ALLEGATO TECNICO

1. Premessa

La fornitura consiste nei moduli hardware, software ed attività di installazione necessarie ad attivare una piattaforma di controllo degli accessi alla rete sia wired che wirelless e una soluzione per creare una rete wireless in grado di dare accesso, ai soli dispositivi abilitati, alle risorse interne della rete dell'ente. La soluzione dovrà essere di Extreme Networks in modo di garantire il massimo livello di integrazione e di riutilizzo degli apparati e del software già di proprietà dell'ente

L'ente ritiene prioritario aumentare la sicurezza della rete agendo non solo sulla parte perimetrale esposta su internet, ma anche sul lato interno. Il sistema richiesto dovrà pertanto evitare che dispositivi non autorizzati possano essere collegati alle prese di rete negli uffici comunali o accedere in modalità wireless anche qualora si conoscano le credenziali di accesso.

Per quanto riguarda la rete wireless, la soluzione proposta dovrà includere gli elementi abilitanti a diffonderla su diverse aree degli uffici dell'ente, ma in questa fase verrà attivata solo in alcuni edifici/uffici in modo da creare un primo ambiente di test. Il dimensionamento dovrà comunque tenere conto della possibilità di espanderla successivamente in diversi edifici in cui già sia presente la rete cablata dell'ente.

La soluzione proposta dovrà anche integrarsi con gli AP Aruba forniti da Lepida su cui è attivo il servizio Emilia Romagna Wifi.
Nella fornitura sono inclusi i servizi di manutenzione ed aggiornamento/supporto software per tre anni dalla data del collaudo

2. Descrizione situazione iniziale

L'infrastruttura di rete dell'ente è interamente basata su apparati Extreme Networks e ha le seguenti caratteristiche principali:

- tutte le sedi sono collegate con doppio percorso in FO di proprietà dell'ente con link a 1/10 GB
- le FO sono attestate in due POP (c/o datacenter dell'ente in piazza Scapinelli e nella sede di Palazzo Prini)
- Nel POP c/o il Ced è installato uno switch di core modulare Extreme Networks BD 8900 con 10 slot che gestisce i collegamenti verso parte delle sedi remote, switch di periferia all'interno della sala macchine, server, enclosure blade, storage, ecc
- Nel POP c/o Palazzo Prini sono installati due switch X670-48x in stack che gestiscono il collegamento con le altri sedi remote le cui fibre arrivano in quel punto

- I due POP sono interconnessi tramite doppio percorso con 2 link 10 GB aggregati e gestito con protocollo LACP
- Nelle altre sedi sono installati circa 90 switch Extreme Networks con sistema operativo XOS di differenti release. Vedi tabella 1 per le tipologie degli apparati

I dispositivi che devono accedere alle risorse di rete rientrano nelle seguenti categorie:

- Desktop
- Portatili
- stampanti di rete
- Timbratori
- Controlli accessi
- Telefoni VOIP switched
- Bacheche elettroniche
- Citofoni IP

Si tenga presente che nella maggioranza dei casi i pc sono collegati a valle dei telefoni switched. Le tipologie dei telefoni VOIP presenti in rete sono riportati in tabella 2.
Sono collegati in rete circa 1400 pc tra desktop e mobili, 250 stampanti di rete, 70 tra controllo accessi e timbratori e 1400 telefoni Voip. Gli utenti che si collegano alla rete sono circa 1600 e nella maggior parte dei casi esiste un rapporto 1 a 1 tra utente / postazione.
All'interno della rete sono attivi due server con ruolo di DHCP/DNS e relay agent sugli switch di periferia; tutti i desktop/portatili che possono accedere alle risorse interne sono registrati all'interno del dominio Active Directory in cui sono memorizzate anche le credenziali di tutti gli utenti. Per utilizzare le postazioni, accedere alle risorse, navigare, ecc. tutti gli utenti si devono autenticare sul dominio.
Per ridurre il traffico di broadcast, la rete dati del Comune è stata suddivisa in varie sottoreti che vengono ruotate da protocolli di routing statico dallo switch di core BD8900.
Le subnet in cui è suddivisa la rete sono riportate in tabella 3

Sugli switch possono essere veicolate diverse VLAN legate a progetti o servizi di diverso genere svincolati dall'attività degli utenti (videosorveglianza, gestione eliminacode, connettività secondaria, internetpoint, ecc…).

L'ente non ha una propria rete wireless ma in alcuni edifici/aree, su cui è diffusa la rete wired dell'ente, con forte accesso al pubblico (es: biblioteche, sale, ecc.) sono attive rete wireless aperte ai cittadini per l'accesso ad internet (es: EmiliaRomagna Wifi, Wisper, Guglielmo). In particolare nel caso di EmiliaRomagna Wifi, su ogni AP sono trasportate più VLAN

L'ente utilizza il software Extreme Network Management Base licenziato per 250 apparati attivi (p/n NMS-BASE-250) e coperto da contratto di manutenzione per gli aggiornamenti sw fino al 31/12/2017

3. Descrizione della fornitura

La soluzione proposta, basata su tecnologia Extreme Networks, deve prevedere la fornitura dell'aggiornamento del software Netsight già in uso all'interno, i dispositivi hardware, le

licenze software e i contratti di manutenzione necessari per rispettare quanto di seguito indicato.
Deve includere funzionalità di gestione centralizzata della rete (wired e wireless integrato) e permettere allo stesso tempo la gestione degli accessi (funzionalità di Radius server e NAC) e di visibilità delle applicazioni (visibilità L7) che sono trasportate dalla rete. Gli elementi di tale soluzione devono essere integrati tra di loro e le informazioni e configurazioni devono poter essere visualizzate e modificate da un'unica interfaccia web. Ovvero i tre prodotti devono avere una base dati comune in cui sono conservate tutte le informazioni.
Tramite una unica GUI web dovranno essere gestiti di tutti gli apparati di rete LAN, wireless AP e Controller, apparati di NAC e di Application Visibility proposti, regolandone il corretto funzionamento e consentendo facilità di monitoraggio, risoluzione dei problemi e reporting.

La soluzione deve prevedere anche la possibilità di poter accedere alla rete mediante tecnologia wireless 802.11 a/b/g/n/ac ovvero deve essere fornita una soluzione wireless Extreme Networks conforme a tale standard costituita da Access point indoor e da controller virtuali. Gli Access Point oggetto della fornitura devono poter essere gestiti anche mediante una piattaforma cloud multitenant ovvero in fase di installazione configurazione della soluzione alcuni Access point potranno essere presi in carico dei controller locali altri dalla piattaforma cloud multitenant fornita del produttore della soluzione.

1. Soluzione per la gestione dell'intera infrastruttura di rete wired e wireless
    a. SW per la gestione di rete
        i. Licenziato fino ad almeno 250 apparati di rete fissa
        ii. Licenziato fino ad almeno 2500 apparati di rete wireless (Access Point)
        iii. DataBase integrato per lo storico dei dati (fino a 180 giorni)
    b. Completa integrazione (unica interfaccia web e DataBase) con la Soluzione per la gestione degli Accessi alla rete e la visualizzazione e analisi delle applicazioni utilizzate in rete

    Le principali funzionalità che dovrà garantire saranno:
    - Interfaccia grafica;
    - Visualizzazione del layout della rete e monitoraggio in tempo reale delle principali funzionalità;
    - Scoperta della topologia di rete e rappresentazione grafica.
    - Possibilità di limitazione del "discovery" ai soli nodi interessati.
    - Gestione e configurazione logica e fisica degli apparati;
    - Segnalazione anomalie e guasti.
    - Tracciamento e visibilità degli utenti autenticati sulla LAN e sul wireless.
    - Visibilità applicativa, monitoraggio delle principali applicazioni, loro statistiche, con possibilità di definire allarmi al superamento di determinate soglie di traffico.

    Tutte le funzionalità sopra indicate devono essere realizzate mediante un unico sistema centralizzato, di tipo client-server con un unico repository dei dati.

2. N° 1 Soluzione per la gestione degli Accessi alla rete

a. SW per la autenticazione, autorizzazione e accounting degli utenti e dei device che accedono alla rete
    i. Funzionalità di Radius server/Proxy radius
    ii. Funizionalità di NAC e Assessment
b. Licenze SW e dimensionamento HW per gestire fino a 3000 utenti e/o device
c. Completa integrazione (unica interfaccia web e DataBase) con la Soluzione per la gestione della rete e la visualizzazione e analisi delle applicazioni utilizzate in rete

Le principali funzionalità che dovrà garantire sono:

- Deve implementare sull'intera rete l'autenticazione e l'autorizzazione dei sistemi finali attraverso il MAC address, 802.1x, posizione fisica dell'apparato, username o l'autenticazione Web
- Per garantire l'accesso in rete non dovrà essere necessario installare nessun tipo di agent software sulle postazioni client
- Il sistema proposto deve supportare il "pass through" del 802.1X (es. dal proxy RADIUS al server RADIUS di backend)
- La soluzione deve essere composta da server NAC dedicati con funzionalità di RADIUS e Proxy RADIUS completamente gestibili da un'applicazione integrata nel sistema monitoraggio degli apparati di rete e wireless
- L'autenticazione per l'accesso alla rete con le modalità descritte deve essere possibile anche senza un proxy radius esterno. Qualora esso sia presente e lo si voglia utilizzare il server NAC oggetto della fornitura dovrà poter dialogare con esso configurandosi come proxy radius. IL server NAC quindi, deve poter verificare le credenziali degli utenti, collegandosi a sistemi LDAP esterni, ed in particolare ad Active Directory. o utilizzando un repository interno di credenziali o MAC Address
- Le regole per l'accesso devono consentire sia l'uso di MAC address singoli che di OUI (primi 6 caratteri del MAC Address)
- Deve essere possibile assegnare differenti policy per accedere alle risorse di rete ad un utente in base a dove esso si collega nella rete, così come in base all'autenticazione (username, mac, 802.1x), si devono poter assegnare permanentemente policy o VLAN indipendemente dalla posizione da cui ci si collega
- Devono essere previsti meccanismi di tracciatura dei MAC e delle identità degli utenti che si collegano in rete per semplificare la gestione degli accessi autorizzati
- Devono essere supportate funzioni per semplificare/autorizare/tracciare l'accesso in forma limitata e solo ad alcune risorse da parte degli utenti Guest
- Deve essere possibile l'integrazione con sistemi di Mobile Device Management per il recupero delle informazioni sui dispositivi aziendali autorizzati all'accesso

3. N° 1 Soluzione per la gestione visualizzazione e analisi delle applicazioni utilizzate in rete e delle performance delle rete e delle applicazioni trasportate dalla rete wireless e wired

a. SW per la gestione visualizzazione e analisi delle applicazioni utilizzate in rete e delle performance delle rete e delle applicazioni
b. Licenze SW e dimensionamento HW per gestire fino a 50000 flussi applicativi per minuto (FPM)
c. Completa integrazione (unica interfaccia web e DataBase) con la Soluzione per la gestione della rete e la gestione degli accessi alla reteOttimizzazione nell'impiego delle risorse e nella capacità di gestione di applicazioni essenziali per l'azienda.

Le principali funzionalità che dovrà garantire saranno:

- Risoluzione dei problemi e servizi di gestione delle applicazioni.
- Visualizzazione del traffico delle applicazioni.
- Visualizzazione del tempo di risposta di rete e delle applicazioni.
- Fornire dati di utilizzo delle applicazioni per report di compliance.
- Analizzare il profilo di utilizzo delle applicazioni da parte dei clienti per poter comprenderli al meglio.

4. Soluzione Wireless – con le seguenti componenti:
   a. Controller Wireless Virtual Appliance per la configurazione e gestione centralizzata degli Access Point, dotato delle licenze per gestire **ALMENO** tutti gli AP forniti, e con le seguenti caratteristiche:
      i. Gestione fino a 525 AP per controller virtuale
      ii. Gestione fino a 8000 utenti per Appliance
      iii. Gestione fino a 1024 Wireless LAN
      iv. Supporto VLAN-VNS
      v. Supporto RADIUS Accounting
   b. ALMENO 15 access point indoor 802.11 a/ac+/b/g/n 2x2 MIMO completi di staffe per installazione a muro
      La fornitura non include i cablaggi per il collegamento degli AP né le attività di posizionamento degli stessi.
      Sono invece incluse le attività di configurazione e quelle propedeutiche all'individuazione dei punti di installazione nelle aree identificate dal personale del servizio Gestione e Sviluppo delle tecnologie per il primo deployment del sistema.

La fornitura include anche i servizi di supporto ed aggiornamento software erogati direttamente dal produttore Extreme Networks dalla data del collaudo ed almeno per TRE anni per tutti i moduli software proposti

Sono incluse tutte le attività di installazione e configurazione dei moduli proposti come indicato di seguito

Il Fornitore dovrà fornire il software di gestione (uno o più moduli) dell'intero sistema, dovrà installare, configurare e caricare la base dati, degli apparati e dell'infrastruttura

realizzata. La Piattaforma fornita dovrà essere in grado di gestire le tipologie di apparati proposti, quelli già esistenti e dovrà essere continuamente allineato con lo stato degli apparati e dell'intera infrastruttura di rete.

Il fornitore dovrà identificare un referente unico di progetto che sarà l'interfaccia con il personale del servizio Gestione e sviluppo delle tecnologie e con cui dovrà essere concordato il piano di attività

Le attività incluse nella fornitura potranno riguardare anche la modifica della configurazione degli apparati di rete: le attività massive su tutte la periferia potranno essere effettuate dal personale del servizio Gestione e sviluppo delle tecnologie, in accordo con quanto concordato con la ditta fornitrice.

Oltre ai requisiti generali della piattaforma indicati sopra la configurazione che dovrà essere attivata deve rispettare i seguenti vincoli:

- permettere l'accesso alla rete interna solo ai dispositivi "conosciuti" e previa verifica che le credenziali fornite siano valide nel dominio Active Directory. Se questa condizione non è rispettata il dispositivo dovrà essere rediretto su una VlAN guest (es: vlan "internet-point") che permette esclusivamente l'accesso ad internet e su cui sono attivi servizi DHCP.
  I dispositivi "conosciuti" sono:
  - dispositivi registrati sul dominio Active Directory (desktop e portatili)
  - dispositivi non registrati sul dominio Active Directory (stampanti / timbratori/ controllo accessi/ telefoni voip / ecc.)
- I dispositivi non registrati nel dominio e da considerare "conosciuti" dovranno essere identificati tramite il MAC address o l'identificativo OUI
- **la verifica dell'esistenza del dispositivo su Active Directory dovrà essere fatta senza dover installare certificati /CA sui pc o nel dominio.**
- Devono essere gestite 2 tipi di autenticazione:
  - basata sul MAC address/OUI per tutti i dispositivi (stampanti / timbratori /telefoni) non in grado di gestire autentica 802.1x
  - 802.1x per pc / portatili / smartphone
- dovranno essere creati gruppi omogenei per i telefoni VOIP, telecamere ed altri dispositivi da trattare analogamente popolato in base all'OUI o tramite meccanismi di importazione il più possibile automatici (es: MDM). Ai telefoni VOIP dovrà essere consentito l'accesso attribuendo una VLAN fissa in modalità tagged, indipendentemente dalla location da cui il telefono tenta l'accesso
- Ai desktop/portali /stampanti / timbratori ecc. autorizzati ad entrare in rete in base alle regole definite sopra dovrà essere attribuita una Vlan corrispondente a quella untagged già definita sulla porta e diversa a seconda del gruppo di switch da cui il dispositivo tenta la connessione. In questo modo sarà possibile gestire le diverse VLAN/subnet della rete
- Per gli AP di EmiliaRomagna Wifi il processo di autorizzazione dovrà consentire lo sblocco della porta e il trasporto delle N Vlan attualmente attive.
- Si dovrà poter gestire un processo di autorizzazione, preferibilmente con indicazione del

periodo di validità, per permettere l'accesso alla rete interna a postazioni (es: portatili di consulenti esterni) non registrati nel dominio

- Dovranno poter essere configurate regole per ridurre problemi di connessione qualora ci siano malfunzionamenti in uno dei componenti coinvolti o nel dialogo tra di essi: ad esempio se lo switch non è in grado di contattare il server nac l'accesso dovrà essere autorizzato con l'attribuzione della VLAN legata all'ubicazione dello switch stesso.
- I dispositivi mobili potranno entrare nella rete interna solo se il loro MAC rientra in quello dei dispositivi autorizzati e le credenziali con cui si tenta l'accesso sono quelle del dominio. Quando la condizione è verificata, verrà attribuita una VLAN/Subnet fissa indipendente dall'AP da cui si è tentato l'accesso.
- Si deve prevedere di configurare anche una fase di audit in cui vengono solamente rilevate le informazioni sui dispositivi che si collegano in modo da avere una base di partenza per la creazione delle regole e dei database degli oggetti non registrati in active directory da autorizzare.
- Si devono mantenere informazioni di log in modo da rintracciare chi si è connesso, da che apparati/porte ecc.
- La configurazione attivata dovrà essere il più possibile non invasiva rispetto alle modalità attuali con cui gli utenti si collegano alla rete e di gestione del parco client effettuata da Servizio gestione e sviluppo delle tecnologie.
- La soluzione proposta deve funzionare correttamente anche con telefoni switched e pc collegati in cascata e pc collegati ad hub/switch su cui non e' attivato 802.1x; il dispositivo autorizzato deve sloccare solo la propria porta e non permettere comunque l'accesso a quelli a valle se non soddisfano le regole suddette.
- Tutte le regole suddette devono valere sia per l'accesso wired che wireles.

Per quanto riguarda la piattaforma wireless le attività previste dal fornitore dovranno includere l'integrazione con reti wireless cittadine già esistenti in alcuni edifici dell'ente.
Ad esempio:

- possibilità di trasportare la rete wireless, per l'accesso alla rete interna anche su gli AP Aruba forniti da Lepida Spa che attualmente rendono disponibile il SSID Wisper e EmiliaRomagna Wifi o su quelli di Guglielmo afferenti alla rete Reggio WiFi. In questo caso dovranno essere attivate le regole per l'accesso viste nei punti precedenti
- possibilità di trasportare Emilia Romagna WIFI sugli apparati wireless inclusi nella presente fornitura

La ditta fornitrice dovrà interfacciarsi con i gestori delle reti wireless suddette sia per le verifiche di fattibilità che per le configurazioni da attivare

Oltre alle attività di cui sopra, nella fornitura sono incluse un pacchetto a scalare di 5 giornate da utilizzare per attività collaterali che potranno emergere dalla data di collaudo al termine del periodo di copertura dei servizi di manutenzione / aggiornamento software compresi.
Rientrano in questa tipologia attività come:

- soluzione di problemi non emersi prima del collaudo
- modifiche alla configurazione attivata che non cambino sostanzialmente la soluzione proposta
- aggiornamenti di release dei moduli della soluzione proposta

4. Condizioni di fornitura

Fornitura ed inizio delle attività di installazione: **entro 30 giorni solari dall'ordine**
Collaudo con esito positivo: entro 6 mesi dall'inizio attività. Il collaudo darà sottoscritto dal responsabile tecnico del servizio Tecnologie e Sistemi Informativi e dal referente tecnico designato dall'aggiudicatario.

IL DIRIGENTE
(Dott.ssa Lorenza Benedetti)

BENEDETTI LORENZA
Firmato digitalmente da BENEDETTI LORENZA
Data: 2018.01.31 10:03:05 +01'00'

Tabella 1 - tipologia switch periferia

Summit X150-24t
Summit X250e-24p
Summit X440-24p
Summit X440-24t
Summit X440-48p
Summit X440-48p-10G
Summit X440-8p
Summit X440G2-24p
Summit X440G2-48p-10G4

Tabella 2 - Tipologie telefoni VOIP

Siemens openstage 15	switched
Siemens openstage 15g	switched
Siemens optipoint 410 economy plus	switched
Siemens optipoint 410 entry	Non switched

Tabella 3 - elenco sottoreti

Ambito [172.16.0.0/16] LAN
Ambito [172.17.0.0/22] Ex Tribunale
Ambito [172.17.4.0/24] Ex Stalloni
Ambito [172.17.5.0/24] Pieve
Ambito [172.17.7.0/24] Villa Cougnet
Ambito [172.17.8.0/24] Musei Ex ACI
Ambito [172.17.9.0/24] VV. UU. - Comando
Ambito [172.17.10.0/24] Foro Boario
Ambito [172.17.11.0/24] Uff. Casa - Polo Centro - Biblio Ospizio
Ambito [172.17.12.0/24] Ex Locatelli VV.UU. 7° Circ.
Ambito [172.17.13.0/24] VV. UU. 6° Circ. - Casa delle Donne
Ambito [172.17.16.0/24] Ex Telecom - Gall. Parmeggiani
Ambito [172.18.1.0/24] Biblioteca Panizzi
Ambito [172.18.2.0/24] Gall. S. Maria
Ambito [172.18.3.0/24] Pal. Prini
Ambito [172.18.4.0/24] Pal. Casotti
Ambito [172.18.5.0/24] Scuole
Ambito [172.18.6.0/24] Ragioneria
Ambito [172.18.7.0/24] Pal. Ancini
Ambito [172.18.9.0/24] Sede
Ambito [172.18.11.0/24] Ex Anagrafe

Ambito [172.18.12.0/24] Ospizio
Ambito [172.18.13.0/24] Guasco
Ambito [172.18.14.0/24] Mazzacurati
Ambito [172.18.15.0/24] VV. UU. Circ. Ovest - Orologio
Ambito [172.18.16.0/24] Polo Sud - Biblio S. Pellegrino
Ambito [172.18.17.0/24] Wybicki
Ambito [172.18.18.0/24] Marzabotto
Ambito [172.18.19.0/24] VV. UU. Circ. Centro
Ambito [172.19.0.0/16] Scapinelli
Ambito [172.20.0.0/16] VDIclient
Ambito [172.30.0.0/16] VOIP