Contratto Quadro SPC Cloud Lotto 1

Servizi di sicurezza - DDoS

Specifiche di Realizzazione

Gestione	Azienda	Riferimento
REDATTO:	Telecom Italia S.p.A.	
REDATTO:	DXC Technology	
APPROVATO:	Telecom Italia S.p.A. (Mandataria), DXC	
N° allegati:	0	

Telecom Italia S.p.A.
(ing. Giovanni Santocchia)

Firmato digitalmente da:
GIOVANNI SANTOCCHIA
Telecom Italia S.p.A./00488410010
Firmato il 22/04/2019 22:11
Seriale Certificato: 443651
Valido dal 05/12/2016 al 05/12/2019
TI Trust Technologies CA

INDICE

1. REGISTRAZIONE MODIFICHE DOCUMENTO

N° Rev.	Descrizione	Data emissione
0	Prima emissione	04/02/2019

2. GENERALITA'

2.1 Applicabilità

Il documento si applica nell'ambito del Contratto Quadro SPC Cloud Lotto1.

2.2 Assunzioni

Non applicabile.

2.3 Riferimenti

Identificativo	Titolo/Descrizione
Gara Cloud Lotto 1	Gara Cloud Lotto 1_Allegato 5B Capitolato Tecnico
Gara Cloud Lotto 1	Gara Cloud Lotto 1_Allegato 5A Capitolato Tecnico Parte Generale
Gara Cloud Lotto 1	Offerta Tecnica del Fornitore Allegato B Relazione Tecnica Lotto 1

2.4 Definizioni ed Acronimi

Definizioni/Acronimi	Descrizione
DDoS	Distributed Denial of Service
ISP	Intenet Service Provider
DC	Data Center
GRE	Generic Routing Encapsulation
IP	Internet Protocol
PA	Pubblica Amministrazione
RTI	Raggruppamento Temporaneo d'Impresa
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività

3. DEFINIZIONE COMPONENTI

Il servizio di DDoS Mitigation Infrastrutturale è offerto dal RTI utilizzando la piattaforma infrastrutturale che TIM ha predisposto già da alcuni anni sia proteggere il proprio IP backbone pubblico da attacchi di tipo DDoS (DDoS Mitigation Infrastrutturale) sia per offrire il servizi ai propri Clienti finali.

Il servizio DDoS consente di effettuare il filtraggio del traffico diretto verso i sistemi Cliente oggetto di attacco DDoS in modo da eliminare le componenti di traffico indesiderate. Il filtraggio viene effettuato reinstradando il traffico diretto ai sistemi Cliente verso la Piattaforma di DDoS Mitigation del RTI. Al termine della fase di filtraggio, il traffico legittimo è instradato verso le destinazioni Cliente.

Il servizio è applicato sulle destinazioni IP pubbliche indicate dal Cliente in fase di implementazione del servizio.

Come indicato nel documento “SPC Cloud Servizi di sicurezza DDoS – specifiche del servizio”, il servizio DDoS sarà applicato esclusivamente alla connettività Internet condivisa presente presso i Centri Servizi del RTI prevista dalla convenzione SPC Cloud Lotto 1 ed utilizzata dalle Amministrazioni che hanno contrattualizzato i servizi infrastrutturali previsti dal Lotto 1. Pertanto il traffico analizzato e protetto è esclusivamente quello indirizzato tramite rete Internet verso i sistemi indicati dall’Amministrazione e ubicati presso i Centri Servizi del RTI aggiudicataria della convenzione SPC Cloud Lotto 1. Conseguentemente viene esclusa l’analisi e la protezione del traffico proveniente da rete Internet e diretto verso indirizzi IP diversi da quelli configurati per ciascuna Amministrazione a livello subnet sulla piattaforma Openstack.

Il servizio non è applicabile alla connettività INFRANET essendo questa realizzata mediante una VPN MPLS. Infatti Il servizio di DDoS Protection protegge esclusivamente IP pubblici esposti su Internet da attaccanti che siano in Internet, pertanto eventuali attacchi provenienti dalla rete INFRANET non sono né rilevabili né gestibili.

La rete INFRANET, essendo realizzata su VPN MPLS, si configura come una rete segregata con accessi dedicati alle sedi della PA e non raggiungibile tramite Internet.

Il servizio è proposto in modalità “reattiva” ovvero sarà l’Amministrazione a segnalare all’Help-Desk (SPOC) tramite il NV o l’apertura di pre-ticket il verificarsi di un attacco/sospetto attacco DDoS.

L’Help-Desk provvederà a coinvolgere la struttura dello RTI competente (Security Operation Center – SOC) per tali tipologie di problematiche.

3.1 Componenti del servizio

Il servizio è realizzato su piattaforma Arbor Networks TMS.

Tutta l’infrastruttura è già operativa poiché utilizzata da TIM stessa per contrastare gli attacchi DDoS sulla propria rete nonché per offrire il servizio a Clienti finali.

Non è inoltre necessaria l’acquisizione di elementi Hardware o Software da parte dell’Amministrazione.

L’attivazione del servizio richiede infatti che venga configurato un tunnel GRE sul router infrastrutturale presente nel Centro Servizi dello RTI aggiudicataria della convenzione SPC Cloud Lotto 1 sul quali è raccolto il traffico Internet indirizzato ai sistemi realizzati mediante l’acquisto delle risorse IaaS (VM e VDC) e/o PaaS da parte delle Amministrazione nell’ambito della convenzione SPC Cloud Lotto 1. Il tunnel GRE è terminato sul router di piattaforma presente nella Server Farm preposta alle attività di Cleaning del traffico (nodo TIM).

4. ARCHITETTURA DEL SERVIZIO

Il servizio DDoS Protection offerto dallo RTI alle Amministrazioni è realizzato su piattaforma Arbor Networks TMS.

L'infrastruttura necessaria all'erogazione del servizio è già attiva ed operativa pertanto non sono necessarie attività sulla componente infrastrutturale.

La figura seguente mostra l'architettura del servizio.

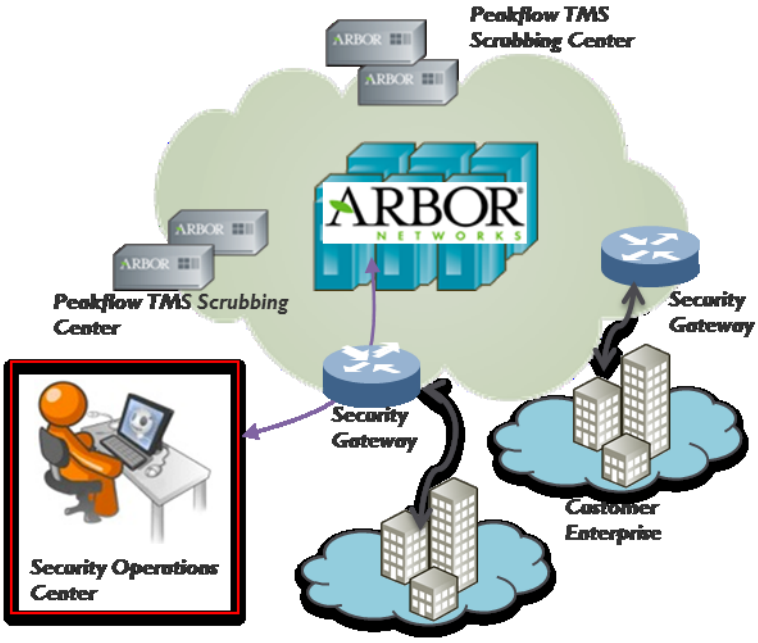

Fig.1: Architettura servizio DDoS

All'interno della propria infrastruttura di rete TIM ha realizzato alcune aree di "cleaning", dette Security Farm, interamente ridondate, dedicate all'erogazione del servizio DDoS. All'interno delle Security Farm sono presenti i "security gateway" ovvero gli apparati verso i quali viene reinstradato il traffico in caso di attacco in modo da poter essere analizzato, ripulito e reindirizzato alla sede Cliente.

La posizione delle Security Farm è stata individuata anche in funzione della vicinanza ai punti di interconnessione internazionale dai quali provengono la maggior parte degli attacchi. Le Server Farm sono collegate con link diretti verso i GW internazionali (GW—ITZ).

La piattaforma mette a disposizione degli operatori del Security Operations Center (SOC) una console tramite la quale è possibile visualizzare cosa sta generando l'attacco DDoS e quali effetti producono le azioni di contro-misura attivate. Mediante tale console il personale operativo può modificare le regole che sottendono alle contro-misure da attivare oppure effettuare un'analisi del traffico in modo da identificare il traffico malevolo.

Quando inizia un'attività di mitigation di un attacco, il personale preposto, agendo sulla piattaforma Arbor è in grado di controllare le tre fasi di:

- diversion,
- cleaning
- reinjection.

Nella fase di diversion vengono creati degli annunci che modificano il piano di controllo BGP della rete TIM e vengono configurate in modo opportuno le risorse di cleaning.

La figura 2 seguente mostra il funzionamento logico del servizio in caso di attacco

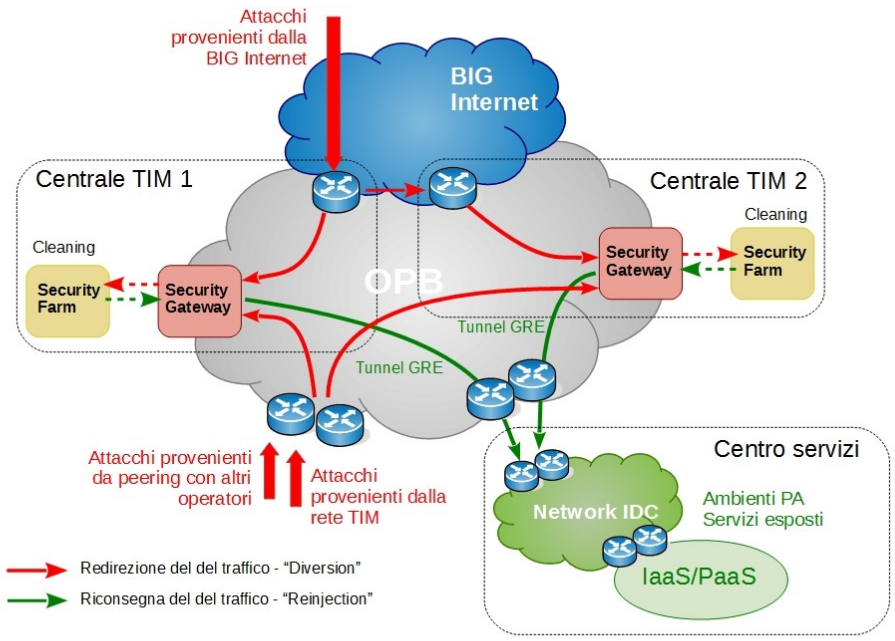

Fig.2: Schema di funzionamento in caso di attacco DDoS

Facendo riferimento alla fig.2, in relazione alle tre fasi sopra menzionate, si evidenzia:

- **fase di *diversion***
  - traffico proveniente dal GW-ITZ di ingresso dell'attacco: in base alla e regole di routing impostate, il traffico (lecito o malevolo che sia) destinato a ciascun IP attaccato e proveniente dalla *Big Internet* **arriva tutto e solamente in uno dei due GW-ITZ**. Al fine di poter sfruttare tutta la capacità di *cleaning*, in caso di attacco, il traffico diretto al *target* in ingresso dal GW-ITZ viene rediretto, mediante l'utilizzo di link dedicati**,** in modalità bilanciata, verso i security gateway e quindi verso le Security Farm
  - traffico proveniente dai punti di accesso o di peering della rete TIM: il traffico destinato a ciascun IP attaccato, raccolto dai segmenti di accesso della rete TIM o dai suoi punti di peering con altri ISP, viene rediretto verso il security-gateway e quindi la Security Farm più vicina **(**in termini di metrica OSPF) al punto di ingresso, in tal modo si garantisce un perfetto bilanciamento nel caso di distribuzione uniforme degli attaccanti nella rete.
- **fase di *cleaning*** del traffico: il personale preposto effettua le configurazioni necessarie ad eliminare la componente malevola del traffico destinato alla risorsa attaccata; la soluzione consente l'utilizzo in bilanciamento di tutti i dispositivi in tecnologia Arbor attivi sulla rete garantendo la possibilità di gestire flussi fino a 160Gbps.

- **fase di *reinjection*** del traffico: per ogni punto di acceso del Cliente viene pre-configurato, in fase di delivery, il **tunnel GRE** chiuso tra la Security Farm ed i router di attestazione del centro servizi che ospita i sistemi oggetto di attacco

Per poter realizzare le tre fasi sopra descritte TIM ha implementato delle configurazioni specifiche sui propri apparati di rete, in particolare:

- sui GW-ITZ è stata implementata una configurazione ad hoc in modo che il traffico proveniente dalla Big Internet e destinato all'attaccato, arrivi alle Server Farm attraverso i link diretti,
- Sulla piattaforma Arbor Peakflow SP è stata implementata un'opportuna configurazione in modo da consentire agli operatori di attivare le azioni di "cleaning" opportune.

4.1 Risorse HW/SW

Viene fornita brochure della piattaforma Arbor Networks.

4.2 Risorse Umane

Il servizio DDoS è caratterizzato da una copertura H24 pertanto il personale dell'Help-Desk ed il NV con PIN specifico del Cliente saranno operativi con copertura H24.

Il servizio sarà erogato operativamente dalla struttura del SOC (Security Operation Center) che si occuperà, per ciascuna Amministrazione contraente, anche della fase di implementazione del servizio e del relativo collaudo.

Il SOC sarà attivato dall'Help-Desk a seguito di segnalazione effettuata dal Referente Cliente mediante chiamata al NV dedicato con PIN o apertura di pre-ticket sul sistema TTM di SPC.

Il personale del SOC, una volta attivato potrà contattare direttamente il referente Cliente per una più efficace gestone della problematica.

Le modalità di interazione tra Referenti Cliente e Referenti del SOC, in caso di attacco o presunto attacco DDoS, saranno tramite chiamata telefonica diretta e/o scambio di mail.

Le mail scambiate avranno un formato prestabilito che sarà concordato in fase di attivazione del servizio.

Per avere indicazioni sulle possibili mail scambiate tra referente Cliente e personale del SOC si veda il parg 3.6 del documento "SPC Cloud Servizi di sicurezza DDoS – specifiche del servizio".

4.3 Collaudo

Non è necessario effettuare alcun collaudo della piattaforma essendo questa già in esercizio da alcuni anni ed in uso a TIM stessa. Si procederà altresì, come descritto nel documento "SPC Cloud Servizi di Sicurezza DDoS – Piano di attivazione" ad effettuare un collaudo per la specifica realtà di ciascuna singola Amministrazione che contrattualizzerà il servizio.