

Allegato B: Requisiti obbligatori

La seguente tabella indica i requisiti tecnici obbligatori che l'offerta, pena l'esclusione dalla valutazione, deve garantire.

La tabella deve essere firmata in ogni sua pagina secondo quanto previsto al paragrafo 18.2

	Caratteristica	Paragrafo di riferimento	Requisito minimo (ove previsto)
Caratteristiche generali	n. sensori categoria A	3	3
	n. sensori categoria B	3	2
	unico produttore per i sensori di cat. a e cat. b	3	-
	unico sistema e unica interfaccia di gestione per i sensori di categoria A e B	3	-
Caratteristiche categoria A	supporto modalità TAP	4	-
	supporto modalità in-line <ul style="list-style-type: none"> • transparent bridge mode • route mode • proxy arp mode 	4	-
Caratteristiche categorie A e B	throughput apparati categoria A	5	1 Gbit/s
	interfacce 10/100/1000 Rame	5	8
	throughput apparati categoria B	5	2 Gbit/s
	interfacce fibra 1000 base sx	5	8
	possibilità di sostituzione con interfacce rame	5	-
Funzionalità IPS	funzionalità IPS		-
	rilevamento anomalia di protocollo	6	-
	rilevamento basato su signature	6	-
	rilevamento backdoor	6	-
	anomalie di traffico	6	-
	network honeypot	6	-
	synflood protection	6	-
	layer 2 detection	6	-
	spoofing detection	6	-
	ricostruzione del traffico	6	-
	signature visibili e modificabili	6	-
	gerarchie delle signature	6	-
	regular expressions	6	-
	raggruppamento signature	6	-
	ispezione https, con almeno 100 certificati webserver caricabili sul sistema	6	-
	garanzia livello minimo del throughput senza disabilitazione della detection in condizioni di carico elevato	6	-
	aggiornamento signature senza caduta delle sessioni attive e senza interruzione del rilevamento	6	-
aggiornamento signature automatica con frequenza almeno giornaliera	6	-	

Tecniche di intervento IPS	supporto drop packet, drop session, close client, close server, close both	7	-
Caratteristiche categoria B	alimentazione ridondata con alimentatore sostituibile a caldo	8	-
	fFunzionalità NAT	8	-
	throughput per dimensione frame da 64 a 1518 byte per traffico in chiaro con FW e IPS attivi contemporaneamente	8	2 Gbit/s
	throughput per dimensione frame da 64 a 1518 byte per traffico criptato IPSEC, 3DES e/o AES in modalità FW	8	1 Gbit/s
	sessioni contemporanee	8	100.000
	tunnel IPSEC contemporanei	8	10.000
	vlan 802.1q	8	500
	security policies	8	25.000
	nuove sessioni al secondo	8	10.000
Sicurezza firewall	protezione a livello rete per almeno Synflood, udp flood, ping of death, land attack, winnuk attack, ip source route attack	8	-
	protezione dai seguenti pacchetti malformati: SYN e FIN bit settati contemporaneamente, nessun flag per pacchetti TCP, FIN senza ACK	8	-
Caratteristiche categoria B	supporto funzionalità router	8	-
	supporto RIP, OSPF, BGP	8	-
	supporto routing statico, multicast, source based, source interface based	8	-
	supporto modalità trasparente con funzionalità firewall e IPS	8	-
	supporto virtualizzazione del routing	8	-
	supporto mantenimento sessioni in caso di variazione del routing	8	-
	aggregazione porte fino a 2 Gbit ethernet e fino a 8 porte 10/100 Mbit/s	8	-
	supporto porte in redundancy	8	-
	supporto alta disponibilità	8	-
	tempo di commutazione impostabile fino al minuto secondo	8	-
	supporto sincronizzazione sessioni firewall chiare e criptate	8	-

Sistema di gestione	unica interfaccia grafica per la definizione delle policy	9	-
	repository unico	9	-
	gestione amministratori	9	-
	gestione permessi lettura/lettura-scrittura	9	-
	numero sensori gestibili	9	100
	gestione aggiornamenti firmware cat A e B se applicabile	9	-
	verifica stato aggiornamento sistemi sulla rete protetta	9	-
	caratterizzazione del traffico sulle reti protette	9	-
	identificazione sistemi vulnerabili mediante confronto con database vulnerabilità	9	-
	supporto common criteria	9	-
Alta affidabilità sistema di gestione	possibilità di configurazione ridondata del sistema di gestione	9	-
	sincronizzazione costante dei sistemi di gestione per quel che riguarda le impostazioni di configurazione	9	-
Caratteristiche di memorizzazione delle informazioni IDP	memorizzazione informazioni IDP: <ul style="list-style-type: none"> • istante di tempo allarme • nome assegnato all'anomalia • azione effettuata sul flusso • interfaccia di ingresso/uscita • indirizzo e porta sorgente/destinazione • sensore che ha generato l'evento • identificativo policy/regola 	9	-
	informazioni su: <ul style="list-style-type: none"> • storia e sul funzionamento dell'attacco • categoria attacco • impatto dell'attacco • patch per il sistema oggetto di attacco • vulnerabilità • commenti del fornitore del sistema oggetto di attacco • indicatori del livello di allarme • prodotti affetti 	9	-
	analisi di dettaglio dei pacchetti IP associati al flusso prima e dopo l'evento con esportazione in formato libpcap e possibilità di configurare il numero di pacchetti memorizzati	9	-
	possibilità di impostazione e salvataggio di viste multiple contemporanee	9	-
	possibilità di impostazione e salvataggio di filtri personalizzati	9	-

Caratteristiche di memorizzazione delle informazioni firewall	memorizzazione eventi firewall: <ul style="list-style-type: none"> • istante di tempo • azione effettuata sul flusso • 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 	9	-
	possibilità di impostazione e salvataggio di viste multiple contemporanee	9	-
	possibilità di impostazione e salvataggio di filtri personalizzati	9	-
Database degli eventi	capacità di memorizzazione degli eventi di log	9	10.000 / sec
	possibilità di archiviazione giornaliera mediante copia file	9	-
	possibilità di esportazione CSV	9	-
Caratterizzazione del traffico per apparati di categoria A	caratterizzazione del traffico di rete	9	-
	informazioni memorizzate: <ul style="list-style-type: none"> • hosts • peering tra hosts • porte applicative utilizzate • applicazioni • comandi passati nei protocolli • utenti e nomi files • sistemi operativi e versione ove possibile 	9	-
Security policy IDS/IPS	configurazione di criteri match traffico (protocollo IP, IP sorgente e destinazione, porte destinazione)	9	-
	possibilità di configurare eccezioni su singola regola	9	-
	criteri detection attacchi	9	-
	criteri di azione	9	-
	criteri di network	9	-
	capacità di memorizzazione del traffico	9	-
	capacità di alerting: <ul style="list-style-type: none"> • icone di avviso • trap snmp • notifica email • messaggi syslog • script custom e/o avvio programmi 	9	-

Security policy firewall	criteri match traffico IP	9	-
	criteri di azione	9	-
	criteri di network	9	-
Caratteristiche ulteriori	aggiornamento incrementale delle policy senza interruzione dell'attività di detection	9	-
	comunicazione criptata, con chiavi asimmetriche a 2048 bit e chiavi simmetriche a 128 bit, tra gli apparati e il sistema di gestione o tra il sistema di gestione e gli eventuali client per amministratori	9	-