

## LA VISIONE ESTERNA DEL VOSTRO AS/BGP

### PROTEGGERSI DALLE MINACCE SU INTERNET

La presenza in internet rappresenta oggi una risorsa irrinunciabile per la vostra azienda: proteggersi da attacchi ostili, errori e eventi imprevedibili è fondamentale per il vostro business. Per questo motivo occorre monitorare costantemente la vostra rete dall'esterno per assicurare una presenza concreta e di qualità su internet.

Sin dagli albori della rete, sono documentati casi clamorosi di attacchi tramite protocollo BGP che dimostrano come la rete possa essere aggirata interrompendone il traffico o creando delle configurazioni erronee capaci di dirottare il passaggio delle informazioni in una specifica zona della rete. È quindi importante mantenere il vostro Autonomous System (AS) al sicuro tenendo costantemente sotto controllo l'intera struttura, verificando la maniera in cui questi viene visto dalla rete, in quale modo i vari carrier recepiscono i vostri annunci e se, a causa di un errore o di un attacco, gli altri ricevono delle comunicazioni distorte di voi.

### COME FUNZIONA IL PROTOCOLLO BGP

Border Gateway Protocol (BGP) è il protocollo di routing più diffuso nel web e parte di uno dei più grandi ambienti di interazione cooperativa mondiale. Internet è una zona libera, una planetaria ragnatela di fili che si congiungono in innumerevoli sottoreti chiamate Autonomous System attraverso cui passa il traffico di chi naviga. Una rete aziendale collegata ad internet che gestisce in autonomia i suoi criteri di instradamento viene definita AS.

I diversi AS dialogano tra di loro tramite il protocollo BGP, che si occupa del routing interdominio all'interno di reti TCP/IP. BGP gestisce infatti le politiche di routing tra i diversi Autonomous System: i nodi BGP scambiano costantemente tra di loro informazioni di routing e di raggiungibilità delle varie reti.

Proprio dalla struttura stessa della rete internet, di natura aperta e globale, possono nascere minacce per la vostra rete (e quindi per il vostro business).

### BGP SENTINEL

BGP Sentinel di INRETE controlla, da diversi punti internet esterni alla vostra infrastruttura, gli annunci BGP relativi al vostro AS e ai vostri indirizzi IP. BGP Sentinel offre un servizio costante 24 ore su 24, 7 giorni su 7, registrando tutte le anomalie e notificandole in brevissimo tempo con varie modalità. Nello specifico BGP Sentinel:

- verifica quali annunci sono corretti e quali al contrario deviano il normale flusso del traffico di rete
- fornisce indicazioni di allarme complete e dettagliate sull'instradamento dei vostri indirizzi di rete
- indica tutti gli annunci attivi in un preciso istante relativi alle vostre reti.

### TRACE CONTROL

Nella gestione di reti complesse e di Autonomous Systems attraverso il protocollo BGP, oltre alla completa conoscenza degli AS path fornita da BGP Sentinel, può essere utile una verifica dell'instradamento sui diversi hop degli AS di peering. Trace Control di INRETE è un servizio che si occupa di controllare con continuità tali percorsi ("traceroute") in ingresso e in uscita, generando opportuni messaggi di allarme per i gestori che operano una diagnosi immediata delle anomalie.

La conoscenza degli AS path, unita alla conoscenza dei percorsi di "traceroute", permette una visione completa del proprio routing e una capacità di intervento immediato nel caso di anomalie. BGP Sentinel e Trace Control: un controllo meticoloso, costante e affidabile per la vostra rete.