Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

DIREZIONE CENTRALE DEI SERVIZI TECNICO-LOGISTICI E DELLA GESTIONE PATRIMONIALE

RISPOSTE AI CHIARIMENTI

Oggetto: Piattaforma di Web Security Gateway – Iniziativa n. 2672546

CHIARIMENTI

Si riportano nel seguito i quesiti formulati e le rispettive risposte:

Domanda Nr 1

In riferimento al par. 15 "Verifica di conformità" di cui al Capitolato Tecnico, pag. 14, e in particolare riguardo al collaudo di conformità rispetto alle funzionalità tecniche minime richieste nel Capitolato stesso, si chiede conferma che sia necessario pena esclusione, per lo snellimento delle operazioni di collaudo e a garanzia della completa conformità delle soluzioni proposte, produrre una "Dichiarazione del possesso delle caratteristiche minime delle apparecchiature offerte, da rendersi ai sensi e per gli effetti del d.P.R. n. 445/2000" da parte del Vendor della soluzione.

Risposta

Si conferma.

Domanda Nr 2

In riferimento al requisito al par. 9 "Deployment e Dimensionamento" di cui al Capitolato Tecnico pag. 10, e in particolare dove viene richiesto "almeno 6 porte 1Gbps di tipo 1000BaseT ed 2 porte 10Gbps di tipo 10GbaseSR" si chiede conferma che si possa leggere "almeno 6 porte 1Gbps di tipo 1000BaseT **o** 2 porte 10Gbps di tipo 10GbaseSR", indicando quindi due possibili opzioni alternative per l'equipaggiamento degli apparati da fornire.

Risposta

Si conferma.

Domanda Nr 3

In riferimento al requisito al par. 8 "Requisiti Funzionali" di cui al Capitolato Tecnico pag. 8, e in particolare dove viene richiesto "La soluzione deve fornire almeno due diversi motori di anti-virus per analisi inboud che outbound del traffico web" si chiede conferma che i due motori antivirus richiesti, al fine di garantire la massima differenziazione e quindi la massima efficacia in termini di sicurezza, siano di due Vendor di sicurezza diversi, a loro volta diversi dal Vendor della soluzione di Web Security Gateway offerta.

Risposta

Si conferma.

Domanda Nr 4

In riferimento al requisito al par. 8 "Requisiti Funzionali" di cui al Capitolato Tecnico pag. 6, dove viene richiesto "La soluzione deve fornire almeno 80 differenti categorie di contenuto (es. Adult, Pornography etc) e 20 categorie di Security Threats (includendo la categoria di "New Seen Domains" tendezialmente utilizzati come base di nuovi attacchi informatici)" si chiede conferma che, con particolare riferimento alla categoria di Threat Intelligence "New Seen Domains", quest'ultima sia ufficialmente documentata tra le categorie di sicurezza all'interno della Threat Intelligence del Vendor che fornisce la soluzione di Web Security Gateway.

Risposta

Si conferma.

Domanda Nr 5

In riferimento al requisito al par. 8 "Requisiti Funzionali" di cui al Capitolato Tecnico pag. 8, dove viene richiesto che "la soluzione di web proxy deve essere integrabile con soluzioni avanzate di machine learning" e in particolare che "La soluzione di machine learning deve essere offerta ed integrata nella soluzione di web proxy proposta tramite opportuna licenza", si chiede conferma che tale integrazione sia da fornire, completa di tutte le eventuali licenze necessarie per l'uso, inclusa nell'offerta oggetto di fornitura.

Risposta

Si conferma.

Domanda Nr 6

In riferimento al requisito al par. 8 "Requisiti Funzionali" di cui al Capitolato Tecnico pag. 9, dove viene richiesto "La soluzione di Web Proxy deve essere integrata nativamente con una soluzione di Threat Hunting inclusa all'interno della fornitura." si chiede conferma che tale integrazione sia da fornire, completa di tutte le eventuali licenze necessarie per l'uso, inclusa nell'offerta oggetto di fornitura.

Risposta

Si conferma. Si specifica che con il termine "nativo" s'intende che la soluzione proposta deve garantire tutte le funzionalità richieste anche con licenze di vendor diversi.

Domanda Nr 7

In riferimento al requisito al par. 8 "Requisiti Funzionali" di cui al Capitolato Tecnico pag. 8-9, dove viene richiesto "La soluzione deve essere nativamente integrata con almeno una soluzione NAC (Network Access Control)" si chiede conferma che a supporto di tale integrazione sia necessaria la presenza di documentazione pubblica a comprova, su almeno uno dei siti internet, rispettivamente del Fornitore della soluzione Web Security Gateway o della soluzione NAC oggetto di integrazione.

Risposta

Si conferma che la soluzione proposta debba garantire la funzionalità richiesta, s'intende quindi che deve essere fornita una soluzione NAC di base. La documentazione a supporto non deve necessariamente essere pubblica.

Domanda Nr 8

In riferimento alla componente di Servizi Professionali, di cui al par.4 pag. 3 "Oggetto di fornitura", e alla "Configurazione sistemi", di cui al par. 11 pag 12, dove si richiedono "40gg di Servizi Professionali a consumo, da erogarsi nell'arco di 36 mesi", si chiede conferma che le attività di configurazione necessarie per la migrazione dal sistema attuale di Web Security Gateway facciano parte dei 40gg di Servizi Professionali richiesti.

Risposta

Si conferma.

Domanda Nr 9

Requisito : I report devono essere generati almeno in formato pdf e in formato CSV.

Domanda : Si richiede di confermare che sia accettato il formato XLS anziché il formato CSV

Risposta

Deve essere fornito almeno uno dei due formati richiesti.

Domanda Nr 10

Requisito : La soluzione deve supportare la funzione di web traffic tap: una sua interfaccia fisica deve poter essere usata per inviare selettivamente traffico http e https (de-cifrato) verso una piattaforma esterna (es. IDS/IPS).
Domanda : Si richiede di confermare che sia accettabile il mirroring e la decodifica del solo traffico https proveniente dal proxy
Risposta
Si conferma come da capitolato tecnico.

Domanda Nr 11

Requisito : Lo score di Web Reputation deve essere customizzabile in base a specifiche esigenze in modo che amministratore possa impostare cosa è permesso, bloccato o ulteriormente analizzato tramite engine di anti-malware.
Domanda : Si richiede di confermare che il requisito è soddisfatto nel caso in cui la soluzione attraverso la console di gestione è in grado di essere personalizzata in base a specifiche esigenze in modo che un amministratore possa impostare cosa è permesso, bloccato o ulteriormente analizzato tramite engine di anti-malware, ma senza la definizione di uno score
Risposta
Non si conferma. Si conferma come da capitolato tecnico.

Domanda nr 12

Requisito : La soluzione deve essere nativamente integrata con almeno una soluzione NAC (Network Access Control) in modo da definire le politiche di accesso ai siti web sulla base delle informazioni di contesto condivise dalla piattaforma NAC tramite tramite API.
Domanda : Si richiede di confermare che sia sufficiente la presenza di API native da usare per integrazione con tecnologie NAC di terze parti.
Risposta
Si vede la risposta alla domanda n. 7.

Domanda nr 13

Requisito : La soluzione di Web Proxy deve essere integrata nativamente con una soluzione di Threat Hunting inclusa all'interno della fornitura.
Domanda : Si richiede di confermare che siano sufficienti i meccanismi, le tecnologie e i processi di Threat
Hunting utilizzati all'interno dei servizi cloud erogati dal vendor nel contesta della elaborazione delle firme **Risposta**
Non si conferma.

Domanda Nr 14

Requisito : Il sizing della soluzione deve supportare 30000 utenti che generano almeno 3000 sessioni http/https per secondo, di cui il 60% di tipo https, con le funzionalità di Url Filering, Reporting, due motori di antivirus abilitati.

La soluzione proposta deve poter gestire almeno 9000 connessioni per secondo (senza alta affidabilità) e 6000 connessioni per secondo considerando un appliance dedicato alle funzionalità di backup. La soluzione proposta deve poter supportare almeno 330000 connessioni contemporanee (senza alta affidabilità) e 220000 connessioni contemporanee considerando un appliance dedicato alle funzionalità di backup.
Tale soluzione deve essere impiegabile con almeno 3 appliances fisici includendo meccanismi di alta affidabilità di tipo N+1 (dove N è pari almeno 2).
Domanda : Si richiede di avere un dimensionamento basato sulle transazioni per secondo (TPS)?
Risposta
Si conferma come da capitolato tecnico.

Domanda nr 15

Requisito : Appliance di web security gateway deve essere composto da una piattaforma con doppia CPU, almeno 64GB di RAM, almeno 9.6 TB per lo storage HD in configurazione RAID10.
Domanda : Si richiede di confermare che il requisito può considerarsi soddisfatto se la soluzione proposta mantiene i log esternamente all'appliance proxy (che ha comunque uno spazio disco interno pari a 2,4 TB), in un repository con dimensione pari o superiore a 9,6 TB
Risposta
Si conferma.

Domanda nr 16

Requisito : Al punto 5 pag.12 del Capitolato d'oneri (**Classi di ammissione**) vengono indicate tre categorie merceologiche il cui possesso è indispensabile per poter partecipare alla gara d'appalto
Domanda : Si richiede di confermare se devono essere posseduti dalla singola impresa tutte e tre le classi indicate o se la partecipazione può essere estesa alle società, che sono qualificate almeno in una delle classi merceologiche riportate a pag. 12 del capitolato d'oneri, garantendo comunque idonea capacità economica ed adeguata competenza nell'esecuzione delle prestazioni contrattuali, anche al fine di garantire l'interesse pubblico ad avere il più ampio numero di potenziali partecipanti"
Risposta
Non si conferma.
Come indicato al Paragrafo 3 del Capitolato d'oneri le Società partecipanti *"che appartengono a una "classe di ammissione" inferiore a quella richiesta dovranno, a pena di esclusione, partecipare al confronto competitivo* ***tramite forme associate*** *(RTI, consorzi ordinari, Aggregazioni)* ***o facendo ricorso all'avvalimento****, come descritto nei successivi Paragrafi 5.1 lettera A) e B).*

Domanda nr 17

REQUISITO: "*La soluzione deve essere integrata nativamente con almeno una soluzione NAC (Network Access Control) al fine di definire le politiche di accesso ai siti web basate sulle informazioni di contesto condivise dalla piattaforma NAC tramite API*"
DOMANDA: al fine di proporre una soluzione che sia in linea con le esigenze dell'Amministrazione, si chiede di fornire maggiori dettagli (eventualmente anche con esempi) per tale requisito.
Risposta

Si veda risposta alla domanda n.7.

Domanda nr 18

REQUISITO: "*La soluzione Web Proxy deve essere integrata nativamente con una soluzione Threat Hunting inclusa nella fornitura*"
DOMANDA: al fine di proporre una soluzione che sia in linea con le esigenze dell'Amministrazione, si chiede di fornire maggiori dettagli per tale requisito. L'organizzazione possiede già una soluzione del genere che può essere sfruttata o si parla di un'ulteriore nuova soluzione?
Risposta
Si conferma che la soluzione proposta debba garantire la funzionalità richiesta, s'intende quindi che deve essere fornita una soluzione di Threat Hunting .

Domanda nr 19

REQUISITO: "*Il sistema di gestione centralizzata deve essere basato su una appliance o un server dedicato alla gestione*"
DOMANDA: Le soluzioni software che possono essere installate su software Hypervisor, come VMWare ESXi, sono rispondenti alle esigenze dell'Amministrazione o è richiesta una apparecchiatura dedicata?
Risposta
Si conferma, non è necessariamente richiesta un'apparecchiature dedicata.

Domanda nr 20

REQUISITO: "*La soluzione deve essere in grado di importare elenchi di nomi host e indirizzi IP (IoC) specifici da server esterni per definire una categoria specifica di feed esterni*"
DOMANDA: al fine di proporre una soluzione che sia in linea con le esigenze dell'Amministrazione, si chiede di fornire maggiori dettagli per tale requisito. Si vuole essere in grado di importare un elenco specifico sul Proxy o dare al proxy la possibilità di prendere un feed da solo?
Risposta
Si conferma che entrambe le soluzioni sono conformi alla richiesta.

Domanda nr 21

REQUISITO: "*Lo score di Web Reputation deve essere customizzabile in base a specifiche esigenze in modo che l'amministratore possa impostare cosa è permesso, bloccato o ulteriormente analizzato tramite engine di anti-malware*"
DOMANDA: Si chiede di chiarire se si sta parlando di una cattiva classificazione di un sito web o della capacità di definire il proprio risk score su un sito web
Risposta
Vedasi risposta alla domanda n.11.

Domanda nr 22

REQUISITO: "*Deployment e dimensionamento*"
DOMANDA: Si richiede di fornire maggiori dettagli sui requisiti specifici per ciascuna soluzione in termini di software o hardware. Si richiede altresì di fornire informazioni più dettagliate sull'utilizzo della larghezza di banda e sul numero di utenti simultanei ricavabili dall'attuale piattaforma in esercizio onde dimensionare opportunamente la nuova fornitura. Inoltre si chiede di

chiarire se quello che viene chiamato "server dedicato" sia un dispositivo virtuale o un server fisico.

Risposta

I dettagli sono quelli già riportati nel capitolato. Si veda risposta alla domanda n.19.

Domanda nr 23

"Requisiti Funzionali" del Capitolato Tecnico, si richiede di chiarire cosa intende l'Amministrazione quando fa riferimento ad una "Soluzione di Threath Hunting".

Risposta

Per soluzione di Threat hunting si intende una piattaforma per effettuare analisi, correlazione e arricchimento degli eventi di compromissione. Tale piattaforma deve essere integrabile tramite API con sorgenti di threat intelligence esterne oltre a quella del vendor proposto per la soluzione di web security gateway. Tramite la soluzione di Threat hunting deve essere possibile effettuare l'analisi degli indicatori di compromissione di una determinata minaccia (es ip, sha file, dominio, url) e verificarne l'esposizione dell'ambiente da proteggere.

Domanda nr 24

In relazione al par. 8 "Requisiti Funzionali" del Capitolato Tecnico, si richiede conferma se obbligatorio includere tale soluzione di threat hunting all'interno della presente fornitura.

Risposta

Si conferma.

Domanda nr 25

In relazione al par. 9 "Deployment e dimensionamento" del Capitolato Tecnico, si richiede di confermare l'effettiva esigenza di includere storage disponibile a bordo degli appliance per quantità pari ad almeno 9.6TB, equivalenti a 4.8 effettivi in RAID10, considerata la bassa necessità di spazio di archiviazione in funzione dei requisiti di gestione centralizzata dei log su componente esternalizzata rispetto all'appliance e dei requisiti di gestione e rotazione dei log stessi indicati nel presente capitolato.

Risposta

Vedasi risposta alla domanda n.15.

domanda nr 26

In relazione al par. 9 "Deployment e dimensionamento" del Capitolato Tecnico, si richiede conferma della possibilità di derogare al punto relativo allo spazio disco se il Vendor conferma di ottenere le stesse (o maggiori) performance con CPU e RAM superiori a quanto indicato nel requisito.

Risposta

Vedasi risposta alla domanda n.15.

Domanda nr 27

In relazione al par. 9 "Deployment e dimensionamento" del presente Capitolato Tecnico, si richiede di confermare se obbligatoria la presenza di porte a 10GB SR sull'Appliance.

Risposta

Vedasi risposta alla domanda nr. 2.

Domanda nr 28

In relazione al par. 10 "Consegna, installazione, posa in opera" del Capitolato Tecnico, si fa riferimento a numero 25.000 utenti. Si richiede conferma del numero di Utenti che dovrà essere oggetto del licensing della soluzione di Web Security Gateway.

Risposta

Il nuovo licensing dovrà prevedere 30.000 utenti.

domanda nr 29

In relazione al par. 11 "Descrizione dei servizi" del Capitolato Tecnico, si richiede conferma che le 40 giornate di servizio richieste siano inclusive delle giornate necessarie alle attività di installazione/migrazione richieste al par. 10 “Consegna, installazione, posa in opera”.

Risposta

Si conferma.

Firmato digitalmente da:
TOMMASO TAFURI
Ministero dell'Interno - Dipartimento della P.S.
Firmato il 27/11/2020 13:24
Seriale Certificato: 3269221743290320306
Valido dal 10/06/2020 al 10/06/2022
ArubaPEC EU Qualified Certificates CA G1