ALLEGATO TECNICO
PER LA FORNITURA DI UNA PROTEZIONE DDOS E DEI SERVIZI CONNESSI DI ATTIVAZIONE, STARTUP E MONITORAGGIO.

1. Premessa

Per proteggere a fondo la propria infrastruttura tecnologica, PuntoZero necessita di tecnologie di sicurezza che offrano:

a) protezione fisica - sia perimetrale che interna;

b) protezione funzionale - che deriva non solo dall'applicazione delle policy sotto forma di controllo granulare dell'accesso, ma anche rilevamento / prevenzione esplicita delle minacce;

c) protezione logica - applicata a tutti i livelli dello stack di elaborazione: servizi/protocolli a livello di rete, applicazioni infrastrutturali, applicazioni aziendali personalizzate e dati.

Pertanto PuntoZero intende dotarsi di una soluzione in grado di fornire una contromisura verso qualunque tipo di minaccia DDoS volta a mettere in crisi la capacità di erogazione del servizio di accesso ad Internet di PuntoZero. PuntoZero intende perciò attivare un sistema di protezione perimetrale DDoS in grado di proteggere il proprio AS.

2. Contesto

PuntoZero si avvale di un punto di accesso alla rete Internet (POP), utilizzato per il traffico di navigazione, per la pubblicazione di tutti i servizi ospitati al Data Center Regionale ed anche per la pubblicazione di alcuni servizi ospitati da DataCenter gestiti autonomamente dagli Enti che sono collegati all'infrastruttura di rete in Fibra Ottica di proprietà PuntoZero. Il servizio di accesso ad Internet di PuntoZero è erogato tramite due router (in configurazione active-active), a cui sono attestate altrettante fibre ottiche, che garantiscono un throughput complessivo di 2,5 Gbps.

PuntoZero è conosciuta al mondo Internet mediante un unico AS.

PuntoZero, inoltre, è dotata di una connettività Internet di backup, che consta di una sola linea ed un unico apparato con un throughput di 1Gbps. Il traffico viene ruotato sulla connettività di backup solo nel caso di un failure completo dell'accesso principale.

3. Fornitura del "Servizio DDoS"

PuntoZero ha necessità di acquisire una soluzione in grado di analizzare e "ripulire" il traffico in ingresso che insiste sull'AS di PuntoZero Scarl e che dovrà avere la capacità di mitigare attacchi DDos di varie tipologie (sotto descritte).

La soluzione proposta dovrà avvalersi di un Servizio di Scrubbing Center contro gli attacchi DDoS sia Volumetrici che Applicativi.

PuntoZero dovrà avere a disposizione una console/portale con cui poter monitorare

lo stato del servizio e gli eventi di traffico memorizzati.

Si stima necessaria l'attivazione e lo startup del servizio e l'erogazione di almeno tre (3) giornate di training-on-the-job per i tecnici di PuntoZero perché siano adeguatamente formati all'utilizzo, alla conduzione ed al monitoraggio del servizio.

3.1 Requisiti tecnico-funzionali della fornitura e configurazione minima

La fornitura della soluzione deve essere conforme ai requisiti minimi di seguito elencati.

Servizio Protezione DDoS (Id=SPD1)

La soluzione proposta potrà prevedere, in alternativa, il servizio di Protezione DDoS in modalità **full cloud** o con installazione **on-premises**.

Configurazione/Architettura Hardware (Id= CAH1)

La soluzione, nel caso di modalità di erogazione del servizio on-premises tramite un'appliance installata in loco, dovrà:

- essere dotata di almeno n. 4 interfacce SFP+ 10G SR, n. 2 interfacce di Management in rame 10/100/1000 e doppio alimentatore hot- swap
- avere un'altezza massima di 2RU e larghezza adatta a rack standard 19"
- essere provvista di by-pass esterno, per gestire almeno n.2 link Multi- mode 10 Gigabit Fiber (SR) e per garantire la continuità del servizio in caso di un guasto dell'appliance stesso
- prevedere che l'attivazione della modalità by-pass possa avvenire anche tramite configurazione manuale e non necessariamente in presenza di guasti hardware o software
- supportare la modalità di funzionamento in transparent mode (L2), senza richiedere quindi nessun tipo di modifica dal punto di vista di architettura di rete
- supportare la modalità di funzionamento "mista", ovvero l'attivazione di una componente di servizio Cloud a saturazione delle capabilities dell'appliance locale.

Configurazione infrastrutturale (Id=CIS1)

La soluzione dovrà:

- avvalersi di almeno 10 scrubbing centers distribuiti Worldwide;
- avvalersi di almeno 1 scrubbing center dislocato in Europa;
- poter gestire due connettività alternative di erogazione del traffico Internet (uno primario ed uno secondario, con il traffico in entrata conferito ad uno alla volta, active - stand-by)

- gestire almeno un Autonomous System
- ispezionare almeno 8 classi “C” di indirizzamento IPV4
- ispezionare solo traffico in ingresso (nessuna ispezione del traffico in uscita)

Gestione del Traffico (Id=SGT1)

- l’ispezione del traffico dovrà avvenire almeno a livello 3 e 4 (OSI)
- la soluzione dovrà garantire la protezione da varie tipologie di attacco DDoS:
  - TCP / UDP / ICMP floods
  - SYN floods
  - TCP flag abuses
  - HTTP GET / POST floods
  - DNS reflection
  - DNS attack
  - SMTP attack
  - SSL/TLS attack
- la soluzione dovrà essere in grado di rilevare e mitigare i flood SSL-based senza la necessità di decrittografare tutto il traffico e senza richiedere le chiavi SSL
- la soluzione dovrà supportare (e quindi analizzare) sia il traffico IPv4 che quello IPv6;

Throughput (Id=STP1)

- la soluzione dovrà poter “assorbire” in entrata un traffico di almeno 5 Gbps
- la soluzione dovrà garantire la restituzione di un traffico “pulito” di almeno 1 Gbps

Gestione e Monitoraggio (Id=SGM1)

- la soluzione dovrà prevedere un portale/console dedicata che offra la possibilità di monitorare lo stato del servizio e del traffico;
- deve essere prevista la disponibilità di opportuna reportistica che permetta l’analisi sia del traffico lecito che di quello illecito per poter determinare in maniera più dettagliata possibile le soglie e le tecniche di mitigazione

La fornitura della soluzione dovrà comprendere l’**attivazione e startup del servizio** (Id=SAS1) in base alle specifiche fornite dal committente. Inoltre dovranno essere previste tre (3) giornate di training-on-the-job, per i tecnici di PuntoZero, sulle funzionalità del portale (Id=SGM1).

3.2 Ulteriori caratteristiche tecniche e funzionali

Sono inoltre da considerare aggiuntive a quelle definite al precedente par. 3.1, le ulteriori caratteristiche tecniche e funzionali di seguito indicate:

Scalabilità

La soluzione che PuntoZero intende acquisire dovrà avere capacità di evoluzione in relazione a possibili scenari di ampliamento della infrastruttura di rete e rispetto all'ubicazione geografica dei DataCenter PuntoZero

Saranno tenuti in considerazione i seguenti fattori:

- capacità della soluzione offerta di gestire un numero di AS superiore ad 1 (uno), rispetto alla configurazione minima richiesta definita al precedente Capitolo 3.2 (Id=CIS1)
- capacità della soluzione offerta di gestire un numero di classi C superiore ad 8, rispetto alla configurazione minima richiesta definita al precedente Capitolo 3.2 (Id=CIS1)
- capacità della soluzione offerta di restituire traffico "pulito" in entrata superiore 1Gbps, superiore rispetto alla configurazione minima richiesta definita al precedente Capitolo 3.2 (Id=STP1)
- capacità della soluzione offerta di poter "assorbire" in entrata un traffico superiore a 5Gbps, superiore rispetto alla configurazione minima richiesta definita al precedente Capitolo 3.2 (Id=STP1)
- un numero di interfacce SFP+ 10G SR superiore a 4, superiore rispetto alla configurazione minima richiesta definita al precedente Capitolo 3.2 (Id= CAH1)

Features architetturali aggiuntive

Le Features architetturali aggiuntive sono basate sulle seguenti caratteristiche principali:

- numero di scrubbing centers worldwide superiore a 10 (Id=CIS1)
- numero di scrubbing centers dislocati in Europa superiore a 1 (Id=CIS1)
- disponibilità di Scrubbing Centers di tipo "Provider Independent"
- erogazione in modalità Always ON

Gestione del traffico

Le funzionalità di Controllo del traffico sono basate sulle seguenti caratteristiche principali:

- La soluzione deve essere in grado di supportare meccanismi di riconoscimento e mitigazione degli attaccanti non basandosi esclusivamente sull'indirizzo IP sorgente. Questo per garantire il corretto funzionamento nel caso in cui gli attaccanti si trovino dietro ad un Proxy o CDN

- Il sistema deve supportare la protezione HTTP DDoS comportamentale a livello di applicazione
- Il sistema deve supportare la rilevazione comportamentale e la mitigazione chirurgica dalle inondazioni di query DNS.