Breaking the Malware Cycle / Operating Inside Encrypted Traffic

The firewall's Web Content Filtering and Enforced

Page request
Page load

CLIENT

Without

SonicWall

DPI-SSL Decryption SonicWall Deep Packet Inspection of Secure Socket Laver (DPI-SSL) technology decrypts the encrypted internet traffic between clients and web servers. NGFW decrypts & inspects all traffic With NGFW intercepts, coming from or reauest & establishes going to client for session in encrypted threats SonicWall place of server Threat Prevention Services NGFW initiates Server completes SSL/TLS handshake handshake & builds with server on secure tunnel between behalf of client itself and NGFW using admin-defined SSL/TLS certificate

Intrusion prevention services

The SonicWall firewall applies an intrusion prevention service to the decrypted traffic to protect against application vulnerabilities and exploits.

The SonicWall firewall then applies its multi-layered threat prevention services to the unencrypted traffic.

Multi-layered threat prevention services

- Gateway Anti-Virus
- Cloud Anti-Virus
- Botnet Filtering
- Geo-IP Filtering
- 3rd Party API Feeds

CAPTURE ATP

SonicWall Capture Advanced Threat Protection (ATP) is a multi-engine cloud-based sandbox. It scans suspect files for malicious behavior, and stops zero-day threats – such as ransomware – from infecting and spreading between endpoints.

A

CLIENT

NGFW re-encrypts safe traffic and sends along to client and blocks encrypted threats

Malware request

Malware infection

Repository server

C&C and data exfiltration

Command & Control server

Spread

Content Filtering Client protects endpoint systems inside or outside the firewall perimeter from visiting inappropriate, illegal and malicious URLs.

Endpoint Security

fographic-BreakingTheMalwareCycle-IMAG-MK