



CASO DI STUDIO

Un provider di servizi Internet e di comunicazioni con sede nell'area EMEA protegge le reti scolastiche con Infoblox

IL CLIENTE: PROVIDER DI SERVIZI DI TELECOMUNICAZIONI CON SEDE NELL'AREA EMEA

Un provider di servizi Internet e di comunicazioni con sede nell'area EMEA responsabile di garantire la sicurezza di Internet e fornire servizi di telecomunicazioni alle istituzioni accademiche è stato selezionato per costruire una rete educativa nazionale su larga scala. Il progetto è stato fondato sulla premessa di fornire una connettività Internet sicura a 4,5 milioni di bambini, utilizzando 700.000 computer scolastici in 25.000 scuole primarie e secondarie.

LA SFIDA

Garantire un accesso sicuro a Internet su una rete di grandi dimensioni

Il provider di servizi di telecomunicazioni voleva assicurarsi che le connessioni di rete e l'esperienza utente non fossero solo stabili ma anche sicure, soprattutto perché gli utenti erano bambini in età scolare. Inoltre, voleva assicurarsi che questi bambini non andassero su siti web inappropriati o scaricassero inavvertitamente malware. Per un progetto così ampio, l'implementazione di gateway web sicuri (SWG) da sola per il filtraggio dei contenuti era un rischio elevato. Nessuno aveva mai fatto un'implementazione così ampia di SWG prima (il traffico di download stimato è superiore a 1 Tbps, che richiede circa 200 appliance dai principali fornitori di SWG). Nel caso in cui qualcosa fosse andato storto, il provider di servizi Internet voleva un modo per aumentare gli SWG. Tuttavia, il provider non voleva affidarsi a soluzioni di sicurezza basate su SaaS. Invece, aveva bisogno che le implementazioni di sicurezza fossero on-premise perché stava costruendo le proprie reti, il cloud e i data center.

L'enorme rete privata che il provider stava costruendo richiedeva collegamenti a 100 megabit con router per ciascuna delle 25.000 scuole. Il progetto è stato suddiviso in tre fasi: fornitura dei collegamenti, fornitura delle apparecchiature di rete e sicurezza. La sicurezza è stata implementata in due fasi. La prima riguardava la sicurezza di base utilizzando ADC (Application Delivery Controller) del DNS e firewall. La seconda prevedeva l'implementazione di gateway web.

Cliente: Provider di servizi Internet e di comunicazioni
Settore: Provider di servizi di telecomunicazioni
Sede: EMEA

OBIETTIVI:

- Costruire una rete stabile per un sistema educativo di grandi dimensioni
- Fornire una connettività Internet sicura
- Implementare una soluzione on-premise

RISULTATI:

- Esperienza di navigazione sicura e pulita
- Mitigazione del malware
- Filtraggio dei contenuti basato su DNS
- Servizi di sicurezza fondamentali
- Soluzione conveniente e scalabile

PRODOTTI:

- NIOS DDI
- Threat Insight

LA SOLUZIONE

Sicurezza di base basata su DNS in una rete privata interna

Infoblox ha valutato il progetto della scuola e ha suggerito che la sicurezza di base basata su DNS doveva essere considerata come un primo passo per proteggere le reti scolastiche. Sebbene anche i fornitori di SaaS si siano rivolti all'azienda, quest'ultima non li ha mai presi in considerazione perché voleva qualcosa che potesse essere implementato sulla rete privata interna che stava costruendo per le scuole. La maggior parte dei provider di servizi costruisce la propria infrastruttura e per questo motivo non utilizzerà un servizio basato su SaaS.

Diversi fattori aggiuntivi hanno portato il fornitore a scegliere Infoblox rispetto ad altri concorrenti:

- Infoblox ha offerto **funzionalità differenziate**, come Threat Insight, che può rilevare il traffico di comando e controllo del malware nascosto nelle query DNS. Può anche rilevare la presenza di tunneling DNS, un metodo comune che alcuni studenti possono potenzialmente utilizzare per aggirare le limitazioni delle politiche di sicurezza SWG.
- Il provider ha ritenuto che Infoblox fosse un **partner tecnico migliore** grazie alla sua competenza tecnica locale, cosa che altri concorrenti non potevano eguagliare perché non disponevano di esperti tecnici nella regione.
- Infoblox ha fornito le referenze di molti altri provider di servizi e implementazioni simili che utilizzano la tecnologia Infoblox.

Come parte delle discussioni, Infoblox ha tenuto un seminario approfondito sulla sicurezza che ha illustrato diversi esempi di malware e il modo in cui utilizzano il DNS per il comando e il controllo. Inoltre, una discussione di base sulla mitigazione del malware con Infoblox si è presto trasformata in una discussione più ampia che comprendeva:

- Come la categorizzazione dei contenuti utilizzando il DNS può migliorare in modo conveniente le prestazioni dei gateway web sicuri
- In che modo l'ispezione del traffico a livello DNS può fornire un aumento stabile e scalabile per gli SWG. Ad esempio, attraverso Infoblox, il provider è ora in grado di impedire agli studenti di accedere a contenuti palesemente inappropriati, come i siti web per adulti, bloccando il traffico a livello DNS. I siti più nebulosi sono stati filtrati in base agli URL utilizzando SWG (Fig. 1).
- Come questo approccio combinato limita la quantità di traffico dannoso che gli SWG devono gestire e riduce il costo totale della difesa dalle minacce

IL RISULTATO

Un'implementazione semplice e stabile che fornisce un valore immediato

Durante la prima installazione su scala limitata, un partner Infoblox ha implementato la soluzione DNS in soli sette giorni per due delle sedi del provider di servizi. Questa implementazione ha dimostrato che la soluzione Infoblox è **facile da implementare e stabile**, dando al provider la fiducia che la soluzione funzionerà per le implementazioni su larga scala. L'implementazione per le altre 16 sedi è in corso, stando a giugno 2019. Il provider ha già notato diversi vantaggi, tra cui la gestione centralizzata delle politiche di sicurezza sui firewall DNS e la mitigazione di problemi temporanei con il controllo del traffico su ADC e SWG grazie al filtraggio dei contenuti sui server DNS di Infoblox, che si è rivelato una valida soluzione di integrazione e di offloading. Grazie a Infoblox, il provider è stato in grado di fornire un'**esperienza di navigazione sicura, protetta e pulita agli studenti di tutta la regione**.

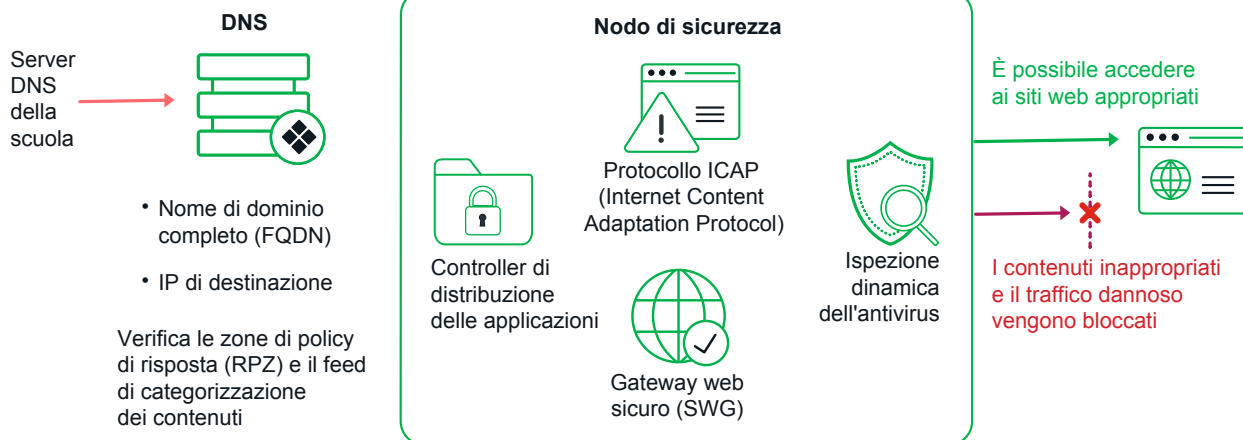


Figura 1: La soluzione Infoblox utilizza la categorizzazione e l'ispezione dei contenuti basata sul DNS per aumentare il filtraggio dei contenuti da parte degli SWG.



Infoblox unisce networking e sicurezza per offrire prestazioni e protezione senza pari. Scelti dalle aziende Fortune 100 e dagli innovatori emergenti, forniamo visibilità e controllo in tempo reale su chi e cosa si connette alla tua rete, in modo che la tua organizzazione funzioni più velocemente e blocchi le minacce in modo più rapido.

Sede centrale
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com