ALLEGATO A - CAPITOLATO TECNICO
CARATTERISTICHE RICHIESTE PER I CONTROLLER

GARA D'APPALTO INFORMALE RELATIVA ALLA FORNITURA, INSTALLAZIONE E MONITORAGGIO DI UNA RETE WIRELESS CONFORME AGLI STANDARD 802.11 A/B/G/N PER IL POTENZIAMENTO DELLA COPERTURA DELLA SEDE CENTRALE DELL'ACCADEMIA DI BELLE ARTI DI BRERA.

Il Wireless Controller è uno strumento di management che dovrà permettere di gestire, configurare, amministrare le reti wireless outdoor ed indoor da una postazione centralizzata.

Il Wireless Controller dovrà offrire all'amministratore strumenti per effettuare:

- policy provisioning;
- ottimizzazione della rete;
- troubleshooting;
- tracking dei client wireless;
- security monitoring;
- gestione degli apparati WLAN.

Funzionalità di sicurezza:

- il sistema dovrà essere in grado di supportare l'accesso guest all'interno della rete wireless;
- gli amministratori potranno configurare una pagina web d'autenticazione guest direttamente sul Wireless Controller, abilitando l'accesso di un utente ad un giorno ed un'ora stabilita;
- dovrà essere presente uno strumento di IPS/IDS (Intrusion Prevention System/Intrusion Detection System) per identificare i dispositivi associati alla rete wireless che inviano traffico malevolo ed escluderli dalla rete;
- il sistema dovrà essere in grado di rilevare e generare allarmi causati da attacchi di tipo RF (Radio Frequency) quali DoS (Denial of Service), Netstumbler e FakeAP;
- il sistema dovrà essere in grado di monitorare le radio frequenze e di individuare i client e gli Access Point non autorizzati, determinare la loro localizzazione ed eventualmente isolarli dalla rete wireless;
- dovrà essere presente uno strumento per la creazione, il controllo ed il miglioramento delle policy di sicurezza, RF (Radio Frequency), Quality of Service (QoS) e gestione di almeno otto VLAN (Virtual LAN);
- gli amministratori dovranno poter configurare proattivamente le liste d'esclusione, per impedire l'associazione d'utenti indesiderati alla rete wireless. Nel caso venga rilevata un'attività inusuale dovrà essere possibile escludere i dispositivi che generano questo tipo di traffico.

Funzionalità di management:

- gli amministratori dovranno avere a disposizione dei template di configurazione per poter configurare gli Access Point;
- gli amministratori dovranno poter raccogliere dai Wireless Controller le informazioni sotto forma di file CSV (Comma Separated Values);
- dovrà essere possibile creare gruppi di amministrazione ed assegnare ad ogni gruppo dei privilegi in base alle funzioni che dovranno svolgere;
- il sistema dovrà poter inviare in tempo reale le configurazioni ai vari Access Point;
- il sistema dovrà supportare il protocollo SNMP v3 per una comunicazione sicura con gli apparati;
- il sistema dovrà supportare i protocolli RADIUS e TACACS+ per l'autenticazione, l'autorizzazione e l'accounting degli utenti;
- l'amministrazione dovrà avvenire tramite un'interfaccia web HTTP o HTTPS.

Configurazioni hardware disponibili e dotazioni del Wireless Controller:

- almeno 2 porte SFP per uplink Gigabit Ethernet (BASE-T, BASE-SX o BASE-LX);
- una Service port 10/100 Mbps Ethernet (RJ45);
- una Utiliy Port 10/100/1000 Mbps Ethernet (RJ45).

Standard di cifratura e sicurezza e protocolli che dovranno essere supportati:

- WPA (Wi-Fi Protected Access);
- IEEE 802.11i - WPA 2 (Wi-Fi Protected Access version 2) e RSN (Robust Security Network);
- MD5 Message-Digest Algorithm;
- supporto per terminazione VPN;
- ESP Triple DES (3DES) Transform;
- HMAC: Keyed Hashing for Message Authentication;
- TLS Protocol Version 1.0;
- Security Architecture for the Internet Protocol;
- HMAC-MD5-96 within ESP and AH;
- HMAC-SHA-1-96 within ESP and AH;
- ESP DES-CBC Cipher Algorithm with Explicit IV;
- IPsec;
- Interpretation for ISAKMP;
- ISAKMP;
- IKE;
- ESP CBC-Mode Cipher Algorithms;
- certificati X.509 PKI e CRL profile;
- AES-CBC Cipher Algorithm e utilizzo con IPSec;
- using AES counter Mode con IPsec ESP;
- encryption:
    - WEP e TKIP-MIC
    - chiavi RC4 statiche o condivise a 40, 104 e 128 bit;
- Secure Sockets Layer (SSL) e TLS: chiavi RC4 a 128bit e chiavi RSA a 1024 e 2048 bit;
- AES: CCM, CCMP;
- IPSec: DES-CBC, 3DES, AES-CBC;
- supporto per IEEE 802.1x;
- supporto per Microsoft Vendor-Specific RADIUS Attributes;
- supporto per PPP EAP-TLS;
- supporto per RADIUS Authentication;
- supporto per RADIUS Accounting;
- supporto per RADIUS Tunnel Accounting;
- supporto per RADIUS Extensions;
- supporto per Dynamic Authorization Extension to RADIUS;
- supporto RADIUS per EAP;
- supporto per IEEE 802.1x RADIUS guidelines;
- supporto per Extensible Authentication Protocol (EAP);
- supporto per Web-based authentication.

Funzionalità e protocolli di management richieste:

- supporto protocollo CAPWAPP per la completa gestione degli apparati remote;
- supporto RADIUS;
- accesso all'apparato tramite:
    - SSH
    - HTTP/HTTPS
    - telnet;
- SNMP v1, v2, v3 (cifrato e non);
- supporto di strumenti di debugging e diagnostic;
- supporto RMON MIB;
- Simple Network Time Protocol (SNTP) per la sincronizzazione dell'ora;
- Trivial File Transfer Protocol (TFTP);
- Dynamic Host Configuration Protocol (DHCP);
- Bootstrap Protocol (BOOTP);
- Syslog.

Conformità e standard supportati:

- RFC 768 UDP;
- RFC 791 IP;
- RFC 792 ICMP;
- RFC 793 TCP;
- RFC 826 ARP;

- RFC 1122 Requirements for Internet Hosts;
- RFC 1519 CIDR;
- RFC 854 Telnet;
- RFC 1155 Management Information for TCP/IP-Based Internets;
- RFC 1156 MIB;
- RFC 1157 SNMP;
- RFC 1213 SNMP MIB II;
- RFC 1350 TFTP;
- RFC 1643 Ethernet MIB;
- RFC 2030 SNTP;
- RFC 2616 HTTP;
- RFC 2665 Ethernet-Like Interface types MIB;
- RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN.

Extensions:

- RFC 2819 RMON MIB;
- RFC 2863 Interfaces Group MIB;
- RFC 3414 Syslog;
- RFC 3418 MIB for SNMP;
- RFC 3636 Definition of Managed Objects for IEEE 802.3 MAUs;
- marchio CE;
- sicurezza:
    - UL 60950-1
    - EN 60950
    - EMI e Susceptibility (Class B)
    - EN 55022
    - EN 55024
    - IEEE 802.1D Spanning Tree Protocol
    - IEEE 802.1Q VLAN
    - IEEE 802.1x
    - IEEE 802.11a
    - IEEE 802.11b
    - IEEE 802.11d
    - IEEE 802.11g
    - IEEE 802.11h
    - IEEE 802.11i
    - IEEE 802.3
    - IEEE 802.3 10BASE-T
    - IEEE 802.3u 100BASE-TX
    - WPA e WPA 2
    - AES
    - TKIP;
- gestione: SNMP versioni 1, 2c, e 3.