JUP1TER
cloud . hybrid · datacenter

XEKURI
Complete Cyber Security Platform

INTRODUCING JUPITER

Jupiter is a manage services provider with focus on data protection, data safety, data storage, colocation and cyber security also provide services such as dedicated servers, cloud computing, private rack, private cage, fast content delivery (CDN), live streaming delivery (LSDN) and connectivity for cloud providers at affordable, reliable and good quality.

XEKURI

XEKURI is an complete cyber security platform provides an all-inclusive security solution for users concerned about mail and website security.

TYPES OF DDOS ATTACK BLOCKED

- TCP SYN Floods
- TCP FIN Floods
- TCP RST Floods
- HTTP GET Floods
- HTTP Post Floods
- HTTP XMLRPC PingBack attacks
- TCP Fragment attacks
- Slowloris
- TCP Syn Spoofed
- ICMP Floods
- HTTP HEAD Floods
- Brute Force
- TCP Ack Floods
- Ping of Death
- DNS NXDomain Floods
- HTTP Cache Control
- HTTP SSL Saturation
- Amplified DNS DDoS
- RUDY
- Smurf
- As well as other attacks

FEATURES

WEB APPLICATION FIREWALL
XEKURI blocks all kinds of web attacks accurately and quickly with the industry-leading logic based analysis detection technology.

DDOS PROTECTION
XEKURI mitigates and blocks DDoS attacks which attempt to exhaust resources and make websites inaccessible. Our advanced DDoS solution protects against the most common one to sophisticated multi-vector and application layer attacks such as Slowloris and R-U-Dead-Yet? (RUDY).

SSL CERTIFICATE
Besides detecting and blocking malicious traffic, XEKURI also provides free SSL certificates that encrypt communication between all visitors and the web server.

ADDITIONAL MAIL PROTECTION
Our solution has been extensively assessed on vulnerabilities and overall security architecture. The conclusion: XEKURI provides a secure email platform to customers. All email communication is performed over GDPR-compliant secure channels.

CLOUD & ON-PREMISE
XEKURI provides cloud and on-premise solutions to protect layer 3, 4 and 7.

PT. Jupiter Jala Arta
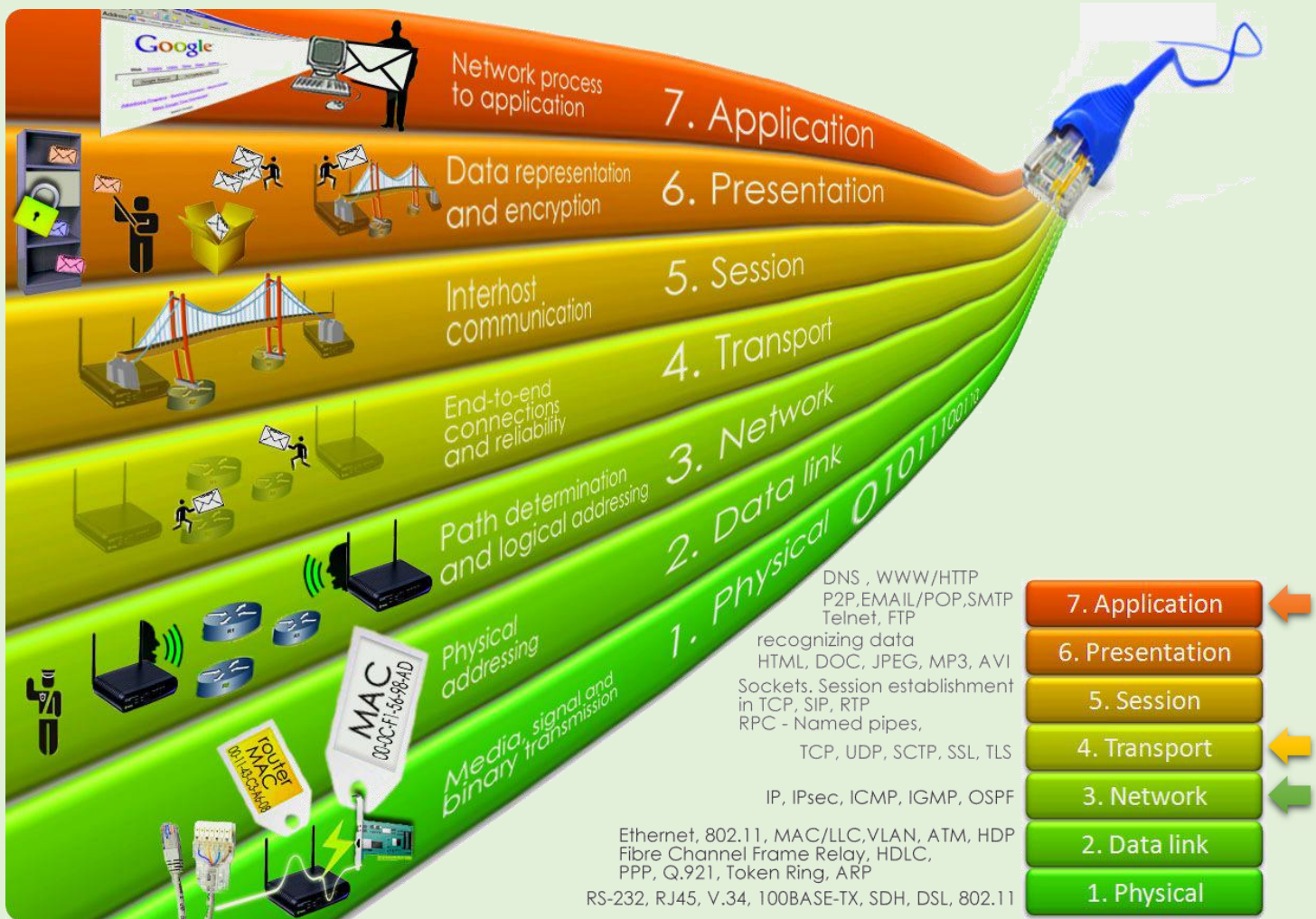Cyber One Building 10^h Floor
Jl. Kuningan Barat No.8,
Jakarta 12710 - INDONESIA
Telp: 6221 5084 7774 | WA: 62 8229 8888 475
sales@jupiter.co.id | www.jupiter.co.id

OSI Model layers:

Network process to application	7. Application
Data representation and encryption	6. Presentation
Interhost communication	5. Session
End-to-end connections and reliability	4. Transport
Path determination and logical addressing	3. Network
Physical addressing	2. Data link
Media, signal and binary transmission	1. Physical

DNS, WWW/HTTP P2P,EMAIL/POP,SMTP Telnet, FTP — 7. Application

recognizing data HTML, DOC, JPEG, MP3, AVI — 6. Presentation

Sockets. Session establishment in TCP, SIP, RTP RPC - Named pipes, — 5. Session

TCP, UDP, SCTP, SSL, TLS — 4. Transport

IP, IPsec, ICMP, IGMP, OSPF — 3. Network

Ethernet, 802.11, MAC/LLC,VLAN, ATM, HDP Fibre Channel Frame Relay, HDLC, PPP, Q.921, Token Ring, ARP — 2. Data link

RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11 — 1. Physical

ONLINE PAYMENT COMPLIANCE

Data leaks for small businesses result in heavy financial losses. With sensitive information being exchanged online, it's important that consumers' personal and financial information is well protected.

As such, all websites with a credit card payment module are required to comply with PCI-DSS 6.6 standards. XEKURI can help website owners become PCI-DSS compliant.

OWASP VULNERABILITIES

XEKURI protects against the top ten vulnerabilities identified by OWASP. To do this, we use 26 rules which allow our cloud WAF to detect and accurately block web attacks with low false positives.

PCI DSS COMPLIANT

OWASP
Open Web Application
Security Project

XEKURI
cyber security platform