

----- Messaggio originale -----

Oggetto: Estensione VPN Aziendale sede di Laconi e sicurezza

Data: Wed, 16 Sep 2015 17:24:58 +0200 (CEST)

Mittente: Dina Ari <dina.ari@asloristano.it>

A: Maria Gesuina Demurtas <gesuina.m.demurtas@asloristano.it>

CC: Direzione Generale ASL Oristano
<direzione.generale@asloristano.it>

Gent.ma,

in previsione della prossima apertura del Poliambulatorio di Laconi è stata richiesta l'attivazione di una linea ADSL come estensione della Rete Aziendale alla Ditta Fastweb.

Inoltre al fine di migliorare il livello di sicurezza informatica Aziendale sono stati richiesti i preventivi per l'installazione di servizi e apparati di sicurezza nelle sedi del Carcere di Massama e di Sassari, collegamento con la neurochirurgia. Considerata l'importanza e l'urgenza delle richieste si chiede di procedere per quanto di competenza.

Saluti

Dina Ari

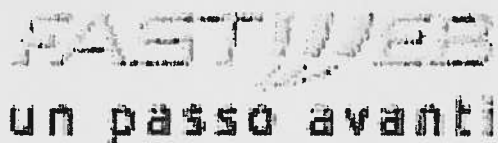
-----Original Message-----

From: Dina Ari [<mailto:dina.ari@asloristano.it>]

Sent: martedì 9 giugno 2015 15:36

To: Corradini Cinzia Cristina; Paradiso Livio; De Cia Mirco

Subject: Estensione VPN Aziendale sede di Laconi

	<p>Progetto Esecutivo Amministrazione : ASL Oristano Protocollo numero: NOCDIF1501796-1 Revisione: 1.0</p>
-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------

Progetto Esecutivo

Convenzione

Telefonia Fissa e Connettività IP 4

Porre re focus re vol

18/05/15 *Albi*

INDICE

1	INTRODUZIONE	3
2	ESIGENZE DELL'AMMINISTRAZIONE	4
2.1	ATTIVAZIONE DI NUOVI ACCESSI DATI E/O CAMBIO DI CONFIGURAZIONE	4
3	MODALITÀ DI ATTIVAZIONE DEI SERVIZI	6
3.1	INFORMAZIONI PRELIMINARI NECESSARIE ALL'ATTIVAZIONE DEI SERVIZI FONIA E DATI	6
3.2	TECNOLOGIA REALIZZATIVA PER I SERVIZI FONIA	7
3.2.1	<i>Accesso diretto in Fibra Ottica</i>	7
3.2.2	<i>Accesso diretto in ULL</i>	8
3.2.3	<i>Accesso in modalità VoIP</i>	8
3.2.4	<i>Accesso in modalità WLR (Wholesale Line Rental)</i>	8
4	PIANO DELLE ATTIVAZIONI	9
4.1	GANTT E TEMPISTICHE	9
4.2	RISORSE FISICHE MESSE A DISPOSIZIONE PER L'IMPLEMENTAZIONE DEL PROGETTO	9
4.3	COLLAUDO	9
4.4	CONDIZIONI GENERALI	9
5	VALORIZZAZIONE ECONOMICA	11
5.1	DETTAGLIO SERVIZI DATI	11

FASTWEB
un passo avanti

Progetto Esecutivo

Amministrazione : ASL Oristano

Protocollo numero: NOCDIF1501796-1

Revisione: 1.0

1 Introduzione

Il presente documento si prefigge lo scopo di illustrare i servizi proposti da Fastweb nell'ambito della Convenzione per i "Servizi di Telefonia Fissa e Connettività IP 4" stipulata tra la Consip S.p.A., per conto del Ministero dell'Economia e delle Finanze, e Fastweb S.p.A. quale aggiudicatario della procedura di gara.

Come previsto dalla Convenzione suddetta, l'Amministrazione è tenuta a verificare i contenuti del presente progetto esecutivo e ad approvarlo dandone conferma a Fastweb secondo le modalità indicate nella guida alla convenzione.

2 Esigenze dell'Amministrazione

Il presente progetto copre le seguenti esigenze

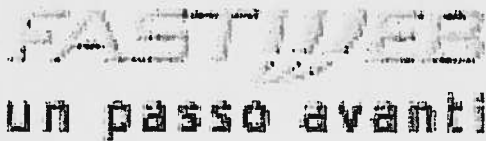
- Attivazione di nuovi accessi dati su infrastruttura Fastweb ovvero modifica di configurazione di accessi esistenti;

2.1 ATTIVAZIONE DI NUOVI ACCESSI DATI E/O CAMBIO DI CONFIGURAZIONE

E' prevista l'attivazione di nuovi accessi dati indicati in tabella distribuite come da tabella.

Profilo	Q.tà Base	Profilo	Q.tà Elevata Affidabilità BASE	Profilo	Q.tà Elevata Affidabilità AVANZATA	Profilo	Q.tà s-vpn
S0							
S1							
S2							
S3							
S4							
S5							
B1							
B2	1						
B3							
B4							
B5							
B6							
B7							
B8							
B9							
Banda aggiuntiva di 10 Mbps per accessi B8							
Banda aggiuntiva di 100 Mbps per accessi B9							

L'assistenza prevista è base

	<p>Progetto Esecutivo Amministrazione : ASL Oristano Protocollo numero: NOCDIF1501796-1 Revisione: 1.0</p>
-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------

Gli accessi saranno configurati secondo quanto definito in un successivo approfondimento progettuale, che terrà conto delle valutazioni tecniche che emergeranno dalle informazioni contenute nel Progetto dei Fabbisogni, nelle schede tecniche e nelle informazioni preliminari descritte nel seguito.

Il nuovo collegamento dati sarà realizzato presso la sede del Poliambulatorio di Laconi in Via Mazzini.

3 Modalità di attivazione dei servizi

In questo paragrafo viene illustrata la procedura con la quale il servizio verrà consegnato (e quindi erogato), nei tempi e con le modalità previste dalla Convenzione stipulata tra Fastweb S.p.A. e Consip S.p.A., nell'intento di ridurre al minimo sia il disservizio arrecato, sia per identificare ed eliminare eventuali disottimizzazioni presso le sedi dell'Amministrazione Contraente.

L'attivazione è subordinata alla disponibilità delle informazioni preliminari di cui alla sezione successiva, necessarie per la corretta configurazione e l'eventuale analisi di fattibilità effettuata sulla base delle informazioni stesse, laddove necessario.

I servizi fonia saranno forniti in modalità FO, ULL o VoIP a seconda della tecnologia disponibile nella singola sede.

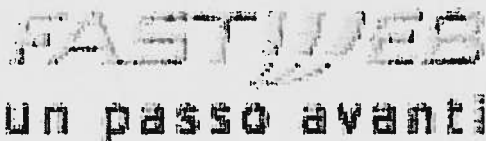
I servizi dati saranno forniti in modalità xDSL (ULL e/o Bitstream) o Fibra Ottica in funzione della tecnologia disponibile nella sede.

La tecnologia con la quale saranno forniti i servizi potrà subire variazioni a seguito di verifiche in fase esecutiva di attivazione con l'operatore nazionale (indisponibilità di risorse fisiche, ecc...); in caso di impossibilità tecnica ad effettuare l'attivazione dei servizi secondo la configurazione originariamente ipotizzata verrà concordata con l'Amministrazione una nuova pianificazione o una diversa soluzione architeturale. Ai servizi forniti secondo tale diversa soluzione architeturale approvata dall'Amministrazione richiedente saranno applicate le corrispondenti condizioni economiche di cui al successivo punto 7.

3.1 INFORMAZIONI PRELIMINARI NECESSARIE ALL'ATTIVAZIONE DEI SERVIZI FONIA E DATI

Al fine di rendere operative le realizzazioni previste dovranno essere fornite, per ogni linea, le seguenti informazioni, indicate di seguito e riassunte nel documento di dettaglio denominato Piano dei Fabbisogni ovvero fornite a Fastweb:

1. indirizzo della sede ed ubicazione nell'edificio della linea. E' importante evidenziare se le linee fonia/ accessi dati di uno stesso edificio siano terminanti in un unico locale tecnico o se siano disperse nell'edificio con richiesta di opere di cablaggio interno.
2. Referenti tecnici centrale e locale
3. Configurazione della Linea fonia, come da moduli di sottoscrizione allegati, ed in particolare:
 - tipologia della linea (ISDN, POTS) e numero di canali (quantità e tipologia)
 - configurazione della linea (numerazioni, servizi base ed avanzati, numerazioni secondarie)

	Progetto Esecutivo Amministrazione : ASL Oristano Protocollo numero: NOCDIF1501796-1 Revisione: 1.0
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------

- richiesta di Prestazione di Number Portability e/o Pubblicazione in elenco
- 4. Configurazione dell'Accesso Dati, come da moduli di sottoscrizione allegati, ed in particolare:
 - tipologia dell'accesso (dial up, IP, Ethernet) e configurazione (profilo, affidabilità)
 - configurazione dei servizi differenziati, internet ed SVPN
 - piano di indirizzamento IP
- 5. utilizzo della linea fonia (teleallarmi, emergenza sanitaria, ufficio, servizi al cittadino, ecc...) ed apparati attestati sulla linea (Centralini telefonici, modem, telefoni....)
- 6. Informazione inerente l'espletamento delle attività realizzative:
 - Orario in cui è possibile accedere ai locali per le attività necessarie
 - Disponibilità ad effettuare operazioni sull'impianto elettrico laddove necessario e previo accordo
- 7. Documentazione necessaria all'attivazione, ed in particolare:
 - Documentazione necessaria ai sensi della vigente normativa in termini di sicurezza sui luoghi di lavoro (DUVRI ed altra necessaria in relazione alla sede);
 - Documentazione di configurazione delle linee telefoniche (bollette, contratti precedenti con altro operatore) e di migrazione (codice di migrazione). In particolare, il contratto ed i moduli di configurazione delle linee sono necessari per procedere con la presa in carico delle stesse.
 - Documentazione contrattuale (es. CIG derivato della commessa)

3.2 TECNOLOGIA REALIZZATIVA PER I SERVIZI FONIA

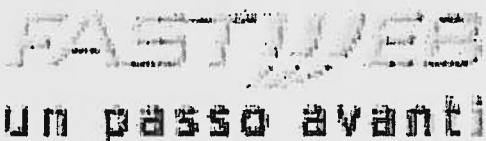
Le linee fonia saranno realizzate in una delle seguenti modalità.

3.2.1 Accesso diretto in Fibra Ottica

L'accesso in fibra ottica si applica tipicamente ad accessi PRA ISDN. In questo caso nella sede dell'Amministrazione è prevista l'installazione di un anello in fibra ottica SDH e di un apparato ADM (Add Drop Multiplexer). L'apparato ADM rende disponibili le interfacce PRA.

Qualora fosse richiesta la prestazione di Number Portability, all'atto dell'attivazione delle nuove linee si installerà sulla sede una smart-box per la gestione del traffico uscente, tale smart-box sarà biattestata sulle linee presenti e sulle linee nuove fino all'attivazione del servizio N.P.

Tale smart-box sarà fornita temporaneamente e gratuitamente in comodato d'uso all'Amministrazione e permetterà l'instradamento automatico verso la rete Fastweb del traffico telefonico uscente in modalità completamente trasparente. La smart-box sarà poi

	Progetto Esecutivo Amministrazione : ASL Oristano Protocollo numero: NOCDIF1501796-1 Revisione: 1.0
-----------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------

rimossa a carico di Fastweb appena non sarà più strettamente necessaria concordando con l'Amministrazione modalità e tempi.

3.2.2 Accesso diretto in ULL

L'accesso in ULL si applica indifferentemente a tutte le tipologie di servizio (POTS, BRA e PRA).

Nel caso di PRA è prevista la realizzazione di un nuovo circuito in rame che sarà biattestato al PBX nella stessa modalità descritta al paragrafo precedente. La realizzazione del nuovo circuito richiede l'installazione di una NT c/o la sede dell'Amministrazione e l'attestazione del doppino al Multiplexer Fastweb collocato nella Centrale Telecom di pertinenza.

Nel caso di linea POTS e BRA è prevista la migrazione su "linea attiva", cioè alle 00:00 della data di migrazione sarà attivata la number portability del numero telefonico (il servizio non è più disponibile) e la mattina seguente sarà effettuata la permuta del doppino telefonico sul Multiplexer Fastweb (il servizio torna disponibile). Nel caso di migrazione di linea BRA è prevista anche l'installazione di una NT c/o la sede dell'Amministrazione.

3.2.3 Accesso in modalità VoIP

L'accesso in VoIP si applica a tutte le tipologie di servizio (POTS, BRA e PRA).

E' prevista l'installazione di un apparato router VoIP, nelle tecnologie Aethra, Amtec o Cisco su cui saranno attestate le interfacce fonia richieste.

3.2.4 Accesso in modalità WLR (Wholesale Line Rental)

L'accesso in WLR si applica a tutte le tipologie di servizio (POTS, BRA e PRA) nelle aree secondarie in cui non è disponibile la modalità di U.L.L.

E' prevista la presa in carico, da parte di Fastweb delle linee telefoniche dell'O.D. senza necessità di attivazione di una ulteriore linea telefonica con necessità di bi attestazione.

4 Piano delle attivazioni

4.1 GANTT E TEMPISTICHE

Per le linee/ servizi di nuova attivazione si procederà alla definizione nel dettaglio del Piani dei Fabbisogni e della fornitura delle informazioni preliminari di cui alle sezioni precedenti.

4.2 RISORSE FISICHE MESSE A DISPOSIZIONE PER L'IMPLEMENTAZIONE DEL PROGETTO

In termini di risorse fisiche saranno allocate per questo progetto le seguenti figure:

- Struttura Commerciale
- Struttura di supporto tecnico alla vendita (Presales)
- Struttura di supporto commerciale alla vendita (Customer Care)
- Struttura di Project Manager/Network Integration
- Struttura di delivery dislocata sul territorio (System Integrator)

In termini di risorse materiali, saranno allocate per questo progetto le seguenti componenti:

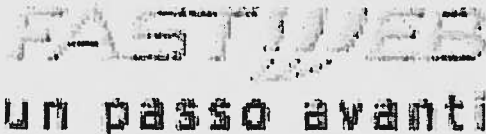
- Componenti HW per la fonia/dati:
- Terminazione di linea RTG, ISDN BRA e PRA e CPE per la rete dati
- CRD per biattestazione

4.3 COLLAUDO

Al rilascio del servizio verrà consegnato all'Amministrazione il "Verbale di Rilascio del Servizio" con il quale si certifica l'attivazione del servizio e la sua conformità a quanto previsto nella Convenzione stipulata.

4.4 CONDIZIONI GENERALI

La verifica definitiva della disponibilità del servizio è subordinata alla disponibilità di adeguate risorse e può avvenire solo in fase di attivazione (al momento della richiesta dei doppi rami all'O.D. ed alla loro qualifica in qualità). Qualora si verificassero situazioni

	<p>Progetto Esecutivo Amministrazione : ASL Oristano Protocollo numero: NOCDIF1501796-1 Revisione: 1.0</p>
-----------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------

tali per cui non fosse possibile rispettare le condizioni riportate nei paragrafi precedenti, verrà presentata all'Amministrazione un nuovo progetto esecutivo riportante la migliore soluzione identificata.

Per quanto non espressamente esplicitato in questo documento, si rimanda alla Convenzione.

5 Valorizzazione economica

I servizi, erogati in accordo alla convenzione in essere stipulata tra Fastweb e CONSIP, prevedono la corresponsione di un canone mensile pari a €.__153,00__


Nei canoni non sono compresi i consumi a volume (es: i consumi relativi al traffico fonia) a cui saranno applicate le tariffe previste in convenzione.

L'assistenza prevista è base come dettagliato precedentemente.

5.1 DETTAGLIO SERVIZI DATI

Di seguito il dettaglio dei servizi Base:

ID Profilo	Quantità	Canone Mensile Servizio Base Unitario (Euro/Mese)	Canone Mensile TOTALE (Euro/Mese)
S0			
S1			
S2			
S3			
S4			
S5			
B1			
B2	1	153,00	153,00
B3			
B4			
B5			
B6			
B7			
B8			
B9			
Banda aggiuntiva di 10 Mbps oltre quella già			

 un passo avanti	Progetto Esecutivo Amministrazione : ASL Oristano Protocollo numero: NOCDIF1501796-1 Revisione: 1.0
-------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------

contrattualizzata, fino a 90 Mbps			
Banda aggiuntiva di 100 Mbps oltre quella già contrattualizzata per l'accesso a 100 Mbps, fino a 1 Gbps			

Offerta

**Fast Security 360°
per l'ASL di Oristano**

**N° NOCDIF1501798 -1
V 1.0**

*Pose ve favorevole
18/07/15 M. M.*

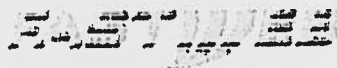
FASTWEB

Business Unit Enterprise

Strettamente confidenziale

FASTWEB

un passo avanti



INDICE

1	FASTWEB	3
2	FAST SECURITY 360°: INTRODUZIONE	4
2.1	AFFIDARE IN OUTSOURCING LA GESTIONE DELLA SICUREZZA INFORMATICA AZIENDALE.....	4
2.2	FAST SECURITY 360°: BENEFICI PER L'AZIENDA.....	5
3	FAST SECURITY 360°: CARATTERISTICHE DEL SERVIZIO	7
3.1	STRUTTURA DEL SERVIZIO	7
3.2	FUNZIONALITÀ DI SICUREZZA	8
3.3	PROPOSTA PER L'ASL DI ORISTANO.....	9
3.4	VALORIZZAZIONE ECONOMICA.....	10

1 FASTWEB

FASTWEB è il principale operatore italiano di servizi di telecomunicazione a larga banda alternativo all'incumbent ed il primo operatore a livello mondiale ad avere sviluppato una rete di nuova generazione interamente in fibra ottica.

Da oltre un decennio FASTWEB ha sviluppato una rete capillare a larga banda, basata su protocollo IP, che ha reso possibile il lancio di servizi voce, dati, video e ICT, tutti fruibili contemporaneamente, con un solo collegamento, da tutte le tipologie di clienti, residenziali e business.



Oggi, per effetto dell'architettura innovativa e della flessibilità della propria rete, FASTWEB raccoglie tutte le sfide tecnologiche del futuro: dagli sviluppi della TV digitale all'Unified Communication al Cloud Computing, per un'offerta sempre più ricca e completa.

Nel segmento "Enterprise" FASTWEB è riconosciuta come partner affidabile e d'eccellenza, annoverando importanti referenze su clienti istituzionali, in settori quali il mondo bancario/finanziario e dell'industria e servizi.

In ambito Pubblica Amministrazione FASTWEB è dal 2006 il fornitore principale per i servizi di telefonia fissa e dati.

Grazie a scelte pionieristiche, oggi replicate in tutto il mondo, FASTWEB, che oggi fa parte del Gruppo Swisscom, ricopre una posizione di assoluta eccellenza nel mercato Italiano e Mondiale.

FASTWEB: il futuro delle telecomunicazioni, oggi.

2 FAST SECURITY 360°: INTRODUZIONE

2.1 AFFIDARE IN OUTSOURCING LA GESTIONE DELLA SICUREZZA INFORMATICA AZIENDALE

Fast Security 360° è il servizio di sicurezza gestita di Fastweb che consente al cliente di esternalizzare (outsourcing) la gestione della sicurezza informatica aziendale presso un MSSP (Managed Security Service Provider). Il servizio offre una soluzione totalmente integrata e completa per rilevare ed eliminare una vasta gamma di attacchi e attività dannose, tra cui virus, worm, intrusioni, spyware e denial-of-service, contenuto Web inappropriato e molto altro, in tempo reale e senza compromettere le prestazioni dell'infrastruttura ICT aziendale.



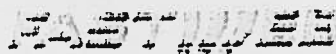
Le minacce alla sicurezza sono estremamente dannose e in continua evoluzione. Molte aziende riconoscono che una protezione inadeguata contribuisce ad aumentare i rischi per la sicurezza e quindi che un'unica linea di difesa non è più sufficiente per proteggere le proprie attività e risorse. Diventa, quindi, sempre più necessario pensare alla sicurezza informatica come un servizio continuativo, sempre vigile e allo stato dell'arte. Solamente una soluzione di sicurezza gestita da personale altamente specializzato che opera tipicamente in un SOC (Security Operations Center) espressamente dedicato alla gestione di realtà Enterprise è in grado di soddisfare le esigenze di protezione a costi accettabili.

L'offerta di Fastweb è stata ideata per offrire il livello più elevato di sicurezza e per fornire una difesa completa in grado di prevenire danni ai sistemi informatici aziendali. Mediante una combinazione di tecnologie all'avanguardia ed il supporto di un SOC dedicato, Fast Security 360° diventa un potente strumento giornalmente attivo nel mantenimento dello stato dell'arte dei meccanismi di protezione, del controllo antivirale, degli aggiornamenti software e nel servizio di assistenza.

Un servizio di sicurezza gestita come Fast Security 360° permette inoltre ad ogni azienda di potersi concentrare sulle proprie attività strategiche ed essere così più efficiente e competitiva senza dover investire in infrastrutture e personale dedicati alla gestione, manutenzione e messa in sicurezza del proprio patrimonio informativo.

L'offerta commerciale è facile e comprensibile dal momento che prevede differenti pacchetti con differenti funzionalità di sicurezza e di protezione evolute (es.: IDS/IPS, Antivirus&Antispyware, Content Filtering, Crittografia, VPN sicure) che costituiscono il primo ed irrinunciabile passo per un'adeguata difesa. Il servizio



Offerta Fast Security 360 Versione 3.0



è venduto a canone (compreso il comodato d'uso degli apparati di sicurezza necessari per l'erogazione del servizio stesso).

2.2 FAST SECURITY 360°: BENEFICI PER L'AZIENDA

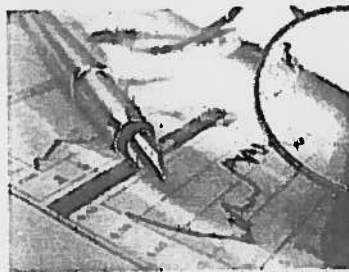
Oltre a garantire un servizio completo di sicurezza informatica, Fast Security 360° offre in particolare importanti vantaggi alle aziende in termini di affidabilità e ottimizzazione delle risorse interne.

- **PROTEZIONE E GESTIONE COMPLETA AD ORARIO CONTINUATO:** Fastweb provvede all'aggiornamento costante della tecnologia e delle minacce di intrusione e virus in continua evoluzione al fine di prevenire e contrastare tutti gli attacchi alla sicurezza e proteggere le infrastrutture e risorse critiche delle aziende nostre clienti. Gli attacchi informatici non seguono il ritmo dell'attività lavorativa, colpendo anche di notte o in pausa pranzo. Il servizio del personale Fastweb Fast Security 360° è sempre attivo, h24, anche con una gestione completa del parco Hardware; ma soprattutto è in grado di riconoscere le nuove minacce in tempo reale, poiché ha visibilità sui gateway di sicurezza di molteplici clienti con differenti configurazioni.
- 
- **FOCALIZZAZIONE DELLE RISORSE SULLE ATTIVITÀ STRATEGICHE DELL'AZIENDA:** l'approccio del servizio di sicurezza gestito permette ad ogni azienda di essere più efficiente concentrandosi sulle proprie attività core e orientando le proprie risorse alla realizzazione delle finalità strategiche dell'impresa. La soluzione Fast Security 360° infatti solleva i clienti dal dover investire tempo e risorse nella gestione, manutenzione e messa in sicurezza del proprio patrimonio informativo delegando ad una terza parte (Managed security Service Provider) le onerose attività operative di gestione dell'infrastruttura di sicurezza. Investire nello sviluppo di soluzioni di sicurezza informatica "in house" spesso non è infatti l'approccio economico più efficiente ed efficace dal momento che richiede un aggiornamento costante in tecnologie e competenze che si evolvono così rapidamente da richiedere l'assegnazione di risorse dedicate. La soluzione gestita consente invece di semplificare il modello ed introduce importanti efficienze economiche sia sugli investimenti che sui costi ricorrenti.
- 

Offerta Fast Security 360 Versione 3.0

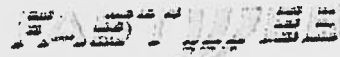
Fast Security 360

- **MASSIMO CONTROLLO SUL SERVIZIO:** esternalizzare non deve comportare una perdita di controllo su un fattore critico dell'infrastruttura Informatica come la sicurezza. Il modello di servizio proposto consente al Cliente di mantenere il completo controllo della Governance della sicurezza: Fastweb Implementa e gestisce con adeguati livelli di servizio le security policies decise in autonomia dal Cliente in funzione dei propri bisogni. Infatti controllare una variabile tecnologica non significa gestirne l'operatività ed impegnare risorse preziose nell'analisi dei *dati*, bensì avere accesso alle *informazioni* chiave attraverso cui dominarla. Fast Security 360° focalizza il cliente su informazioni di sintesi che permettano di controllarne l'evoluzione nel tempo attraverso adeguati tool di reportistica.



Fast Security 360° è quindi la soluzione di OUTSOURCING ottimale, poiché:

- gestisce le variabili tecnologiche e logistiche,
- affianca il cliente nelle scelte di configurazione,
- monitora e gestisce,
- e mette a disposizione un tool di verifica e di analisi della sicurezza.



3 FAST SECURITY 360°: CARATTERISTICHE DEL SERVIZIO

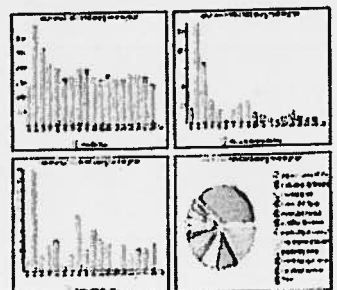
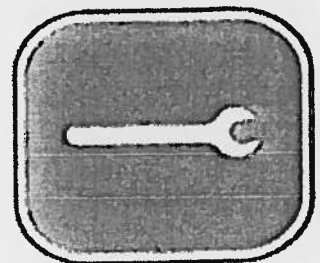
L'approccio Fast Security 360° si basa su un servizio composto da tre blocchi base (Installazione; Gestione, Reportistica) basato su apparati di sicurezza Firewall o UTM (Unified Threat Management) che operano presso la sede del cliente. Il framework di servizio consente l'attivazione da diverse funzionalità di sicurezza, che partono dal Firewalling e che possono essere estese alle funzionalità di IDS/IPS, Antivirus, Content Filtering, Secure VPN, ecc.

3.1 STRUTTURA DEL SERVIZIO

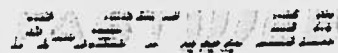
Ogni attività operativa nelle varie fasi dell'erogazione del servizio (progetto, attivazione e gestione) è interamente gestita da personale altamente specializzato appartenente al SOC (Security Operation Center) dedicato alla gestione dei Clienti Enterprise di Fastweb.

In particolare il servizio è costruito su diversi elementi che concorrono a fornire una soluzione consistente ed affidabile.

- **Progetto:** la soluzione di sicurezza viene dimensionata e progettata in accordo con il Cliente sulla base delle specifiche esigenze di protezione (definizione dei requisiti di sicurezza e relative policy).
- **L'attivazione del servizio:** può essere effettuata on-site e/o da remoto.
- **La gestione del servizio.** Si basa su differenti attività:
 - *monitoring ed il logging* degli apparati di sicurezza che avviene attraverso una console di management centralizzata in grado di rilevare eventuali fault e di raccogliere gli eventi critici;
 - *gestione del fault management*, attraverso interventi da remoto o on-site qualora necessari;
 - *change management & patching* eseguiti principalmente da remoto;
- **Apparati di sicurezza necessari all'erogazione del servizio e forniti in comodato d'uso.**
- **Le informazioni sullo stato del servizio sono fornite tramite l'invio di reportistica base (via mail), contenente i tentativi di violazione delle policy impostate per periodo di competenza (settimana, mese); è disponibile inoltre un servizio di reportistica avanzata accessibile tramite un sito web, in grado di consentire un'analisi avanzata degli eventi verificatisi, con esecuzione di query su tutti i campi disponibili (origine attacco, IP,**



Offerta Fast Security 360 Versione 3.0

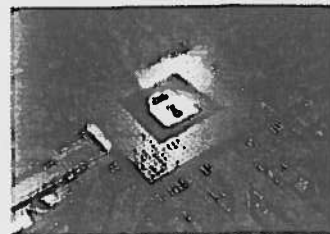


protocolli, ecc).

Maggiori dettagli sul servizio sono presenti nella scheda tecnica Fast Security 360°.

3.2 FUNZIONALITÀ DI SICUREZZA

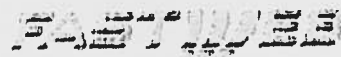
Fast Security 360° offre una protezione estesa del gateway di accesso, sia esso ad Internet o interno ad una VPN MPLS; sono disponibili diverse funzionalità (Firewall, IPS, VPN, Url Filtering, Antivirus/Antispyware, Controllo Applicativo ecc.). Le funzionalità sono pacchettizzate in un'offerta scalabile e quindi adattabile a tutte le esigenze e specializzata in differenti configurazioni.



L'approccio Fast Security 360° prevede sempre la fornitura delle seguenti funzionalità tipicamente implementate su apparati UTM (Unified Threat Management):

- Firewalling che può essere fornita in modalità stand-alone oppure integrata con gli altri servizi di sicurezza;
- IPS (Intrusion Prevention);
- Traffic shaping ;
- VPN Site to site per implementare connessioni sicure via internet con sedi remote (ad esempio all'estero);
- Antivirus & AntiSpyWare : la protezione da Virus, Worm e più in generale da una vasta gamma di codice maligno in grado di installarsi sui PC aziendali (Spyware) è tradizionalmente affidata a software installati direttamente nel client; tuttavia non è sufficiente contrastare solo localmente le infezioni, ma è preferibile bloccarle a monte, cioè prima ancora che questa possa raggiungere il suo bersaglio all'interno della LAN.
- Content Filtering: si intende un'area talvolta non propriamente considerata legata alla sicurezza, e cioè la verifica della congruità della navigazione Internet alle policy aziendali; l'accesso ad Internet è l'area più corretta per bloccare oltre alle intrusioni anche la raggiungibilità di siti di pornografia, gaming, musica, ecc (filtering) che, oltre non essere legati propriamente all'attività lavorativa, spesso sono veicoli di minacce informatiche o legali.
- Crittografia: è un'area propriamente legata alla sicurezza informatica; tradizionalmente è utilizzata per la cifratura delle comunicazioni interaziendali (ad esempio per VPN IPsec via Internet verso sedi remote), ma oggi è usata con successo anche per costruire un livello di riservatezza aggiuntivo per il traffico intraziendale (LAN) e per l'accesso ad alcuni server particolarmente critici (comunicazioni direzionali, applicativi gestionali, database clienti/trattative, ricerca e sviluppo. ecc) .
- Telelavoro: quest'area è particolarmente sensibile alle tematiche di sicurezza perché riguarda l'accesso via Internet a risorse ed apparati posti all'interno della LAN. Grazie alla tecnica del tunneling (Tunnel IPSEC / SSL) è possibile abilitare gli utenti mobili ad accedere ad esempio alle cartelle di rete o alla posta anche quando si trovano al di fuori dei confini aziendali.

Offerta Fast Security 360 Versione 3.0



INFRASTRUTTURA

L'infrastruttura si basa su un sistema di management console ed un sistema di reporting web. I sistemi di sicurezza multi-threat consentono l'installazione di un unico CPE di servizi di sicurezza installato in sede del cliente. Tutte le funzionalità di sicurezza sono monitorate da remoto ed è garantito l'intervento di sostituzione in caso di guasto, secondo gli SLA previsti dal livello di servizio sottoscritto.

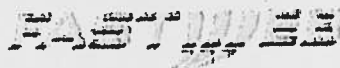
3.3 PROPOSTA PER L'ASL DI ORISTANO

Per l'ASL di Oristano proponiamo la soluzione Fast Security 360° Bundle in configurazione Full con apparati Fortigate FG-40C.

Saranno attivati i servizi di sicurezza con ridondanza di apparati in modalità fail over per i collegamenti che l'ASL di Oristano ha attivi con Fastweb in convenzione SPC presso le seguenti sedi:

- V. MONTE GRAPPA 82 SASSARI SS
- LOC. MASSAMA SNC ORISTANO

Configurazione di servizio	
BASE	Firewall, IDS/IPS, Traffic Shaping, S-VPN, Reportistica e-mail.
FULL	Firewall, IDS/IPS, Traffic Shaping, S2S VPN, Antivirus, Web Content Filtering, B2E (SSL/IPSec-VPN), Reporting web.



3.4 VALORIZZAZIONE ECONOMICA

I servizi prevedono la corresponsione di UT pari a € 1.800,00 e di un canone mensile pari a € 222,00

Di seguito il dettaglio dei servizi:

Descrizione	Quantità	UT	Canone mese	TOT UT	TOT Canone
Attivazione del servizio - Configurazione FULL	2	€ 700,00		€ 1.400,00	
Attivazione ridondanza di apparati in modalità fail over	2	€ 200,00		€ 400,00	
Canone mensile servizio	2		€ 111,00		€ 222,00
TOT				€ 1.800,00	€ 222,00

CONDIZIONI DI FORNITURA

Fatturazione una tantum: All'installazione
Canoni: Mensili posticipati
Esclusioni: IVA e quant'altro non indicato in offerta
Pagamenti: 30 giorni fine mese data fattura
Validità offerta: fino al 20/07/2015

Disponibili per ogni chiarimento si rendesse necessario, in attesa di gradito riscontro con l'occasione porgiamo cordiali saluti


Fastweb SpA

FASTWEB

Business Unit Enterprise

<https://grandlaziende.fastweb.it/>



un passo avanti