PA-400 Series für verteilte Unternehmen

Zuverlässige Sicherheit für Filialen

Zur Steigerung der Agilität, Geschwindigkeit und Innovation weiten große verteilte Unternehmen die digitale Transformation auf ihre Filialen und Ladengeschäfte aus. Doch dadurch steigt auch das Sicherheitsrisiko. Unternehmen mit Niederlassungen an verschiedenen Standorten drohen komplexe Angriffe in jeder Filiale, denn Angreifer sehen kleinere Zweigstellen oft als Möglichkeit, sozusagen „durch die Hintertür“ in ein größeres Unternehmen einzudringen. Dabei haben sie vor allem wertvolle Kundendaten und Finanztransaktionen im Visier.

Aus diesem Grund muss jede Filiale über das gleiche Maß an Sicherheit verfügen wie der Hauptsitz und die Rechenzentren. Insbesondere verteilte Unternehmen wie Banken, Krankenhäuser, Einzelhändler und Anbieter von Managed Security Services (MSSP) sollten sich darüber informieren, wie sie ihre Netzwerke in einer zunehmend mobilen Welt mit cloudbasierten Ressourcen schützen können.

Vorteile für Kunden

- Zero-Trust-Netzwerksicherheit in Filialen und sicherer kontextbasierter Zugriff für alle Benutzer und Geräte
- Vermeidung bekannter Bedrohungen und Zero-Day-Angriffe in Echtzeit mithilfe von eingebettetem maschinellen Lernen (ML) und nativ integrierten Cloud-Delivered Security Services
- Vereinfachte Bereitstellung einer großen Anzahl von Firewalls durch Zero Touch Provisioning
- Zentrale Verwaltung über Panorama™ für einen umfassenden Überblick über die Netzwerksicherheit
- Minimaler Wartungsaufwand dank ausfallsicherem Design

Die PA-400 Series

Die PA-400 Series von Palo Alto Networks umfasst die PA-460, PA-450, PA-440 und PA-410 und bietet ML-gestützte Funktionen einer Next-Generation Firewall (NGFW) für die verschiedenen Filialen und Einzelhandelsstandorte von verteilten Unternehmen. Mit der weltweit ersten ML-gestützten NGFW können Unternehmen selbst in kleinen Filialen bisher unbekannte Bedrohungen abwehren, profitieren von umfassenden Einblicken in und durchgehendem Schutz für die gesamte IT-Umgebung – auch für Geräte im Internet der Dinge (IoT) – und vermeiden mit automatisierten Richtlinienempfehlungen Bedienfehler.

Die PA-400 Series nutzt das Betriebssystem PAN-OS®, wie alle NGFWs von Palo Alto Networks – von der leistungsstarken PA-7080 über die flexible VM-Series bis hin zur cloudbasierten Prisma® SASE-Lösung. PAN-OS klassifiziert nativ den gesamten Netzwerkverkehr (einschließlich aller Anwendungsdaten, Bedrohungen und legitimen Inhalte) und ordnet die einzelnen Pakete dann unabhängig vom Standort oder Gerätetyp einem Benutzer zu. In Abhängigkeit von den Anwendungen, Inhalten und Benutzern (also den Faktoren, die für das Geschäft relevant sind) wird dann entschieden, welche Sicherheitsrichtlinien anzuwenden sind. Das stärkt den Sicherheitsstatus und beschleunigt effektive Reaktionen auf Sicherheitsvorfälle.

Wichtige Funktionen

Zuverlässige Sicherheit dank effizientem PAN-OS

PAN-OS ist die Software, die unseren ML-gestützten Next-Generation Firewalls zugrunde liegt. Mit den Technologien, die nativ in PAN-OS integriert sind – App-ID™, Content-ID™, Device-ID™ und User-ID™ –, erhalten Sie einen umfassenden Überblick und die Kontrolle über die Anwendungen sämtlicher Benutzer und Geräte an allen Standorten. Da die Inline-ML-Modelle, Anwendungen und Bedrohungssignaturen die Firewalls automatisch mit den neuesten Informationen aktualisieren, können Sicherheitsteams darauf vertrauen, dass der genehmigte Datenverkehr keine bekannten oder unbekannten Bedrohungen enthält.

Überblick über Anwendungen, Benutzer und Inhalte

Mit App-ID können Netzwerksicherheitsadministratoren alle in einem Netzwerk vorhandenen Anwendungen sehen und erhalten Einblick in ihre Funktionsweise, ihr Verhalten und ihr relatives Risiko für das Unternehmen. Das Tool identifiziert alle Anwendungen, die Daten durch das Netzwerk senden, und zwar unabhängig von Port, Protokoll, Umgehungstechniken und Verschlüsselung (TLS/SSL). Dabei werden richtlinienbasierte Aktionen (wie Zulassen, Ablehnen, Planen, Untersuchen und Traffic-Shaping zur Bandbreitenverwaltung) entsprechend der jeweiligen Anwendung anstatt auf Basis des Ports durchgeführt. Außerdem identifiziert App-ID alle Nutzdaten innerhalb einer Anwendung (wie Dateien und Datenmuster), um schädliche Dateien zu blockieren und Ausschleusungen zu verhindern.

Für neue Benutzer können mithilfe des integrierten Policy Optimizer ältere Layer-4-Regelsätze sicher zu App-ID-basierten Regeln konvertiert werden. Damit erhalten Administratoren einen Regelsatz, der sicherer und einfacher zu verwalten ist. Darüber hinaus bietet PAN-OS die Möglichkeit, benutzerdefinierte App-ID-Kennzeichnungen für eigene Anwendungen zu erstellen oder bei Palo Alto Networks die Zuweisung einer App-ID für neue Anwendungen anzufordern.

Weitere Details finden Sie in der Lösungsbeschreibung zu App-ID.

Sicherheitsrichtlinien basierend auf Benutzeraktivitäten

PAN-OS setzt Sicherheitsmaßnahmen orts- und geräteübergreifend durch und passt Richtlinien anhand von Benutzeraktivitäten an. Es bietet detaillierte Informationen, Sicherheitsrichtlinien, Berichte und Forensikdaten auf der Grundlage von Benutzern und Gruppen – nicht nur von IP-Adressen. Außerdem setzt es dynamische, auf dem Benutzerverhalten basierende Sicherheitsmaßnahmen durch, um die Aktivitäten verdächtiger oder böswilliger Benutzer einzuschränken.

PAN-OS lässt sich leicht in eine Vielzahl von Repositorys integrieren, um Benutzerinformationen abzurufen, unter anderem WLAN-Controller, VPNs, Verzeichnisserver, SIEMs und Proxys. Es wendet für alle identifizierten Benutzer konsistente Richtlinien an, unabhängig von deren Standort (z. B. Büro, Homeoffice oder unterwegs) und Gerät (iOS- und Android®-Mobilgeräte; macOS®-, Windows®-, Linux-Desktops oder -Laptops; Citrix- und Microsoft-VDI- und -Terminalserver).

Absicherung des verschlüsselten Datenverkehrs

Mehr als 90 Prozent des Internetverkehrs werden verschlüsselt. Daher müssen Netzwerksicherheitsadministratoren Datenverkehr direkt in der NGFW absichern können (d. h. entschlüsseln, absichern und wieder verschlüsseln). PAN-OS ist dafür ideal, da es den ein- und ausgehenden mit TLS/SSL verschlüsselten Datenverkehr untersucht – auch, wenn dieser TLS 1.3 oder HTTP/2 nutzt – und Ihre Richtlinien darauf anwendet. Es umfasst die notwendigen Tools, um schon vor der Entschlüsselung detaillierte Einblicke in den TLS-Verkehr zu ermöglichen, zum Beispiel zur Ermittlung des Umfangs des verschlüsselten Datenverkehrs sowie der TLS/SSL-Versionen und Cipher-Suites.

Mit PAN-OS lässt sich über integrierte Protokolldateien zur Fehlerbehebung die Verwendung veralteter TLS-Protokolle, unsicherer Cipher-Suites und falsch konfigurierter Zertifikate verhindern, um Risiken zu minimieren und die unternehmensweite Entschlüsselung zu vereinfachen. Und zur Erfüllung der Compliance- und Datenschutzvorgaben können Netzwerksicherheitsadministratoren unter PAN-OS die Entschlüsselung für URL-Kategorien, Quell- und Zielzonen, Adressen, Benutzer, Benutzergruppen, Geräte und Ports aktivieren oder deaktivieren.

Weitere Informationen zur Absicherung des verschlüsselten Datenverkehrs finden Sie im Whitepaper Entschlüsselung: Warum, wo, wie?.

ML-gestützte Next-Generation Firewall

Die PA-400 Series mit PAN-OS ist eine ML-gestützte NGFW, die maschinelles Lernen (ML) nutzt, um eine signaturlose Inline-Abwehr dateibasierter Angriffe zu bieten und bisher unbekannte Phishingversuche zu erkennen und sofort zu stoppen. Mithilfe in der Cloud bereitgestellter, nativ integrierter Services und cloudbasierter ML-Prozesse werden Signaturen und Anweisungen in Echtzeit an die NGFW gesendet und Verhaltensanalysen durchgeführt, um IoT-Geräte zu erkennen und Richtlinienempfehlungen abzugeben. Außerdem werden Richtlinienempfehlungen im Allgemeinen automatisiert, sodass Unternehmen Zeit sparen und das Risiko von Bedienfehlern reduzieren können.

Eine umfassende Beschreibung der PAN-OS-Funktionen finden Sie im Datenblatt zu den Firewall-funktionen.

Erkennung und Abwehr komplexer Bedrohungen mit Cloud-Delivered Security Services

Moderne ausgeklügelte Cyberattacken können innerhalb von 30 Minuten auf bis zu 45.000 Varianten anwachsen. Dabei werden mehrere Bedrohungsvektoren und komplexe Techniken eingesetzt, um Schadcode einzuschleusen. Herkömmliche Punktlösungen verursachen Sicherheitslücken in Unternehmen, erhöhen den Arbeitsaufwand von Sicherheitsteams und beeinträchtigen die Produktivität durch inkonsistenten Zugriff und unzureichende Transparenz.

Unsere Cloud-Delivered Security Services dagegen können nahtlos in unsere branchenführenden NGFWs integriert werden und nutzen unser Netzwerk aus 80.000 Kunden, um Threat Intelligence sofort zu koordinieren und Schutz vor allen Bedrohungen und Bedrohungsvektoren zu bieten. Auf diese Weise lassen sich Sicherheitslücken an allen Standorten schließen und die Vorteile erstklassiger Sicherheitsfunktionen ausschöpfen, um auch vor den komplexesten und am besten getarnten Bedrohungen geschützt zu sein. Dabei werden alle nötigen Informationen konsistent über eine zentrale Plattform bereitgestellt.

- **Threat Prevention** – bietet mehr Sicherheit als ein herkömmliches IPS (Intrusion Prevention System), da alle bekannten Bedrohungen für den gesamten Datenverkehr in einem Durchlauf (Single Pass) und ohne Leistungseinbußen abgewehrt werden.
- **Advanced URL Filtering** – sorgt für erstklassigen Schutz vor webbasierten Bedrohungen und eine Steigerung der betrieblichen Effizienz dank branchenweit erster Echtzeit-Präventionslösung für Webangriffe sowie branchenführender Phishingabwehr.
- **WildFire®** – schützt Dateien durch die automatische Erkennung und Abwehr unbekannter Malware mit branchenführenden cloudbasierten Analysen und Threat Intelligence von mehr als 42.000 Kunden.
- **DNS Security** – nutzt ML, um Bedrohungen über das DNS in Echtzeit zu erkennen und abzuwehren. Sicherheitsteams erhalten so die Kontextinformationen, die sie zur Ausarbeitung von Richtlinien und zur schnellen und wirkungsvollen Abwehr von Bedrohungen benötigen.
- **IoT Security** – bietet die umfassendste IoT-Sicherheitslösung der Branche für einen detaillierten Überblick, eine effektive Abwehr und eine zuverlässige Richtliniendurchsetzung – alles auf einer einzigen ML-gestützten Plattform.
- **Enterprise DLP** – ist die branchenweit erste cloudbasierte DLP-Lösung für Unternehmen, die sensible Daten über alle Netzwerke, Clouds und Benutzer hinweg konsistent schützt.
- **SaaS Security** – stellt integrierte SaaS-Sicherheitsfunktionen bereit, mit denen Sie neue SaaS-Anwendungen erkennen und sichern, Daten schützen und Zero-Day-Bedrohungen abwehren können – und das zu den niedrigsten Gesamtbetriebskosten.

PA-400 Series für verteilte Unternehmen

Die ML-gestützten NGFWs der PA-400 Series wurden speziell zum Schutz von Zweigniederlassungen und unabhängigen kleinen Standorten entwickelt. Von ihnen profitieren sowohl kleine und mittelständische Unternehmen mit wenigen Filialen als auch große verteilte Unternehmen (wie Banken, Einzelhändler und Gesundheitsdienstleister) mit Hunderten oder sogar Tausenden Filialen.

Verhinderung von Datenlecks und niedrige Gesamtbetriebskosten

Herausforderung

Kleine Zweigstellen sind ebenso wie ein Hauptsitz oder Rechenzentrum auf zuverlässige Sicherheitslösungen mit Cloud-Delivered Security Services angewiesen, um ihre Netzwerke effektiv vor komplexen Bedrohungen zu schützen. Sie benötigen moderne, leistungsstarke NGFWs vor Ort, die bekannte und unbekannte Bedrohungen mithilfe von ML inline abwehren, Sicherheitsservices zum Schutz des Netzwerks bereitstellen und den Datenverkehr zur rechtzeitigen Aufdeckung von Bedrohungen entschlüsseln.

Lösung

Die ML-gestützten NGFWs der PA-400 Series verfügen über sämtliche Funktionen von PAN-OS und unterstützen somit alle Cloud-Delivered Security Services zum Schutz vor komplexen Bedrohungen. Außerdem sind sie leistungsstark genug für die Entschlüsselung.

Da die Services direkt auf der PA-400 Series bereitgestellt werden, sind alle Netzwerksicherheitsfunktionen in einem Gerät konsolidiert und keine separaten UTM-, IPS- oder Web-/URL-Filtering-Appliances notwendig. Und dank unserer Single-Pass-Architektur arbeitet die PA-400 Series auch bei voller Auslastung ohne Einschränkungen. Durch die Konsolidierung der Sicherheitsservices bei gleichbleibender Leistung gehören die Gesamtbetriebskosten für die PA-400 Series für Netzwerksicherheit in Filialen zu den niedrigsten der Branche.

Um die Anschaffung und Einführung der Cloud-Delivered Security Services möglichst schnell und einfach zu gestalten, bieten wir spezielle Subscriptions an. Für die PA-400 Series sind zwei Subscriptions verfügbar: Professional und Enterprise.

Weitere Informationen zu den PA-400 Subscriptions finden Sie hier.

Tabelle 1: Cloud-Delivered Security Services für die PA-400 Series

Cloud-Delivered Security Services	Professional Subscription	Enterprise Subscription
Threat Prevention (TP)	√	√
WildFire (WF)	√	√
Advanced URL Filtering (AURL-F)	√	√
DNS Security	√	√
SD-WAN		√
IoT Security (DRDL)		√
SaaS Security Inline		√

Segmentierung zum Schutz kritischer Daten, Anwendungen und Ressourcen

Herausforderung

Um Unternehmensnetzwerke vor neuartigen Angriffen zu schützen, müssen Zweigstellen den lokalen Datenverkehr segmentieren und die unterschiedlichen Netzwerkbereiche isolieren. Durch die Segmentierung wird sichergestellt, dass bei einem Angriff auf einen Teil des Netzwerks keine anderen wichtigen Bereiche kompromittiert werden.

Lösung

Die PA-400 Series verfügt über bis zu acht 10/100/1000-RJ45-Ports, die zur Segmentierung des lokalen Datenverkehrs in Filialen genutzt werden können, also um wichtige Netzwerkbereiche voneinander abzugrenzen.

Die technische Dokumentation zum Schutz des Perimeters und zur Segmentierung finden Sie unter Perimeter Security for the Campus and Branch (Schutz des Perimeters für Campusnetzwerke und Filialen).

Flexible Bereitstellung und zentrales Management

Herausforderung

In der Regel gibt es in verteilten Unternehmen ein zentrales Netzwerksicherheits- bzw. IT-Team, das für die Sicherheit im gesamten Unternehmen zuständig ist. Für ein effizientes Sicherheitsmanagement müssen solche Teams alle NGFWs remote bereitstellen und anschließend zentral verwalten können. Ebenso wichtig ist die Möglichkeit, Richtlinien zu konfigurieren und einen Überblick über den Netzwerkverkehr und die Bedrohungen zu behalten.

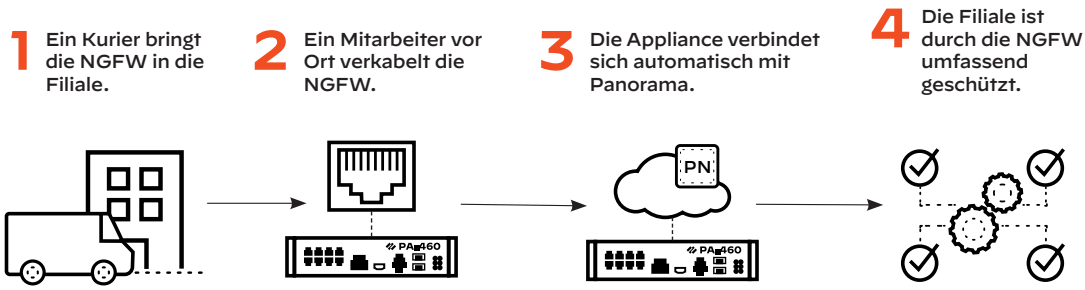


Abbildung 1: Einfacheres Onboarding von Filialen dank Zero Touch Provisioning

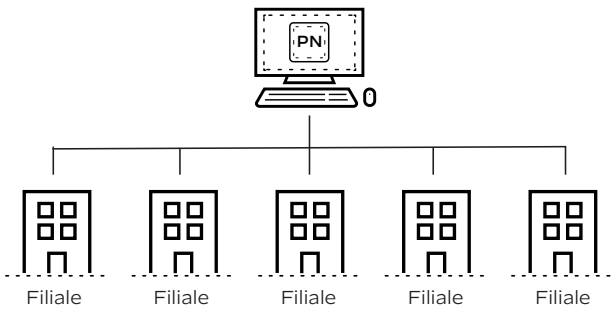
Lösung

Zero Touch Provisioning (ZTP) wird standardmäßig auf allen Appliances der PA-400 Series unterstützt und muss zentral über Panorama verwaltet werden. ZTP soll den Onboardingprozess für neue Firewalls auf dem Panorama-Server straffen und automatisieren. Mit ZTP lässt sich die Ersteinrichtung von Firewalls vereinfachen, da Unternehmen diese direkt an die Filialen liefern können. Nachdem die Firewall mit dem Palo Alto Networks ZTP-Service verbunden wurde, wird sie automatisch dem Panorama-Server hinzugefügt. Da IT-Administratoren die neuen Firewalls in den Filialen nicht manuell installieren müssen, sparen Unternehmen Zeit und Ressourcen. Nach dem Onboardingprozess können ZTP und die Firewalls über Panorama konfiguriert und verwaltet werden.

Zentrales Management mit Panorama

Panorama ermöglicht die zentrale Verwaltung, Konfiguration und Überwachung mehrerer verteilter NGFWs der PA-400 Series (unabhängig von Standort oder Umfang) in einer einheitlichen Benutzeroberfläche. Es vereinfacht die gemeinsame Nutzung von Konfigurationen durch Vorlagen und Gerätegruppen und skaliert die Protokollerfassung nach Bedarf. So können Tausende Firewalls in einer zentralen Konsole verwaltet und konfiguriert werden.

Weitere Informationen erhalten Sie im Datenblatt zu Panorama.



1. Vereinfachte Bereitstellung einer großen Anzahl von Firewalls mit Zero Touch Provisioning
2. Zentrale Verwaltung und Konfiguration der Netzwerksicherheit für Filialen
3. Durchsetzung einheitlicher Richtlinien im gesamten verteilten Unternehmen

Abbildung 2: Zentrales Management mit Panorama für verteilte Unternehmen

Minimaler Wartungsaufwand dank ausfallsicherem Design

Herausforderung

Die Filialen eines verteilten Unternehmens stellen spezielle Anforderungen an die IT-Ausstattung, einschließlich Firewalls. Da in den meisten Zweigstellen kein IT-Experte beschäftigt wird, ist es wichtig, dass auch Mitarbeiter ohne Technikkenntnisse die vorkonfigurierte Firewall schnell und einfach anschließen können. Die Firewalls müssen ausfallsicher sein, da andernfalls die Gefahr besteht, dass Wartungsarbeiten an externen Standorten die Gesamtbetriebskosten eines großen Unternehmens in die Höhe treiben. Wenn es sich bei den Filialen um kleine Zweigstellen mit Kundenkontakt handelt, muss der Betrieb zudem leise sein. Nicht immer sind dort spezielle Racks oder Schränke verfügbar, sodass es weiterhin möglich sein sollte, die Appliances auf andere Weise zu montieren.

Lösung

Alle NGFWs der PA-400 Series werden ohne Lüfter gekühlt und bieten daher einen nahezu lautlosen Betrieb für kleine Büros und Läden mit Kundenverkehr. Weil sie keine beweglichen Teile umfassen, sind die NFGWs zudem ausfallsicher. PA-460, PA-450 und PA-440 verfügen zur Vermeidung von Ausfällen zusätzlich über eine (optionale) duale redundante Stromversorgung. Die Appliances der PA-400 Series haben einen kompakten Formfaktor, sind leise im Betrieb und bieten diverse Montageoptionen (Desktop, Rack oder Wand) für verschiedene Einsatzbereiche.

Fazit

Für zuverlässige Sicherheit in kleinen Büros und Filialen sowie an unabhängigen Unternehmensstandorten benötigen diese Zugriff auf dieselben Tools, die Rechenzentren und großen Campusnetzwerken zur Verfügung stehen – und zwar in vollem Funktionsumfang. Denn die Bedrohungen bleiben gleich. Mit den neuen ML-gestützten NGFWs der PA-400 Series von Palo Alto Networks stehen Netzwerksicherheitsadministratoren verschiedene kostengünstige Optionen für kompromisslose Sicherheitsmaßnahmen zur Verfügung.

Sie können PAN-OS mit denselben Funktionen und Cloud-Delivered Security Services nutzen, die auch Premium-NGFWs bieten, und daher auf zuverlässige Sicherheit an allen Standorten vertrauen. Unsere Cloud-Delivered Security Services für ML-gestützte NGFWs der PA-400 Series sind jetzt als übersichtliche und anwenderfreundliche Subscriptions verfügbar. Und für Unternehmen mit mehreren Standorten können Netzwerkadministratoren ganz einfach Panorama für die zentrale Verwaltung nutzen und so von Zero Touch Provisioning profitieren.

Sie haben Interesse an unseren ML-gestützten Next-Generation Firewalls? Dann registrieren Sie sich doch gleich für einen Ultimate Test Drive.

Über Palo Alto Networks

Palo Alto Networks ist ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, das mit seinen bahnbrechenden Technologien die Weichen für eine cloudorientierte Zukunft stellt und die Arbeitsweise von Unternehmen und ihren Mitarbeitern von Grund auf modernisiert. Wir haben uns das Ziel gesetzt, zum bevorzugten Cybersicherheitspartner für Unternehmen zu werden und gemeinsam mit ihnen unseren digitalen Lebensstil zu schützen. Dazu gehen wir durch kontinuierliche Innovation die größten Herausforderungen rund um die Cybersicherheit an, mit denen Unternehmen derzeit konfrontiert sind. Dabei kommen die neuesten Forschungsergebnisse aus den Bereichen künstliche Intelligenz, Analyse, Automatisierung und Orchestrierung zum Einsatz. Mit einer integrierten Plattform und einem wachsenden Partnernetzwerk schützt Palo Alto Networks die Clouds, Netzwerke und Mobilgeräte Zehntausender Unternehmen und arbeitet unermüdlich für eine Welt, in der jeder Tag ein bisschen sicherer ist als der Tag zuvor. Weitere Informationen erhalten Sie unter www.paloaltonetworks.de.

Oval Tower, De Entrée 99–197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de

parent_wp_pa-400-for-distributed-enterprises_081221