

Next Generation Firewall - Überblick

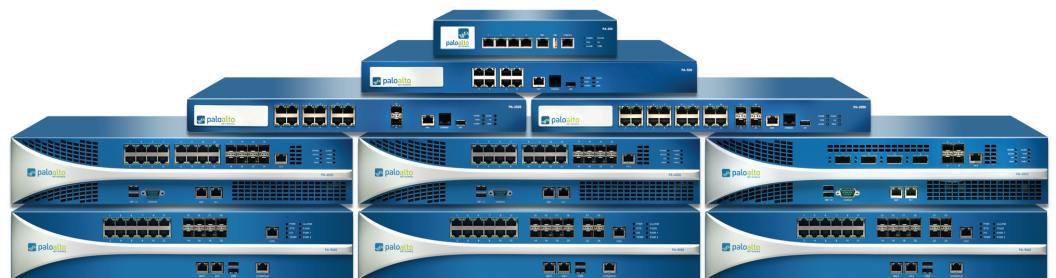
Jüngste Änderungen von Anwendungsverhalten und Nutzungsmustern untergraben den von traditionellen Firewallsystemen gebotenen Schutz immer weiter. Nicht selten greifen die Benutzer von beliebigen Standorten aus auf die unterschiedlichsten Anwendungen zu, um ihre Arbeit zu erledigen. Viele dieser Anwendungen verwenden keine dem Standard entsprechenden Ports, wechseln zwischen den Ports oder setzen eine Verschlüsselung ein, um den Benutzern einen einfachen und optimierten Zugriff zu bieten und die Firewall zu umgehen. Cyberkriminelle nutzen diese uneingeschränkte Nutzung der Anwendungen hemmungslos aus, um eine neue Klasse hochspezialisierter moderner Malware zu verbreiten. Dies bewirkt, dass die herkömmliche Firewall, die sich auf Ports und Protokolle konzentriert, die Anwendungen und Bedrohungen die sich durch Netz bewegen, nicht mehr identifizieren und kontrollieren kann.

Versuche, die Kontrolle über die Anwendungsnutzung und den Schutz digitalen Eigentums für alle Benutzer zurückzuerlangen, haben zu doppelt angelegten, lokalen und verteilten Sicherheitsrichtlinien geführt, die von einer ganzen Branche mittels eigenständiger oder integrierter Firewall-Helfer unterstützt werden. Dieser Ansatz kann zu Inkonsistenzen führen und löst keinesfalls die Probleme im Hinblick auf Transparenz und Kontrolle aufgrund einer fehlerhaften oder unvollständigen Klassifizierung des Netzwerktraffics, komplexen Managements und der erhöhten Latenz beim mehrfach Scannen des Netzwerktraffics. Die Wiederherstellung der Transparenz bedingt einen völlig neuen Komplettansatz für die sichere Aktivierung von Anwendungen, den nur eine Firewall der nächsten Generation mitsichbringt.

Die wichtigsten Anforderungen an die Next Generation Firewall:

- Identifikation von Anwendungen, nicht von Ports. Präzise Identifikation der Anwendung über alle Ports, unabhängig von Protokoll, Verschlüsselung (SSL oder SSH) oder Umkehrmethoden, und Nutzung der Identität als Grundlage für alle Sicherheitsrichtlinien.
- Identifikation von Benutzern, nicht von IP-Adressen. Nutzung von in Unternehmensverzeichnissen gespeicherten Benutzer- und Gruppendaten für Transparenz, Sicherheitsrichtlinien, Reporting und forensische Untersuchungen, unabhängig davon, wo sich der Benutzer gerade befindet (anonymisierbar).
- Verhinderung von Bedrohungen in Echtzeit. Schutz gegen den gesamten Lebenszyklus eines Angriffs, einschließlich gefährlicher Anwendungen, Schwachstellen, Malware, URLs mit erhöhtem Risiko und zahlreicher böswilliger Dateien und Inhalte.
- Vereinfachte Verwaltung. Sichere und geschützte Aktivierung von Anwendungen durch ein benutzerfreundliches grafisches Frontend und einen einheitlichen Richtlinien-Editor.
- Verwenden eines logischen Perimeters. Schutz aller Benutzer, einschließlich von Geschäftsreisenden und Telearbeitern. Die dadurch entstehende konsistente Sicherheit erweitert den physischen Perimeter zum logischen Perimeter.
- Multi-Gigabit-Durchsatz. Die Kombination speziell angefertigter Hard- und Software sorgt für niedrige Latenz und Multi-Gigabit-Durchsatz bei gleichzeitiger Nutzung aller Funktionen.

Die Next Generation Firewalls von Palo Alto Networks bieten ein beispielloses Maß an Transparenz sowie Kontrolle über Anwendungen, Benutzer und Inhalte. Dazu werden drei einzigartige Identifizierungstechniken angewendet: App-ID™, User-ID und Content-ID. Diese Identifizierungstechnologien, die man in allen Firewalls von Palo Alto Networks antrifft, gestatten es Unternehmen, die Nutzung von Anwendungen sicher und geschützt zu aktivieren, während gleichzeitig die Gesamtbetriebskosten durch eine Konsolidierung der Geräte wesentlich reduziert werden.



App-ID: Klassifizierung aller Anwendungen auf allen Ports und zu jedem Zeitpunkt

Eine exakte Klassifizierung des Datenverkehrs bildet das Kernstück jeder Firewall der nächsten Generation. Das Ergebnis wird zur Grundlage der Sicherheitsrichtlinie. Herkömmliche Firewalls klassifizieren Verkehr nach Port und Protokoll, was in der Vergangenheit einen ausreichenden Mechanismus für die Sicherung des Netzwerks darstellte. Heute sind Applikationen in der Lage, eine herkömmliche portbasierte Firewall ganz einfach zu umgehen: durch Port-Hopping mit SSL und SSH, Tunneln über Port 80 oder die Nutzung nicht standardisierter Ports. App-ID zielt auf die Transparenzbeschränkungen bei der Verkehrsklassifizierung, unter der herkömmliche Firewalls gelitten haben. Dazu werden mehrere Klassifizierungsmechanismen auf den Verkehrsstrom angewendet, sobald die Firewall diesen sieht, um die genaue Identität von Anwendungen im Netzwerk zu erkennen.

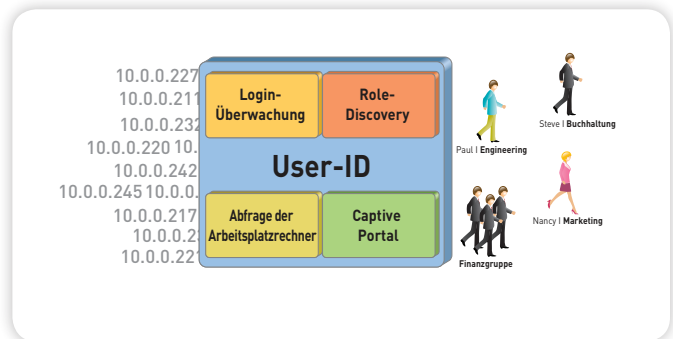
Anders als Add-on-Angebote, die nur auf IPS-Signaturtypen basieren, welche nach der portbasierten Klassifizierung implementiert wurden, verwendet jede App-ID automatisch bis zu vier verschiedene Verkehrsklassifizierungsmechanismen, um die Anwendung zu identifizieren. App-ID überwacht fortlaufend den Anwendungsstatus, klassifiziert das Verkehrsaufkommen neu und identifiziert die verschiedenen verwendeten Funktionen. Die Sicherheitsrichtlinie bestimmt, wie die Anwendung zu behandeln ist: Blockieren, Zulassen oder sicheres Aktivieren (auf eingebettete Bedrohungen hin überprüfen und diese blockieren, mit QoS auf unerlaubte Dateiübertragungen und Datenmuster oder -formen untersuchen).



User-ID: Anwendungen nach Benutzern und Gruppen aktivieren

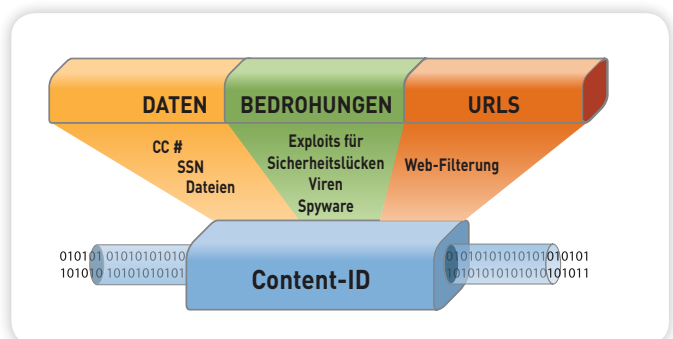
In der Vergangenheit wurden Sicherheitsrichtlinien basierend auf IP-Adressen angewendet, aber nachdem die Benutzer und auch die Programmierung zunehmend dynamischer geworden sind, hat sich die alleinige Verwendung von IP-Adressen für die Überwachung und Kontrolle von Benutzeraktivitäten als unwirksam erwiesen. User-ID gestattet es Unternehmen, die benutzer- oder gruppenbasierten Aktivierungsrichtlinien für Anwendungen auf Microsoft- Windows-, Apple Mac OS X-, Apple iOS- und Linux-Benutzer zu erweitern.

Benutzerinformationen können aus Unternehmensverzeichnissen (Microsoft Active Directory, eDirectory und Open LDAP) und Terminal Service-Angeboten (Citrix und Microsoft Terminal Services) ermittelt werden, während die Integration in Microsoft Exchange, ein Captive Portal und ein XML API den Unternehmen ermöglichen, ihre Richtlinien auf Apple Mac OS X-, Apple iOS- und UNIX-Benutzer zu erweitern, die sich in der Regel außerhalb der Domäne befinden.



Content-ID: Schutz von zulässigem Verkehr

Viele moderne Anwendungen bieten maßgebliche Vorteile, aber sie werden von moderner Malware und Bedrohungen auch als Bereitstellungswerkzeug genutzt. In Verbindung mit App-ID gestattet es Content-ID dem Administrator, sehr gezielt Anwendungen zu erlauben und gleichzeitig das Netzwerk zu schützen. Nachdem App-ID eingesetzt wurde, um unerwünschte Anwendungen zu identifizieren und zu blockieren, können die Administratoren zulässige Anwendungen sicher aktivieren, indem sie die Nutzung von Schwachstellen, moderne Malware, Viren, Botnets und andere Malware daran hindern, sich über das gesamte Netzwerk zu verbreiten, und zwar unabhängig von Port, Protokoll, oder Umgehungsmethode. Die von Content-ID unterstützten Steuerelemente werden durch eine umfassende URL-Datenbank abgerundet, um das Websurfen und Datenfilterfunktionen zu kontrollieren.



Sicheres Aktivieren von Anwendungen

Die nahtlose Integration von App-ID, User-ID und Content-ID gestattet es Unternehmen, konsistente Richtlinien für die Zulassung von Anwendungen einzurichten, in vielen Fällen bis hinunter zur Funktionsebene der Anwendungen, die weit über ein einfaches ‚Erlauben‘ oder ‚Verbieten‘ hinausgehen. Mit GlobalProtect™ können dieselben Richtlinien, die die Benutzer innerhalb der Unternehmensniederlassung schützen, auf alle Benutzer erweitert werden, unabhängig davon, wo diese sich gerade befinden, wodurch ein logischer Perimeter für Benutzer außerhalb des Netzwerks eingerichtet wird.

Sichere Aktivierungsrichtlinien beginnen mit App-ID, das die Identität der Anwendung bestimmt, die dann mit User-ID dem jeweiligen Benutzer zugeordnet wird, während gleichzeitig die Anwendungsdaten mittels Content-ID auf Bedrohungen, Dateien, Datenmuster und Webaktivität überprüft werden. Diese Ergebnisse werden im Application Command Center (ACC) angezeigt, wo der Administrator in Echtzeit erfahren kann, was im Netzwerk gerade passiert. Im Richtlinien-Editor können dann die in ACC über Anwendungen, Benutzer und Inhalte angezeigten Informationen in entsprechende Sicherheitsrichtlinien umgewandelt werden, die unerwünschte Anwendungen blockieren, während andere sicher zugelassen und aktiviert werden. Schließlich können beliebige detaillierte Analysen, Berichte oder forensische Untersuchungen erstellt werden, die ebenfalls auf Anwendungen, Benutzern und Inhalt basieren.

Application Command Center: Wissen ist Macht

Das Application Command Center (ACC) erstellt einen Überblick über die Protokolldatenbank, um die einzelnen Anwendungen im Netzwerk zu kennzeichnen, die jeweiligen Benutzer und die potenziellen Auswirkungen auf die Sicherheit. ACC wird dynamisch aktualisiert und nutzt dazu die von App-ID stetig durchgeführte Verkehrsklassifizierung; wenn eine Anwendung die Ports oder ihr Verhalten wechselt, beobachtet App-ID den Verkehr weiterhin und zeigt die Ergebnisse in ACC an. Neue oder unbekannte Anwendungen, die in ACC angezeigt werden,

können mit einem Klick schnell untersucht werden. Auf diese Weise werden eine Beschreibung der Anwendung, ihre wichtigsten Funktionen, ihre Verhaltenseigenschaften und ihre Benutzer angezeigt. Die zusätzliche Transparenz im Hinblick auf URL-Kategorien, Bedrohungen und Daten bietet ein vollständiges und abgerundetes Bild der Netzwerkaktivität. Mit Hilfe von ACC kann ein Administrator schnell mehr über den Verkehr im Netzwerk erfahren und diese Information dann in eine fundiertere Sicherheitsrichtlinie umwandeln.

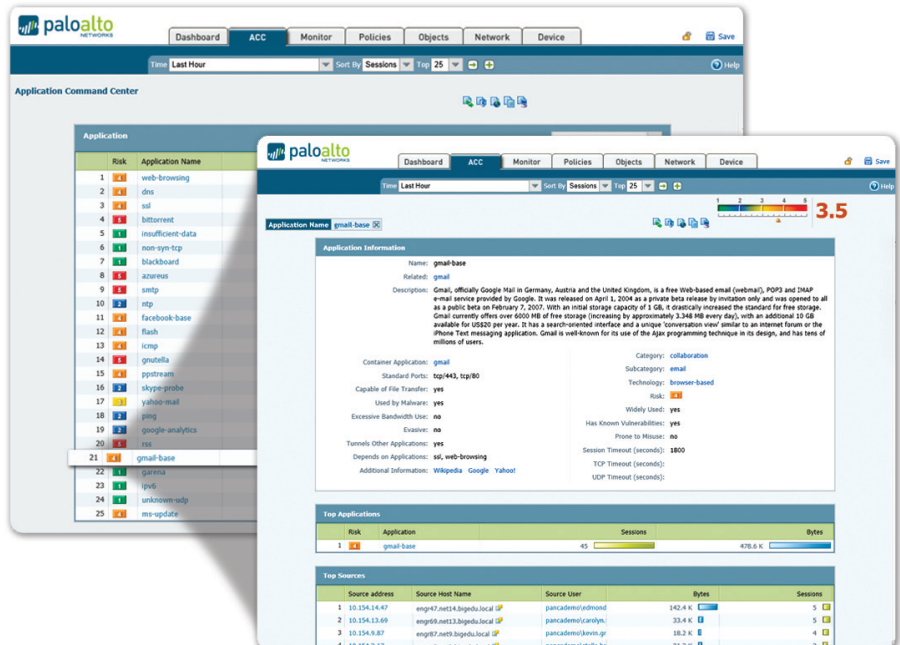
Richtlinien-Editor: Erkenntnisse in sichere Aktivierungsrichtlinien umwandeln

Mit dem Wissen, welche Anwendungen im Netzwerk von welchen Benutzern verwendet werden, und welche potenziellen Sicherheitsrisiken vorliegen, können Administratoren schnell, systematisch und kontrolliert Aktivierungsrichtlinien umsetzen, die auf Anwendungen, Anwendungsfunktionen und Ports basieren. Die Reaktionen der Richtlinien können von „offen“ (zulassen) über „angepasst“ (einige Anwendungen oder Funktionen werden aktiviert, anschließend gescannt oder gestaltet, eingeplant usw.) bis hin zu „geschlossen“ (ablehnen) reichen. Beispiele dafür sind unter anderem:

- Schutz einer Oracle-Datenbank, indem der Zugriff auf Gruppen aus der Buchhaltung eingeschränkt wird, Erzwingen des Verkehr über Standardports und Überprüfung des Verkehrs auf Sicherheitslücken in den Anwendungen.
- Nur der IT-Gruppe gestatten, eine feste Palette verteilter Managementanwendungen (z.B. SSH, RDP, Telnet) über ihre Standardports zu verwenden.
- Festlegen und Durchsetzen einer Unternehmensrichtlinie, die eine bestimmte Webmail- und Instant-Messaging-Nutzung zulässt und überprüft, aber die jeweiligen Funktionen zur Dateiübertragung blockiert.
- Zulassen von Microsoft SharePoint Administration nur für das Administrationsteam, und Zulassen des Zugriffs auf Microsoft SharePoint Documents für alle anderen Benutzer.

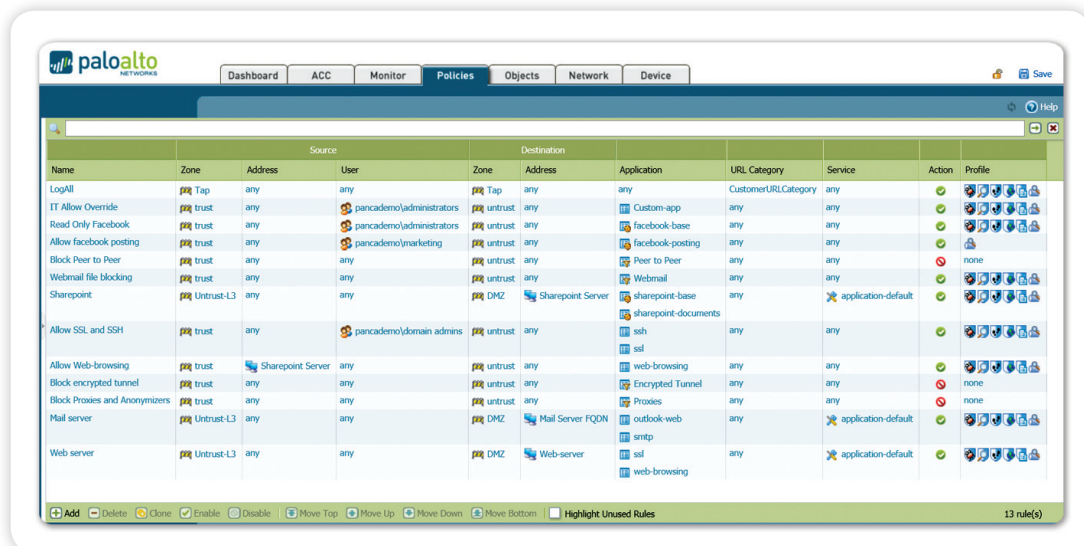
Anwendungstransparenz

Die Firewall zeigt die Aktivitäten im Zusammenhang mit Anwendungen in einem klaren und leicht zu interpretierenden Format an. Fügen Sie Filter hinzu und entfernen Sie diese wieder, um weitere Informationen über die Anwendung, ihre Funktionen und ihre Benutzer zu erhalten.



Einheitlicher Richtlinien-Editor

Das vertraute Aussehen und Verhalten des Regelwerks ermöglicht die schnelle Entwicklung und Implementierung von Richtlinien, die für Anwendungen, Benutzer und Inhalte definiert werden.



- Implementierung von Richtlinien für die Webaktivierung, die den Datenverkehr zu geschäftlich genutzten Websites zulassen und überprüfen, während der Zugriff auf offensichtlich für private Zwecke genutzte Websites blockiert wird, und „Coaching“ des Zugriffs auf andere Websites unter Verwendung benutzerdefinierter Sperrseiten.
- Implementierung von Richtlinien, die die Verwendung bandbreitenintensiver Medienanwendungen und Websites zulassen, aber ihren Einfluss auf VoIP-Applikationen beschränken.
- Entschlüsselung von SSL-Verkehr zu Websites von sozialen Netzwerken und Webmail und Überprüfung auf Malware und die Ausnutzung von Sicherheitslücken.
- Zulassen von Downloads ausführbarer Dateien von nicht kategorisierten Websites nur dann, wenn der Benutzer zugestimmt hat, um Drive-by-Downloads über Zero-Day-Attacks zu verhindern.
- Ablehnen des gesamten Verkehrs aus bestimmten Ländern oder Blockieren von unerwünschten Anwendungen wie P2P-Filesharing, Umgehungsprogrammen und externen Proxies.

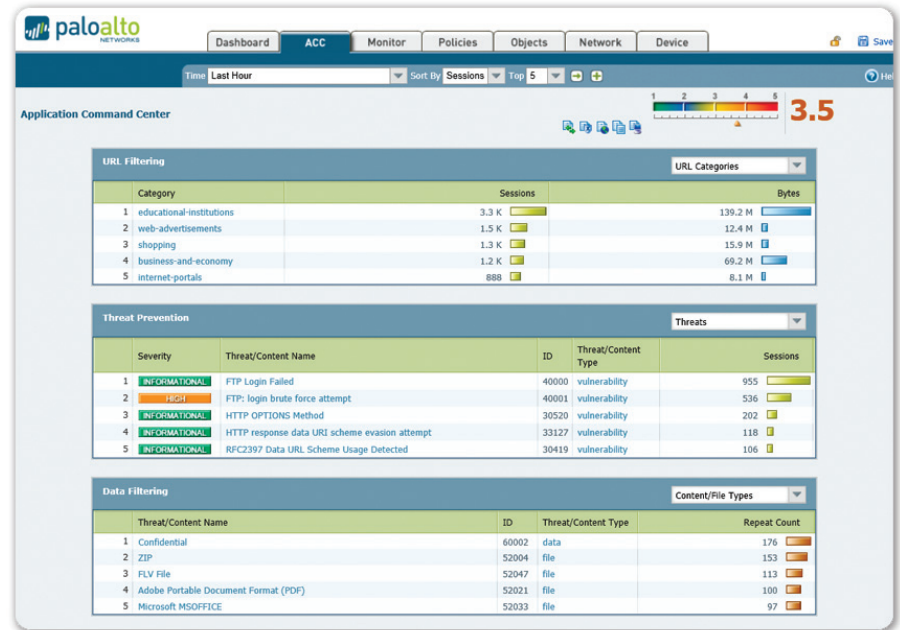
Die enge Integration einer auf Benutzern und Gruppen basierenden Anwendungskontrolle und die Möglichkeit, den zugelassenen Verkehr auf die unterschiedlichsten Bedrohungen zu überprüfen, gestattet es dem Unternehmen, die Anzahl der verwendeten Richtlinien dramatisch zu reduzieren und das, auch wenn neue Mitarbeiter eingestellt werden oder sich Mitarbeiter im Unternehmen verändern.

Richtlinien-Editor: Schutz zugelassener Anwendungen

Die sichere Aktivierung von Anwendungen bedeutet, dass Zugriff auf die Anwendungen gestattet wird, und anschließend spezielle Richtlinien für den Schutz vor Bedrohungen und das Blockieren von Dateien oder zur URL-Filterung angewendet werden. Alle in Content-ID enthaltenen Elemente können für einzelne Anwendungen konfiguriert werden.

- **Intrusion Prevention System (IPS):** Das Modul zum Schutz vor Schwachstellen und Exploits integriert Intrusion Prevention System (IPS)-Funktionen, um Sicherheitslücken in der Netzwerk- und Anwendungsschicht zu erkennen, Pufferüberläufe und Denial-of-Service-Attacks zu verhindern sowie Port Scans daran zu hindern, die Datenressourcen des Unternehmens zu gefährden und zu beschädigen.
- **Netzwerk-Antivirus:** Stream-basierter Antiviren-Schutz blockiert Millionen von Malware-Varianten, unter anderem PDF-Viren und in komprimierten Dateien oder in Webverkehr verborgene Malware (komprimiertes HTTP/HTTPS). Eine auf Richtlinien basierende SSL-Entschlüsselung gestattet es den Unternehmen, sich gegen Malware zu schützen, die über SSL-verschlüsselte Anwendungen eindringt.
- **URL-Filterung:** Eine vollständig integrierte, anpassbare Datenbank für die URL-Filterung ermöglicht es Administratoren, präzise Richtlinien für das Browsen im Web zu erstellen, die Anwendungstransparenz zu ergänzen, Richtlinien zu kontrollieren und das Unternehmen vor einer ganzen Palette an rechtlich kritischen oder der Produktivität abträglichen Risiken zu schützen.
- **Datei- und Datenfilterung:** Die Datenfilterung gestattet Administratoren, Richtlinien zu implementieren, die die Risiken bei Datei- und Datenübertragungen minimieren. Dateiübertragungen und Downloads können kontrolliert werden, indem die Datei (und nicht nur die Dateinamenerweiterung) überprüft wird, um festzustellen, ob sie zugelassen werden sollte oder nicht. Ausführbare Dateien, die man typischerweise in Drive-by-Downloads findet, können blockiert werden, wodurch das Netzwerk vor einer nicht erkannten Malware-Verbreitung geschützt wird. Schließlich können die Datenfilterfunktionen die Übertragung vertraulicher Datenmuster (Kreditkarten- und Sozialversicherungsnummern) erkennen und kontrollieren.

Transparenz von Inhalt und Risiken
Zeigt URL-Kategorien, Bedrohungen sowie die Anzahl von übertragenen Dateien/Daten in einem klaren und leicht zu interpretierenden Format an. Fügen Sie Filter hinzu oder entfernen Sie sie, um weitere Informationen zu einzelnen Elementen zu erhalten.



Erkennen und Verhindern moderner Malware

Malware hat sich zu einer erweiterbaren vernetzten Anwendung weiterentwickelt, die den Angreifern beispiellosen Zugriff auf das anvisierte Netzwerk bietet und ihnen eine maßgebliche Übernahme der Kontrolle darin gestattet. Mit der zunehmenden Leistung moderner Malware ist es unabdingbar geworden, dass Unternehmen in der Lage sind, diese Bedrohungen unmittelbar zu erkennen, noch bevor die Bedrohung eine definierte Signatur besitzt. Die Firewalls der nächsten Generation von Palo Alto Networks bieten einen vielseitigen Ansatz, der auf der direkten Analyse sowohl ausführbarer Dateien als auch des Netzwerkverkehrs basiert, um ihre Netzwerke auch zu schützen, bevor Signaturen zur Verfügung stehen.

- **WildFire™:** Unter Verwendung eines auf der Cloud basierenden Ansatzes deckt WildFire zuvor unbekannte, böswillige ausführbare Dateien auf, indem es ihr Verhalten in einer sicheren virtualisierten Umgebung direkt beobachtet. WildFire sucht nach böswilligen Aktionen innerhalb von Microsoft Windows-Programmdateien, wie beispielsweise die Änderung von Registry-Werten oder Betriebssystemdateien, die Deaktivierung von Sicherheitsmechanismen oder die Einspeisung von Code in laufende Prozesse. Diese direkte Analyse identifiziert Malware schnell und genau, selbst wenn kein Schutzmechanismus dafür zur Verfügung steht. Die Ergebnisse werden unmittelbar an den Administrator weitergegeben, damit dieser entsprechend reagieren kann, und es wird automatisch eine Signatur entwickelt und im nächsten Inhalts-Update allen Kunden bereitgestellt.
- **Verhaltensabhängige Botnet-Erkennung:** App-ID klassifiziert den gesamten Datenverkehr auf Anwendungsebene und deckt damit jeden unbekannten Verkehr im Netzwerk auf, was häufig ein Hinweis auf Malware oder andere bedrohliche Aktivitäten ist. Der Botnet-Verhaltensbericht analysiert Netzwerkverhalten, das auf eine Botnet-Infektion hindeutet, wie beispielsweise wiederholter Besuch von Malware-Sites, Verwendung von dynamischem DNS, IRC und anderes potenziell verdächtiges Verhalten. Die Ergebnisse werden in Form einer Liste potenziell infizierter Hosts angezeigt, die als mögliche Elemente eines Botnet untersucht werden können.

Verkehrsüberwachung: Analyse, Reporting und Forensik

Die Best Practices der Sicherheit fordern von den Administratoren einen Mittelweg zwischen einerseits proaktivem, stetigem Lernen und entsprechender Anpassung, um das Firmenvermögen zu schützen, und andererseits reaktivem und investigativem Verhalten sowie dem Erstellen von Analysen und Berichten zu Sicherheitsvorfällen. ACC und der Richtlinien-Editor können mit zahlreichen Tools für die Überwachung und das Reporting genutzt werden, um proaktiv Richtlinien für die Zulassung von Anwendungen einzusetzen. Damit werden den Unternehmen die erforderlichen Mittel an die Hand gegeben, die Anwendungen, Benutzer und Inhalte, die die Palo Alto Networks-Firewall der nächsten Generation durchlaufen, zu analysieren und Berichte dazu zu erstellen.

- **App-Scope:** App-Scope ergänzt den aktuellen Einblick in den Datenverkehr durch ein dynamisches, vom Benutzer anpassbares Fenster mit Blick auf die Netzwerkaktivität. App-Scope zeigt, was sich im Laufe der Zeit ereignet hat und lokalisiert problematisches oder unregelmäßiges Verhalten.
- **Reporting:** Vordefinierte Berichte können im Ist-Zustand verwendet, angepasst oder miteinander zu einem Report gruppiert werden, um den spezifischen Anforderungen zu entsprechen. Alle Berichte können ins CSV- oder PDF-Format exportiert und nach Zeitplan ausgeführt und per E-Mail versendet werden.
- **Logging:** Das Log-Filtern in Echtzeit ermöglicht eine schnelle forensische Untersuchung jeder Sitzung im Netzwerk. Logs können zur Offline-Archivierung oder zur zusätzlichen Analyse in eine CSV-Datei exportiert oder an einen Syslog-Server gesendet werden.
- **Tool zum Nachverfolgen von Sitzungen (Trace Session Tool):** Schnelle forensische Untersuchungen oder Recherchen nach einzelnen Vorfällen mithilfe einer zentralen, zusammenhängenden Ansicht aller Logs des Datenverkehrs, der Bedrohungen, URLs und Anwendungen, bezogen auf individuelle Sessions.

GlobalProtect: Durchgängige Sicherheit an jedem Ort

Nicht nur die Anwendungen ändern sich im Unternehmen. Immer mehr Endbenutzer erwarten völlig selbstverständlich, dass sie von jedem Standort aus und mit jedem beliebigen Gerät eine Verbindung einrichten und arbeiten können. Die IT-Teams haben deshalb alle Hände voll zu tun, um die Sicherheit auf diese Geräte und Standorte zu erweitern, die sich weit über den herkömmlichen Perimeter des Unternehmens hinaus erstrecken können. GlobalProtect erfüllt diese Herausforderung, indem es konsistent die Sicherheitsrichtlinien auf alle Benutzer ausweitet, unabhängig von ihrem Standort und dem verwendeten Gerät.

First, GlobalProtect stellt eine sichere Konnektivität für alle Benutzer sicher: durch ein transparentes VPN, das zahlreiche Geräte unterstützt, unter anderem unter Microsoft Windows, Apple Mac OS X und Apple iOS. Nach der Verbindung wird der gesamte Verkehr von der Firewall klassifiziert, die Aktivierungsrichtlinien werden angewendet, Verkehr wird auf Bedrohungen überprüft und das Netzwerk und die Benutzer werden geschützt.

Darüber hinaus kann GlobalProtect zusätzliche Kontrollen anwenden, die vom Status des Endbenutzergeräts abhängig sind. Beispielsweise könnte einem Benutzer der Zugriff auf bestimmte Anwendungen oder sicherheitskritische Netzwerkbereiche verboten werden, wenn das Gerät nicht über ein aktuelles Virenschutzprogramm verfügt oder wenn die Datenträgerverschlüsselung nicht aktiviert ist. Auf diese Weise kann die IT die Verwendung von Anwendungen für unterschiedlichste Endbenutzer-Gerätetypen sicher aktivieren, während ein konsistenter Ansatz für die Sicherheit der nächsten Generation beibehalten wird.

GlobalProtect
Durchsetzen konsistenter
Richtlinien für die sichere
Aktivierung von Anwendungen für
alle Benutzer, unabhängig davon,
wo diese sich gerade befinden.

