**ALLEGATO "C"**

PER GLI OPERATORI ECONOMICI


**Programma Operativo Nazionale**

***"Per la scuola - Ambienti per l'apprendimento" 10.8.1 A1***

Oggetto: realizzazione e l'ampliamento delle infrastrutture di rete LAN/WLAN

PROGETTO 10.8.1.A1-FESRPON-2015-VE-240

CIG: **ZDD188F8C1**

CUP: **I96J15000550007**

**CAPITOLATO TECNICO**

**A. Specifiche Tecniche minime richieste per gli AP con tecnologia DUAL RADIO (2.4 e 5GHz), Dual Band, ALTA DENSITA' :**

1. Tutti gli AP proposti devono essere compliant contemporaneamente con TUTTI i seguenti standard 802.11a, 802.11b, 802.11g, 802.11n e 802.11ac.

2. Devono supportare l'autenticazione WPA2 Personal e Enterprise con AES/CCMP encryption.

3. Devono essere certificati dalla Wi-Fi Alliance e supportare i seguenti standard: WMM, WMM-PS, 802.11d, 802.11h and 802.11e.

4. Devono possedere le seguenti certificazioni : EN 50385, EN 62331, EN 60950, ETSI EN 300 328, ETSI EN 300 019, ETSI EN 301 489, ETSI EN 301 893

5. Devono poter essere alimentabili a scelta dell'utente finale con PoE standard 802.3af

6. Devono supportare 802.11n e 802.11ac [chip based] Transmit Beamforming.

7. Devono possedere uno o più pattern di antenne **direzionali adattivi per reti WiFi ad ALTA DENSITÀ**. In questo modo l'antenna deve possedere la capacità di concentrare tutta la sua energia a destinazione verso il client in modo da ottimizzare le performance e minimizzare il livello di interferenza radio percepito attorno all'ap stesso.
    a. si deve specificare che tale funzionalità sia compatibile con 802.11n e 802.11ac spatial multiplexing.
    b. si richiede di specificare che le antenne dell'AP sono capaci di selezionare automaticamente fra polarizzazione orizzontale, verticale **e una combinazione di esse**, in modo da adattarsi perfettamente all'orientazione dell'antenna del client.
    c. Il sistema di antenne integrato deve poter garantire almeno 4dBi di guadagno ed 10dB di riduzione dell'interferenza

8. Devono supportare le seguenti tecnologie radio standard :
    a. Polarization Diversity con Maximal Ratio Combining (PD-MRC) per migliorare la ricezione indipendentemente dall'orientamento del client.
    b. Maximum Likelihood Decoding (MLD) per migliorare le performance di uplink del client.
    c. Low Density Parity Check (LDPC) per migliorare le performance di uplink del client.
    d. Space Time Block Coding (STBC) per migliorare le performance di downlink del client.
    e. Packet Aggregation per migliorare le performance di downlink del client

9. Devono supportare DFS (Dynamic Frequency Selection) come da normative sulla banda a 5Ghz e devono essere perlomeno compliant EN 301 893 v1.6.1.

10. La comunicazione fra gli AP e l'eventuale controller, se non integrato nell'AP stesso, deve poter essere messa in sicurezza e cifrata per garantire il massimo livello di sicurezza.

11. Gli AP devono poter automaticamente essere aggiornati all'ultima release passata loro dal controller già dalla prima registrazione su di esso e devono poter essere aggiornabili centralmente dal controller, anche per ogni aggiornamento successivo. Inoltre si richiede che non sia necessario nessun prerequisito, a livello di SW sull'AP o sull'eventuale controller per far sì che il controller possa effettuare un upgrade, neanche la presenza di "coperture" o "garanzie" attive.

12. Devono poter essere installati sulla stessa LAN del controller o laddove necessario, su differenti LAN separate anche a livello tre da switch o router

13. Devono selezionare dinamicamente il proprio canale utilizzando i seguenti metodi:
    a. Automaticamente misurando il throughput effettivo in real-time e cambiando canale automaticamente se la capacità scende sotto il livello statistico medio di quella misurata su tutti gli altri canali, senza utilizzare il background scanning come metodo di selezione automatic
    b. Automatico utilizzando background scanning
    c. Manuale selezionando i canali per ap e per radio
    d. Channel blacklisting (questo deve poter essere disponibile anche nel caso in cui si utilizzino meccanismi automatici di selezione dei canali)

14. Supporto di 802.11k, 802.11r, 802.11v

15. Gli AP devono supportare tecniche radio di accesso al mezzo che prevengano situazioni per le quali client più lenti impattino le performance di client che potrebbero trasmettere a data rate più elevate, in modo da essere già pronti per il BYOD.

16. Devono supportare meccanismi per il bilanciamento automatico dei client su più access points in modo da distribuire equamente il carico fra gli ap, soprattutto in casi di alta densità. Inoltre tale funzionalità deve poter garantire la possibilità di configurare il livello del RSSI del client che stabilisce quando il client deve poter essere spostato da un ap all'altro dal client load balancing.

17. Gli AP devono poter operare an anche nel caso in cui non siano connessi ad una porta Eternet . Devono poter raggiungere la backhole-core networks utilizzando un link radio ( Wireless Mesh). Il Mesh deve essere supportato nei seguenti modi:
    a. L'instaurazione di un backhaul mesh link deve essere automatico, senza dover stabilire a priori canali o ap coinvolti nel mesh
    b. Nel caso in cui un link mesh cada, data una sufficiente vicinanza di un altro ap a cui connettersi, l'ap deve automaticamente potersi riconnettere al nuovo ap senza alcun intervento manuale.

18. Devono avere tutti antenne integrate al fine di minimizzare l'impatto estetico e rendere più resistenti gli stessi da eventuali vandalismi.

19. Gli ap devono avere almeno 2 porte Ethernet per poter mettere in cascata un secondo ap o per qualsiasi altro dispositivo con porta Ethernet. Inoltre:
    a. Si richiede la possibilità di poter abilitare e disabilitare la porta
    b. Le porte Ethernet devono poter supportare 802.11q VLAN tagging e Trunk, General e Access modes
    c. Le porte Ethernet devono supportare 802.1x Authenticator o Supplicant modes

20. Supporto di LLDP

21. L'ap deve supportare 802.1q VLAN tagging e la possibilità di taggare ciascun WLAN individualmente. Inoltre:
    a. Si richiede la possibilità di poter sovrascrivere il tag di una WLAN per ciascun ap

22. **L' access point deve poter supportare fino a 500 client contemporanei**, documentabile da brochure ufficiale del prodotto da allegare a sistema.

23. Gli ap devono supportare funzionalità di analisi di spettro sia per il 2.4 che 5Ghz.

24. Gli ap devono supportare il riconoscimento dei pacchetti taggati con ToS, supportare code multiple per utente, riconoscere e adeguatamente mappare pacchetti marchiati con 802.1p ed inoltre gli ap devono supportare meccanismi di marchiatura dei pacchetti per scopi di Quality of Service.

25. Gli ap devono supportare meccanismi di conversione del traffico da multicast ad unicast.

26. Gli ap devono supportare l'option 82 del DHCP per servizi specifici di localizzazione.

27. L'amministratore deve avere la possibilità di catturare da remoto frames 802.11 e/o 802.3, senza creare disservizio per gli utenti connessi.

28. Il costruttore deve aver la possibilità di offrire anche access point da esterno che siano compliant con lo standard IP67 e che supportino almeno un range di temperature da -40°C a 65°C, integrabili in futuro alla rete in creazione, in modo da coprire anche gli spazi esterni se dovesse diventare richiesto per altri progetti ora non definibili.

29. Tutti gli AP devono supportare HotSpot 2.0 (WFA Passpoint)

**B. Specifiche Tecniche minime per il FIREWALL :**

Tutti i servizi richiesti devono essere disponibili gratuitamente per almeno con 3 anni dalla data di positivo collaudo.

- Almeno 7 porte RJ45 x 10/100/1000 Ethernet attive ed indipendenti
- Almeno 3,2 Gbps Mbps velocita' Firewall
- Almeno 1,2 Gbps velocita' VPN
- Almeno 515 Mb velocita' UTM (anche con la massima sicurezza abilitata)
- Almeno 1.700.000 sessioni bidirezionali
- Almeno 50 Tunnel BOVPN
- Almeno 75 Mobile User VPN IPSec
- Almeno 75 Mobile User VPN SSL
- Zero Day Protection
- Proxy Trasparenti HTTP, SMTP, DNS, POP3, FTP, SIP e H323.
- Gestione tramite software proprietari (gratuiti, es : WSM), oppure Web UI o CLI
- Single Sign On (Autenticazione Trasparente) Active Directory, Radius e Ldap.
- Multi WAN load Balancing
- WAN Failover
- Failover VPN
- Server Load Balancing
- Policy Based Routing
- Alta Affidabilità A/A e A/P
- Routing Dinamico
- Blocco spamming
- Filtraggio URL
- Gateway AV/IPS
- Reputation Enable Defense
- Application Control (per le 1000 applicazioni multiformato più diffuse),
- Supporto attivo 24/7h, 4 ore tempo di risoluzione problematica

- Massimo 1 unita' rack-mount
- L'ispezione dei contenuti a livello di applicazione riconosce e blocca le minacce non rilevabili dai normali firewall stateful packet inspection (SPI).
- Intrusion Prevention Service (IPS) - fornisce la protezione in tempo reale dagli exploit dannosi, inclusi gli overflow del buffer, gli attacchi SQL injection e di cross site scripting.
- WebBlocker controlla l'accesso ai siti che contengono materiali discutibili o comportano rischi per la sicurezza della rete.
- Gateway AntiVirus (GAV) analizza il traffico di tutti i principali protocolli per bloccare malware e virus.
- spamBlocker fornisce la protezione continua dalle e-mail indesiderate e pericolose.
- Reputation Enabled Defense assicura una navigazione del Web più veloce e sicura, con analisi della reputazione cloud-based.
- Scelta tra diversi tipi di VPN (IPSec, SSL, L2TP) per l'accesso remoto protetto, incluso il supporto per i dispositivi Android e Apple iOS.
- Deve proporre una soluzione per la visibilità e il monitoraggio della rete compatibile con il cloud pubblico e privato che trasforma istantaneamente i dati grezzi in security intelligence, della stessa marca del firewall e compresa nel prezzo del prodotto; Il monitoraggio e i report interattivi in tempo reale, inclusi gratuitamente, devono offrono una panoramica dell'attività di protezione della rete, per consentire azioni correttive o interventi preventivi immediati.
- la console di gestione deve gestire centralmente tutte le funzionalità di sicurezza.

- FUNZIONALITÀ DI PROTEZIONE FIREWALL :
    - Stateful packet inspection,
    - deep packet inspection,
    - firewall proxy
    - Proxy applicativi
    - HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3

- PROTEZIONE DALLE MINACCE
    - Attacchi DoS,
    - pacchetti frammentati e malformati,
    - minacce combinate e altro

- VoIP
    - H.323,
    - SIP,
    - impostazione delle chiamate
    - protezione delle sessioni

- OPZIONI DI FILTRAGGIO
    - Safe Search per browser,
    - YouTube for Schools

- VPN E AUTENTICAZIONE
    - Crittografia DES, 3DES, AES a 128, 192, 256 bit
    - IPSec
    - SHA-1, SHA-2, MD5, chiave IKE precondivisa, certificati esterni
    - Single sign-on
    - Supporta Windows, Mac OS X, sistemi operativi mobili

- AUTENTICAZIONE
    - RADIUS,
    - LDAP,
    - Windows Active Directory
    - VASCO
    - RSA SecurID
    - database interno

- Gestione Log e notifiche
- IPv6 Ready Gold (routing)
- WEEE, RoHS, REACH
- Routing Statico, dinamico (BGP4, OSPF, RIP v1/v2), VPN basato su policy
- Alta disponibilità (opzionale, ma deve essere possibile)
    - Attiva/Passiva
    - Attiva/Attiva
    - Con bilanciamento del carico
- QoS
- 8 code di priorità, DiffServ, Modified Strict Queuing
- Aggregazione link
- 802.3ad dinamica, statica, attiva/backup
- Indipendenza delle porte

- FAILOVER
    - bilanciamento del carico multi-WAN
    - bilanciamento del carico server
    - modalità trasparente/drop-in

**C. Specifiche Tecniche minime richieste per i FIREWALL 620Mbps :**

Tutti i servizi richiesti devono essere disponibili gratuitamente per almeno con 3 anni dalla data di positivo collaudo.

- Almeno 5 porte RJ45 x 10/100/1000 Ethernet attive ed indipendenti (di cui una POE)
- Almeno 620 Mbps velocita' Firewall
- Almeno 150 Mbps velocita' VPN
- Almeno 135 Mb velocita' UTM (anche con la massima sicurezza abilitata)
- Almeno 200.000 sessioni bidirezionali
- Almeno 40 Tunnel BOVPN
- Almeno 25 Mobile User VPN IPSec
- Almeno 25 Mobile User VPN SSL
- Zero Day Protection
- Proxy Trasparenti HTTP, SMTP, DNS, POP3, FTP, SIP e H323.
- Gestione tramite software proprietari (gratuiti, es : WSM), oppure Web UI o da linea di comando
- Single Sign On (Autenticazione Trasparente) Active Directory, Radius e Ldap.
- Multi WAN load Balancing
- WAN Failover
- Failover VPN
- Server Load Balancing
- Policy Based Routing
- Alta Affidabilita' A/A e A/P
- Routing Dinamico
- Blocco spamming
- Filtraggio URL
- Gateway AV/IPS
- Reputation Enable Defense
- Application Control (per le 1000 applicazioni multiformato più diffuse),
- Supporto attivo 24/7h, 4 ore tempo di risoluzione problematica
- L'ispezione dei contenuti a livello di applicazione riconosce e blocca le minacce non rilevabili dai normali firewall stateful packet inspection (SPI).
- Intrusion Prevention Service (IPS) - fornisce la protezione in tempo reale dagli exploit dannosi, inclusi gli overflow del buffer, gli attacchi SQL injection e di cross site scripting.
- WebBlocker controlla l'accesso ai siti che contengono materiali discutibili o comportano rischi per la sicurezza della rete.
- Gateway AntiVirus (GAV) analizza il traffico di tutti i principali protocolli per bloccare malware

e virus.
- spamBlocker fornisce la protezione continua dalle e-mail indesiderate e pericolose.
- Reputation Enabled Defense assicura una navigazione del Web più veloce e sicura, con analisi della reputazione cloud-based.
- Scelta tra diversi tipi di VPN (IPSec, SSL, L2TP) per l'accesso remoto protetto, incluso il supporto per i dispositivi Android e Apple iOS.
- Deve proporre una soluzione per la visibilità e il monitoraggio della rete compatibile con il cloud pubblico e privato che trasforma istantaneamente i dati grezzi in security intelligence, della stessa marca del firewall e compresa nel prezzo del prodotto; Il monitoraggio e i report interattivi in tempo reale, inclusi gratuitamente, devono offrono una panoramica dell'attività di protezione della rete, per consentire azioni correttive o interventi preventivi immediati.
- la console di gestione deve gestire centralmente tutte le funzionalità di sicurezza.

- FUNZIONALITÀ DI PROTEZIONE FIREWALL :
    - Stateful packet inspection,
    - deep packet inspection,
    - firewall proxy
    - Proxy applicativi
    - HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3

- PROTEZIONE DALLE MINACCE
    - Attacchi DoS,
    - pacchetti frammentati e malformati,
    - minacce combinate e altro

- VoIP
    - H.323,
    - SIP,
    - impostazione delle chiamate
    - protezione delle sessioni

- OPZIONI DI FILTRAGGIO
    - Safe Search per browser,
    - YouTube for Schools

- VPN E AUTENTICAZIONE
    - Crittografia DES, 3DES, AES a 128, 192, 256 bit
    - IPSec
    - SHA-1, SHA-2, MD5, chiave IKE precondivisa, certificati esterni
    - Single sign-on
    - Supporta Windows, Mac OS X, sistemi operativi mobili

- AUTENTICAZIONE
    - RADIUS,
    - LDAP,
    - Windows Active Directory
    - VASCO
    - RSA SecurID
    - database interno

- Gestione Log e notifiche
- IPv6 Ready Gold (routing)
- WEEE, RoHS, REACH
- Routing Statico, dinamico (BGP4, OSPF, RIP v1/v2), VPN basato su policy
- Alta disponibilità (opzionale, ma deve essere possibile)
    - Attiva/Passiva
    - Attiva/Attiva
    - Con bilanciamento del carico

- QoS
- 8 code di priorità, DiffServ, Modified Strict Queuing
- Aggregazione link
- 802.3ad dinamica, statica, attiva/backup
- Indipendenza delle porte

- FAILOVER
    - bilanciamento del carico multi-WAN
    - bilanciamento del carico server
    - modalità trasparente/drop-in

**D. Specifiche Tecniche minime richieste per gli switch :**

8 Porte PoE+ -Switch -8 ports -Managed L3 -Desktop, rack-mountable, Gigabit Ethernet Ports 8 x 10/100/1000 (PoE+) + 2 x Gigabit SFP, Power Over Ethernet PoE+, PoE Budget: 180W, Performance Throughput : 14.8 Mpps Routing/switching capacity : 20 Gbps, Layer 2 switching, auto-negotiation, ARP support, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, Syslog support, port mirroring, Weighted Round Robin (WRR) queuing, IPv6 support, Spanning Tree Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP) support, Multiple Spanning Tree Protocol (MSTP) support, Access Control List (ACL) support, Quality of Service (QoS), Jumbo Frames support, MLD snooping, Cable Diagnostics Function, STP Root Guard, DHCP relay, Port Security, DHCP client, dual firmware images, Strict Priority Queuing (SPQ), port isolation, static routing, Class of Service (CoS), Single IP Management (SIM) Standards IEEE 802.3, IEEE 802.3u, IEEE 802.3i, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.1ab (LLDP), IEEE 802.3at, IEEE 802.3az. Garanzia "lifetime" del produttore.

**E. Specifiche Tecniche minime richieste per il notebook :**

- Windows Pro
- Display 15,6" non glare
- CPU minimo Processore Core i3-4005u
- RAM 4GB DDR3-1600mhz
- Hard Disk 500GB 7200rpm
- Intel® Wi-Fi (802.11 ac/a/b/g/n) & Bluetooth™ 4.0
- Ethernet 10/100/1000, HDMI, 1xUsb3, 2xUsb2
- Dimensioni e peso massimi : 379.0(W)x258(D)x23.95(H)mm - 2.3kg