
Labris
NETWORKS
Close Security in
Cyber War
Labrispeed
Labrisupportive
Labrisage
Labrisafe

Labris NETWORKS

Labris UTM Series

Next Generation Firewall

Labris UTM Series next generation network security appliances provide you with integrated security against internet-based threats that are developing and becoming more complex day by day, while also meeting your legal obligations under log recording law.

The advanced technology used in the Labris UTM product family has been developed in Cyber Warfare Lab by a creative team that knows the risks and requirements. Labris also promises you a solution partnership (CSS-Close Security Support) as well as offering technological features.

Labris UTM series products have logging, reporting and instant monitoring capabilities. UTM series products have internal log areas. The logs collected on the appliances also offer a graphical, fast analysis tool that administrative managers can easily understand with the integrated reporting module integrated with the appliances, including visual analysis of your current traffic in real time.

Next-Generation Firewall
New generation firewall can control packet content, source-target and user behavior without sacrificing performance. It can offer features such as Firewall, IPSec VPN, SSL VPN, Intrusion Detection and Prevention (IDS/IPS), application recognition and control, virus / malicious content control, URL category checking, content filtering and bandwidth management.

Labris NETWORKS

Hotspot Module

Labris WAUTH+

Labris WAUTH+
Labris WAUTH+; It is different from the hotspot solutions in the market and considers this as a part of security and offers flexible and comprehensive solutions that can be integrated into all kinds of internet networks, according to user type and user authorization scenario.

It provides Web-based management with Turkish and English interface support, many features such as logging in accordance with legal obligations and e-signature laws, SMS and manual user registration, user authorization option with Active Directory integration, authorization from L3 remote points such as IPSec, MPLS.

Commercial Lawful Interception, Labris LOG
Labris LOG presents the infrastructure that will enable you to fulfill your legal obligations with high-level technology and security knowledge, and considers logging as an important building block of your security. With WAUTH, an integrated and easy-to-manage authorization (HotSpot) solution, it authorizes mobile or guest users that may create important security vulnerabilities. With its powerful reporting infrastructure, Labris LOG can provide detailed reports about what's going on in your network, and it provides the opportunity to closely monitor network traffic with its instant monitoring screen.

Labris NETWORKS

HARPP DDoS Mitigator

DDI™ (Deep DDoS Inspection) Technology

The unique DDI™ (Deep DDoS Inspection) technology of Harpp DDoS Mitigator appliances is designed as an intelligent shield against dynamic and complex DDoS attacks at the Advanced Persistent Threat (APT) level. The state-of-the-art DDoS Attack Protection Functions of the appliance provide high-level protection to your DNS and Web infrastructure with normalization, blocking and protocol-specific attack mitigation methods. In addition, priority protection functions always work proactively day and night. Harpp DDoS Mitigator appliances around the world create a vast real-time security intelligence network that is instantly accessible. The most important feature of Harpp DDoS Mitigator appliances is its manageable and adjustable structure in desired detail.

Defense
Harpp DDoS Mitigator appliances ensure that your network and business are safe against DDoS attacks that threaten your business continuity and online presence. The appliance's state-of-the-art DDoS Attack Protection Functions provide high-level protection to your DNS and Web infrastructure with normalization, blocking and protocol-specific security methods.

Management and Reporting
In a cleverly designed complex DDoS attack, a control panel that will graphically visualize the dynamic attack characteristic is vital. Thanks to the unique AVS™ (Attack Visualization System), you will find the most critical information graphically in front of your eyes at the time of attack and you will be able to quickly implement the most accurate steps.

Labris NETWORKS

DDOS CERT

Harpp DDoS CERT

Harpp DDOS CERT is a specialized cyber security operation (CERT) service designed to provide comprehensive protection against DDoS attacks. As Distributed Denial of Service (DDoS) attacks become increasingly common and sophisticated, Labris SoC and Harpp DDoS CERT offers a powerful defense solution for businesses and organizations seeking to protect their online operations. With its advanced technology and expert team of security professionals, DDoS CERT delivers round-the-clock monitoring and analysis, quick detection of potential threats, and proactive measures to prevent and mitigate attacks. By choosing DDoS CERT, clients can enjoy the peace of mind that comes with knowing that their online operations are protected by a top-tier security service.

Mitigating DDoS attacks requires a deep understanding of network infrastructure and security protocols, as well as knowledge of the latest attack techniques and trends. Technical expertise is critical in successfully detecting and responding to DDoS attacks, as it enables the security team to quickly identify the source of the attack, evaluate its severity, and determine the most effective countermeasures. Without technical expertise, organizations may struggle to respond to DDoS attacks effectively, leaving them vulnerable to prolonged downtime and reputational damage. In addition, technical expertise is crucial in developing and implementing proactive security measures to prevent future attacks. The security experts at Harpp DDoS CERT and Labris SoC possess the technical knowledge and experience necessary to handle any DDoS attack, from simple to complex, and provide clients with the best possible protection against cyber threats.

cyber warfare lab

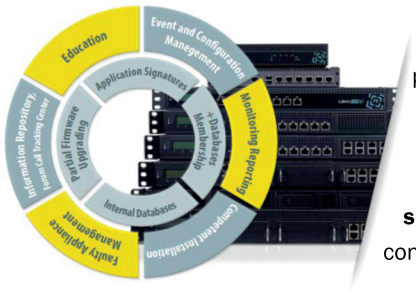
Cyber Warfare Lab (CWL)

In order to overcome threats, we need to constantly improve ourselves, keep our knowledge up to date, and take precautionary measures. We have to act faster and earlier than the enemy, and to eliminate dangers by thinking like him. In "Cyber Warfare Lab", we develop the most important analysis and decision components of cyber defense tools by following other cyber threats and spreads in the world. Our aim is to progress developments and take precautions and prevent being caught unprepared for threats. World's one of the first anti DDoS product, Harpp DDoS Mitigator, was developed by an expert team with DDoS and Anti-DDoS expertise, especially on the points where attackers threaten institutions or states with DDoS attacks over the internet.

Close Security Support

Close Security Support (CSS)

The CSS service of Labris Networks is the closest, fastest and solution-oriented support in the industry, shaped according to your needs with different SLA levels, directly provided by the vendor. Web, telephone or direct support channel alternatives and CSS service are offered with the difference of fast response and quick solution.



Please review your Labris Support Services Datasheet for the appropriate SLA packages that you can obtain with your product.

You can contact us by using **support@labrisnetworks.com** contact information for the most suitable life cycle for your product and operation.

Labris NETWORKS

Close Security in Cyber War

info@labrisnetworks.com
www.labrisnetworks.com

7 · 24 · 365
GLOBAL SUPPORT