UTM UR-915

ShareTech

In addition to high network speed, a business needs collective and profound security protection as well. ShareTech UR-915 is a multi-functional firewall that processes of speed and safety. Besides firewall, it provides security features such as Anti-Virus, Anti-Spam, IDP, BOTNET Defense, Qos, User-Definable Networks, anomalous IP analysis, Co-Defense, Application Access Control, ARP Spoofing Defense, Switch management, Load Balance, Content Filtering, CMS, IPSec VPN , etc. UR-915 fits companies ranging from small branch offices to middle businesses; it is an appliance that makes security simple and profound to companies yet highly effective at the time.

Features

Firewall

UR-915 SPI (Stateful Packet Inspection) provides DoS detection and prevention against some popular attack modes, such as SYN flooding, port scans, and packet injection. When the unusually high rates of new connection are detected, the system will issue an alert notification or block anomalous session. In addition, UR-915 SPI protects against packet-injection attacks by checking several components of TCP and UDP sessions.

IP V4 / V6 Dual Mode

IPv4 address exhaustion has occurred sooner than being predicted. To cope with IPv4 depletion, UR-915 provides a solution that covers both IPv4 and IPv6 network and can be configured for IPv4 only, IPv6 only, or to support both protocols simultaneously. Also, UR-915 has been certificated with “IPv6 Ready” logo by the IPv6 forum.

Virus Protection

UR-915 offers Clam AV for virus scanning which can detect over 800,000 kinds of viruses, worms, and Trojans. Its utilities include a command line scanner, automatic database updater and a scalable multi-threaded daemon, running on an anti-virus engine from a shared library. ShareTech UR-915 can be configured as a proxy for SMTP and POP3 servers. Once suspicious emails are detected, the administrator can decide to delete or block them. Moreover, virus scanning is offered for website and FTP so that all the packages will be scanned once the function of anti-virus is enabled in policy.

Spam Protection

UR-915 employs 6 solutions: Fingerprinting, Bayesian Filtering, ST-PIC multi-dimensional; graphics pattern recognition, Auto learning, personal Blacklist/ Whitelist and Spam characteristics filtering. The functions help industries to update the latest spam and create their own database. In addition, the actions to the spam mails could be deleted, quarantined, and non-filtered. Spam-filtering mechanism serves as the defense line to blocks 95% spam.

Intrusion Detection and Prevention (IDP)

Built-in IDP (IDS+IPS) inspects the packets from OSI layer 4 (transport layer) to OSI layer 7 (application layer) by using Deep Packet Inspection (DPI), and block concealed malicious code, such as worms and buffer overflow attacks. As soon as an attack is suspected, UR-915 will immediately notify the IT administrator. Moreover, integrated IDP system with automatic attack-signature database updates capability.

BotNet Co-Defense

The detecting appliance can explicitly point out which is the real attack running hidden while internal users mailing spam through the mail server. Though BotNet is blocked, the malicious computer keeps infecting ordinary users' computers. To ensure CPU recourse not being wasted on the same matter, administrator can enable BotNet Co-Defense and directly shut down switch port of infected computers. It not only saves resources but also suspense malicious software spreading in the internal network.

ARP Spoofing Defense

It has been the most difficult for UTM to detect broadcast package sent out on the local network such as ARP spoofing and private DHCP server because of congenital defects of communication protocols. UR-915 detecting appliances can effectively defect who is the man-in-the-middle attack. With a Co-defense switch, physical IP destination can be marked.

Anomaly IP Analysis

UR-915 provides the excellent function of anomaly traffic detection because the appliances can detect outgoing/ incoming concurrent sessions, upload flow and download flow. If employee are violating the rules and exceeding more downloading flow, they will be logged and blocked. In addition, IT administrator is allowed to define the trusted IP list. If an IP address is added to the trusted IP list, then it will not be detected, and the selected action will not be implemented to that IP address as well.

Co-Defense SNMP

An advanced protection of UTM, CO-Defense SNMP, is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. When anomalous flow occurs, it will be blocked and the administrator will be notified and assisted to this abnormal situation. Defects can be known on which computer and which switch port at the earliest possible time which prevents business network from failure. UR-915 Co-Defense makes network management fairly easy because it does not need any change from network structure, habits of individual user, buying expensive Switch (with Layer 2), and extra detecting appliances.

Content Filtering

IT administrator can remove specific undesirable objects from HTTP traffic, such as ActiveX objects or Java applets that may pose a security threat in certain situations. In addition, UR-915 will block vicious websites which may cause damage to PCs according to the Black-list. IT administrator can also add both keywords and URLs of specified websites or webpages to Blacklist and Whitelist.

URL database

The database collect almost 10, 000, 00 URLs and updates every period of time without additional charge. All these URLs and their contents were analyzed and classified into 12 categories, including Aggressive, Audio-Video, Drugs, Gambling, Hacking, Porn, Proxy, Redirector, Spyware, Suspect, Violence, and Warez. To ensure regulatory compliance, IT administrator is able to block any category in the database.

Load Balance

UR-915 provides outbound load balancing, which distribute the traffic across available links. When one of the links is down, the other link will take over the work and handle the traffic until troubled link returns to normal, in manual or auto mode.

QoS

UR-915 provides Smart QoS solution, offering more agile bandwidth management for industries and organizations. All the servers and users can be configured their minimum and maximum bandwidth; the remaining bandwidth will be allotted to the other users according to their configuration.

Application Access Control

To prevent data leakage and ensure regulatory compliance, the access to applications which unrelated to work should be controlled during working hours. UR-915 can block file sharing via P2P applications in addition to IM access controls, preventing data leakage and helping organizations and industries meet the requirements of regulatory compliance.

Authentication

In most industries and organizations, internet access control is indispensible for defending network security. UR-915 offers the best security protection that manages and controls users who try to access internet. When a user first opens a web browser and begins to access an internet site they will be prompted to authenticate before using internet service. UR-915 offers two authentication methods: Active Directive (AD), and POP3.

VPN

VPN, Virtual Private Network, supplies private connectivity over public lines. Deploying VPNs enables businesses of any size to deliver secured connectivity for mobile employees, branch offices, and clients.

PSec VPN

IPsec VPN securing the site-to-site connections allows the head quarter and its branch offices on the same network and sharing resources among offices. For industries, IPSec is the best way to connect for transmitting encrypted data over the network.

PTP VPN

PPTP VPN offers point to point connection for employee at home. PPTP VPN enables employee get access to industry's network securely and easily.

CMS

CMS (Central Management System) provides a useful management and monitoring solution, which allows industries to manage distributed appliances installation across remote offices and clients.

Diagnostic Tool

UR-915 provides diagnostic tools that help IT administrator find out network problem without wasting time, including Ping, Traceroute, DNS Query, Server link, etc.

Lan Bypass

It is a fault-tolerance feature that protects your essential communications in the event of power outage. WAN1 and LAN1 ports will be bridged together when the power runs out. When used with Drop-in Mode, such failure would be completely transparent to the network. Therefore, the network connectivity is fully protected.

Technical Specification

- Interface
  2WAN / 1LAN / 1DMZ
- Memory
  1G
- System Management
  HTTP/ HTTPS
- Envirement
  Storage Tempe: 0℃ ~ 45℃
  Humidity: -20% ~ 70% RH
- User Limit
  Unlimited
- Form Factor
  1Urack-mountble
- Network Speed
  10/100 /1000Mbps
- Power
  100V~240V / 60W
- Certification
  FCC/ CE
- Packing Dimensions
  44mm(H)×430mm(W)×255mm(D)
- Corporation Size
  50~75 clients
- Hard Disk
  160G