efficient iP™
DEFINING SMART DDI

Datasheet

DNS FIREWALL

Protege y defiende la infraestructura de la red contra malware

DNS es un componente crítico de trabajo que garantiza la accesibilidad a prácticamente cualquier dispositivo que esté conectado. Es un sistema diseñado como servicio abierto a los dispositivos de la red que ofrece conectividad a cualquier servicio TI de empresas públicas o privadas. La función principal de los servicios DNS ha sido identificada por los hackers, convirtiéndose en su vector de ataque favorito, especialmente para el malware/ APT (91% según el Informe de Seguridad Cisco 2016).

En el entorno actual, en constante evolución, en el que la proliferación de los dispositivos móviles e IoT, y el BYOD se está convirtiendo en la norma, DNS Firewall de EfficientIP ofrece una capa de defensa específica rellenando el hueco que dejan las soluciones tradicionales de seguridad para conseguir una protección contra las amenazas a DNS.

DNS Firewall ofrece un filtrado avanzado de consultas DNS combinadas con fuentes dinámicas de inteligencia de amenazas que permiten la rápida identificación de dispositivos sospechosos, evitando las infecciones por malware y su propagación por las redes, así como las campañas de phishing y de exfiltración de datos.

Principales Ventajas:

- Bloqueo activo del tráfico DNS contra destinos maliciosos
- Inteligencia automatizada contra amenazas para adaptar la protección a un escenario permanentemente cambiante
- Protección proactiva contra malware
- Prevención del phishing
- Mitigación de los riesgos de exfiltración de datos
- Identificación y localización de dispositivos infectados

Políticas de respuesta DNS

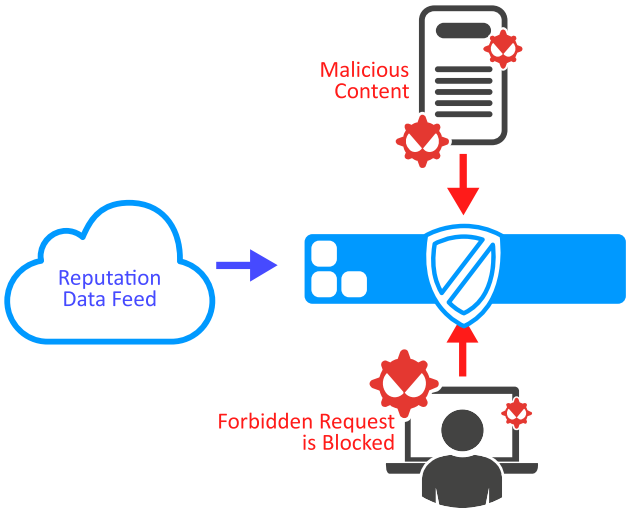
Domain Name Service Response Policy Zones (DNS RPZ) es un mecanismo que se implanta en todos los motores DNS recursivos actuales. Permite modificar dinámicamente las respuestas DNS que se obtienen del Domain Name System global, y aporta respuestas alternativas a cualquier consulta DNS. Este mecanismo se equilibra dentro del DNS Firewall para que los administradores DNS puedan definir las reglas de filtrado y redireccionamiento que se aplican al tráfico DNS en función de:

- El nombre de dominio consultado
- El NameServer NS requerido
- Una dirección IP resultante de una consulta DNS computarizada

Esto permite aplicar diversas políticas basadas en el tipo de tráfico:

- Redireccionar a otro CNAME o dirección IP
- Responder como dominio no existente (NXDOMAIN)
- Responder como sin datos (NODATA)
- Forzar TCP
- Passthru
- Caída

La solución DNS Firewall de EfficientIP ofrece una capa de seguridad adicional para complementar cualquier solución de seguridad de red ya existente. Esta última ofrece un rendimiento con limitaciones a lo que no sean direcciones IP y características de flujo estático, tales como protocolos y puertos. Sin embargo, aunque el cortafuegos NG ofrezca varias funcionalidades, éstas se ven limitadas a la hora de garantizar el rendimiento, dado que estos dispositivos se enfrentan a enormes cantidades de tráfico heterogéneo. Por contra, el DNS Firewall está especializado en evitar cualquier proceso de resolución de dirección IP para cualquier dominio que sea reconocido como malicioso, inhibiendo cualquier conexión a sus direcciones IP asociadas.



Feed de datos inteligente contra amenazas

La mejor manera de proteger la infraestructura de red y a sus usuarios contra campañas de phishing y malware consiste en evitar toda conexión con servicios reconocidos como maliciosos que roban las credenciales o extienden la carga inicial de infección por malware. No obstante, mantener unas reglas de filtrado adecuadas respecto a los dominios maliciosos conocidos resulta difícil debido a las propiedades dinámicas de las amenazas. Los atacantes utilizan múltiples dominios, a menudo creados al azar (DGA - Domain Generating Algorithms) para controlar sus botnets y equilibrar la enorme cantidad de servidores mal asegurados para desarrollar sus actividades. Apoyarse en un repositorio de reglas de filtrado actualizado dinámicamente que pueda extenderse mediante una política de filtrado personalizada, resulta la solución más sostenible.

El DNS Firewall de SOLIDserver™ incluye este tipo de feed de datos dinámicos construido a partir de varias fuentes distribuidas. Agrupa informes de actividad sospechosa de direcciones IP o dominios identificados, tales como MailSecurity, PhishTank, OITC y PhishLabs. En las listas suministradas se ofrecen diversas combinaciones de filtros basados en las siguientes categorías:

- Abusos y spam
- Phishing
- Malware
- Sitios web con fisuras

Asegurar una protección proactiva y eficaz contra el uso malintencionado de los servicios DNS

Prevención contra el phishing

Los ataques de phishing buscan dirigir al visitante a sitios web comprometidos, bien para conseguir que el usuario descargue software malicioso, o para directamente robarle información confidencial. Basándose en servicios inteligentes contra amenazas SOLIDserver™ DNS Firewall evita automáticamente que los usuarios accedan a dichos sitios, incluso cuando utilizan su propio dispositivo dentro de la red corporativa. Esto reduce significativamente el riesgo de robo de datos a los usuarios, a los que se intenta direccionar erróneamente para que desvelen sus credenciales mediante aplicaciones maliciosas.

Propagación de contenidos de malware y exfiltración de datos

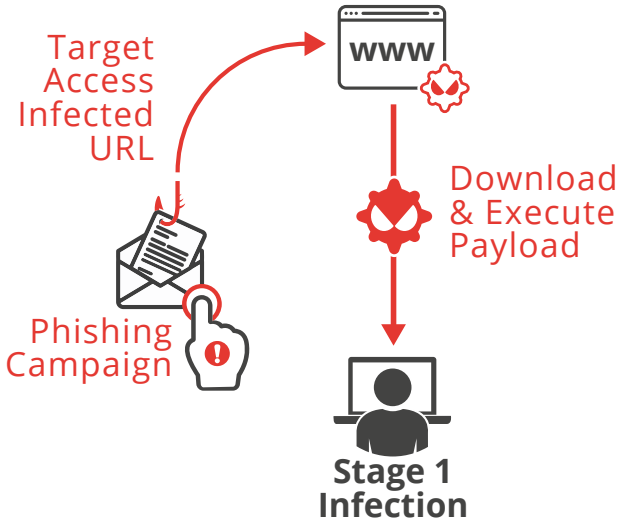
Se sabe que el malware está diseñado para alterar el funcionamiento de los sistemas para recoger información confidencial, acceder a infraestructuras privadas, pedir rescates a los usuarios o mostrar publicidad no solicitada. En cuanto un dispositivo se conecta a Internet, se ve expuesto a ataques de malware. Teniendo en cuenta el escenario actual de amenazas y el aumento de los ataques, evitar la proliferación a una red se ha convertido en una prioridad urgente.

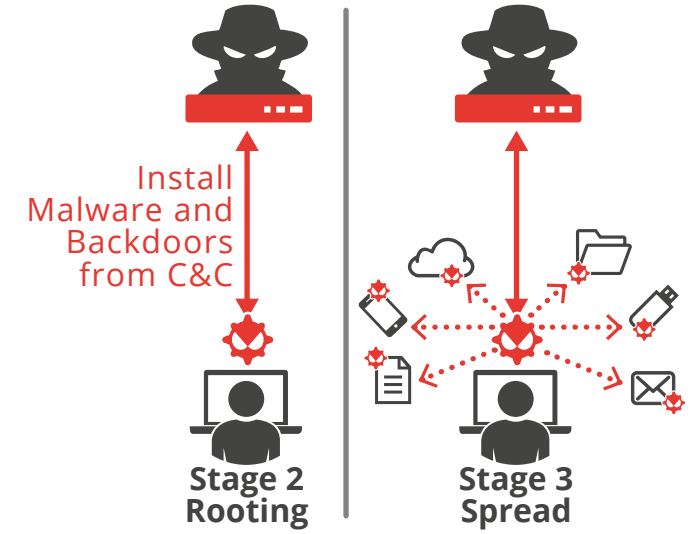
Las soluciones de seguridad existentes cubren una amplia gama de posibles vectores de ataque, tales como:

- Ataques de malware por correo electrónico, generalmente mitigados con filtros anti spam
- Ataques de malware en páginas web/descargas, generalmente mitigados mediante antivirus de pasarelas web
- Propagación de malware al compartir archivos, generalmente mitigados mediante antivirus

Les falta la posibilidad de identificar amenazas procedentes de dispositivos de red sin gestionar, especialmente ataques creados específicamente, que no siguen patrones existentes. SOLIDserver™ DNS Firewall evita la infección de un dispositivo con malware bloqueando las consultas sospechosas que en caso de no hacerlo redireccionarían al usuario a dominios y direcciones IP identificadas como maliciosas, independientemente del patrón de tráfico.

Reduce además la capacidad ofensiva de cualquier malware que hubiera infectado ya a algún dispositivo "conectado pero móvil", tales como un ordenador portátil, tableta o teléfono móvil. Lo hace bloqueando las comunicaciones con servidores de Comando y Control conocidos que evitan la actualización del malware y la mayoría de los intentos de exfiltración de datos.





Incluso es posible una protección más avanzada, combinando DNS Firewall con DNS Guardian. Éste último equilibra la inspección de tráfico DNS en tiempo real y la detección de actividades de comportamiento malicioso, disparando contramedidas automáticas adaptadas cuando son necesarias. Esto mitiga las técnicas de túnel más avanzadas y protege proactivamente cualquier motor DNS recursivo contra cualquier tipo de ataque DNS, asegurando el acceso de cualquier aplicación de los sistemas informáticos.

Identificar dispositivos infectados

La contención de una amenaza no es solamente bloquear el tráfico y aislar el agente contagioso. Requiere una intervención rápida en el dispositivo infectado para analizar y aplicar un tratamiento a la infección.

Apoyándose en políticas de acceso adecuadas, DNS Firewall consigue identificar rápidamente cualquier dirección IP que esté originando las consultas sospechosas. Combinándolo con un IPAM y su herramienta asociada de detección en red, se consigue una rápida localización de los dispositivos infectados para aplicar una solución inmediatamente.

Informes avanzados sobre amenazas

Combinando las capacidades de acceso de SOLIDserver™ con un gestor de eventos existente (o SIEM - Security Information and Event Manager) se posibilita la exportación de los registros de DNS Firewall en formato syslog estándar. Esto a su vez permite ejecutar analíticas avanzadas del tráfico DNS sospechoso, generando informes apropiados con modelos personalizados o cualquier plugin compatible con la solución instalada (por ejemplo, Splunk o Graylog).

DNS Firewall forma parte de la solución exclusiva de seguridad 360º de EfficientIP, diseñada para proteger infraestructuras DNS públicas y privadas, sea cual sea el tipo de ataque.

efficient iP™

REV: B-1708

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
101C Telok Ayer Street #04-00
SINGAPORE 068574
+65 6678 7752