VM-SERIES NEXT-GENERATION FIREWALL

Unternehmen erweitern ihre Cloud- und -Virtualisierungsinitiativen weltweit über konventionelle Rechenzentrums- und Cloud-Bereitstellungen hinaus. Die neuen Initiativen umfassen Sicherheitslösungen wie etwa eine NFV-Komponente oder eine umfassendere Multi-Tenancy-Lösung.

Die virtualisierte VM-Series Next-Generation Firewall

Unterstützt eine Vielzahl von Cloud- und Virtualisierungsumgebungen, einschließlich VMware® NSX™, ESXi™, vCloud® Air™, Citrix® Netscaler® SDX™, Microsoft® Azure® und Hyper-V®, Amazon® Web Services, Google® Cloud und KVM mit optionalem Support für das OpenStack®-Plug-In.

- Identifizierung und Steuerung von Anwendungen innerhalb Ihrer Cloud- oder Virtualisierungsumgebung, Zugriffsbegrenzung basierend auf Benutzern und Eliminierung bekannter und unbekannter Bedrohungen
- Isolierung und Segmentierung wichtiger Anwendungen und Daten unter Verwendung von Zero Trust-Prinzipien
- Optimierte Workflow-Automatisierung, um mit den Änderungen innerhalb Ihrer Cloud Schritt zu halten
- Zentrale Richtlinienverwaltung auf physischen und virtualisierten Firewalls für einen konsistenten Sicherheitsstatus

Herausforderungen hinsichtlich der Cloud-Sicherheit: öffentlich, privat und hybrid

Sie profitieren durch die Implementierung von Cloud-Technologien von gesteigerter Flexibilität und Skalierbarkeit und können schneller auf sich ändernde Geschäftsbedingungen reagieren. Neben diesen Vorteilen gelten jedoch auch ähnliche sicherheitstechnische Herausforderungen wie in einem lokalen Rechenzentrum. Hierzu zählen ein Mangel an Anwendungstransparenz und -steuerung, die Unfähigkeit, Cyberattacken abzuwehren sowie schwerfällige Prozesse für die Richtlinienaktualisierung, die zu Verzögerungen zwischen der Arbeitslastbereitstellung und der Aktualisierung der Sicherheitsrichtlinien führen. Um weiterhin Erfolge zu erzielen, muss die Cloud-Sicherheitslösung eines Unternehmens die folgenden Anforderungen erfüllen:

- Identifizierung und Steuerung von Anwendungsarbeitslasten unabhängig vom verwendeten Port
- Steuerung der Nutzerrechte für Anwendungen sowie Zugriffsgewährung basierend auf Anforderungen und Anmeldedaten
- Ausdehnung konsistenter Sicherheitsrichtlinien vom Netzwerk auf die Cloud und Remote-Geräte
- Vermeidung der Einschleusung und lateralen bzw. Ost-West-Bewegung von Malware in der Cloud
- Vereinfachung des Managements und Minimierung von Verzögerungen durch Aktualisierungen von Sicherheitsrichtlinien bei Änderungen der virtuellen Arbeitslasten

Die VM-Series unterstützt die gleichen Funktionen (Next-Generation Firewall und Advanced Threat Prevention), die auch in unseren Sicherheitsanwendungen verfügbar sind. Somit können Sie Ihre Anwendungen und Daten vom Netzwerk bis zur Cloud schützen.

Einführung der VM-Series

Um Kunden bei der Verwaltung mehrerer Clouds und den wachsenden Leistungsanforderungen zu unterstützen, haben wir die VM-Series optimiert und erweitert. Sie bietet jetzt auf fünf Modellen einen branchenführenden App-ID-fähigen Firewall-Durchsatz bis 16 Gbit/s. Kunden können ihre Cloud- und Virtualisierungsinitiativen mit den gleichen Sicherheitsfunktionen wie denen ihrer physischen Netzwerke schützen. Dies ermöglicht einen konsistenten Cloud- und standortübergreifenden Sicherheitsstatus. Die VM-Series-Modelle umfassen:

- **VM-50**: Minimaler Ressourcenverbrauch, Unterstützung von CPU-Überbelegung sowie App-ID-fähiger Firewall-Durchsatz bis 200 Mbit/s für virtuelle Niederlassungen, Installationen beim Kunden vor Ort und hochdichte Multi-Tenant-Umgebungen
- **VM-100 und VM-300**: Für den App-ID-fähigen Durchsatz von 2 Gbit/s bzw. 4 Gbit/s für hybride Clouds, Segmentierungen und Internetgateways optimiert
- **VM-500 und VM-700**: Branchenführender App-ID-fähiger Firewall-Durchsatz von 8 Gbit/s bzw. 16 Gbit/s, Bereitstellung als NFV-Sicherheitskomponenten in vollständig virtualisierten Rechenzentrums- und Dienstanbieterumgebungen

Dank der vielfältigen Optionen und der gesteigerten Leistung können Sie Ihre Anwendungen und Daten durch einen konsistenten Sicherheitsstatus im Netzwerk und in der Cloud schützen.

Die VM-Series: Schutz für alle Clouds

Die VM-Series ermöglicht den Wechsel zu einem Cloud-First-Bereitstellungsmodell mit verbesserter Unterstützung für Ihr Geschäft. Durch Verwendung der VM-Series in Ihrer Cloud werden die vorhandenen Anwendungen und Daten mit demselben Sicherheitsstatus geschützt, der gegebenenfalls auch in Ihrem physischen Netzwerk gilt.

Die VM-Series analysiert nativ den gesamten Datenverkehr in einer Single-Pass-Architektur, um die Anwendungsidentität, den Inhalt und den Benutzer zu ermitteln. Dies sind die Kernelemente Ihrer Sicherheitsleitlinie, die auch für die Transparenz, das Reporting und die Vorfalluntersuchung genutzt werden.

Anwendungstransparenz für fundiertere Sicherheitsentscheidungen

Die VM-Series bietet über mehrere Ports hinweg Anwendungstransparenz. Sie erhalten dadurch relevanter Informationen über Ihre Cloud-Umgebung und können fundierte Richtlinienentscheidungen treffen.

Segmentierung/Positivliste für Datensicherheit und Compliance

Moderne Cyberbedrohungen gelangen in der Regel über eine einzelne Workstation oder einen einzelnen Benutzer in Ihr Netzwerk. Dadurch, dass sie sich anschließend lateral innerhalb des Netzwerks bewegen, gefährden sie Ihre unternehmenskritischen Anwendungen und Daten ungeachtet des Standorts. Sie können die Kommunikation von Anwendungen über verschiedene Subnetze hinweg mithilfe von Richtlinien für die Segmentierung und Positivlisten steuern, um die immer strengeren Sicherheitsrichtlinien und gesetzlichen Auflagen zu erfüllen. Indem Sie Ihre Segmentierungsrichtlinien durch Cloud-basierte Threat Prevention- und WildFire®-Bedrohungsanalysedienste ergänzen, können Sie sowohl bekannte als auch unbekannte Bedrohungen blockieren und verhindern, dass sich diese lateral zwischen Arbeitslasten bewegen.

Benutzerbasierte Richtlinien optimieren den Sicherheitsstatus

Die Integration in eine größere Anzahl an Benutzer-Repositories wie z. B. Microsoft® Active Directory®, LDAP und Microsoft Exchange führt die Benutzeridentität als Richtlinienelement ein und ergänzt die Anwendungspositivliste somit um eine weitere Zugriffskontrollenkomponente. Mithilfe von benutzerdefinierten Richtlinien können Sie Zugriff auf kritische Anwendungen und Daten basierend auf den Anmeldeinformationen und dem jeweiligen Bedarf der Benutzer erteilen. Wird die VM-Series in Verbindung mit der GlobalProtect™-Netzwerksicherheit für Endpunkte bereitgestellt, können Sie Ihre unternehmensweiten Sicherheitsrichtlinien standortunabhängig auf mobile Geräte und Benutzer ausdehnen.

Abwehr fortschrittlicher Angriffe auf Anwendungsebene

Angreifer können ähnlich wie zahlreiche Anwendungen beliebige Ports nutzen, wodurch herkömmliche Schutzmechanismen wirkungslos werden. Die VM-Series bietet Ihnen die Möglichkeit, mithilfe von Threat Prevention und WildFire™ anwendungsspezifische Richtlinien zur Abwehr von Bedrohungen anzuwenden, um zu verhindern, dass Exploits, Malware und bislang unbekannte Bedrohungen Ihre Cloud infizieren.

Zentralisierte Verwaltung sorgt für Richtlinienkonsistenz

Neben Ihren physischen Sicherheits-Appliances können Sie mit dem Panorama™-Netzwerksicherheitsmanagement Ihre VM-Series-Bereitstellungen in mehreren Cloud-Bereitstellungen verwalten. Sie gewährleisten dadurch die Konsistenz und den Zusammenhang Ihrer Richtlinien. Dank umfangreicher zentralisierter Protokollierungs- und Reporting-Funktionen erhalten Sie einen transparenten Einblick in virtualisierte Anwendungen, Benutzer und Inhalte.

Automatisierte Sicherheitsbereitstellung und Richtlinienaktualisierungen

Die VM-Series enthält verschiedene Managementfunktionen, mit deren Hilfe Sie Ihre Cloud-First-Entwicklungsprojekte sicherer gestalten können.

- Bootstrapping stellt automatisch eine Firewall mit einer funktionierenden Konfiguration einschließlich Lizenzen und Abonnements bereit und registriert sich automatisch bei Panorama.
- Zur Automatisierung von Richtlinienaktualisierungen bei sich ändernden Arbeitslasten stehen der VM-Series eine vollständig dokumentierte XML API sowie Dynamic Address Groups (dynamische Adressgruppen, DAGs) zur Verfügung, um externe Daten in Form von Tags zu verarbeiten und somit dynamische Richtlinienaktualisierungen zu ermöglichen.
- Erstellen und betreiben Sie sichere Cloud-Bereitstellungen, einschließlich der Integration in native Cloud-Dienste wie Amazon Lambda und Azure sowie in Funktionen und Automatisieriungs-Tools wie Ansible® und Terraform® und viele mehr.

Zusammen mit neuen Anwendungen und Arbeitslasten lassen sich gleichzeitig auch innovative Sicherheitsfunktionen auf automatisierte Weise bereitstellen. Sie gewährleisten dadurch, dass Ihr Sicherheitsstatus mit Ihren Geschäftsabläufen Schritt hält.

Cloud-orientierte Skalierbarkeit und Verfügbarkeit

Skalierbarkeits- und Verfügbarkeitsanforderungen müssen in einer Cloud- oder Virtualisierungsumgebung mit einem konventionellen Rechenzentrum oder einem Cloud-orientierten Ansatz bewerkstelligt werden. Bei einem Cloud-orientierten Ansatz werden die Skalierbarkeits- und Verfügbarkeitsanforderungen durch die vorhandenen Cloud-Infrastrukturdienste erfüllt. Durch die Nutzung bestehender Anwendungsgateways und Loadbalancer-Dienste auf AWS® und Azure kann die VM-Series die für geschäftskritische Anwendungen erforderliche Skalierbarkeit und Verfügbarkeit unterstützen.

Flexibilität bei der Bereitstellung

Die VM-Series kann in einer Vielzahl von Cloud- und Virtualisierungsumgebungen bereitgestellt werden.

VM-Series für VMware NSX

Die VM-Series für NSX ist eine eng integrierte Lösung. Sie vereint die VM-Series Next-Generation Firewall, Panorama und VMware NSX zu einem Software-Defined Data Center (softwaredefiniertes Rechenzentrum, SDDC). Erfahren Sie mehr über die **VM-Series für NSX**.

VM-Series für VMware ESXi

Die VM-Series für ESXi-Server eignet sich optimal für Netzwerke, in denen sich durch Virtualisierung die Bereitstellung vereinfacht und die Flexibilität erhöht. Zu den gängigen Bereitstellungsszenarien zählen Umgebungen mit begrenztem Platzangebot sowie entlegene Standorte, an die sich Hardware nur schwer versenden lässt. Erfahren Sie mehr über die **VM-Series für ESXi**.

VM-Series für Microsoft Hyper-V

Die VM-Series für Hyper-V ermöglicht die sichere Bereitstellung von Anwendungen innerhalb Ihres Rechenzentrums mit Hyper-V. Erfahren Sie mehr über die **VM-Series für Hyper-V**.

VM-Series für Microsoft Azure

Die VM-Series für Azure ermöglicht die sichere Erweiterung Ihrer auf dem Microsoft-Stack (Windows Server, SQL Server, .NET Framework) aufgebauten Anwendungen in die öffentliche Cloud. Erfahren Sie mehr über die **VM-Series für Azure**.

VM-Series für Amazon Web Services

Mit der VM-Series für AWS können Sie Ihre AWS-Bereitstellung mithilfe unserer Next-Generation Firewall und sowie unseren Advanced Threat Prevention-Funktionen schützen. Erfahren Sie mehr über die **VM-Series für AWS**.

VM-Series für Citrix SDX

Die VM-Series für Citrix NetScaler SDX bietet die Konsolidierung von Sicherheits- und Application Delivery Controller-Funktionen auf einer einzigen Plattform. Dies ermöglicht die Bereitstellung einer umfassenden Sammlung Cloud-basierter Dienste, die die Verfügbarkeit, Sicherheit und Leistung von Anwendungen erhöhen. Erfahren Sie mehr über die **VM-Series für Citrix SDX**.

VM-Series für KVM

Mit der VM-Series auf einer Kernel Virtual Machine können sowohl Dienstanbieter als auch Unternehmen ihren Linux-basierten Virtualisierungen (CentOS/RHEL und Ubuntu®) und Cloud-basierten Initiativen Next-Generation Firewalls und Advanced Threat Prevention-Funktionen hinzufügen. Erfahren Sie mehr über die **VM-Series für KVM**.

VM-Series für VMware vCloud Air

Die VM-Series für vCloud Air bietet Ihnen die Möglichkeit, Ihre VMware-basierte öffentliche Cloud mit denselben Richtlinien für die sichere Anwendungsaktivierung zu schützen, die Sie auch für Ihre ESXi-basierte private Cloud verwenden. Erfahren Sie mehr über die **VM-Series für vCloud Air**.

VM-Series für die Google Cloud Platform

Mit der VM-Series für die Google Cloud Platform können Sie die VM-Series in Ihren Anwendungsentwicklungsprozess einbetten. Sie schützen dadurch Ihre Anwendungen und Daten und reduzieren Geschäftsunterbrechungen. Erfahren Sie mehr über die **VM-Series für die Google Cloud Platform**.

VM-Series für Cisco ACI

Mit der VM-Series für Cisco® ACI® lassen sich Palo Alto Networks Next-Generation Firewalls automatisch in ACI-Bereitstellungen integrieren. Erstellen Sie für einen umfassenden Schutz dynamische Sicherheitsleitlinien, die auf ACI-Attributen basieren, wie etwa Endpunktgruppen. Erfahren Sie mehr über die **VM-Series für Cisco ACI**.

VM-Series für OpenStack

Mit der VM-Series für OpenStack® können Sie Firewalldienste automatisch in Mirantis® OpenStack-Bereitstellungen integrieren. Die HEAT-Vorlagen für die VM-Series verwenden Juniper® Contrail® als Netzwerkdienst und überwachen die OpenStack-Telemetrie zur automatischen Skalierung der Sicherheitsfunktionen. Erfahren Sie mehr über die **VM-Series für OpenStack**.

3000 Tannery Way
Santa Clara, CA 95054
Zentrale: +1/408/75 34 000
Vertrieb: +1/866/32 04 788
Support: +1/866/89 89 087
www.paloaltonetworks.com

vm-series-next-generation-firewall-ds-012218