

## Proposta Bozza per Business-e

### Soluzione ad hoc per l'autenticazione e l'autorizzazione del sistema di accesso Telecom Italia basato sul protocollo Radius

#### **Descrizione dell'architettura**

Business-e ha richiesto lo studio di un sistema di autenticazione ed autorizzazione altamente affidabile per il controllo degli accessi ad una rete (ospitante numerosi servizi applicativi) protetta da un firewall CheckPoint Firewall-1 NG.

Sulla base delle informazioni raccolte negli incontri con il committente, Hacking Team ha studiato una possibile architettura per il sistema di autenticazione. Questo documento ne descrive le caratteristiche tecniche e l'effort necessario alla sua realizzazione.

Il servizio di autenticazione ed autorizzazione é implementato mediante una batteria di server radius indipendenti. Le richieste di autenticazione provenienti dal firewall sono distribuite sui server radius mediante un dispositivo di load balancing di livello applicativo.

La logica di autenticazione ed autorizzazione é implementata da un modulo di estensione dei server radius sviluppato ad hoc. Tale modulo accede ad un servizio Active Directory remoto (in sola lettura) e ad un repository locale che contiene la definizione delle policy che il firewall deve applicare ad ogni utente.

Il servizio radius può essere amministrato tramite una interfaccia per la definizione delle utenze e dei profili ad esse associati.

Data documento:	Autore:	Revisore:	Codice documento:	Pagina:
2 Marzo 2005	Marco Bettini, Gianluca Vadruccio	Valeriano Bedeschi	Bozza per Business-e	1 di 7

# ]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

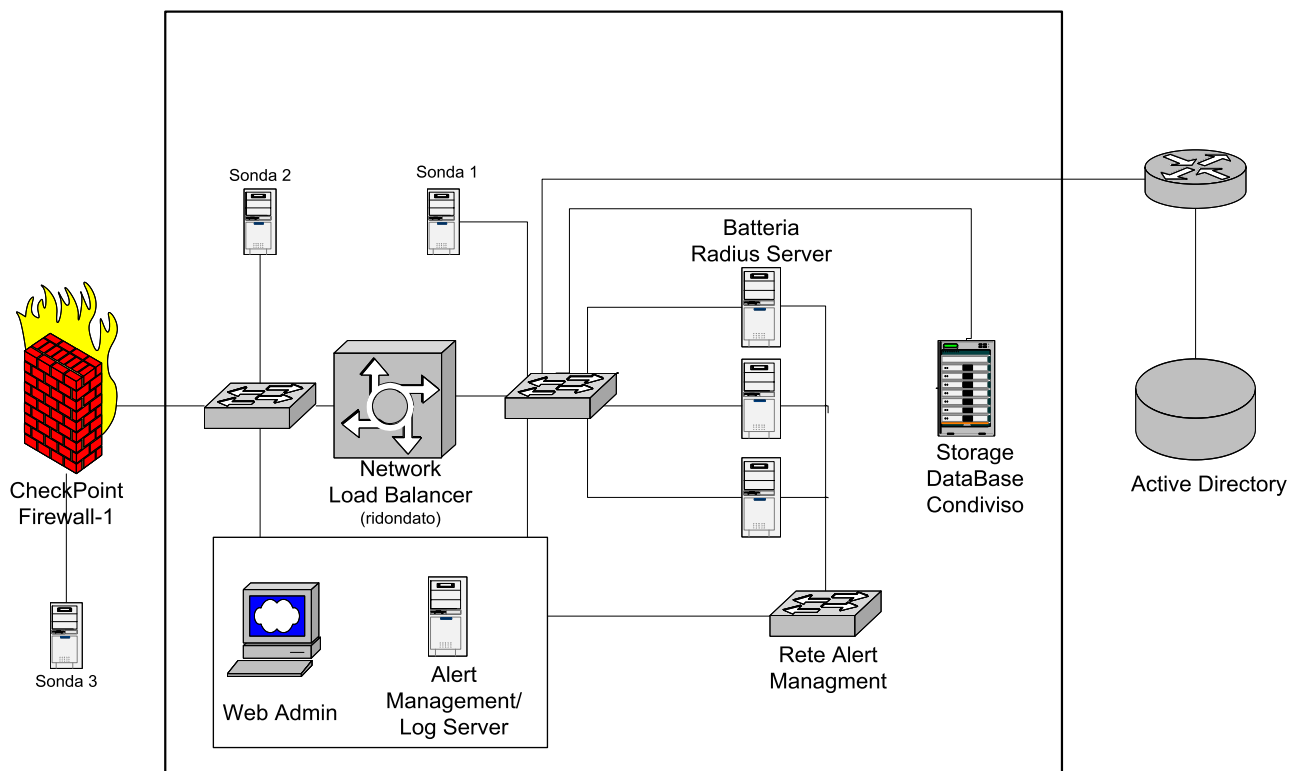
P.IVA: 03924730967 – Capitale Sociale: € 100.000,00

N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Le prestazioni del sistema sono monitorate in modo continuativo da un insieme di agent che misurano e registrano i tempi di risposta dei singoli moduli software che lo compongono.

Lo stato di funzionamento del servizio é inoltre costantemente monitorato da un sistema di alerting che permette di rilevare condizioni anomale di funzionamento e di intraprendere misure correttive. Questo sistema, unitamente alla duplicazione di tutte le componenti critiche, deve garantire un livello di disponibilità del servizio non inferiore al 99,98%.

L'architettura descritta é riportata nella seguente figura e si basa sulle informazioni avute fino ad oggi. Considerando che i requisiti del progetto non sono ancora completamente identificati, tale architettura sarà suscettibile di variazioni.



□

Data documento:	Autore:	Revisore:	Codice documento:	Pagina:
2 Marzo 2005	Marco Bettini, Gianluca Vadrucchio	Valeriano Bedeschi	Bozza per Business-e	2 di 7

## **Caratteristiche della fornitura**

Con riferimento all'architettura sopra descritta, Hacking Team svilupperà i seguenti moduli.

- 1) Modulo di estensione dei server radius per l'implementazione della logica di autenticazione ed autorizzazione richiesta dal Committente. I server Radius saranno installati su hardware Sun con sistema operativo Solaris. I server, il cui numero può essere variato in funzione del carico, devono disporre di un dispositivo di storage condiviso. Tale storage sarà utilizzato per la gestione dei repository locali.
- 2) Modulo di amministrazione per la definizione delle utenze e dei profili ad esse associati. Il sistema di gestione delle utenze, che dovrà accedere sia al servizio Active Directory remoto, sia al repository locale, sarà sviluppato con tecnologia web java-based (jsp, servlet, ecc.).
- 3) Modulo di monitoring delle prestazioni del servizio di autenticazione ed autorizzazione. Il sistema di monitoring delle prestazioni sarà costituito da una serie di sonde che verificano in modo periodico i tempi di risposta delle singole componenti architetture. Tali sonde comunicano con un servizio centralizzato di raccolta dei log, attestato su hardware separato ed opportunamente ridondato.

Nello specifico, alle sonde sarà assegnato il compito di monitorare le seguenti componenti:

- Tempi di risposta del front-end web di autenticazione CheckPoint FW-1 (Sonda 3)
- Tempi di risposta del Network Load Balancer e della batteria di server Radius (Sonda 2)
- Tempi di risposta dei singoli server Radius (Sonda 1)

Tutti i tempi di risposta saranno valutati sulla base di interrogazioni al servizio di cui la componente si fa carico.

Data documento:	Autore:	Revisore:	Codice documento:	Pagina:
2 Marzo 2005	Marco Bettini, Gianluca Vadruccio	Valeriano Bedeschi	Bozza per Business-e	3 di 7

# ]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

P.IVA: 03924730967 – Capitale Sociale: € 100.000,00

N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

- 4) Modulo di alerting per la rilevazione di anomalie e la definizione degli opportuni interventi correttivi. Questo modulo sarà costituito da agent installati sui server Radius e da una console centralizzata di controllo e di gestione automatica degli interventi correttivi a fronte di anomalie. Il server sarà in grado di coordinare gli eventuali interventi correttivi che verranno svolti dagli agent (esempio; riavvio di un servizio, reboot della macchina) per riportare il sistema nelle normali condizioni di funzionamento. Data la sua criticità, il sistema di alerting insiste su risorse hardware e software dedicate. In particolare, ogni server radius sarà dotato di una scheda di rete dedicata per la comunicazione con la console di controllo; quest'ultima sarà installata su un cluster che garantisce i requisiti di disponibilità richiesti.

## **Tempistiche**

Gli effort (in gg/uomo) per la realizzazione dei moduli descritti sono i seguenti:

<i>Modulo</i>	<i>Effort</i>
Modulo di autenticazione	48
Modulo di gestione delle utenze	29
Modulo di monitoring	24
Modulo di alerting	58
<b>Totale</b>	<b>159</b>

Data documento:	Autore:	Revisore:	Codice documento:	Pagina:
2 Marzo 2005	Marco Bettini, Gianluca Vadruccio	Valeriano Bedeschi	Bozza per Business-e	4 di 7

# ]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

P.IVA: 03924730967 – Capitale Sociale: € 100.000,00

N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

## Metodologia

La seguente tabella riporta le principali fasi previste dalla metodologia di sviluppo che Hacking Team intende adottare. Per ogni fase é riportato l'effort corrispondente alle attività che ricadono in essa.

<i>Fase</i>	<i>Effort</i>
Project Setup	10
Project Management	8
Definizione e formalizzazione dei requisiti	13
Disegno della soluzione	16
Sviluppo	66
Manuali utente	7
Documentazione tecnica	9
Testing	16
Collaudo	14
<b>Totale</b>	<b>159</b>

## Risorse

La seguente tabella riporta l'impegno stimato da Hacking Team, suddiviso per figure professionali.

<i>Risorsa</i>	<i>Effort</i>
Security Engineer	45
Senior Security Engineer	59
Security Specialist	47
Project Manager	8
<b>Totale</b>	<b>159</b>

Data documento:	Autore:	Revisore:	Codice documento:	Pagina:
2 Marzo 2005	Marco Bettini, Gianluca Vadruccio	Valeriano Bedeschi	Bozza per Business-e	5 di 7

## **Impegno economico**

La seguente tabella riporta l'impegno economico suddiviso per ognuna delle risorse impegnate nel progetto e comprendente la parte di assistenza e manutenzione.

<i>Componente</i>	<i>Prezzo (euro)</i>
Security Engineer	18.000
Senior Security Engineer	28.000
Security Specialist	24.000
Project Manager	5.000
<b>Totale chiavi in mano</b>	<b>75.000</b>
Assistenza 1° anno	15.000

Il costo totale “chiavi in mano” sopra riportato non include il servizio di assistenza per il primo anno.

I canoni per l'assistenza del secondo e del terzo anno saranno valutati sulla base dell'impegno profuso nel primo anno, ma non potrà subire un aumento superiore al 15% del costo del primo anno.

Il canone di assistenza comprende:

- Manutenzione software per tutto il tempo necessario al fissaggio di eventuali bugs
- Supporto telefonico e/o email
- Supporto on-site per soluzione bugs:
  - fino a 5 giornate se la responsabilità accertata è di Hacking Team

Nel caso in cui la responsabilità accertata non sia di Hacking Team o per richieste specifiche del Cliente stesso, il costo giornaliero dell'intervento è di €540 + spese di trasferta.

Data documento:	Autore:	Revisore:	Codice documento:	Pagina:
2 Marzo 2005	Marco Bettini, Gianluca Vadruccio	Valeriano Bedeschi	Bozza per Business-e	6 di 7

# ]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

P.IVA: 03924730967 – Capitale Sociale: € 100.000,00

N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

---

Al fine di garantire lo sviluppo, il debug e il servizio di assistenza post produzione, il Cliente doterà Hacking Team di un ambiente architettturalmente simile a quello di produzione anche se di potenzialità inferiore.

Tutti i prezzi esposti sono IVA esclusa.

Le modalità di fatturazione e pagamento verranno concordate alla stipula del contratto.

Data documento:	Autore:	Revisore:	Codice documento:	Pagina:
2 Marzo 2005	Marco Bettini, Gianluca Vadruccio	Valeriano Bedeschi	Bozza per Business-e	7 di 7