Spezzare il ciclo del malware / Operando nel traffico crittografato

Con SonicWall

Decrittografia DPI-SSL

La tecnologia d'ispezione Deep Packet del traffico SSL (DPI-SSL) di SonicWall decripta il traffico internet crittografato tra i client e i server web.

Il firewall NGFW intercetta la richiesta e stabilisce una sessione al posto del server

Il firewall NGFW decripta e ispeziona tutto il traffico proveniente da o diretto al client, alla ricerca di minacce crittografate

Servizi di prevenzione delle minacce

Il firewall NGFW inizia l'handshake SSL/TLS con il server per conto del client usando il certificato SSL/TLS definito dall'amministratore

Il server completa l'handshake e crea un tunnel sicuro tra sé e il firewall NGFW

Servizi di prevenzione delle intrusioni

Il firewall SonicWall applica il servizio di prevenzione delle intrusioni al traffico decrittografato, fornendo protezione da vulnerabilità delle applicazioni ed exploit.

Il firewall SonicWall applica poi i suoi servizi di prevenzione delle minacce multilivello al traffico non crittografato.

Servizi di prevenzione delle minacce multilivello

- Gateway Anti-Virus
- Cloud Anti-Virus
- Filtraggio botnet
- Filtraggio GeoIP
- Feed API di terze parti

CAPTURE ATP

SonicWall Capture Advanced Threat Protection (ATP) è una sandbox multi-engine basata sul cloud che analizza i file sospetti rilevandone il comportamento sospetto e blocca le minacce zero-day, come ad es. i ransomware, per prevenire un'infezione e la loro diffusione tra gli endpoint.

Il firewall NGFW ricodifica il traffico sicuro, lo invia al client e blocca le minacce crittografate

CLIENT

Protezione degli endpoint

I servizi Web Content Filtering e Enforced Content Filtering Client del firewall proteggono i sistemi endpoint all'interno e all'esterno del perimetro del firewall impedendo l'accesso a URL inappropriati, illegali e dannosi.

INTERNET

Richiesta di una pagina

Caricamento della pagina

CLIENT

Esecuzione dell'exploit kit

Senza SonicWall

Esecuzione dell'exploit kit

CLIENT/VITTIMA

Richiesta del malware

Server che ospita il malware

Infezione da malware

C&C e sottrazione di dati

Server di repository

Server di comando e controllo

Diffusione

VITTIMA