Bgtech
Soluzioni Innovative srl

wiface

WiFace

Security Enty Level

UTM Firewall

Ideale per piccole aziende o Uffici fino a 10 postazioni o Laboratori Scolastici fino a 20 postazioni con Content Filter, Antivirus Perimetrale e Autenticazione sulla Rete Internet

Codice Mepa: Wifacefi001 per Firewall con 4 Porte RJ45 personalizzabili

Codice Mepa: Wiface002 per Firewall con 6 Porte RJ45 personalizzabili

Prodotto: Firewall Entry Level Layer7

Caratteristiche Tecniche

Misure: 126 x 134 x 41 mm (Ultra Compatto)

Processore: Quadcore Intel J1900

Ram: 4 Gb SoDIMM

Hard Disk: Solid State Disk da 64 GB

Temperatura di Lavoro : -10° a + 60°

Porte : 2 USB (nr. 1 2.0 + nr. 1 3.0)

Connettività: 4 Schede di rete LAN Intel I211 Configurabili WAN/LAN + Supporto WI-FI
(oppure 6 Schede LAN configurabili per la versione da 6 Porte)

Video : HDMI e VGA
VGA (per la versione 6 Porte);

Alimentazione DC 12 Volt Incluso

FUNZIONALITA' SISTEMA OPERATIVO

Sistema Accessibile tramite interfaccia WEB

Funzionalità del Software configurabile

- Bilanciamento e Failover di connessioni multiple a Internet;
- Connessioni UMTS/HSDPA mediante modem 3G connesso ad una porta LAN
- Server RADIUS per fornire autenticazione e gestione automatica delle chiavi di cifratura alle reti Wireless 802.11b, 802.11g e 802.11a supportando il protocollo 802.1x nella forma EAP-TLS, EAP-TTLS e PEAP; sono supportate le modalità WPA con TKIP e WPA2 con CCMP conforme allo standard 802.11i; il server RADIUS può inoltre, in base allo username, il gruppo di appartenenza o MAC Address del supplicant smistare l'accesso su di una VLAN 802.1Q assegnata ad un SSID;
- Captive Portal per il supporto del web login su reti wireless e wired. Il sistema agisce da gateway per la rete su cui è attivo il Captive Portal e su cui gli indirizzi IP (di solito appartenenti a classi private) vengono forniti dinamicamente dal DHCP. Un client che accede a questa network privata deve autenticarsi mediante un web browser con username e password Kerberos 5 prima che il firewall di gli permetta di accedere alla LAN pubblica.
- Gestione Username e Password di accesso secondo la profilazione per Banda, Traffico, Ora o tariffa a consumo secondo le esigenze con stampa dei voucer

- Gestione del QoS (Quality of Service) e traffic shaping per il controllo del traffico su reti congestionate. Si possono imporre vincoli sulla banda minima garantita, sulla banda massima e sulla priorità di un pacchetto (utile nelle connessioni realtime come le VoIP). Tali vincoli potranno essere applicati sulle interfacce Ethernet, sulle VPN, sui point to point PPPoE, sui bridge e sui bonding (aggregati) di VPN. La classificazione del traffico può avvenire anche mediante i filtri Layer 7 che permettono il Deep Packet Inspection (DPI) e quindi di regolare la banda e la priorità da assegnare ai flussi di applicazioni come VoIP e P2P;
- HTTP Proxy con antivirus open source ClamAV in grado di bloccare in maniera centralizzata le pagine web contenenti Virus. Il proxy, realizzato con HAVP, potrà funziona in modalità transparent proxy, intendendo con ciò, che non è necessario configurare i web browser degli utenti per utilizzare il server proxy, ma, le richieste http verranno automaticamente reindirizzate a quest'ultimo. È ovvio, che in questo caso, la macchina che fa da proxy deve essere anche un gateway (router IP o bridge);
- l'autenticazione avviene tramite EAP-TLS o PEAP sfruttando il server RADIUS integrato;
- VPN host-to-lan con protocollo L2TP/IPsec in cui L2TP (Layer 2 Tunneling Protocol) autenticato con username e password Kerberos v5 viene incapsulato all'interno di IPsec autenticato mediante IKE con certificati X.509;
- VPN lan-to-lan con incapsulamento delle trame Ethernet in tunnel SSL/TLS, con supporto per VLAN 802.1Q e aggregabili in load balancing (incremento di banda) o fault tollerance (incremento di affidabilità);
- Router con route statiche e dinamiche (RIPv2 con autenticazione MD5 o plain text e algoritmi Split Horizon e Poisoned Reverse);
- Bridge 802.1d con protocollo Spanning Tree per evitare loop anche in presenza di percorsi ridondati;
- Firewall Packet Filter e Stateful Packet Inspection (SPI) con filtri applicabili sia in routing sia in bridging su tutti i tipi di interfaccia di rete comprese le VPN e le VLAN;
- Controllo mediante Firewall e Classificatore QoS del traffico di tipo File sharing P2Pe Content Filter con Black List e White List ;
- NAT per utilizzare sulla LAN indirizzi di classi private mascherandoli sulla WAN con indirizzi pubblici;
- TCP/UDP port forwarding (PAT) per creare Virtual Server, ovvero cluster di server reali visti con un unico indirizzo IP (l'indirizzo del Virtual Server). Le richieste sul server virtuale saranno smistate sui server reali in Round-Robin (ciclicamente) preservando le connessioni e le sessioni già esistenti. Si può così ottenere il load balancing su web farm, cluster SQL e farm di calcolo;

- Server DNS multizona e con gestione automatica della Reverse Resolution in-addr.arpa;
- Server DHCP multi subnet con possibilità di assegnare l'indirizzo IP in base al MAC Address del richiedente;
- Virtual LAN 802.1Q (tagged VLAN) applicabili sulle interfacce Ethernet, sulle VPN lan-to-lan, sui bonding di VPN e sui bridge composti da interfacce Ethernet, VPN e bond di VPN;
- Client PPPoE per la connessione alla WAN tramite linee ADSL, DSL e cavo;
- Client DNS dinamico che permette la rintracciabilità su WAN anche quando l'IP è dinamico. Gestione dinamica del record dns MX per l'instradamento SMTP della posta elettronica su mail server con IP variabile;
- Server e client NTP (Network Time Protocol) per mantenere gli orologi degli Host sincronizzati;
- Server syslog per la ricezione e la catalogazione dei log di sistema prodotti da host remoti quali sistemi Unix, router, switch, access point WI-FI, stampanti di rete e altro compatibile con protocollo syslog;
- Autenticazione Kerberos 5 mediante un KDC integrato e cross autenticazione tra domini;
- Autorizzazione LDAP, NIS e RADIUS;
- Autorità di certificazione X.509 per l'emissione e la gestione di certificati elettronici;