Separately with Multi-Channel Encryption
- ➢ Performing Both Router and Switch Functions with Multi-Layer Operation
- ➢ Isolation within the Internal Network Thanks to Different VLANs
- ➢ Access Control Management Provided by Layer 2 - 4 Access Control Lists
- ➢ Traffic Prioritization with Layer 2 - 4 QoS

- ➢ Implementing Global Policies with Centralized Management
- ➢ Distributing Updates via Centralized Management Tracking
- ➢ Accessibility of Endpoints
- ➢ Preparing Configuration in Advance for Newly Opening Locations

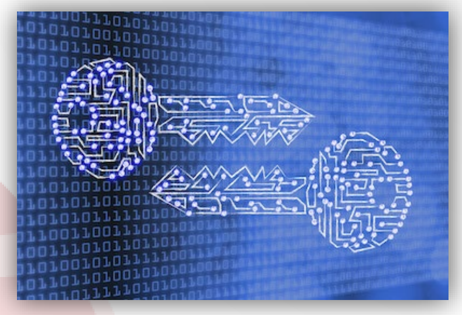


Dual Layer SD-WAN antikor

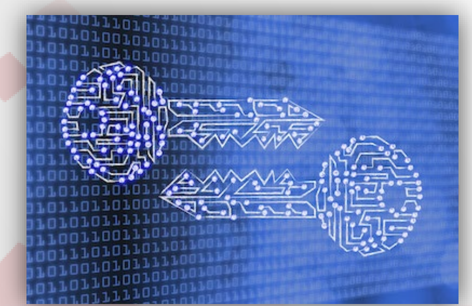
# – Strong Encryption

NIST Approved
Strong Symmetric
Encryption Algorithms

Periodic Session Re-Keying



NIST Approved
KEX (Key Exchange)
Algorithms



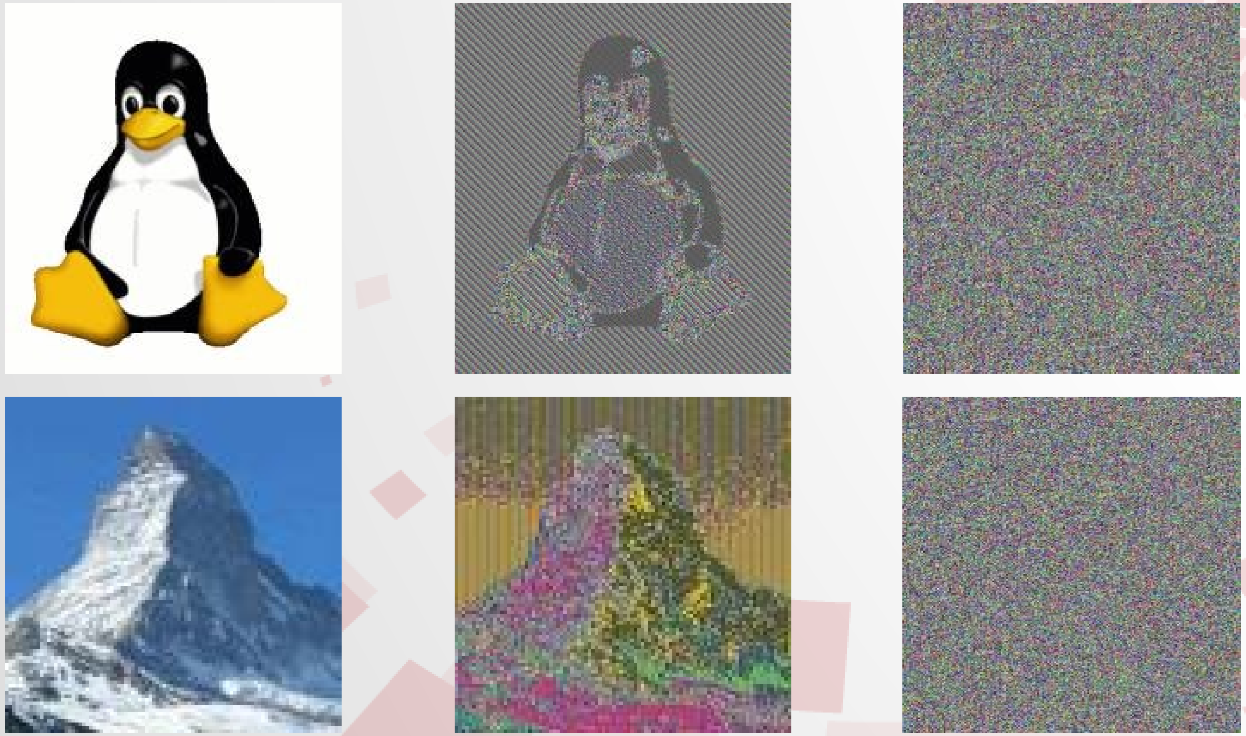
Integrated Authentication
and Integrity Checks

High Performance
(AES-NI, QAT)

# – Strong Encryption

## ➢ Is Block Cipher Really Secure?

Orginal Data | Block Cipher | Counter Mod Block Cipher

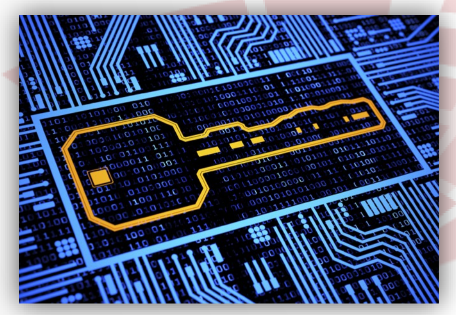


- The methods used to encrypt network traffic is very important.
- The risk of predictability of the data increases when the encrypted data generated from a package with the same pattern is the same as the previous one.
- As shown in the figure, Counter Mod Block Cipher is safer even same data encrypted.

# – Strong Encryption

- **AES256-GCM16**

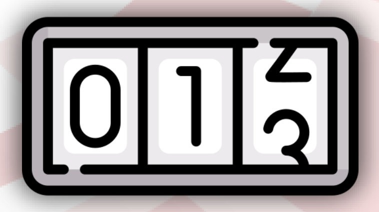
AEAD
Authenticated Encryption
Authenticated Decryption



256 bit Key

128 bit Initalization Vector

Integrated Authentication and Integrity Check



Native Counter Mode Support

# – Crypto Security

ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/

Product Use Cases Developers Company Pricing Log In Start for Fr

## Resistance to Quantum Computing

The threat of quantum computing to cryptography has been well-publicized. Quantum computers work very differently than classical ones, and quantum algorithms can make attacks against cryptography much more efficient.

In the case of asymmetric encryption algorithms (like RSA), quantum computing completely breaks them. However, for symmetric algorithms like AES, Grover's algorithm – the best known algorithm for attacking these encryption algorithms – only weakens them. Grover's algorithm decreases the effective key length of a symmetric encryption algorithm by half, so AES-128 has an effective key space of 2^64 and AES-256 has an effective key space of 2^128.

However, while this seems significant, it doesn't break either algorithm. With the right quantum computer, AES-128 would take about 2.61*10^12 years to crack, while AES-256 would take 2.29*10^32 years. For reference, the universe is currently about 1.38×10^10 years old, so cracking AES-128 with a quantum computer would take about 200 times longer than the universe has existed.

antikor

Unified Cyber Security System

# Thank You

epati

ePati Cyber Security

www.epati.com.tr