

Kontrolle der Internetaktivitäten durch URL-Filterung



Die perfekte Ergänzung zur policy-basierten Anwendungssteuerung durch App-ID ist die On-Box-URL-Filter-Datenbank, die volle Kontrolle über zugehörige Web-Aktivitäten ermöglicht. Durch den URL-Filter wird fehlende Transparenz und Kontrolle auf Applikations- und Netzwerkebene beseitigt. Im Zusammenspiel mit App-ID schützt die Lösung optimal vor Risiken durch Verstöße aus den Bereichen Policy, Richtlinien, Produktivität und Ressourcennutzung.

Funktionsweise

Die Lösung teilt sich in zwei Datenbanken auf. Die erste lokale Datenbank ist direkt auf der Box gespeichert und beinhaltet die am häufigsten aufgerufenen Adressen. Diese werden dynamisch durch das Surf-Verhalten der Anwender gesteuert und in regelmäßigen Abständen mit der zentralen Masterdatenbank abgeglichen. Damit wird sichergestellt, dass die lokale Datenbank immer die aktuelle Kategorisierung kennt. Die zweite Datenbank ist die zentrale Masterdatenbank in der Cloud. Diese wird immer dann abgefragt, wenn in der lokalen kein Eintrag für die Webseite existiert oder dieser veraltet ist.

Die Filterung von Webseiten basiert auf 62 vordefinierten Kategorien bzw. Block- oder Erlaublisten. Zusätzlich ist eine granulare Filterung auf einzelne User bzw. User-Gruppen über die UserID möglich.

Beim Aufruf einer gesperrten Seite wird dem Anwender entweder eine vordefinierte oder kundenspezifische Seite angezeigt. Zusätzlich kann für Seiten/Kategorien eine Warn-Seite angezeigt werden, damit der Anwender informiert wird, dass er eine Seite aufruft, die zwar erlaubt aber potenziell unerwünscht ist. Darüber hinaus ist es möglich, eine einmalige Deaktivierung der URL-Filterung für eine Seite durch Eingabe eines Kennwortes durch eine berechtigte Person (Administrator) durchzuführen.



Abbildung 1: Funktionsweise der URL-Filterung

Ein beliebter Trick, um eine URL-Filterung zu umgehen, ist eine Suche auf Google (oder Bing/Yahoo) durchzuführen und sich dann im Cache-Modus die gewünschte Seite anzusehen. Dies kann durch die Safe-Search Einstellungen der Suchmaschinen gesperrt werden. Mittels der URL-Filterung kann diese Einstellung erzwungen werden. Damit ist eine Benutzung der Suchmaschine nur möglich, wenn im lokalen Browser die Safe-Search-Option aktiviert ist.

Durch die Anwendung von SSL-Entschlüsselungsrichtlinien auf den Netzwerkverkehr ist eine weitere tiefere Kontrolle möglich. Hierdurch kann die URL-Filterung auch auf den verschlüsselten Verkehr angewendet werden. Dies schützt die Anwender zusätzlich.

Architekturmodell

Die unbegrenzte Benutzerlizenz hinter jeder URL-Filterung-Subscription und die hohe Leistung der Palo Alto Networks Next Generation Firewall bedeutet, dass nur ein einziges Gerät benötigt wird, um Web-Aktivitäten für eine gesamte Domäne zu kontrollieren, ohne sich um Kostenschwankungen wegen benutzerbasierter Lizenzierungen sorgen zu müssen.

Leistungen

Die Experten von iT-CUBE SYSTEMS planen und installieren Ihre neue Next Generation Firewall. Diese integrieren wir in bereits bestehende SIEM (Security Information & Event Management) und Log Management-Systeme. Sind Sie bereits im Besitz einer Next Generation Firewall? Gerne integrieren wir die Lösung in bereits vorhandene NGFW. Darüber hinaus sind wir stets um eine Erweiterung und Auditierung des Regelwerks bemüht.

iT-CUBE unterstützt Sie dabei, die Anforderungen an einem sicheren Zugang zum Internet in einem bestehenden IT-Security-Konzept auf den neuesten Stand zu bringen und zu integrieren oder ein neues IT-Security-Konzept zu erstellen.

Nutzen

Unsere Mitarbeiter sind zertifizierte Palo Alto Networks Accredited Sales Experts und Certified Network Security Engineers und Teil des Palo Alto Network Authorized Support Center.

Unsere Experten haben bereits viele Projekte mit unterschiedlichsten Produkten erfolgreich umgesetzt. Wir nutzen diese jahrelange Erfahrung, um die NGFW von Palo Alto Networks perfekt in Ihre bestehende Infrastruktur zu integrieren. Firewall-Systeme können etwa genutzt werden, um einzelne Systeme oder ganze Abteilungen zu separieren.

Die Mitarbeiter von iT-CUBE stehen im engen Kontakt mit Palo Alto Networks. Dadurch können technische sowie organisatorische Probleme schnell und reibungslos gelöst werden. Schon kurz nachdem Palo Alto Networks den europäischen Markt betrat, starteten wir bereits mit gemeinsamen Projekten durch.

Um Sie besser auf Sicherheitsvorfälle und den Umgang mit der Lösung zu schulen, bietet iT-CUBE speziell auf Ihre Bedürfnisse zugeschnittene Workshops für Ihre Mitarbeiter an.

