efficient iP™

Datasheet

DNS Firewall

Netzwerkinfrastruktur vor Malware schützen und verteidigen

Highlights:

- Aktives Blockieren von DNS-Verkehr zu bösartigen Zielen
- Automatisierter Threat Intelligence Schutz, der sich der ständig weiterentwickelnden Bedrohungslandschaft anpasst.
- Proaktiver Schutz vor Malware
- Phishing Prävention
- Minimierung des Risikos von Datenexfiltration
- Identifikation und Lokalisierung von infizierten Geräten

DNS ist eine geschäftskritische Netzwerkkomponente, die den Zugang jedes vernetzten Dienstes sicherstellt. Dieses System ist von Haus aus ein offener Dienst für Netzwerkgeräte, der Konnektivität an öffentliche oder private IT-Services von Unternehmen anbietet. Die zentrale und kritische Rolle der DNS-Dienste wurde durch Hacker identifiziert und zu einem favorisierten Angriffspunkt gemacht, besonders für Malware/APT (91% nach 2016 Cisco Security Report).

In diesem sich ständig weiterentwickelnden Umfeld, in dem mobile und IoT-Geräte überall zu sehen sind und BYOD zur Norm wird, bietet die DNS-Firewall von EfficientIP eine spezielle Schutzschicht, um die Lücke zwischen traditionellen Sicherheitslösungen zu füllen und vor DNS-Bedrohungen zu schützen.

Die DNS-Firewall bietet erweiterte Funktionen zum Filtern von DNS-Abfragen mit Dynamic Threat Intelligence Feeds, die schnelle Identifizierung von verdächtigen Geräteaktivitäten ermöglichen, was Infektion und Verbreitung innerhalb des Netzwerkes von Malware, sowie Phishingkampagnen und Datenexfiltration verhindert.

DNS Response Policy Zonen

„Domain Name Service Response Policy Zones“ (DNS-RPZ) ist ein Mechanismus, der in allen modernen rekursiven DNS-Engines implementiert ist. Es ermöglicht es, die aus dem Global Domain Name System erhaltenen DNS-Antworten dynamisch zu ändern, und bietet alternative Antworten auf DNS-Abfragen. Dieser Mechanismus wird innerhalb der DNS-Firewall genutzt, damit DNS-Administratoren die genaue Filterung und die Umleitung des DNS-Traffics entsprechend folgender Kriterien bewerkstelligen zu können:

- Eines angefragten Domainnamens
- Eines angefragten Nameserver NS
- Einer IP-Adresse, die aus einer berechneten DNS-Abfrage entstanden ist

Dies ermöglicht die Anwendung der verschiedenen Policies/Regeln, je nach Typ des Datenverkehrs:

- Umleitung zu einem anderen CNAME oder einer anderen IP-Adresse
- Antwort mit nicht vorhandener Domain (NXDOMAIN)
- Antwort ohne Daten (NODATA)
- „Force TCP“
- „Passthru“
- „Drop“

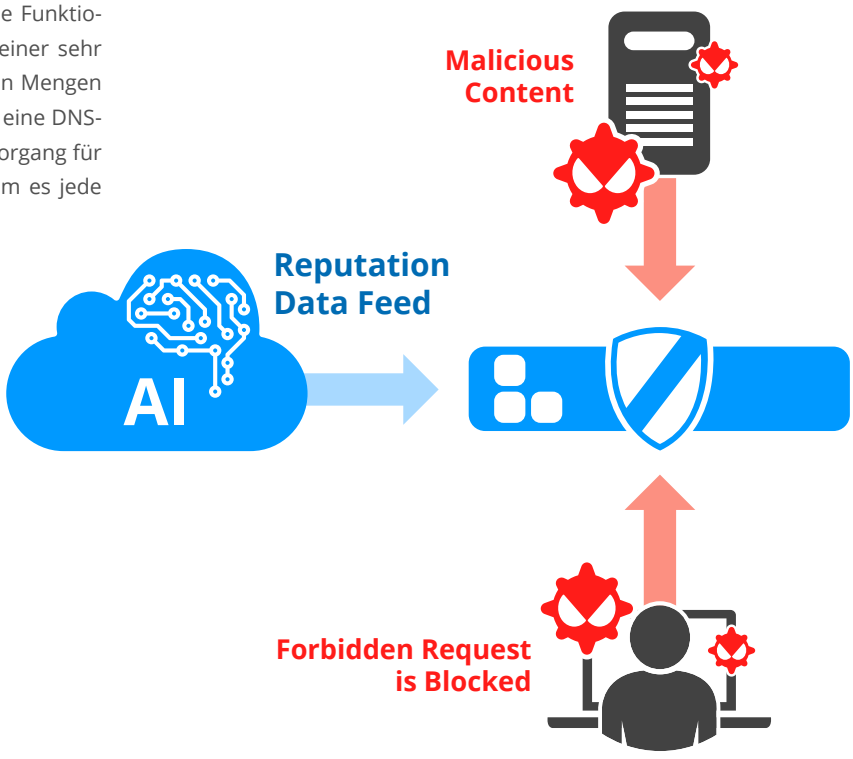
EfficientIP’s DNS Firewall Lösung bietet eine zusätzliche Sicherheit, um eine bestehende Netzwerksicherheitslösung zu ergänzen. Letzteres bietet begrenzte Leistung beim Filtern von anderem als IP-Adressen und statischen Flow- Eigenschaften, wie Protokolle und Ports. Allerdings, auch wenn die NG Firewall verschiedene Funktionalitäten bietet, sind diese leider nur zur Sicherstellung einer sehr begrenzten Leistung geeignet, da diese Geräte mit riesigen Mengen von heterogenem Verkehr arbeiten. Im Gegenteil dazu ist eine DNS-Firewall spezialisiert darin, jeglichen IP-Adressauflösungsvorgang für alle bekannten schädlichen Domains zu verhindern, indem es jede Verbindung zu den zugehörigen IP-Adressen blockiert.

Threat Intelligence Data Feeds

Der beste Weg, um eine Netzwerkinfrastruktur und seine Benutzer vor Phishing und Malwarekampagnen zu schützen, ist jede Verbindung zu bekannten schädlichen Dienstleistungen, die verwendet werden, um Anmeldeinformationen zu stehlen, oder die den „initial infection payload“ liefern, zu verhindern. Aber die Aufrechterhaltung der Filterregeln zu bekannten schädlichen Domains ist schwierig aufgrund der dynamischen Eigenschaft der Bedrohung. Angreifer nutzen mehrere, oft zufällig generierte Domains (DGA-Domain Generierung von Algorithmen) um ihre Bot-Netze zu steuern und die riesige Menge von schlecht gesicherten Servern zu nutzen, um ihre Aktivität anzutreiben. Es ist die nachhaltigste Lösung, sich auf eine dynamisch aktualisierte Repository Regel zu stützen, das durch eine angepasste Filter-Policy erweitert werden kann.

SOLIDserverTM’s DNS Firewall wird mit dieser Art von dynamischen Daten aus verschiedenen verteilten Quellen geliefert. Sie erstellt Berichte über verdächtige Aktivität von identifizierten IP-Adressen oder Domänen wie MailSecurity, PhishTank, OITC und PhishLabs. Die zur Verfügung gestellten Listen bieten verschiedene Filterkombinationen nach den folgenden Listenkategorien:

- Missbrauch und Spam
- Phishing
- Malware
- gefälschte Websites



Stellen Sie proaktiven und effizienten Schutz gegen bösartige Verwendung von DNS-Diensten sicher

Phishing Prävention

Kriminelle nutzen Phishing-Angriffe um nichtsahnende User beim Besuch eines manipulierten Webservice zu ködern, oder indem der Benutzer dazu gebracht wird, schädliche Software zu downloaden, um vertrauliche Informationen zu stehlen. SOLIDserver»-DNS-Firewall schützt Benutzer durch „Threat intelligence services“ und kann User somit automatisch davon abhalten, solche Missbrauchsseiten im Internet aufzurufen, selbst wenn sie ihre eigenen Geräte im Unternehmensnetzwerk verwenden. Dies reduziert deutlich das Risiko der Exfiltration persönlicher Daten von Nutzern, die fehlgeleitet werden um Ihre Anmeldeinformationen in gefälschten und schädlichen Anwendungen zur Verfügung zu stellen.

Beinhaltet Malware Spread und Daten-Exfiltration

Böswillige Software ist bekannt dafür, Systemoperationen zu unterbrechen, sensible Informationen zu sammeln, sich Zugang zur privaten Infrastruktur zu verschaffen, Lösegeld von Nutzen zu fordern oder die unerwünschte Werbung zu zeigen. Sobald ein System eine Internetverbindung herstellt, wird es Angriffen durch Malware ausgesetzt. Angesichts der aktuellen Bedrohungslage und der Verstärkung der Angriffe ist die Verhinderung der Ausbreitung über ein Netzwerk eine dringende Priorität geworden.

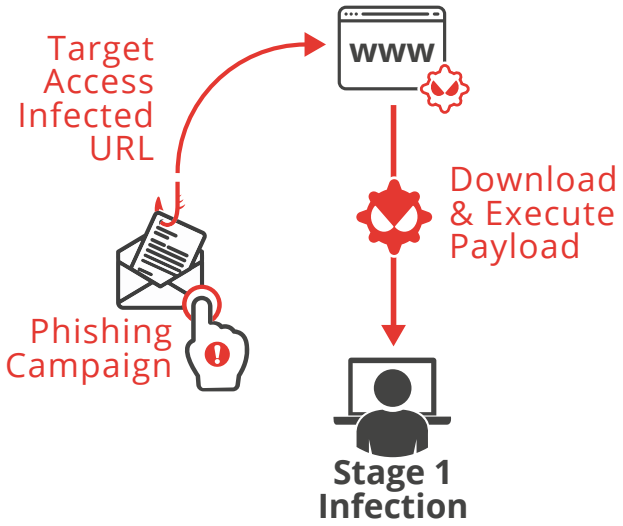
Bestehende Sicherheitslösungen decken ein breites Spektrum an möglichen Angriffsmethoden ab:

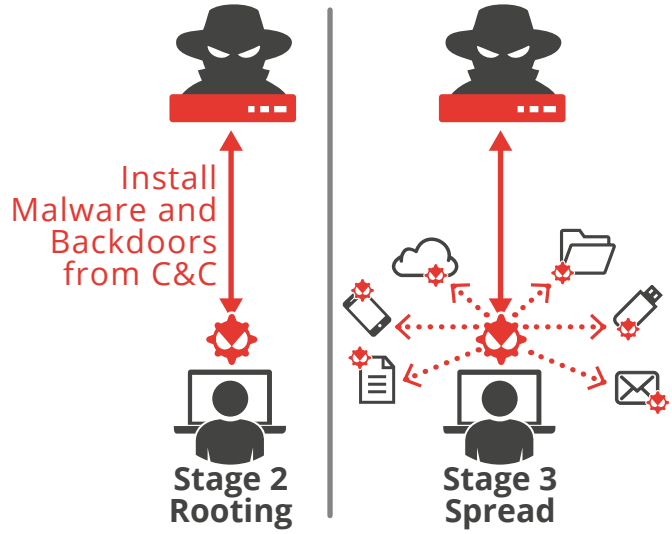
- E-Mail Malware, die in der Regel durch Anti-Spam-Filter unschädlich gemacht wird
- Webseite / Download von Malware, die allgemein durch die Nutzung von Web Gateway Anti Virus unschädlich gemacht wird
- File Sharing verbreitet Malware, die in der Regel durch Anti Virus unschädlich gemacht wird.

Ihnen fehlt jedoch die Fähigkeit, Bedrohungen, die von nicht verwalteten Netzwerkgeräten stammen und speziell konstruierte Angriffe, die nicht mit den vorhandenen Bedrohungsmustern übereinstimmen, zu identifizieren. SOLIDserver»-DNS-Firewall verhindert die erste Malware Infektion eines Geräts durch das Blockieren verdächtiger Abfragen, die sonst ein Benutzer zu Domains und IP-Adressen weiterleiten würde, die im Zusammenhang mit bösartigen Aktivitäten stehen, unabhängig vom Verkehrsmuster.

Es verringert auch die offensiven Fähigkeiten der Malware, die bereits ein bestehendes „verbundenes oder mobiles“ Endgerät infiziert haben, so wie Laptops, Tablet-PCs oder Handys. Sie tut dies durch das Blockieren der Kommunikation mit einem bekannten „Command- und Control-Servers“, welche Malware Updates, Remote Steuerung und Versuche, Daten zu extrahieren, vermeiden. Weiterer Schutz kann erreicht werden...

...durch die Kombination einer DNS-Firewall mit DNS-Guardian. Dieses Produkt nutzt Echtzeit-DNS-Daten-Verkehrs-Analyse DNS Traffic Inspection (DTI) und „Human Malicious Activity Detection“, die, wenn notwendig, automatische und adaptive Gegenmaßnahmen auslösen. Dies mindert die fortschrittlichsten DNS-Tunneling-Techniken und schützt proaktiv die rekursiven DNS-Engines gegen jede Art von DNS-Angriffen, mit denen der Zugang für jede Anwendung eines Informationssystems sichergestellt werden kann.





Finden von infizierten Geräten

Eine Bedrohung bedeutet aber nicht nur das Blockieren des Datenverkehrs und Isolierung des ansteckenden Agenten. Es erfordert schnelle Intervention auf dem infizierten Gerät zur Analyse und Behandlung der Infektion.

Die auf entsprechenden Protokollierungsrichtlinien basierende DNS-Firewall ermöglicht eine schnelle Identifizierung jeder beliebigen IP-Adresse, von der die erkannten verdächtigen Abfragen ausgehen. In Kombination mit einem IPAM und dem zugehörigen Netzwerk Discovery Tool ermöglicht es die schnelle Lokalisierung infizierter Geräte für eine sofortige Lösung.

Erweitertes Bedrohungsreporting

Die Kombination von SOLIDserverTM's Logging Funktionen mit vorhandenem Event Manager (oder SIEM-Security Information und Event Manager) ermöglicht einen einfachen Export von DNS-Firewall Logs im Standard-Syslog-Format. Dies wiederum erlaubt die Ausführung von Advanced Analytics auf dem verdächtigen DNS-Verkehr und erstellt entsprechende Berichte mit benutzerdefinierten Modellen oder allen verfügbaren Plugins, die kompatibel mit der eingesetzten Lösung (zum Beispiel Splunk oder Graylog) sind.

Die DNS-Firewall ist Teil der einzigartigen „EfficientIP 360° Security-Lösung", die konzipiert wurde, um öffentlichen und privaten DNS-Infrastrukturen sowohl vor internen als auch externen DNS-Bedrohungen zu schützen, unabhängig vom Typ des Angriffs.

efficient iP™

REV: C-190104

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
33 Ubi Avenue 3
08-25 Vertex Building, Singapore 408868
+65 6678 7752