



Presidenza del Consiglio dei Ministri
SECRETARIATO GENERALE
Dipartimento per le Risorse Umane ed i Servizi Informatici
Ufficio Informatica e Telematica

**Fornitura di un sistema IDP (Intrusion Detection & Prevention)
per il s.i. della Presidenza del Consiglio dei Ministri**

CIG n. 00998059AE

CAPITOLATO TECNICO-AMMINISTRATIVO

INDICE

1.	Definizioni, abbreviazioni e convenzioni generali.....	4
2.	Architettura di riferimento.....	4
3.	Oggetto della fornitura	5
4.	Modalità di funzionamento dei sensori di categoria A.....	6
5.	Caratteristiche delle interfacce dei sensori	6
5.1	Caratteristiche e numero di interfacce per apparati di categoria A	6
5.2	Caratteristiche e numero di interfacce per apparati di categoria B	6
6.	Tecniche di rilevazione degli attacchi (funzionalità IPS)	7
6.1	Rilevamento multi metodo	7
6.1.1	Anomalia di protocollo	7
6.1.2	Rilevamento basato su Signature.....	7
6.1.3	Backdoor Detection	7
6.1.4	Anomalie di traffico.....	7
6.1.5	Network Honeypot.....	7
6.1.6	Synflood Protection	7
6.1.7	Layer-2 detection.....	8
6.1.8	Spoofing Detection	8
6.2	Metodi ulteriori e caratteristiche nella detection.....	8
6.2.1	Ricostruzione del traffico	8
6.2.2	Signature Detection.....	8
	<i>Gerarchie delle Signature</i>	8
	<i>Regular expressions</i>	8
	<i>Raggruppamento delle signature</i>	8
6.2.3	Ispezione del traffico HTTPS.....	8
6.2.4	Gestione del throughput	9
6.3	Aggiornamento delle signature e decodifica dei nuovi protocolli	9
7.	Tecniche di intervento nel caso di rilevamento di attacchi (funzionalità IPS).....	9
8.	Ulteriori caratteristiche e funzionalità firewall.....	9
8.1	Prestazioni.....	10
8.2	Caratteristiche di sicurezza per la funzionalità firewall	10
8.3	Routing e interconnessione alla rete esistente	10
8.4	Caratteristiche di affidabilità per le interfacce	11
8.5	Alta disponibilità.....	11
9.	Sistema di amministrazione e controllo	12
9.1	Caratteristiche generali.....	12
9.2	Caratteristiche hardware e software	12
9.3	Attività di analisi degli eventi generati dai moduli IDP.....	13
9.4	Attività di analisi degli eventi per moduli con funzionalità firewall	14
9.5	Il database degli eventi.....	14
9.6	Caratterizzazione del traffico di rete, per gli apparati di categoria A.....	14
9.7	Security Policies per le funzionalità IPS/IDS.....	15
9.7.1	Criteri di match del traffico IP	15
9.7.2	Criteri di detection degli attacchi.....	15
9.7.3	Criteri di azione	15
9.7.4	Criteri di network	16
9.7.5	Capacità di memorizzazione del traffico in caso di attacco	16
9.7.6	Capacità di alerting.....	16
9.8	Security Policy per funzionalità firewall.....	16

9.8.1	Criteri di match del traffico IP	16
9.8.2	Criteri di azione	16
9.8.3	Criteri di network	17
9.9	Distribuzione delle Policy.....	17
10.	Installazione e predisposizione al collaudo	17
10.1	Installazione.....	17
10.2	Configurazione e predisposizione al collaudo.....	18
11.	Corso di formazione	19
12.	Collaudo.....	19
13.	Erogazione di un servizio di supporto sistemistico	19
14.	Garanzia e manutenzione	20
15.	Penali	20
16.	Subappalto.....	21
17.	Risoluzione anticipata del contratto.....	21
18.	Informazioni generali di gara.....	21
18.1	Busta A - requisiti di ordine generale art.38 decreto legislativo 163/2006	22
18.2	Busta B - offerta tecnica	24
18.3	Busta C - offerta economica	25
19.	Validità dell’offerta.....	25
20.	Procedura di gara.....	26
21.	Aggiudicazione.....	27
22.	Stipulazione del contratto.....	27
23.	Modalità di pagamento.....	28
24.	Legge 675/1996	28
25.	Obblighi di riservatezza della ditta e diritti di proprietà dell’amministrazione	29
26.	Contatti con l’amministrazione	29
	Elenco degli allegati.....	29

1. Definizioni, abbreviazioni e convenzioni generali

Nel presente capitolato sono utilizzate le seguenti abbreviazioni e sigle:

- Presidenza, amministrazione, PCM: Presidenza del Consiglio dei Ministri
- DRUSI: Dipartimento per le Risorse Umane ed i Servizi Informatici della Presidenza
- UIT: Ufficio Informatica e Telematica del DRUSI
- Società, Ditta, Fornitore: ditta, società, impresa o raggruppamento temporaneo di imprese aggiudicatario della gara

Per *formato dei dati*, *formato aperto*, *tecnologia proprietaria*, *formato proprietario* e termini simili si intende quanto definito nella Direttiva del 19/12/2003 del Ministro per l'Innovazione e le Tecnologie, vale a dire:

- per *formato dei dati*, la modalità con cui i dati vengono rappresentati elettronicamente in modo che i programmi informatici possano elaborarli; il formato specifica la corrispondenza fra la rappresentazione binaria e i dati rappresentati (testo, immagini statiche o dinamiche, suono, ecc.); esempi di formati sono Bitmap, GIF, JPEG, ecc.;
- per *formato aperto*, un formato dei dati reso pubblico e documentato esaustivamente;
- per *tecnologia proprietaria*, una tecnologia posseduta in esclusiva da un soggetto che in genere ne mantiene segreto il funzionamento;
- per *formato proprietario*, un formato di dati utilizzato in esclusiva da un soggetto che potrebbe modificarlo a proprio piacimento.

Le sedi della Presidenza in merito alle quali dovranno essere svolte le attività di cui al presente capitolato sono ubicate nel territorio urbano di Roma.

Le dizioni *giorno lavorativo* e *orario lavorativo* utilizzate nel presente capitolato hanno il significato di seguito specificato:

- per *giorno lavorativo* si intendono i giorni della settimana dal lunedì al venerdì, esclusi i giorni considerati festività nazionale in Italia;
- per *orario lavorativo* si intende il periodo dalle ore 9.00 alle 14.00 e dalle ore 14.30 alle 17.30 di qualunque giorno lavorativo.

La lingua utilizzata per tutte le comunicazioni ed i servizi di cui al presente capitolato è la lingua italiana, salvo casi particolari espressamente accettati dalla Presidenza.

2. Architettura di riferimento

Oggetto del presente paragrafo è la descrizione dei componenti necessari per la realizzazione di un'architettura di sicurezza mediante l'uso di sistemi di rilevamento e prevenzione delle intrusioni, che consentano di identificare e di interrompere azioni aventi come obiettivo la violazione o la compromissione del funzionamento di un sistema informatico, di un apparato o dell'intera infrastruttura di rete.

L'architettura prevede un sistema basato sull'impiego di differenti tipologie di sensori di "*intrusion prevention*", distribuiti all'interno dei diversi siti e sull'interfaccia d'accesso alla rete Internet. Tali sensori faranno riferimento ad un sistema di gestione centralizzato, anch'esso oggetto della fornitura, installato su un sistema hardware dedicato.

Sensori di tipo IDS

I sensori di rilevamento delle intrusioni sono in grado di identificare tramite diverse tecniche il traffico di rete malevolo, il cui scopo può essere di

- interrompere l'erogazione di un servizio, o
- consentire ad un soggetto malintenzionato di prendere il controllo di un'apparecchiatura connessa in rete, o
- consentire ad un soggetto malintenzionato di intercettare il traffico che transita su un segmento di rete, o

- in generale, di modificare l'operatività della rete o delle apparecchiature da essa connesse in modo contrario a quanto impostato dai legittimi amministratori della stessa.

Tali sistemi sono nel seguito identificati con la sigla *IDS*.

Sensori di tipo IPS

I sensori che, oltre alle funzionalità descritte prima per gli apparati *IDS*, sono in grado di interrompere, mediante varie tecniche, le operazioni malevole, sono apparati di rilevamento e prevenzione delle intrusioni e saranno nel seguito indicati con la sigla *IDS/IPS* oppure semplicemente *IPS*.

Sensori IPS con funzionalità firewall

I sensori, oltre alle funzionalità di un apparato *IPS*, possono consentire anche di configurare mediante impostazioni attuate dagli amministratori, ed indipendentemente dalle funzionalità *IPS*, il tipo di traffico che può transitare sulla rete, in termini di protocolli abilitati, sorgenti e destinazioni del traffico, limiti di banda, ecc. Tali sensori sono apparati *IPS* con funzionalità *firewall* e saranno indicati nel seguito come *IPS con funzionalità firewall* o *IPS/firewall* o *firewall/IPS*.

Sistema di gestione

L'insieme dei sensori è controllato per mezzo di un sistema di gestione centralizzato, che consente agli amministratori di configurarli e monitorarne il funzionamento.

3. Oggetto della fornitura

Oggetto del presente capitolato è la fornitura, installazione, configurazione e primo avvio di un sistema di rilevamento delle intrusioni composto di apparati *IPS* e *firewall/IPS* e di un sistema di gestione centralizzato.

A seconda della sezione di rete da proteggere, sono richiesti sensori appartenenti alle seguenti categorie, con caratteristiche descritte nel seguito:

- **categoria A:** sensori *IPS* che supportano 1Gb/s di throughput;
- **categoria B:** sensori *IPS/firewall*, che supportano 2Gb/s di throughput.

La società aggiudicataria dovrà fornire:

- tre sensori di categoria A;
- due sensori di categoria B;
- un sistema di amministrazione e di controllo (sistema di gestione).

I sensori di categoria A e quelli di categoria B offerti dovranno essere tutti prodotti dallo stesso vendor.

Tutte le apparecchiature fornite dovranno essere installate presso il CED della Presidenza.

Dovranno essere fornite, inoltre, tutte le componenti hardware e software necessarie al funzionamento, secondo le specifiche richieste, dei sensori e del sistema di gestione, comprese le licenze del software applicativo e dei sistemi operativi. Dovrà essere fornito il materiale necessario al montaggio dei sensori e della stazione di gestione nei rack del CED della Presidenza del Consiglio dei Ministri nonché tutti i cavi di collegamento alla infrastruttura di rete e all'alimentazione elettrica.

I rack sono del tipo standard 19" marca APW modello IMServ.

Tutte le caratteristiche richieste nel presente capitolato devono essere attestate dalla documentazione pubblicamente disponibile dei prodotti forniti rilasciata dal produttore, ad esempio sul proprio sito internet. Insieme all'offerta, la società dovrà allegare copia della suddetta documentazione, con l'indicazione della fonte di provenienza.

La società dovrà infine svolgere un corso di formazione orientato all'amministrazione del sistema per gli utenti dell'UIT.

4. Modalità di funzionamento dei sensori di categoria A

Considerata l'architettura di riferimento precedentemente descritta i sensori dovranno essere in grado di supportare tutte le seguenti modalità di funzionamento.

Modalità TAP

In questa modalità il sensore è collegato ad un HUB o ad una porta di mirroring di uno switch/router ed analizza il traffico di rete che passa attraverso lo switch/router stesso. Il sistema sarà posizionato in questo modo per avere le sole funzionalità di Intrusion Detection.

Modalità in-line

La modalità in-line prevede l'installazione del sensore sulla linea di comunicazione tra due sezioni della rete. Il sensore collegato in questo modo sarà in grado di implementare sia le funzionalità IDS sia quelle IPS, bloccando eventuali attacchi a livello applicativo.

Il sensore dovrà inoltre essere capace di individuare gli attacchi e/o intrusioni in modalità bidirezionale per il traffico che transita tra le due sezioni.

Per questo tipo di modalità si richiede il supporto delle tre seguenti possibili configurazioni:

- *Transparent/Bridge Mode*
In questo tipo di configurazione il sistema inoltra i pacchetti a livello 2 puro, rendendosi completamente trasparente rispetto al routing. Utilizzando questo tipo di configurazione è richiesto il supporto dello spanning tree protocol
- *Route Mode*
In questa modalità il sistema diventa un nodo di rete con funzioni di forwarding di livello 3. Si richiede inoltre il supporto di più istanze virtuali di routing.
- *Proxy Arp mode*
In questa modalità il sistema agisce come un proxy per i messaggi ARP trasferendo le richieste e le risposte tra le reti e annunciando il proprio MAC address per indirizzi remoti.

5. Caratteristiche delle interfacce dei sensori

I sensori oggetto della fornitura saranno dotati di interfacce di tipo Ethernet Rame 10/100/1000Mb/sec e/o fibra, nel numero indicato nei successivi paragrafi. Almeno un'interfaccia fisica di tipo Ethernet su ogni apparato sarà dedicata alla gestione del sensore stesso per l'out of band management.

5.1 Caratteristiche e numero di interfacce per apparati di categoria A

I sensori di categoria A sono in grado di analizzare il traffico passante in modalità in-line, senza degrado delle prestazioni indipendentemente dalla dimensione e dal tipo di pacchetti IP in transito, con throughput minimo pari a 1Gbit/s.

Tali apparati devono essere dotati di almeno 8 interfacce Ethernet 10/100/1000 in rame, per l'attività di sensing, e di almeno una interfaccia Ethernet in rame per la gestione out of band.

Le interfacce in rame utilizzate per la connessione alla rete in modalità in-line devono disporre della funzionalità di bypass integrato all'interno dell'apparato in caso di guasto del sensore.

5.2 Caratteristiche e numero di interfacce per apparati di categoria B

I sensori con funzionalità firewall di categoria B sono in grado di analizzare con funzionalità firewall e IPS il traffico passante in modalità in-line, senza degrado delle prestazioni indipendentemente dalla dimensione dei pacchetti IP in transito, con throughput minimo pari a 2Gbit/s.

Tali apparati devono essere dotati di almeno 8 porte Gb in fibra 1000 Base SX con la possibilità di sostituirle con almeno 8 interfacce Ethernet 10/100/1000 in rame, per l'attività di sensing, e di almeno una interfaccia Ethernet in rame per la gestione out of band.

Per le caratteristiche degli apparati di categoria B, si veda anche il paragrafo 8.

6. Tecniche di rilevazione degli attacchi (funzionalità IPS)

I sensori di entrambe le categorie A e B devono soddisfare le specifiche richieste nel presente paragrafo.

6.1 Rilevamento multi metodo

I sensori dovranno supportare e poter combinare fra di loro diversi metodi di individuazione degli attacchi/intrusioni. Questi metodi dovranno condividere le informazioni per poter intercettare intrusioni sia a livello rete che a livello applicativo e minimizzare la percentuale di falsi positivi.

Si richiede che i sensori supportino almeno gli otto metodi descritti di seguito, che devono essere applicabili contemporaneamente in qualunque condizione di carico degli apparati.

6.1.1 Anomalia di protocollo

I sensori dovranno essere in grado di analizzare i flussi ed identificare eventuali anomalie nei protocolli comunemente utilizzati nell'ambito delle reti IP, in accordo con le definizioni date dagli standard, ad esempio RFC emessi dal IETF, per i protocolli aperti.

I sensori dovranno inoltre prevedere meccanismi di individuazione di "shellcode" (istruzioni in linguaggio assembler presenti tipicamente in applicazioni compilate) all'interno dei flussi di traffico, per individuare attacchi di tipo buffer overflow.

6.1.2 Rilevamento basato su Signature

Il sistema dovrà essere in grado di applicare l'analisi basata su signature in un ambito/protocollo applicativo ben definito e legato al tipo di signature (ad es. una specifica signature può fare riferimento al solo traffico SMTP e non agli altri tipi di traffico) e, all'interno di questo ambito/protocollo, verificare la presenza della signature in un particolare contesto di riferimento; ad esempio, nel caso di traffico SMTP, la signature potrebbe dover essere analizzata nella parte relativa al command mode e non nel contenuto del messaggio vero e proprio (o viceversa). Attraverso tale tecnica il sistema dovrà essere in grado di abbassare la percentuale di falsi positivi. Il sistema dovrà inoltre essere in grado di correlare diverse signature all'interno dei flussi di traffico che, prese singolarmente, non rappresentano attacchi, ma che combinate possono rilevare possibili intrusioni.

6.1.3 Backdoor Detection

Il sistema dovrà essere in grado di individuare la presenza di backdoor sui sistemi mediante l'analisi delle interazioni tra un sistema interno ed uno esterno. Il meccanismo deve basarsi sull'analisi del traffico di tipo interattivo tra client e server su porte standard e non standard, a prescindere dalla presenza di signature o metodi di protocol anomaly per il tipo di traffico.

6.1.4 Anomalie di traffico

I sensori dovranno essere in grado di rilevare anomalie di traffico di rete, non legate ad uno specifico attacco di tipo applicativo. In particolare dovrà individuare attività di tipo network scan o port scan.

6.1.5 Network Honeypot

Il sistema dovrà prevedere una configurazione di honeypot per impersonare servizi ricercati mediante meccanismi di network scanning ed, eventualmente, identificare le sorgenti di attacco.

6.1.6 Synflood Protection

Il sistema dovrà proteggere da DoS attacks mediante meccanismi di SynFlood detection, tipicamente flooding di sessioni che non completano il 3-Way handshake.

Il meccanismo di Synflood protection deve supportare il metodo syn cookie.

6.1.7 Layer-2 detection

Il sistema deve essere in grado di rilevare attacchi al Layer-2, incluso il poisoning dell'ARP table e lo spoofing di MAC addresses (con blocco opzionale del traffico ricevuto in MAC spoofing).

6.1.8 Spoofing Detection

Il sistema deve essere in grado di rilevare traffico proveniente da IP manipolati. Tipicamente attacchi di questo tipo sono volti ad ingannare i sistemi cambiando il proprio IP sorgente non permesso con altro IP permesso.

6.2 Metodi ulteriori e caratteristiche nella detection

6.2.1 Ricostruzione del traffico

Il sistema deve essere in grado di riassemblare il traffico a livello di pacchetto/flusso per poter ricostruire il flusso nello stesso modo in cui lo riceverà la macchina target. Deve inoltre normalizzare il traffico mediante la rimozione di caratteri estranei in modo da assicurarsi che non vi sia ambiguità circa quello che i pacchetti o il flusso contengono. Questo può includere deframmentazione di pacchetti, rimozione di pacchetti in overlap, riordino di pacchetti per la corretta interpretazione dei flussi.

6.2.2 Signature Detection

Per dare maggiore controllo sulle operazioni effettuate dai meccanismi di Stateful Signature Detection, si richiede che le signature messe a disposizione dal produttore del sistema siano visibili dall'amministratore e che siano espresse per mezzo di un meccanismo esaurientemente dettagliato nella documentazione che accompagna il sistema.

L'amministratore dovrà inoltre avere la possibilità, in caso di necessità, di configurare signature personalizzate. I parametri di personalizzazione delle signature devono consentire la creazione di signature multiple basate sul protocollo applicativo applicabili a uno specifico contesto all'interno di esso. Si devono poter scrivere signature che includano anche anomalie di protocollo. Deve essere possibile scrivere signature in grado di individuare attacchi complessi che interessano l'uso di diversi protocolli.

Gerarchie delle Signature

Il sistema deve prevedere la possibilità di gestire gerarchie di signature in modo che, se per una data gerarchia tutte le signature scatenano un evento di allarme, nello strumento di amministrazione che mostra gli eventi, venga mostrato il solo evento relazionato alla signature radice della gerarchia (correlazione degli eventi).

Regular expressions

Il sistema che consente di configurare le signature deve supportare uno dei due formati aperti denominati *regular expressions* (POSIX - RegEx) o *Perl regular expressions* (RE nello standard espresso dal linguaggio di programmazione PERL), per consentire di incorporare versioni multiple dello stesso exploit in una singola signature. La configurazione delle regular expressions deve essere semplificata e aiutata, all'interno dello strumento di configurazione delle signature, mediante apposito menù

Raggruppamento delle signature

Le *attack signatures* devono poter essere raggruppate in termini di tipo di attacco e livello di severità dell'attacco, in modo da agevolarne l'identificazione e l'impiego nelle regole. Deve essere consentita la creazione di gruppi personalizzati di signature o di altri gruppi. Deve essere possibile creare gruppi statici (che contengono solo gli oggetti specificati) o gruppi dinamici che vengono popolati dinamicamente da oggetti basati su criteri di selezione a scelta dell'amministratore.

6.2.3 Ispezione del traffico HTTPS

Il sistema deve essere in grado di ispezionare il traffico HTTPS lato server previa decrittazione del medesimo. A tal fine, deve essere possibile importare nel sistema almeno 100 certificati web server.

6.2.4 Gestione del throughput

Il sistema deve garantire il livello minimo di throughput richiesto, senza disabilitare alcun metodo di detection, anche in condizioni di carico elevato.

6.3 Aggiornamento delle signature e decodifica dei nuovi protocolli

Il produttore del sistema deve disporre di una struttura in grado di rilasciare, in ogni giorno lavorativo, aggiornamenti delle signature. In caso di vulnerabilità di particolare gravità, la struttura dovrà essere in grado di fornire un aggiornamento 7 giorni su 7 e 24 ore su 24.

Il sistema deve supportare l'aggiornamento delle signature, ovvero l'introduzione della decodifica di nuovi protocolli e nuove compound signatures, senza la necessità di riavviare il sensore stesso, e senza caduta delle sessioni attive, durante l'aggiornamento.

Il sistema deve essere in grado di aggiornare le signature automaticamente, senza l'intervento manuale dell'operatore, in base a programmazione effettuata dall'utente, con frequenza almeno giornaliera.

7. Tecniche di intervento nel caso di rilevamento di attacchi (funzionalità IPS)

Le specifiche richieste nel presente paragrafo si applicano ai sensori di entrambe le categorie A e a B.

Il sistema, nel caso rilevi un attacco, deve essere in grado di impedirne l'esecuzione per mezzo delle seguenti tecniche:

- drop packet (scarto del pacchetto);
- drop session (scarto della sessione);
- close client (mandare un segnale di chiusura [RESET] lato client);
- close server (mandare una segnale di chiusura lato server [RESET]);
- close both (mandare un segnale di chiusura [RESET] ad entrambi gli estremi della connessione, client e server).

Per consentire la limitazione del traffico, tramite imposizione della QOS da parte degli apparati di rete, il sensore deve essere in grado di modificare il *diffserv* del pacchetto in caso si verifichino determinati attacchi o per particolari applicazioni.

La marcatura deve poter essere impostata tramite regola, secondo la definizione data in seguito.

8. Ulteriori caratteristiche e funzionalità firewall

Le specifiche richieste nel presente paragrafo si applicano ai sensori di categoria B.

I sensori di categoria B, oltre alle funzionalità IDS/IPS specificate precedentemente, dovranno essere dotati di funzionalità firewall.

Tali apparati, dovranno consentire di controllare il traffico di rete ai livelli 3 e 4 della pila ISO/OSI tra i segmenti connessi alle interfacce tramite la configurazione di opportune regole, indipendenti da quelle configurate per l'ispezione del traffico effettuata dalle funzioni IDS e IDP. In particolare, le regole relative alla funzionalità firewall consentiranno di bloccare o autorizzare il traffico tra due entità in rete, secondo le specifiche del paragrafo 9.8.

Gli apparati di categoria B devono supportare una configurazione ad alta affidabilità mediante l'impiego di due apparati fisicamente distinti.

Gli apparati di categoria B devono prevedere alimentazione ridondata con alimentatori sostituibili a caldo (hot swap).

Il produttore degli apparati di categoria B deve essere lo stesso di quelli di categoria A.

È richiesta la possibilità di creare nel dispositivo un motore di routing virtuale da dedicare all'interfaccia di Management, in modo da poter realizzare il management in "out of band" senza interazioni con le tabelle di routing dei virtual routers dedicati al forward del traffico.

Gli apparati devono consentire di realizzare la funzionalità di traduzione degli indirizzi di rete (NAT).

8.1 Prestazioni

Si richiedono le seguenti prestazioni minime:

- Throughput di 2 Gb/s per dimensioni dei frame da 64 Bytes a 1518 Bytes, per traffico in chiaro con funzionalità firewall e IPS contemporaneamente attive
- Throughput di 1 Gb/s per dimensione dei frame da 64 Bytes a 1518 Bytes, per traffico criptato IPSEC 3DES e/o AES in modalità firewall
- 100.000 sessioni contemporanee
- 10.000 tunnel IPSEC contemporanei
- 500 VLAN 802.1q
- 25.000 security policies
- 10.000 nuove sessioni al secondo

8.2 Caratteristiche di sicurezza per la funzionalità firewall

La componente di firewall degli apparati deve effettuare l'inoltro dei pacchetti sulla base della sessione firewall.

Il componente firewall deve realizzare la protezione a livello di rete almeno per i seguenti attacchi DOS e DDOS noti:

- Syn flood. Con funzionalità syn proxy (syn cookie accelerato in ASIC).
- UDP flood.
- Ping of death.
- Land Attack.
- WinNuke Attack.
- IP Source Route Attack.

Il componente firewall deve consentire la protezione almeno dai seguenti tipi di pacchetti malformati:

- SYN e FIN bit settati contemporaneamente.
- Nessun flag settato per i pacchetti TCP.
- FIN senza ACK.

Il firewall deve essere del tipo "stateful inspection" con gestione dinamica delle aperture delle sessioni per i seguenti protocolli (Application Layer Gateway):

DNS, FTP, HTTP, IMAP, SMTP, POP3, PPTP, RSH, H.245, Q.931, RAS, PORTMAPPER (SUN RPC), SIP, SQL*NET V2, TALK, TFTP, RealMedia, RTSP, VDOLive, XING, MSRPC.

8.3 Routing e interconnessione alla rete esistente

Oltre alle caratteristiche fisiche descritte in precedenza, i sistemi di categoria B devono avere le seguenti caratteristiche atte all'integrazione nella rete esistente:

- **Supporto della modalità routing.** Il sistema supporta le funzionalità di router. In caso di high availability il cluster di sistemi deve essere visto dai routers/hosts adiacenti come un sistema con unico indirizzo IP a cui puntare per il forwarding del traffico. In questa modalità il sistema deve supportare RIP V1/V2, OSPF, BGP, oltre a routing statico, multicast, source based routing, source interface based routing.
- **Supporto della modalità trasparente.** Il sistema si configura come elemento trasparente rispetto ai segmenti di rete attestati alle interfacce. I sistemi attestati sui segmenti di rete connessi in modalità trasparente risiedono in unico dominio di broadcast. Il sistema anche in questa modalità è in grado di realizzare le funzionalità di statefull firewall a livello 3 e 4, e le funzionalità di IPS-IDS ove siano configurati gli appositi componenti dedicati allo scopo.

Il sistema deve supportare un livello di virtualizzazione del routing: in ogni sistema si devono poter configurare istanze di routing virtuale, ciascuna delle quali in grado di avere proprie tabelle di routing e proprie adiacenze per i protocolli di routing sopra elencati: deve essere possibile esportare o importare rotte da o verso un differente virtual router definito all'interno del sistema, o mantenere isolati i virtual routers tra loro. Deve essere possibile assegnare ai virtual routers interfacce fisiche o logiche (sub interface con VLAN 802.1q, interfacce aggregate o in ridondanza, tunnel interface, interfacce loopback). Deve essere possibile definire come next hop per determinate rotte un altro virtual router all'interno del sistema

In caso avvenga un cambiamento di routing che impone al traffico una differente interfaccia di uscita il sistema deve essere in grado di:

- preservare le sessioni di firewalling esistenti per il traffico in chiaro entrante e uscente;
- aprire nuove sessioni di firewalling entranti e uscenti utilizzando le stesse policy di sicurezza;
- preservare le sessioni di traffico criptato che debba utilizzare nella nuova condizione tunnel differenti, sia per traffico entrante che per traffico uscente (security associations).

8.4 Caratteristiche di affidabilità per le interfacce

L'apparato deve essere in grado di supportare l'aggregazione di porte, fino a 2 porte gigabit Ethernet e fino a 8 porte Ethernet 10/100 Mb/s. La distribuzione del traffico tra la porte fisiche aggregate deve avvenire almeno mediante algoritmo round robin su base pacchetto.

Deve essere permessa la creazione di porte in redundancy, la creazione cioè di porte logiche ciascuna delle quali sia composta da almeno due porte fisiche, in modo da utilizzare connessioni agli switch in dual homing: le porte fisiche componenti la singola porta logica devono poter essere connesse ciascuna a uno switch differente sulla medesima VLAN e il sistema effettuerà l'inoltro del traffico su una delle due porte evitando loop di livello due con o senza meccanismi di spanning-tree. In caso di caduta della porta primaria, il sistema deve essere in grado di utilizzare una delle secondarie, preservando le sessioni di traffico, lo stato delle interfacce logiche, le security association (SA di IPSEC).

8.5 Alta disponibilità

Oltre ai sistemi di ridondanza e aggregazione a livello di porta, e alla persistenza delle sessioni ove vi sia cambiamento di routing, deve essere possibile creare cluster di due unità per l'alta disponibilità dell'intero sistema. Deve essere possibile configurare un componente del cluster in condizione attiva, l'altro in condizione passiva. In caso di fault dell'unità primaria, la seconda diverrà operativa. Il tempo di commutazione deve poter essere configurabile e deve poter essere portato sotto il minuto secondo.

In alternativa è accettata una configurazione in cui i due apparati sono in modalità load sharing.

Il sistema deve garantire che la configurazione degli apparecchi che costituiscono il cluster sia sincronizzata, e deve avvisare l'operatore quando ciò non sia possibile, ad esempio per guasto di uno dei costituenti.

Il sistema operativo degli apparecchi di categoria B, deve garantire la sincronizzazione degli oggetti variabili tipicamente presenti nei sistemi di firewalling. In particolare occorre che le due unità del cluster siano sincronizzate per le sessioni di firewalling del traffico in chiaro e del traffico criptato, per i dati PKI (certificati) eventualmente presenti, e le security associations di Fase 1 e Fase 2 per l'IPSEC. Lo switching del cluster deve avvenire in maniera trasparente per il traffico che attraversa i sistemi.

Ciascun sistema deve prevedere almeno due interfacce Ethernet 100Mb dedicate in modo esclusivo al colloquio di sincronizzazione e stato del cluster e si deve poter definire una ulteriore interfaccia aggiuntiva tra quelle a disposizione per il traffico normale che venga utilizzata per il traffico di heartbeat del cluster. Questo per far sì che in caso di perdita di entrambi i link di high availability non avvenga il fenomeno dello split brain, con entrambi i sistemi del cluster in condizione attiva.

9. Sistema di amministrazione e controllo

Il sistema di amministrazione e controllo, nel seguito chiamato sistema di gestione, deve essere capace di memorizzare centralmente lo stato dei sensori, i dati provenienti da essi e le impostazioni di configurazione di ciascuno di essi.

Il sistema di gestione deve consentire a più amministratori di effettuare, indipendentemente e contemporaneamente, ciascuno dalla propria postazione di lavoro, l'analisi dei dati e la visualizzazione dello stato dei sensori.

Il sistema di gestione deve consentire agli amministratori la configurazione e l'amministrazione centralizzata dei sensori tramite pacchetti di impostazioni di configurazione, nel seguito chiamati "*policy*".

Il sistema di gestione, deve consentire di effettuare le attività sopra riportate per mezzo di una interfaccia grafica (GUI) che raggruppi tutti gli strumenti di gestione, accessibile dalla postazione di lavoro dei singoli utenti.

La comunicazione tra i vari componenti del sistema dovrà essere crittografata e autenticata.

9.1 Caratteristiche generali

Il sistema di gestione dovrà essere in grado di:

- Gestire e definire le *policy* tramite un'unica interfaccia grafica, in modo centralizzato, indipendentemente dagli apparati su cui verranno installate.
- Consolidare i dati provenienti da differenti sensori in un singolo repository.
- Permettere a più utenti amministratori, ciascuno identificato per mezzo di un account personale, di gestire i sensori; non deve essere presente un limite al numero di amministratori definibili. Un solo amministratore privilegiato deve essere abilitato ad aggiungere o a eliminare gli altri amministratori; deve essere possibile attribuire permessi individuali agli amministratori per quel che riguarda l'accesso alle funzioni del sistema; in particolare per ogni amministratore dovrà essere possibile almeno discriminare tra l'accesso in sola lettura o in lettura e scrittura.
- Gestire più apparati contemporaneamente fino ad almeno 100 apparati.
- Gestire l'aggiornamento del firmware dei sensori di categoria A e di categoria B.

Il sistema dovrà essere in grado, oltre ad intercettare intrusioni ed attacchi, di rilevare dalle attività di rete le caratteristiche dei sistemi informatici presenti, al fine di:

- verificare che i sistemi di interesse siano sempre correttamente aggiornati con i livelli di patching di sicurezza richiesti;
- verificare che i sistemi non stiano generando traffico di tipo diverso da quello per il quale sono stati installati (caratterizzazione del traffico);
- individuare sistemi soggetti ad eventuali vulnerabilità confrontando un database di vulnerabilità con le versioni di software installate, rilevate dall'analisi di rete.

Le seguenti funzioni devono soddisfare i requisiti espressi dalle specifiche "Common Criteria":

- Audit Table: completezza e accuratezza
- Audit Log Migration: I log di auditing di formato precedente devono poter essere emigrati nel nuovo formato
- Gestione spazio disco residuo per i log di Auditing: il sistema di log può rimuovere vecchie voci di log prima di inserirne di nuove per liberare spazio disco se necessario
- Blocco dei "log in": possibilità di bloccare il "log in" da un certo IP dopo un certo numero di fail

9.2 Caratteristiche hardware e software

Per consentire al personale tecnico dell'Ufficio per l'informatica e la telematica una efficiente gestione dei sistemi forniti, l'hardware e il software di sistema del sistema di gestione dovranno rispettare le seguenti caratteristiche.

- Le macchine che compongono il sistema di gestione devono essere di architettura x86 e devono essere in ogni caso compatibili col software di gestione descritto nel presente paragrafo.
- Qualora il software di sistema fornito sia Windows, dovrà essere fornito Windows 2003 server e non superiore. Qualora il software di sistema fornito sia Red Hat Linux, dovrà essere fornito Red Hat Enterprise 4.0 o superiore. Il software di sistema fornito deve essere in ogni caso compatibile col software di gestione descritto nel presente paragrafo.

Il sistema di gestione dovrà avere almeno le seguenti caratteristiche hardware:

- Sistema biprocessore con frequenza di clock di CPU pari almeno a 3GHz.
- Memoria 2GB estendibile a 4GB.
- Dischi SCSI 10000 rpm e controller RAID hardware. I dischi forniti, in configurazione RAID5, dovranno avere almeno dimensione complessiva pari a 180GB.
- 2 Ethernet adapter 10/100/1000 su rame.

Il sistema di gestione deve consentire una configurazione ridondata in alta affidabilità su due macchine distinte. In caso di guasto di una delle due macchine, i client e i sensori si collegano automaticamente all'altra, senza interruzione di servizio. Per quel che riguarda le attività di configurazione e monitoraggio, le due macchine durante il funzionamento normale devono essere costantemente sincronizzate, in modo che in caso di guasto la funzionalità del sistema è automaticamente ripristinata senza intervento manuale dell'operatore.

Per quel che riguarda la sola funzione di memorizzazione dei log generati dai sensori, è ammesso che questa avvenga sulla sola macchina attiva.

9.3 Attività di analisi degli eventi generati dai moduli IDP

Il sistema di gestione dovrà prevedere la memorizzazione centralizzata delle informazioni di log generate dai sensori distribuiti all'interno dell'infrastruttura di rete. In particolare dovrà essere possibile visualizzare e classificare gli eventi presenti nel repository dei log in funzione di:

- istante di tempo in cui l'allarme viene ricevuto;
- nome assegnato dal produttore e/o da enti indipendenti alla signature/anomalia;
- azione effettuata sul flusso, ad es. se il flusso è stato bloccato o accettato; nel caso sia stato bloccato, la modalità di effettuazione del blocco;
- interfaccia di ingresso e di uscita del flusso che ha generato l'allarme;
- indirizzo sorgente e destinazione/porta sorgente e destinazione del flusso;
- sensore che ha generato l'evento;
- identificativo della policy/regola che ha generato l'evento.

Il sistema dovrà essere in grado di fornire informazioni dettagliate relative al tipo di evento, facendo eventualmente riferimento anche a fonti esterne. Ove applicabile, quindi, deve essere presente un insieme esteso di informazioni per l'oggetto attacco inerente alla linea di log. In particolare devono essere indicati:

- La descrizione con la storia dell'attacco e informazioni dettagliate sul funzionamento dell'attacco.
- L'indicazione della categoria dell'attacco, come caratterizzato dal sistema IDP.
- Impatto dell'attacco. Deve essere descritto in dettaglio l'impatto sulle risorse colpite in caso l'attacco sia compiuto con successo, includendo informazioni su crash di sistema e/o il tipo di accesso guadagnato dall'attaccante.
- Patches. La lista delle eventuali patches disponibili presso il produttore del sistema sotto attacco, con informazioni su come prevenire l'attacco stesso e/o affrontarne le conseguenze.
- Informazioni tecniche, informazioni sulla vulnerabilità sfruttata, sui comandi eseguiti durante l'attacco, sulle conseguenze sui sistemi oggetti dell'attacco.
- Commenti dal fornitore; indicazioni sul piano di rilascio per le fix ove non siano state ancora rilasciate.
- Indicatori del livello di allarme. Lista di eventi sospetti che potrebbero indicare il successo dell'attacco.

- Prodotti affetti. Lista dei prodotti affetti dalla vulnerabilità che ha generato l'evento in log.

Si dovrà inoltre avere la possibilità di analizzare nel dettaglio i pacchetti IP associati al flusso, prima e dopo il verificarsi dell'evento. Il numero di pacchetti memorizzati dal sistema di management deve essere configurabile all'interno delle policy da parte dell'amministratore.

Il sistema di visualizzazione deve poter impostare viste multiple e contemporanee, utilizzando differenti criteri di visualizzazione per poter agevolare la comparazione tra i dati e organizzare le viste in maniera flessibile. Il sistema di visualizzazione dei log deve consentire di visualizzare informazioni sul pacchetto e sulla policy che ha generato l'evento. Il visualizzatore dei log deve avere una sezione che contenga la descrizione dell'attacco rilevato, il pattern della signature ove applicabile e le referenze che contengano i link ai siti di analisi delle vulnerabilità dove viene descritto l'attacco stesso; deve essere possibile, cliccando sui link di riferimento, aprire la relativa pagina nel browser predefinito.

Lo strumento di visualizzazione deve consentire di configurare e salvare filtri personalizzati in base a parametri di visualizzazione.

9.4 Attività di analisi degli eventi per moduli con funzionalità firewall

Il sistema di gestione dovrà obbligatoriamente prevedere la memorizzazione centralizzata delle informazioni di log generate dai moduli con funzionalità firewall distribuiti all'interno dell'infrastruttura di rete. In particolare dovrà essere possibile visualizzare e classificare gli eventi legati alla funzionalità firewall, presenti nel repository dei log in funzione almeno di:

- istante di tempo in cui l'informazione sulla sessione è ricevuta;
- azione effettuata sul flusso, ad es. se il flusso è stato bloccato o accettato; nel caso sia stato bloccato, la modalità di effettuazione del blocco;
- interfaccia di ingresso e di uscita del flusso;
- indirizzo sorgente e destinazione/porta sorgente e destinazione del flusso;
- apparato che ha generato l'informazione;
- identificativo della policy/regola che ha generato l'azione.

Il sistema di visualizzazione deve poter impostare viste multiple e contemporanee, utilizzando differenti criteri di visualizzazione per poter agevolare la comparazione tra i dati e organizzare le viste in maniera flessibile.

Lo strumento di visualizzazione deve consentire di configurare e salvare filtri personalizzati in base ai parametri di visualizzazione.

9.5 Il database degli eventi

Il database per gli eventi registrati dal sistema di gestione deve poter scrivere almeno 10.000 eventi di log al secondo. La dimensione del database e il numero di eventi memorizzabili non devono avere limiti se non quelli imposti dai dispositivi fisici di memorizzazione.

Ciascuna porzione del database deve poter essere archiviata su base almeno giornaliera mediante semplici comandi di copia files. Il ripristino deve avvenire mediante copia dei file rimossi nella apposita directory del sistema di management.

Se la capacità massima del database viene raggiunta, il sistema deve provvedere alla cancellazione dei dati in eccesso, a partire dai più vecchi.

Il database deve poter essere esportato almeno nel formato testo CSV (comma separated values).

9.6 Caratterizzazione del traffico di rete, per gli apparati di categoria A

Il sistema di gestione deve prevedere, per i soli sensori di categoria A, un componente di analisi del traffico di rete che aiuti gli amministratori a caratterizzare il tipo di traffico presente all'interno della propria rete.

Il sistema deve essere in grado di caratterizzare il traffico che attraversa il sensore in base al tipo di traffico e agli elementi che lo compongono.

In particolare la caratterizzazione dovrà comprendere:

- gli hosts;
- il peering tra hosts (i flussi tra coppie di hosts);
- le porte applicative utilizzate (protocolli non IP, porte TCP/UDP, programmi RPC) e dati dal livello 7 della pila ISO-OSI che identifichino in maniera univoca hosts;
- applicazioni;
- comandi passati nei protocolli;
- utenti e nomi files;
- sistemi operativi e ove possibile la versione dei sistemi operativi (OS Fingerprinting / Application Fingerprinting).

Il sistema è così in grado di monitorare e raccogliere in un apposito database dati sui dispositivi di rete (server, servizi, router, etc.) quali MAC/IP addresses e numeri di porte.

Il sistema può essere in grado di caratterizzare il traffico di rete fornendo informazioni sulle applicazioni (versioni, tipo, piattaforma) in uso sulla rete.

E' richiesto un tool grafico che consenta di visualizzare in tempo reale i flussi applicativi che passano in rete basandosi sui dati di log e report, nonché su profili definibili.

9.7 Security Policies per le funzionalità IPS/IDS

Il sistema di management deve consentire un approccio basato su rule/policies che consenta la scansione/protezione della rete mediante un'unica security policy per l'intera infrastruttura di rete. Ciascuna security policy è costituita da insiemi di regole. Ogni regola deve permettere di selezionare differenti meccanismi di detection tra quelli disponibili. Inoltre ogni regola deve consentire di configurare almeno i seguenti parametri:

- criteri di match per il traffico;
- criteri di detection degli attacchi;
- criteri di azione da intraprendere;
- criteri di network;
- memorizzazione del traffico in caso di attacco;
- metodi di alerting.

9.7.1 Criteri di match del traffico IP

I criteri di match del traffico devono avvenire in base a:

- protocollo IP;
- IP sorgente e destinazione, espressi come singoli indirizzi, sottoreti, o intervalli di indirizzi;
- porte di destinazione.

L'amministratore deve avere la possibilità di configurare eccezioni sulla singola regola, in qualsiasi momento.

Deve essere possibile escludere dalla regola singoli indirizzi IP, reti e subnets o intervalli di indirizzi. L'eccezione deve essere configurata in modo indipendente dalla regola stessa, e deve avere la forma di una sottoregola di eccezione che contiene le esclusioni: il meccanismo deve quindi consentire la rapida definizione delle eccezioni e la loro eventuale rimozione.

9.7.2 Criteri di detection degli attacchi

I criteri di detection degli attacchi specificano per ogni regola, quali sono gli attacchi la cui individuazione è abilitata.

Il sistema deve poter permettere la creazione di gruppi di attacchi ed i gruppi debbono poter essere sia statici che dinamici secondo quanto descritto in precedenza in questo documento.

9.7.3 Criteri di azione

I criteri di azione della regola definiscono quale azione prendere nei confronti della specifica sessione contenente un attacco o una anomalia rilevata nella regola:

- do nothing (non fare nulla);
- drop packet (scarto del pacchetto);

- drop session (scarto della sessione);
- close client (mandare un segnale di chiusura [RESET] lato client);
- close server (mandare una segnale di chiusura lato server [RESET]);
- close both (mandare un segnale di chiusura [RESET] ad entrambi gli estremi della connessione, client e server).

Allo stesso tempo si devono poter definire le azioni di notifica da intraprendere, secondo quanto specificato al paragrafo 9.7.6 "Capacità di Alerting".

9.7.4 Criteri di network

I criteri di network stabiliscono esattamente su quali sensori si vuole applicare la regola.

Se sul sensore sono configurate VLAN, deve essere possibile specificare la VLAN a cui applicare la regola.

Una volta che sia stata definita una regola, il sistema di management centrale deve applicarla automaticamente ai sensori indicati nella regola stessa.

9.7.5 Capacità di memorizzazione del traffico in caso di attacco

Il sistema deve poter consentire il packet logging, ovvero il salvataggio di pacchetti prima, durante e dopo l'attacco in formato libpcap: dalla postazione operatore deve essere possibile richiamare una applicazione integrata oppure una esterna, impostata dall'amministratore, per analizzare i pacchetti catturati per un dato evento quando nella regola sia stata attivata l'opzione che consente il salvataggio dei pacchetti.

Deve potersi impostare il numero massimo di pacchetti da salvare.

9.7.6 Capacità di alerting

Il sistema deve prevedere almeno i seguenti 5 metodi differenti di alerting per gli eventi.

I metodi standard devono essere almeno quelli di:

- mostrare icone di avviso sulla console operatore;
- messaggi via trap SNMP;
- notifica via e-mail a destinatario definito;
- messaggi syslog;
- esecuzione di script custom e/o avvio di programmi esterni al sistema di management, tramite le funzioni offerte dal sistema operativo.

I meccanismi di alerting devono obbligatoriamente poter essere definiti granularmente a livello di singola regola, in modo da poter avere differenti meccanismi attivati su differenti regole.

9.8 **Security Policy per funzionalità firewall**

L'unica security policy per l'intera infrastruttura di rete, descritta al paragrafo 9.7, deve contenere anche le regole per l'impostazione della funzionalità firewall, applicabile ai dispositivi di categoria B. L'insieme delle regole deve consentire di specificare il traffico di rete ammesso o bloccato. Inoltre ogni regola deve consentire di configurare almeno i seguenti parametri:

- criteri di match per il traffico;
- criteri di azione da intraprendere;
- criteri di network.

9.8.1 Criteri di match del traffico IP

I criteri di match del traffico devono avvenire in base a:

- protocollo IP
- IP sorgente e destinazione, espressi come singoli indirizzi, sottoreti, o intervalli di indirizzi
- porte di destinazione.

9.8.2 Criteri di azione

I criteri di azione della regola definiscono quale azione prendere nei confronti della specifica sessione definita dai criteri di network:

- Accetta la sessione,
- Rifiuta la sessione,
- Scarta la sessione.

Nel caso la sessione sia accettata, deve essere possibile definire se il traffico risultante debba essere sottoposto anche al controllo del componente IDP. In questo ambito deve essere possibile scegliere se il traffico da far controllare dal motore IPS-IDS debba passare attraverso il motore IPS-IDS o ne debba essere mandata una copia.

9.8.3 Criteri di network

I criteri di network stabiliscono esattamente su quali sensori si vuole applicare la regola.

Se sul sensore sono configurate VLAN, deve essere possibile specificare la VLAN a cui applicare la regola.

Una volta che sia stata definita una regola, il sistema di management centrale deve applicarla automaticamente ai sensori indicati nella regola stessa.

9.9 Distribuzione delle Policy

Le policy sono definite mediante la GUI operatore e, quindi, su comando dell'amministratore installate automaticamente sugli apparati interessati.

L'aggiornamento deve avvenire in maniera incrementale: durante la fase di update il sensore interessato deve continuare il proprio lavoro di detection e blocco del traffico basandosi sulla precedente versione delle policy. Al momento del caricamento delle nuove regole le connessioni presenti sull' IPS-IDS non devono essere cancellate.

La comunicazione tra i componenti del sistema deve essere cifrata mediante algoritmo a chiavi asimmetriche di almeno 2048 bit e simmetriche di almeno 128 bit.

10. Installazione e predisposizione al collaudo

Tutto il materiale oggetto della fornitura dovrà obbligatoriamente essere consegnato presso la sede centrale della PCM, o altra sede/i indicata/e, entro 50 giorni solari dalla data di accettazione dell'ordine. Successivamente a tale termine saranno applicate le penali di cui al paragrafo 15.

Le attività di installazione, configurazione e predisposizione al collaudo, dovranno terminare con la dichiarazione formale di disponibilità al collaudo entro 90 giorni solari dalla data di accettazione dell'ordine. Successivamente a tale termine saranno applicate le penali di cui al paragrafo 15.

È facoltà dell'amministrazione estendere, ove ritenuto necessario, tali periodi dandone comunicazione per iscritto alla società.

10.1 Installazione

Tutte le apparecchiature fornite, sensori e stazione di gestione, dovranno essere di tipo "rack mountable".

La società dovrà provvedere all'installazione degli apparati forniti, nei locali indicati dall'amministrazione, secondo le indicazioni dei tecnici che ne fanno parte. Le sedi di installazione sono in Roma.

Gli apparati saranno installati all'interno dei rack, che non sono oggetto della fornitura, secondo le indicazioni dell'amministrazione. I rack sono del tipo standard 19" marca APW modello IMServ.

La società dovrà fornire tutto il materiale necessario al montaggio delle apparecchiature nei rack, il materiale necessario al cablaggio per il collegamento all'infrastruttura di rete e quello necessario al collegamento alla rete elettrica, utilizzando gli impianti presenti in ogni sito di installazione.

La società dovrà collegare e configurare le interfacce delle apparecchiature di categoria A e B all'infrastruttura di rete secondo le specifiche dei tecnici dell'amministrazione. La società dovrà etichettare le bretelle di collegamento degli apparati forniti agli apparati di rete dell'amministrazione, indicando il nome dell'apparato e il riferimento all'interfaccia dell'apparato.

L'attività di installazione dovrà essere condotta in modo da limitare al minimo eventuali interruzioni dei servizi di rete dell'amministrazione. Qualora tali interruzioni siano necessarie, sarà

concordato con l'amministrazione l'orario di svolgimento delle attività relative, che potranno avvenire al di fuori dell'orario lavorativo definito al paragrafo 1. In particolare, a seconda dell'entità del disservizio, potrà essere richiesto di svolgere tali attività nella fascia oraria 7-8 o 19-21 oppure nel pomeriggio del sabato o durante la domenica.

La società dovrà provvedere, al momento dell'installazione, all'eventuale aggiornamento del software/firmware delle apparecchiature fornite all'ultima versione disponibile.

Al termine dell'installazione la società dovrà fornire all'amministrazione documentazione scritta delle attività svolte. In particolare, dovranno essere indicati almeno l'elenco dei materiali e delle apparecchiature forniti, la posizione degli apparati installati (numero del rack, nome del locale e sede), le porte e gli apparati di rete su cui gli apparati forniti sono stati attestati, la configurazione delle interfacce di rete degli apparati forniti.

10.2 Configurazione e predisposizione al collaudo

Dopo l'installazione nei rack e il collegamento all'infrastruttura di rete, per facilitare le attività di configurazione, la società potrà configurare tutti gli apparecchi forniti in modo che per un periodo massimo di sette giorni solari acquisiscano informazioni sul traffico che transita attraverso di essi, senza l'attivazione delle funzionalità firewall/IDP.

Successivamente la società procederà alle attività di prima configurazione delle funzionalità firewall e IDP, secondo quanto esposto nei paragrafi successivi.

Le attività di cui al presente paragrafo dovranno essere svolte da personale provvisto di certificazione individuale relativa all'uso delle apparecchiature fornite, ove questa sia prevista dal produttore.

L'attività di configurazione dovrà essere condotta in modo da limitare al minimo eventuali interruzioni dei servizi di rete dell'amministrazione. Qualora tali interruzioni siano necessarie, sarà concordato con l'amministrazione l'orario di svolgimento delle attività relative, che potranno avvenire al di fuori dell'orario lavorativo definito al paragrafo 1. In particolare, a seconda dell'entità del disservizio, potrà essere richiesto di svolgere tali attività nella fascia oraria 7-8 o 19-21 oppure nel pomeriggio del sabato o durante la domenica.

Prima configurazione per funzionalità firewall

La società dovrà effettuare la prima configurazione delle apparecchiature di categoria B, per quel che riguarda le funzionalità firewall, secondo le specifiche dei tecnici dell'amministrazione e in affiancamento ad essi, consentendo il solo traffico relativo alle applicazioni installate sui server che si trovano sul segmento di rete protetto, al momento dell'installazione, basandosi sulle informazioni acquisite dal sensore stesso.

L'attività dovrà essere svolta in non più di tre giorni lavorativi consecutivi.

Al termine, la società fornirà all'amministrazione la documentazione scritta delle attività di configurazione della funzionalità firewall.

Prima configurazione per funzionalità IDS/IDP

La società dovrà effettuare la prima configurazione delle apparecchiature di categoria A e B, per quel che riguarda le funzionalità IDS/IDP, secondo le specifiche dei tecnici dell'amministrazione e in affiancamento ad essi, minimizzando il numero di eventi di tipo "falso positivo" in base al traffico rilevato sul segmento di rete protetto al momento dell'installazione.

L'attività di configurazione dovrà essere svolta in non più di cinque giorni lavorativi consecutivi.

La società dovrà configurare l'aggiornamento automatico delle signature, in accordo con quanto descritto nel paragrafo 6.3 "Aggiornamento delle signature e decodifica dei nuovi protocolli".

Al termine, la società fornirà all'amministrazione la documentazione scritta delle attività di configurazione della funzionalità IDS/IDP.

Al termine delle attività di configurazione, la società invierà all'amministrazione la dichiarazione di disponibilità al collaudo; alla dichiarazione saranno allegati il sommario delle

attività svolte e della documentazione fornita e, in particolare, la documentazione delle attività di configurazione della funzionalità firewall e della funzionalità IDS/IDP.

11. Corso di formazione

Dopo l'installazione di cui al paragrafo 10.1 la società dovrà erogare un corso di formazione all'uso del sistema, da tenersi presso la sede dell'amministrazione, nei locali da essa indicata. Il corso sarà erogato in moduli della durata di 4 ore, da tenersi al mattino e/o al pomeriggio, in orario lavorativo, secondo le indicazioni dell'amministrazione. Il corso dovrà consentire al personale partecipante di configurare le funzionalità IDP, firewall e del sistema di gestione previste nel presente capitolato e di gestire le esigenze ad esse relative emerse durante l'installazione. Il corso di formazione fornirà inoltre una panoramica delle ulteriori funzionalità eventualmente disponibili sul sistema fornito. La società concorderà con l'amministrazione il programma del corso e il calendario di erogazione dei moduli. Il corso sarà composto da almeno 4 moduli.

Tutti i moduli previsti per il corso dovranno essere erogati entro un periodo di 15 giorni solari dopo il ricevimento della dichiarazione di disponibilità al collaudo, salvo diversa indicazione dell'amministrazione.

I corsi dovranno essere tenuti da personale provvisto di certificazione individuale relativa all'uso delle apparecchiature fornite, ove questa sia prevista dal produttore. La società dovrà fornire i nominativi dei docenti e i dettagli relativi alle certificazioni possedute prima dell'erogazione delle attività di formazione.

12. Collaudo

Il collaudo dei beni e servizi forniti sarà eseguito, in contraddittorio fra le due parti, entro 30 giorni solari dalla data più recente fra la data di ricevimento della dichiarazione di disponibilità al collaudo e la data di erogazione dell'ultimo modulo di formazione.

In caso di esito negativo del collaudo, la società dovrà provvedere entro il termine massimo di 15 giorni solari all'eliminazione dei vizi e delle difformità riscontrati. Successivamente a tale termine saranno applicate le penali di cui al paragrafo 15.

13. Erogazione di un servizio di supporto sistemistico

Superato positivamente il collaudo, durante l'esercizio del sistema la società renderà disponibile un servizio di supporto sistemistico secondo le seguenti modalità.

Il servizio consisterà nell'assistenza di tecnici della società in attività di installazione e/o configurazione dei prodotti hardware e/o software forniti.

L'attività sarà composta da un massimo di 15 giornate, da utilizzare in periodi distinti della durata minima di un giorno lavorativo, entro un anno dall'esito positivo del collaudo.

Il servizio sarà erogato in seguito a richiesta scritta dell'amministrazione. L'attività dovrà iniziare entro 10 giorni solari a partire dalla richiesta e si svolgerà in orario lavorativo nelle sedi della Presidenza.

Il servizio sarà erogato mediante tecnici in possesso, se applicabile, di certificazione rilasciata dal fornitore del prodotto e/o del software per cui è stato richiesto l'intervento. La società produrrà di volta in volta i nominativi dei tecnici coinvolti nelle attività di supporto e la documentazione relativa alle certificazioni possedute.

Le attività comprese nell'ambito della garanzia non fanno parte del servizio descritto nel presente paragrafo.

L'amministrazione non si impegna ad utilizzare il servizio. Il servizio dovrà essere quotato a parte all'interno dell'offerta economica. Il pagamento dell'attività avverrà a consuntivo, in base alle giornate richieste ed effettivamente erogate.

14. Garanzia e manutenzione

Il sistema hardware dovrà essere coperto da garanzia e manutenzione on site per un periodo di 36 mesi dalla data del collaudo.

Tutti i prodotti software che saranno rilasciati, di base/ambiente o applicativo, di tipo proprietario o open source, pacchettizzato, personalizzato, dovranno essere coperti da garanzia e manutenzione per un periodo di almeno 12 mesi dalla data di collaudo.

Durante il periodo di validità della garanzia e manutenzione la società dovrà mantenere o riportare in buone condizioni di funzionamento i prodotti forniti senza alcun addebito e nel rispetto dei seguenti livelli minimi di servizio.

Malfunzionamento	Livello minimo di servizio
Aggiornamenti del software, siano essi release o versioni, rilasciati dal fornitore/produttore nel periodo di validità della garanzia/manutenzione	Installazione entro un mese solare dalla data di effettivo rilascio degli aggiornamenti
Errori o guasti bloccanti relativi all'hardware (il servizio dovrà coprire tutti gli eventuali componenti di ricambio)	Risoluzione entro tre giornate lavorative dalla chiamata
Errori o guasti non bloccanti relativi all'hardware (il servizio dovrà coprire tutti gli eventuali componenti di ricambio)	Risoluzione entro cinque giornate lavorative dalla chiamata
Errori o guasti bloccanti relativi al software per i quali siano disponibili patch	Risoluzione degli errori/guasti entro tre giornate lavorative dalla chiamata
Errori o guasti non bloccanti relativi al software per i quali siano disponibili patch	Risoluzione degli errori/guasti entro cinque giornate lavorative dalla chiamata

Il tipo, bloccante o non bloccante, di errore o guasto sarà giudicato motivatamente dall'UIT.

La società specificherà nell'offerta tecnica le modalità specifiche del servizio di garanzia e manutenzione, che dovrà garantire almeno i livelli di servizio sopra specificati. Per mancato rispetto dei livelli di servizio saranno applicate le penali di cui al Paragrafo 15 "Penali".

15. Penali

Le penali sono applicabili per mancato rispetto delle condizioni di erogazione dei servizi e fornitura di beni previste nel presente capitolato.

Tali condizioni possono riferirsi a mancato svolgimento delle attività o ritardo nella loro esecuzione o mancato raggiungimento degli obiettivi di qualità. Per mancato svolgimento delle attività o ritardo nella loro esecuzione si intendono quelli non giustificati e non sanati con sospensioni o proroghe accordate dall'UIT ed esclusivamente imputabili a cause dovute alla società o da essa provocate.

Le penali applicate saranno scalabili dalle fatture emesse, con emissione da parte della società di una nota di credito dello stesso importo della penale, e/o saranno incamerate dal deposito cauzionale definitivo prestato dalla società. In tale ultimo caso, l'applicazione della penale darà luogo all'incameramento della corrispondente quota dalla cauzione, con obbligo della società di provvedere alla sua reintegrazione entro 15 giorni solari.

La società riconosce alla Presidenza il diritto di applicare le penali di seguito riportate.

1. Qualora i servizi di formazione degli utenti e di assistenza funzionale agli utenti, di cui al paragrafo 11 “*Corso di formazione*”, non siano erogati secondo i livelli di qualità previsti e concordati, l’UIT provvederà ad inviare una prima lettera formale di richiamo alla società con l’indicazione delle carenze rilevate. Qualora si verificassero successivamente ulteriori problemi di qualità, l’UIT potrà inviare una seconda lettera di richiamo ed applicare una penale di € 100 per ogni episodio contestato.
2. Per ogni giorno (giorno lavorativo) di ritardo rispetto alle attività di cui al paragrafo 10 “*Installazione e predisposizione al collaudo*” è stabilita una penale di € 200.
3. Per ogni giorno (giorno lavorativo) di mancata prestazione rispetto alle calendarizzazioni previste delle attività di supporto sistemistico di cui al paragrafo 13 è stabilita una penale di € 200.
4. Per ogni giorno lavorativo di ritardo rispetto ai livelli di servizio di garanzia e manutenzione, previsti al paragrafo 14, è stabilita una penale di € 250.
5. Per ogni giorno lavorativo di ritardo rispetto a quanto previsto al paragrafo 12 per il collaudo è stabilita una penale di € 500.

Nel calcolo dei giorni di ritardo di cui al presente paragrafo non saranno computate le frazioni di giorno.

16. Subappalto

Per il subappalto si applica l’art. 118 del decreto legislativo 163/2006.

La ditta dovrà indicare nell’offerta la linea di lavoro che intende subappaltare e la percentuale sul totale della fornitura del servizio.

In caso di subappalto, le certificazioni tecniche richieste dovranno essere possedute anche dal personale della ditta subappaltatrice.

17. Risoluzione anticipata del contratto

Fatta salva ogni altra disposizione normativa che consente al committente la risoluzione anticipata del contratto, tale facoltà è prevista esplicitamente per la Presidenza nei seguenti casi:

1. applicazioni delle penali previste per un importo complessivo superiore al dieci per cento dell’importo contrattuale;
2. inadempienze gravi degli obblighi contrattuali che si protraggano oltre il termine perentorio assegnato dall’UIT alla società per porre fine all’inadempimento;
3. violazione degli obblighi di riservatezza;
4. violazione dei brevetti industriali e diritti d’autore.

In caso di risoluzione anticipata del contratto, fatto salvo ogni altro diritto, la Presidenza avrà potestà di rivalsa sulla cauzione prestata dalla società.

18. Informazioni generali di gara

L’offerta dovrà essere redatta in conformità alla vigente normativa comunitaria e nazionale in materia di appalti pubblici di servizi, decreto legislativo 163/2006, ed implica l’accettazione di quanto contenuto nel presente capitolato.

La gara per l’appalto - procedura aperta - della fornitura del servizio oggetto del presente capitolato verrà aperta, in seduta pubblica, nel giorno e all’ora indicati nel bando di gara ed avrà luogo presso la sede del Dipartimento per le Risorse Umane e i Servizi Informatici – Ufficio Informatica e Telematica - sito in Roma, Via della Mercede 96, secondo le modalità e prescrizioni dettate dal presente capitolato.

La relativa offerta dovrà pervenire, con qualsiasi mezzo, alla “Presidenza del Consiglio dei ministri - Dipartimento per le Risorse Umane e i Servizi Informatici - Ufficio informatica e telematica – **presso l’Ufficio accettazione corrispondenza di Palazzo Chigi, Piazza Colonna 370 – 00187 ROMA**” pena l’esclusione – non oltre il termine indicato nel bando di gara, in un plico chiuso controfirmato e sigillato sui tutti i lembi di chiusura, con apposta, oltre ai dati identificativi del mittente, la seguente dicitura:

“NON APRIRE – Gara per la fornitura di un sistema IDP
per il s.i. della Presidenza del Consiglio dei Ministri”

Ai fini di partecipazione alla gara, faranno fede la data e l’ora di ricezione del plico e non quelle di spedizione. Non saranno in nessun caso presi in considerazione i plichi-offerta pervenuti oltre il termine, anche se spediti prima della data di scadenza sopra indicata, o a indirizzi diversi.

Il plico, pena l’esclusione, dovrà contenere all’interno tre buste separate, chiuse controfirmate e sigillate su tutti i lembi di chiusura, recanti, oltre ai dati identificativi del soggetto offerente, le seguenti diciture:

- BUSTA **A** – DOCUMENTI
- BUSTA **B** – OFFERTA TECNICA
- BUSTA **C** – OFFERTA ECONOMICA

Si farà luogo all’esclusione dalla gara nel caso in cui manchi o risulti incompleto od irregolare anche uno solo dei documenti richiesti ai fini dell’ammissione alla gara e contenuti nelle rispettive buste A, B e C, ovvero, anche uno solo di tali documenti pervenga in modo diverso da come prescritto dal presente capitolato.

Nei limiti previsti dagli artt. da 38 a 45 trova applicazione l’art. 46 del decreto legislativo 163/2006.

18.1 Busta A - requisiti di ordine generale art.38 decreto legislativo 163/2006

Pena l’esclusione il concorrente dovrà inserire nella busta A i seguenti documenti:

1. **Dichiarazione sostitutiva**, ai sensi del DPR 445/2000, successivamente verificabile, ai sensi e per gli effetti delle disposizioni di legge vigenti in materia, resa e sottoscritta dal rappresentante legale del soggetto concorrente singolarmente, ovvero dai rispettivi legali rappresentanti in caso di riunione temporanea di concorrenti, con allegata, pena l’esclusione, fotocopia non autenticata di un documento d’identità personale, valido, del sottoscrittore, che attesti:
 - a. iscrizione alla C.C.I.A.A. per l’attività inerente la fornitura in oggetto oppure, nel caso di impresa non soggetta a tale iscrizione o residente in altri stati dell’Unione europea, requisito equivalente;
 - b. nominativo del legale rappresentante e idoneità dei suoi poteri alla sottoscrizione degli atti di gara;
 - c. nominativo di tutti i soci ed amministratori con potere di rappresentanza;
 - d. che non sussiste, a proprio carico, alcuna condizione ostativa alla contrattazione con la Pubblica amministrazione né condizioni ostative previste dalla legislazione antimafia;
 - e. di non trovarsi in stato di fallimento, di liquidazione coatta, di concordato preventivo e di non avere in corso procedimenti per la dichiarazione di una di tali situazioni;
 - f. di non avere pendente procedimento per l’applicazione delle misure di prevenzione di cui all’art. 3 della legge 27 dicembre 1956, n. 1423 o di una delle cause ostative previste dall’art. 10 della legge 31 maggio 1965, n. 575;
 - g. che nei propri confronti non è stata pronunciata sentenza di condanna passata in giudicato, o emesso decreto penale di condanna divenuto irrevocabile, o emessa sentenza di applicazione della pena su richiesta, ai sensi dell’articolo 444 del codice di procedura penale, per reati gravi in danno dello Stato o della Comunità che incidono sulla moralità professionale;

- h. di non aver violato il divieto di intestazione fiduciaria posto dall'articolo 17 della legge 19 marzo 1990, n. 55;
- i. di non aver commesso gravi infrazioni debitamente accertate alle norme in materia di sicurezza e a ogni altro obbligo derivante dai rapporti di lavoro, risultanti dai dati in possesso dell'Osservatorio;
- j. di non aver commesso violazioni, definitivamente accertate, rispetto agli obblighi relativi al pagamento delle imposte e tasse, secondo la legislazione italiana o quella dello Stato in cui sono stabiliti;
- k. che nell'anno antecedente la data di pubblicazione del bando di gara non ha reso false dichiarazioni in merito ai requisiti e alle condizioni rilevanti per la partecipazione alle procedure di gara, risultanti dai dati in possesso dell'Osservatorio;
- l. di non aver commesso violazioni gravi, definitivamente accertate, alle norme in materia di contributi previdenziali e assistenziali, secondo la legislazione italiana o dello Stato in cui sono stabiliti;
- m. di essere in regola ai fini dell'assolvimento degli obblighi di cui alla legge 12 marzo 1999, n. 68;
- n. che nei propri confronti non è stata applicata la sanzione interdittiva di cui all'articolo 9, comma 2, lettera c), del decreto legislativo dell'8 giugno 2001, n. 231 o altra sanzione che comporta il divieto di contrarre con la pubblica amministrazione;
- o. di non trovarsi, con riferimento alla fornitura oggetto dell'appalto, con altri concorrenti alla gara, in una situazione di controllo o di collegamento di cui all'articolo 2359 del codice civile e di non partecipare alla gara in più di un'associazione temporanea, e neppure in forma individuale qualora abbia partecipato alla gara in associazione;
- p. di accettare, senza condizione o riserva alcuna, tutte le norme e disposizioni contenute nel bando di gara e nel capitolato tecnico-amministrativo;
- q. di possedere all'atto della presentazione della domanda di partecipazione al bando di gara il Nulla Osta di Sicurezza.
Pena l'esclusione, il NOS dovrà essere posseduto:
 - in caso di RTI da tutti i componenti il raggruppamento;
 - in caso di subappalto da ognuna delle società subappaltatrici.

La sottoscrizione dovrà contenere la dicitura "consapevole delle responsabilità penali, amministrative e civili nel caso di falsità in atti e di dichiarazioni mendaci, e del fatto che l'amministrazione si riserva la facoltà di effettuare controlli anche a campione sulle dichiarazioni prodotte, acquisendo la relativa documentazione, anche in ipotesi ulteriori rispetto a quelle strettamente previste dalla legge".

I requisiti di cui alle precedenti lettere da a) a q) devono essere dichiarati, oltre che dal legale rappresentante:

- da tutti i soci mandatari, nel caso di società in accomandita semplice;
- da tutti i componenti la società, nel caso di società in nome collettivo;
- da tutti gli amministratori muniti di poteri di rappresentanza, nel caso di società di qualunque altro tipo.

Ai fini degli accertamenti relativi alle cause di esclusione di cui al presente articolo, nei confronti di candidati o concorrenti non stabiliti in Italia, la Presidenza chiede ai concorrenti di fornire i necessari documenti probatori, chiedendo, se del caso, la cooperazione delle autorità competenti.

Se nessun documento o certificato è rilasciato da altro Stato dell'Unione Europea, costituisce prova sufficiente una dichiarazione giurata, ovvero, negli Stati membri in cui non esiste una siffatta dichiarazione, una dichiarazione resa dall'interessato innanzi a autorità giudiziaria o amministrativa competente, a un notaio o a un organismo professionale qualificato a riceverla del Paese di origine di provenienza.

2. **Cauzione provvisoria** I concorrenti dovranno prestare una garanzia di € 6.500,00, pari al 2% dell'importo di € 325.000,00 (importo a base d'asta IVA esclusa) nelle modalità e con le indicazioni previste dall'art. 75 del D.Lgs 163/2006. In caso di raggruppamento temporaneo d'impresе la garanzia dovrà essere costituita non soltanto a firma della mandataria ma a firma di tutto il raggruppamento. La cauzione provvisoria, per essere pienamente operativa in termini di garanzia a fronte dei possibili inadempimenti, deve richiamare la natura collettiva della partecipazione alla gara di più imprese; deve identificare le dette imprese singolarmente e contestualmente; deve dichiarare di garantire non solo per il caso di mancata sottoscrizione ma anche per qualsivoglia altro inadempimento ad obblighi derivanti alle imprese dalla partecipazione alla gara.
3. **Requisiti di capacità economica e finanziaria** - Artt. 41 e 42 decreto legislativo 163/2006 Dichiarazione sostitutiva ai sensi del DPR 445/2000, successivamente verificabile, ai sensi e per gli effetti delle disposizioni di legge vigenti in materia, resa e sottoscritta esclusivamente dal rappresentante legale del soggetto concorrente singolarmente, ovvero esclusivamente dai rispettivi legali rappresentanti in caso di riunione temporanea di concorrenti, con allegata copia di un documento di identità del soggetto dichiarante, che attesti che il fatturato globale dell'impresa conseguito nel triennio antecedente la data di pubblicazione del bando di gara (somma dei fatturati degli anni 2004, 2005 e 2006) non sia inferiore al doppio dell'importo a base d'asta.
Nel caso di associazione temporanea di concorrenti, la suddetta dichiarazione dovrà essere resa da ciascun componente il raggruppamento, tenendo presente che il suddetto requisito di capacità economica deve essere posseduto nella misura minima del 40% dalla capogruppo e mandataria.
4. **Idonee referenze bancarie**, rilasciate in busta chiusa, da parte di almeno un primario istituto di credito. In caso di raggruppamento di imprese, le referenze devono essere presentate da ciascuna impresa partecipante al raggruppamento.
5. **Ricevuta in originale del versamento di € 30,00 (trenta/00)** all'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture, richiesto ai sensi della delibera 10 gennaio 2007 (G.U. n. 12 del 16/01/2007) della medesima Autorità. Nel versamento dovrà essere obbligatoriamente specificato il seguente codice identificativo (CIG) attribuito dall'Autorità alla gara: 00998059AE. In luogo della ricevuta in originale, il concorrente potrà presentare fotocopia della stessa corredata da dichiarazione di autenticità e copia di un documento di identità in corso di validità.

Le dichiarazioni sostitutive possono essere scritte secondo quanto riportato nel modello di cui all'Allegato A, compilando le parti richieste.

18.2 Busta B - offerta tecnica

Il concorrente dovrà inserire nella busta B l'offerta tecnica che dovrà contenere quanto di seguito specificato:

1. la descrizione della soluzione offerta, nella quale saranno esposti in modo dettagliato ed esaustivo tutti i beni e servizi richiesti nel presente capitolato, evidenziandone l'aderenza ai requisiti richiesti;
2. la documentazione, di cui al paragrafo 3, pubblicamente disponibile rilasciata dai produttori, con l'indicazione della fonte di provenienza, sulle caratteristiche dei prodotti offerti (tale documentazione potrà contenere anche parti in lingua inglese);
3. il documento sull'aderenza della soluzione offerta ai requisiti obbligatori richiesti riportato in Allegato B, firmato in ogni sua pagina dal legale rappresentante della società;
4. le modalità specifiche del servizio di garanzia e manutenzione di cui al paragrafo 14;

5. il presente capitolato tecnico-amministrativo, firmato per accettazione in ogni sua pagina dal legale rappresentante della società.

Ai sensi dell'art. 118 del D.L.vo 163/2006 e s.m.i., nel caso di subappalto il concorrente dovrà obbligatoriamente indicare la linea di lavoro che intende subappaltare e la percentuale sul totale della fornitura del servizio.

Tutti i documenti di cui al presente paragrafo devono essere sottoscritti in ogni loro pagina dalla persona o dalle persone abilitate ad impegnare legalmente la società concorrente (ovvero tutte le società in caso di raggruppamento temporaneo di impresa).

Qualora nella busta B venisse riscontrata la mancanza anche di uno solo dei documenti succitati o la difformità dei documenti rispetto a quanto previsto nel presente paragrafo, la commissione di aggiudicazione inviterà il concorrente a presentare i documenti mancanti e/o a presentarli nella forma richiesta entro i tempi indicati dalla commissione stessa pena l'esclusione dell'offerta dalla gara.

Tutta la documentazione di cui al presente paragrafo deve essere priva di qualsivoglia indicazione, riferimento, menzione (diretta o indiretta) delle condizioni economiche, pena l'esclusione dell'offerta dalla gara.

18.3 Busta C - offerta economica

Il concorrente dovrà inserire nella busta C l'offerta economica che dovrà essere scritta secondo il modello riportato nell'Allegato C.

L'offerta dovrà essere scritta su carta da bollo da € 10,33, dovrà essere redatta esclusivamente in lingua italiana, non potrà presentare correzioni valide se non espressamente confermate e sottoscritte dal concorrente stesso e dovrà essere espressa attraverso l'indicazione, in cifre e in lettere, degli importi. In caso di discordanza tra gli importi indicati in cifre e gli importi indicati in lettere saranno ritenuti validi questi ultimi.

L'offerta dovrà essere corredata con i dati dell'impresa, che dovrà altresì indicare il codice fiscale (imprese italiane) e quello della partita IVA.

L'offerta dovrà - pena l'esclusione - essere datata e sottoscritta con firma leggibile e per esteso dal legale rappresentate o procuratore del soggetto concorrente singolarmente, ovvero dal rispettivo legale rappresentante o procuratore di ogni componente un costituendo raggruppamento temporaneo di concorrenti.

Si avverte che nel caso trattasi di soggetto straniero, si dovrà provvedere alla nomina di un rappresentante fiscale, ai sensi dell'art. 17, comma 2, del D.P.R. 26/10/1972, n. 633 e successive modificazioni e integrazioni.

Inoltre, ai sensi dell'art. 86, comma 5, del decreto legislativo 163/2006, l'offerente dovrà indicare, le giustificazioni necessarie che hanno portato l'offerente medesimo alla costituzione dell'offerta economica, in particolare dovranno essere presi in considerazione gli elementi pertinenti, tra quelli previsti dall'art. 87 comma 2 lettere da a) a g).

19. Validità dell'offerta

I partecipanti alla gara sono vincolati al rispetto di tutte le condizioni indicate nell'offerta per un periodo di 180 giorni dalla data di scadenza del termine per la presentazione delle offerte.

L'amministrazione è vincolata solo successivamente all'avvenuta registrazione del contratto da parte degli organi di controllo.

20. Procedura di gara

L'aggiudicazione avverrà con il criterio del prezzo più basso, ai sensi dell'art. 82 del D.Lgs. 163/2006.

Le operazioni di gara avranno inizio nel giorno, ora e luogo indicati nel bando di gara e si svolgeranno come di seguito illustrato.

Prima di procedere all'apertura delle buste delle offerte presentate, l'amministrazione richiederà, ai sensi dell'art. 48 del D.Lgs 163/2006, ad un numero di offerenti non inferiore al 10 per cento delle offerte presentate, arrotondato all'unità superiore, scelti con sorteggio pubblico, di comprovare, entro dieci giorni dalla data della richiesta medesima, il possesso dei requisiti di capacità economico-finanziaria e tecnico-organizzativa richiesti nel presente capitolato e nel bando di gara, presentando la documentazione indicata in detto bando. Quando tale prova non sia fornita, ovvero non confermi le dichiarazioni contenute nella domanda di partecipazione o nell'offerta, l'amministrazione procederà all'esclusione del concorrente dalla gara, all'escussione della relativa cauzione provvisoria e alla segnalazione del fatto all'Autorità per i provvedimenti di cui all'articolo 6, comma 11, del D.Lgs 163/2006. L'Autorità dispone altresì la sospensione da uno a dodici mesi dalla partecipazione alle procedure di affidamento.

Il Presidente della Commissione aggiudicatrice appositamente incaricata dalla Presidenza disporrà l'apertura pubblica dei plichi pervenuti entro il termine con le modalità indicate nel presente capitolato.

All'apertura potrà presenziare un rappresentante per ogni offerente, munito di delega.

Si procederà alla gara anche nel caso sia pervenuta una sola offerta valida.

Previa constatazione della presenza all'interno di ciascun plico delle tre distinte buste, come sopra specificato, il Presidente disporrà l'apertura delle buste A e verificherà con gli altri membri della Commissione la presenza della documentazione richiesta per l'ammissione alla gara secondo le prescrizioni dettate dal presente capitolato.

Successivamente la Commissione, in seduta riservata, verificherà la piena validità della documentazione contenuta nelle buste A e, quindi, darà luogo all'apertura delle buste B e passerà all'esame del contenuto della medesima, valutandone la corrispondenza a quanto richiesto dal capitolato. Le offerte non corrispondenti saranno escluse dalla gara.

Successivamente, la Commissione, in seduta pubblica, aprirà le buste C delle offerte ammesse alla gara.

Le offerte anormalmente basse ai sensi dell'art. 86 del decreto legislativo 163/2006 saranno sottoposte a verifica ai sensi dell'art. 87 e 88 del medesimo decreto legislativo. All'uopo la Commissione, dopo aver verificato la documentazione presentata ai sensi del comma 5 dell'art. 86, chiederà alle imprese offerenti di integrare la documentazione e l'eventuale esclusione avverrà dopo la verifica, in contraddittorio, con la ditta. Dell'esclusione di tali offerte anomale sarà data comunicazione alla Commissione U.E.

La Commissione, infine, formerà la graduatoria e disporrà l'aggiudicazione provvisoria in favore del concorrente primo classificato.

In caso di parità i concorrenti saranno invitati a presentare in busta chiusa un'ulteriore offerta al ribasso.

La Commissione trasmetterà quindi la documentazione di gara al Dipartimento per le Risorse Umane ed i Servizi Informatici.

Ai sensi dell'art. 81, comma 3, del decreto legislativo 163/2006 la Presidenza, comunque, può decidere di non procedere all'aggiudicazione nel caso nessuna offerta risulti conveniente o idonea in relazione all'oggetto del contratto.

21. Aggiudicazione

Prima di procedere all'aggiudicazione definitiva, l'amministrazione verificherà la rispondenza dei requisiti dichiarati dalla società vincitrice.

Ove venga accertata la mancanza, la carenza o la non rispondenza di quanto dichiarato, l'amministrazione procederà all'annullamento dell'aggiudicazione provvisoria, con conseguente escussione della cauzione provvisoria, e potrà eventualmente disporla in favore del concorrente che segue nella graduatoria formulata in sede di espletamento della gara.

L'aggiudicazione definitiva è, altresì, subordinata al positivo accertamento in ordine alla insussistenza a carico dell'aggiudicatario degli impedimenti previsti dalla normativa vigente in materia di lotta alla mafia.

A seguito dell'esito positivo delle verifiche di cui sopra, l'amministrazione procederà all'aggiudicazione definitiva dell'appalto ai sensi dell'art. 12 del decreto legislativo 163/2006. L'affidatario dell'appalto è tenuto a presentare all'amministrazione, entro il termine di venti giorni lavorativi dal ricevimento della richiesta, tutta la documentazione necessaria alla stipulazione del contratto d'appalto, ivi compresa la cauzione definitiva, di importo pari al 10% dell'importo di aggiudicazione, come previsto dall'art. 113 del decreto legislativo 163/2006, da costituirsi mediante fidejussione bancaria o assicurativa, a garanzia dell'esatta e corretta esecuzione dei servizi di che trattasi. Tale deposito sarà svincolato al momento in cui tutte le obbligazioni contrattuali saranno state onorate.

Nel caso in cui risulti aggiudicatario un raggruppamento temporaneo, questo dovrà costituirsi nella forma giuridica ai sensi dell'art. 37 del decreto legislativo 163/2006.

L'impresa aggiudicataria è tenuta a versare ai sensi della legge 27 dicembre 1975, n.790, entro cinque giorni dalla data di stipulazione del contratto, l'importo delle spese di copia, stampa, carta bollata ed altre inerenti al contratto, nonché le spese di registrazione secondo la distinta che sarà indicata dal DRUSI dopo l'aggiudicazione stessa, pena l'applicazione dell'indennità di mora.

22. Stipulazione del contratto

Il contratto verrà stipulato in forma pubblica amministrativa.

Le spese contrattuali e di registrazione, nessuna esclusa, saranno a carico dell'impresa contraente.

Il rappresentante dell'impresa risultata aggiudicataria dovrà presentarsi, previo invito da parte dell'amministrazione, munito di procura, alla stipulazione del contratto nei tempi previsti dall'art. 11, comma 10, del decreto legislativo 163/2006. Ove tale termine non venga rispettato, senza giustificati motivi, l'amministrazione potrà unilateralmente dichiarare, senza bisogno di messa in mora, la decadenza dall'aggiudicazione, con possibilità di procedere all'aggiudicazione nei confronti del concorrente che segue in graduatoria, ovvero dare inizio alla procedura in danno per un nuovo esperimento di gara, con rivalsa delle spese e di ogni altro danno sul deposito provvisorio, ed incamerando, a favore dell'erario, la parte residua di quest'ultimo.

Ai sensi dell'art. 38, comma 3, del decreto legislativo 163/2006, l'impresa contraente ha l'obbligo di presentare la certificazione di regolarità contributiva di cui all'art. 2 del decreto legge 25 settembre 2002, n. 210 convertito dalla legge 22 novembre 2002 n. 266 e di cui all'art. 3, comma 8, del decreto legislativo 14 agosto 1996, n. 494 e successive modificazioni e integrazioni.

In sede di stipula del contratto l'impresa dichiarerà di avere piena conoscenza delle norme di seguito riferite:

- la legge e il regolamento di contabilità generale dello Stato (Legge 18/11/1923 n. 2240, R.D. 23/05/1924 n. 827 e successive modificazioni);
- il decreto legislativo 12 aprile 2006 n. 163, Codice degli appalti e s.m.i.;
- il presente capitolato tecnico;
- il Decreto del Presidente del Consiglio dei ministri 9 dicembre 2002, concernente la disciplina dell'autonomia finanziaria e contabile della Presidenza del Consiglio dei ministri.

Ai sensi dell'art. 7, comma 11, della legge 19/03/1990, n. 50, e successive modifiche e integrazioni, l'impresa aggiudicataria è tenuta a comunicare tempestivamente all'amministrazione

ogni modifica intervenuta negli assetti societari, nella struttura dell'impresa e negli organi tecnici ed amministrativi.

23. Modalità di pagamento

Il pagamento della fornitura seguirà a presentazione di fattura emessa, dopo favorevole collaudo, dalla ditta.

Gli importi derivanti dalle prestazioni di cui al paragrafo 13 saranno fatturati separatamente con cadenza trimestrale.

La ditta dovrà indicare nelle fatture le modalità di pagamento (coordinate bancarie), che potranno avvenire tramite accredito delle somme dovute presso l'istituto di credito o l'ufficio postale presso il quale la ditta stessa intrattiene il proprio conto. Il pagamento avverrà entro 60 giorni a decorrere dalla data di ricezione della fattura da parte dell'amministrazione.

24. Legge 675/1996

Per la presentazione dell'offerta, nonché per la stipula del contratto con l'aggiudicatario, è richiesto ai concorrenti di fornire dati e informazioni, anche sotto forma documentale, che rientrano nell'ambito di applicazione della legge 31 dicembre 1996, n. 675.

Ai sensi e per gli effetti della citata normativa, all'amministrazione compete l'obbligo di fornire alcune informazioni riguardanti il loro utilizzo.

16.1 Finalità del trattamento

In relazione alle finalità del trattamento dei dati forniti si precisa che:

- i dati sensibili eventualmente contenuti nei documenti presentati nelle buste A, B e C vengono acquisiti ai fini della partecipazione ed, in particolare, della effettuazione della verifica delle capacità amministrative e tecnico-economiche del concorrente, ai fini dell'esecuzione della fornitura nonché dell'aggiudicazione e, comunque in ottemperanza alle disposizioni indicate dalla legge 241/90 e successive modificazioni e integrazioni;
- i dati da fornire da parte del concorrente aggiudicatario vengono acquisiti ai fini della stipula del contratto e dell'esecuzione dello stesso, ivi compresi gli adempimenti contabili ed il pagamento del corrispettivo contrattuale.

16.2 Modalità del trattamento dei dati

Il trattamento dei dati verrà effettuato in modo da garantire la sicurezza e la riservatezza e potrà essere attuato mediante strumenti informatici e telematici, idonei a memorizzarli, gestirli e trasmetterli. Tali dati potranno essere abbinati a quelli di altri soggetti in base a criteri qualitativi e temporali di volta in volta individuati.

16.3 Categorie di soggetti ai quali i dati possono essere comunicati

I dati potranno essere comunicati a:

- soggetti esterni i cui nominativi sono a disposizione degli interessati, facenti parte della Commissione di aggiudicazione e di collaudo che verranno di volta in volta costituite;
- altri concorrenti che facciano richiesta di accesso ai documenti di gara nei limiti consentiti dalla legge 7 agosto 1990, n. 241.

Relativamente ai suddetti dati, al concorrente, in qualità di interessato, vengono riconosciuti i diritti di cui all'art. 13 della citata legge n. 675/1996.

Acquisite le suddette informazioni, ai sensi dell'art. 10 della citata legge 675/1996, con la presentazione dell'offerta e la sottoscrizione del contratto il concorrente acconsente espressamente al trattamento dei dati personali secondo le modalità indicate precedentemente.

Il concorrente potrà specificare, nelle premesse della relazione tecnica, se e quale parte della documentazione presentata ritiene coperta da riservatezza, con riferimento a marchi, brevetti, ecc.

In tal caso l'amministrazione non consentirà l'accesso a tale documentazione in caso di richiesta di altri concorrenti. Sul resto della documentazione tecnica l'amministrazione consentirà l'accesso.

25. Obblighi di riservatezza della ditta e diritti di proprietà dell'amministrazione

1. Il soggetto aggiudicatario ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati di cui venga in possesso e di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione dell'appalto.
2. L'obbligo di cui al comma 1 non concerne i dati che siano o divengano di pubblico dominio, nonché le idee, le metodologie e le esperienze tecniche che il soggetto aggiudicatario sviluppa o realizza in esecuzione delle prestazioni dovute.
3. Il soggetto aggiudicatario è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché dei propri eventuali subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di riservatezza anzidetti nonché del rispetto dei regolamenti interni dell'amministrazione in tema di sicurezza e riservatezza.
4. In caso di inosservanza degli obblighi di riservatezza, l'amministrazione appaltatrice ha la facoltà di dichiarare risolto di diritto il contratto, fermo restando che l'appaltatore sarà tenuto a risarcire tutti i danni che dovessero derivare all'amministrazione appaltatrice.
5. Il soggetto aggiudicatario potrà citare i termini essenziali del contratto laddove ciò fosse condizione necessaria per la partecipazione dell'impresa stessa a gare e appalti.
6. Il soggetto aggiudicatario si impegna, altresì, a rispettare quanto previsto dal D.L.vo 30/06/2003 n. 196.

26. Contatti con l'amministrazione

Ai sensi dell'art. 71 del decreto legislativo 163/2006, per eventuali **richieste di chiarimenti** necessari alla formulazione dell'offerta, le ditte partecipanti alla gara potranno rivolgersi all'indirizzo "Presidenza del Consiglio dei Ministri, Dipartimento per le risorse umane e i servizi informatici - Ufficio informatica e telematica - Via della Mercede, 96 - Roma", specificando obbligatoriamente in oggetto la dizione "Gara per la fornitura di un sistema IDP per il s.i. della Presidenza del Consiglio dei Ministri: richiesta di chiarimenti".

Le richieste dovranno pervenire per iscritto, anche a mezzo fax al numero + 39 06 6779 4446, entro 30 giorni dalla data di pubblicazione del bando.

I chiarimenti saranno forniti almeno quindici giorni solari prima del termine di scadenza per la presentazione dell'offerta, a mezzo fax, senza alcuna indicazione relativa all'identità del richiedente, contemporaneamente a tutti i concorrenti che avranno comunicato il proprio numero di fax oppure, entro gli stessi termini di tempo, pubblicati sul sito della Presidenza del Consiglio dei Ministri www.governo.it.

Elenco degli allegati

Allegato A - Modello di dichiarazione sostitutiva

Allegato B - Elenco dei requisiti obbligatori

Allegato C - Modello di presentazione dell'offerta economica