Forcepoint Next Generation Firewall mit Microsoft Azure

Die sicherste und effizienteste Enterprise-Firewall – zentral verwaltet, immer aktiv und kompromisslos

Herausforderung

- Unternehmen und Organisationen müssen dasselbe Sicherheitsniveau in Cloud- und Hybrid-Umgebungen einhalten wie in den traditionellen lokalen Infrastrukturen.
- Es kann teuer und technisch herausfordernd sein, eine sichere Cloud- oder Hybrid-Infrastruktur zu erstellen und zu warten.
- Die Einhaltung gesetzlicher Vorschriften kann sich schwierig gestalten und ein technisches Problem darstellen.

Lösung

- Die softwareorientierte Lösung von Forcepoint Next Generation Firewall wurde allein dafür konzipiert, maximale Sicherheit mit minimalen Kosten und minimaler Komplexität bereitzustellen.
- Mit Forcepoint Security Management Center (SMC) können Teams Tausende von Firewalls verwalten, Prozesse optimieren und unübertroffene Transparenz mit granularen Kontrollen nutzen.
- Unsere Lösung ermöglicht optimierte Initiativen zur Vorschrifteneinhaltung in virtuellen und physischen Netzwerken und einfachen Zugriff auf Prüfberichte.

Ergebnis

- Maximale Cloud- und Hybrid-Sicherheit mit minimaler Komplexität
- Beschleunigte Reaktionen auf Vorfälle
- Optimierte Einhaltung gesetzlicher Vorschriften, Umsetzung und Verwaltung
- Geringere Gesamtbetriebskosten (TCO) für Netzwerkinfrastruktur und -sicherheit

Forcepoint Next Generation Firewall verbindet und schützt anspruchsvolle, verteilte Unternehmensnetzwerke. Flexible Zero-Touch-Installation und ein Zero-Trust-Ansatz für die Netzwerksicherheit bieten die Effizienz, Zuverlässigkeit und hohe Sicherheit, die Sie für die Verteidigung Ihres Netzwerkrands benötigen.

Die Netzwerksicherheitslösungen von Forcepoint werden von Tausenden von Kunden weltweit geschätzt und stehen über den Microsoft Azure Marketplace zur Verfügung. Sie ermöglichen es Unternehmen und Organisationen, kritische Probleme effizient und ökonomisch anzugehen und sich gegen Angriffe zu wehren.

Forcepoint-Sicherheit für öffentliche Cloud-Umgebungen

Durch Cloud-basierte Dienste und virtuelle Bereitstellungen werden Unternehmen aller Arten und Größen umgeformt. Traditionelle lokal installierte Hardware verschwindet rapide, weil Unternehmen mehr Effizienz, Agilität und Kostenkontrolle ohne die Belastung durch Wartung und Mehraufwand benötigen. Damit die Kunden weiterhin wettbewerbsfähig bleiben, hat Forcepoint die Netzwerksicherheitslösungen strategisch softwareorientiert konzipiert, damit Sie diese beim Wechsel in die Cloud beibehalten können. Die weit verbreitete Einführung von Cloud-Architekturen stellt Sicherheitsexperten und IT-Verantwortliche vor die zusätzliche Aufgabe, sicherzustellen, diese neuen Umgebungen genauso zu schützen wie ihre physischen Vorgänger.

Die softwareorientierten Lösungen von Forcepoint Next Generation Firewall wurde allein dafür konzipiert, maximale Sicherheit mit minimalen Kosten und minimaler Komplexität bereitzustellen. Unser Security Management Center (SMC) bietet eine einheitliche Plattform, die Ihnen unübertroffene Transparenz, Kontrolle und konsistente Durchsetzung von Richtlinien bereitstellt und Sie dabei unterstützt, die Einhaltung von Vorschriften in physischen, virtuellen und Cloud-basierten Umgebungen sicherzustellen.

Cloud-Sicherheit von Microsoft Azure

Zur Sicherung von Cloud-Umgebungen bietet Forcepoint die führende Firewall-Technologie der nächsten Generation für Azure – mit erprobter Skalierbarkeit, operationaler Effizienz und starker Sicherheit. Erweitern Sie einfach und sicher das Netzwerk Ihrer Organisation – von Rechenzentren und dem Netzwerkrand bis zu Ihren Zweigstellen und Remote-Standorten – über ein sicheres VPN-Gateway (Virtual Private Network) auf Ihre Azure-Cloud-Umgebung. Unsere zentralisierte Verwaltung ermöglicht es Ihnen, Richtlinien zügig und konsistent für alle Systeme zu erstellen und anzuwenden. Sie können schnell feststellen, was sowohl in Ihrer Azure-Umgebung als auch in Ihrem physischen Netzwerk geschieht.

Kunden, die zu Forcepoint Next Generation Firewall wechseln, berichten von einem Rückgang der Cyber-Angriffe um 86 %, einer um 53 % geringeren zeitlichen Belastung der IT-Abteilung und einem Rückgang der geplanten Wartungsarbeiten um 70 %.

Maximale Sicherheit, minimale Komplexität

Die softwareorientierte Architektur der Sicherheitslösungen von Forcepoint, wie erweiterter Schutz vor Bedrohungen, detaillierte Paketüberprüfung und Kontrolle auf Anwendungsebene, sind für eine einfache, flexible Bereitstellung lokal, virtuell oder in der Cloud konzipiert. Granulare Benutzer-, Anwendungs- und Protokollkontrollen ermöglichen es Ihrem Sicherheitsteam, mit Hilfe von automatisierten Prozessen, die Komplexität und die Zeit, die für alltägliche Sicherheitsmaßnahmen aufgewendet wurde, zu reduzieren. Die umfassende und integrierte mehrschichtige Verteidigung von Forcepoint kann auf die spezifischen Anforderungen jeder Person, jedes Ortes oder jeder Anlage zugeschnitten werden; dazu gehören einzelne oder mehrere Firewalls, VPN, IPS und URL-Filterungsschutz. Unsere umfassende Firewall der nächsten Generation bietet alle vorhandenen Funktionen einer modernen hardwarebasierten Appliance, wie zustandsabhängige Inspektion, granulare Richtlinien- und Zugriffskontrolle sowie redundante ISP-Verbindungen – allerdings ohne Box.

Transparenz und Kontrolle in Echtzeit

Forcepoint Next Generation Firewall bietet vollständige Transparenz und Kontrolle über den Datenverkehr in virtuellen und Cloud-Umgebungen, die herkömmliche Managementkonsolen nicht bieten können. Unser renommiertes SMC bietet eine schnelle Berichterstellung sowie automatische Ausfallsicherung, um Administratoren zu alarmieren, wenn ein System auszufallen droht, und um automatisierte Entscheidungen auf der Grundlage vorkonfigurierter Regeln zu treffen, damit eine Unterbrechung der Nutzung verhindert wird. Verwalten Sie eine beliebige Anzahl oder Kombination von physischen oder virtuellen Forcepoint-Geräten oder -Clustern sowie softwarebasierte Versionen, die auf Standard-x86-Hardware ausgeführt werden. Das SMC erhöht auch die virtuelle Systemsicherheit mit einem ganzheitlichen Überwachungs-Dashboard mit umfassender Anwendungstransparenz und granularer Kontrolle.

Vereinfachte Einhaltung von Vorschriften

Die Einhaltung der neuesten gesetzlichen Anforderungen wie PCI DSS, HIPAA, Sarbanes-Oxley und FISMA in der physischen Welt ist schwierig, aber die Einhaltung von Vorschriften im digitalen Bereich ist eine noch größere Herausforderung. Die traditionellen Kontrollen bei den Anwendungen sind in einer virtuellen Umgebung nicht gegeben. Dies macht es fast unmöglich, festzustellen, welche Informationen von wem und wann abgerufen wurden, und wird bei einer Prüfung wahrscheinlich zu Sicherheitswarnungen führen. Das Forcepoint SMC bietet Ihnen die Funktionen für Überwachung, Analyse und Berichterstellung, die erforderlich sind, um die Einhaltung von Vorschriften in physischen und virtuellen Netzwerken sicherzustellen. Es sammelt umfassende Daten für alle Netzwerkereignisse und stellt sie in klaren und verständlichen Prüfprotokollen zusammen. Das SMC listet ferner Sicherheitseinstellungen auf, protokolliert Systemänderungen und bietet die von Ihnen benötigten genauen Prüfberichte – alles mit nur einem Klick auf eine Schaltfläche.

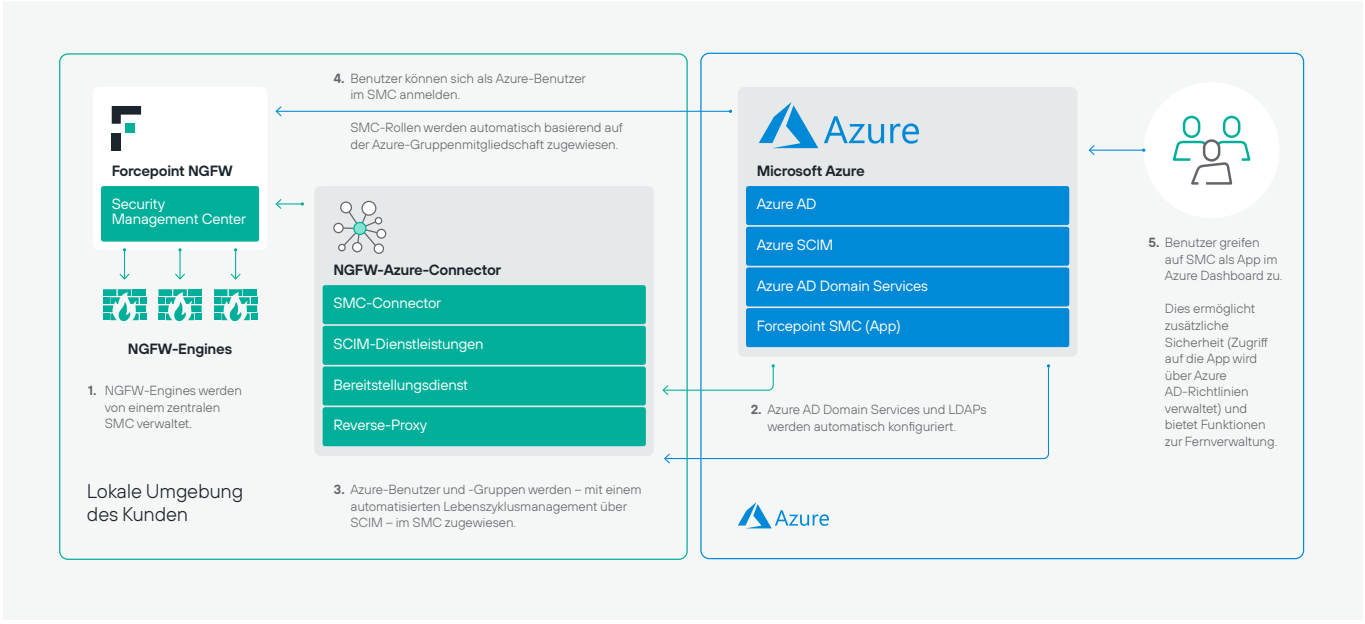
Schnelle und flexible Bereitstellung

Um Forcepoint Next Generation Firewall in Ihrer Microsoft Azure-Umgebung bereitzustellen, besuchen Sie einfach den Microsoft Azure Marketplace.

→ Marketplace besuchen

Forcepoint Next Generation Firewall und Microsoft Azure-Lösungen

Machen Sie mehr aus Ihrer Azure-Investition und erweitern Sie die Funktionen Ihrer Forcepoint-Lösungen mit unseren einzigartigen Integrationen. Weitere Informationen zu unseren Integrationen und Schritt-für-Schritt-Anleitungen für die Implementierung finden Sie unter forcepoint.github.io



Azure Active Directory (AD) – Integration des sicheren Hybridzugriffs

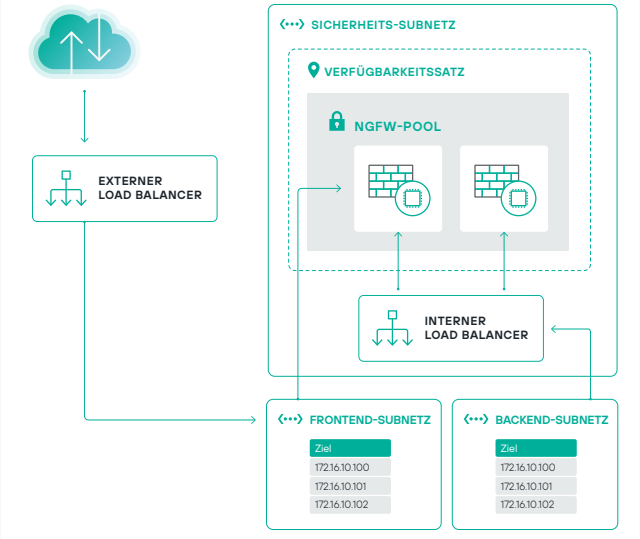
Ermöglicht Forcepoint SMC-Zugriff und Authentifizierung über Azure AD-Benutzer und -Richtlinien.

- → Verwendet das SMC als Azure-App für entfernte Verwaltungsfunktionen.
- → Ausgewählte Azure AD-Benutzer können unterschiedlichen Zugriffsebenen im SMC zugewiesen werden, wodurch mehrere Fernverwaltungsszenarios in einer ganzen Reihe von NGFW-Engines ermöglicht werden.
- → Bietet zentralisierte Verwaltung und Kontrolle im SMC mit der zusätzlichen Sicherheit der Authentifizierungsrichtlinien von Azure AD.

Hochverfügbarkeit mit der Integration von Azure Resource Manager (ARM)

Automatisiert die Bereitstellung eines redundanten Satzes an NGFW-Engines in Azure, indem eine ARM-Vorlage genutzt wird, die für die Bereitstellung des gesamten Stacks konfiguriert wurde.

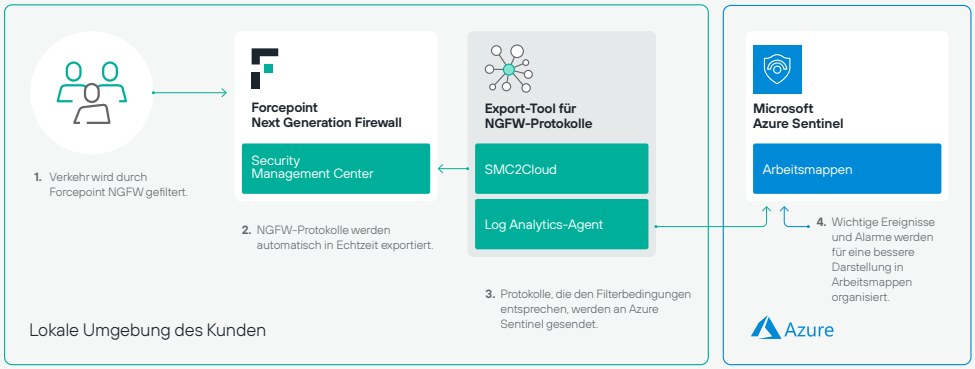
- → Die ARM-Vorlage wurde für die Bereitstellung eines Stacks konfiguriert, der zwei Netzwerk-Load-Balancer und drei Subnetze enthält, um den Datenverkehr zwischen internen und externen Netzwerken zu verwalten.
- → Ermöglicht den Betrieb von NGFW-Engines im Hochverfügbarkeitsmodus, um einen unterbrechungsfreien Netzwerkfluss zwischen Benutzern und Workloads zu gewährleisten.



Azure Sentinel-Integration

Ermöglicht den Export von relevanten Protokolldaten von NGFW gemäß benutzerdefinierten Filtern.

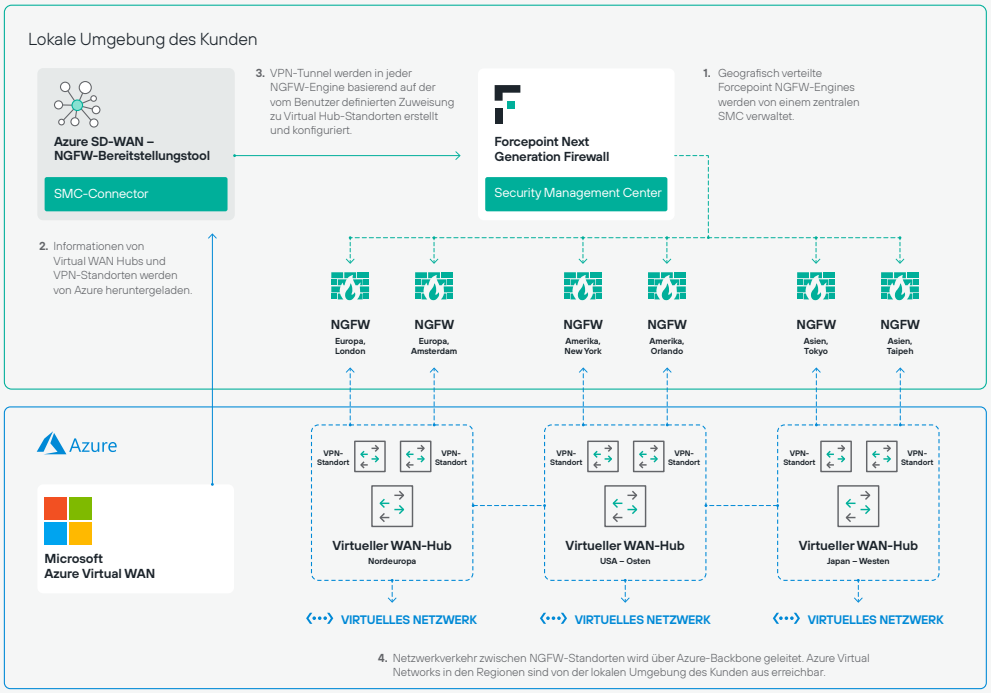
→ Automatischer Export von Protokollereignissen von NGFW nach Azure Sentinel in Echtzeit.
→ Aufnehmen von Protokollen in Azure Sentinel-Protokollanalysen und Visualisieren von Ereignissen mit Hilfe von Arbeitsmappen.



Integration von Azure Virtual WAN

Ermöglicht die automatische Erstellung und Konfiguration von IPsec-Tunneln zwischen einer Reihe von NGFW-Engines, die von Forcepoint SMC kontrolliert werden, und geografischen Virtual WAN-Standorten.

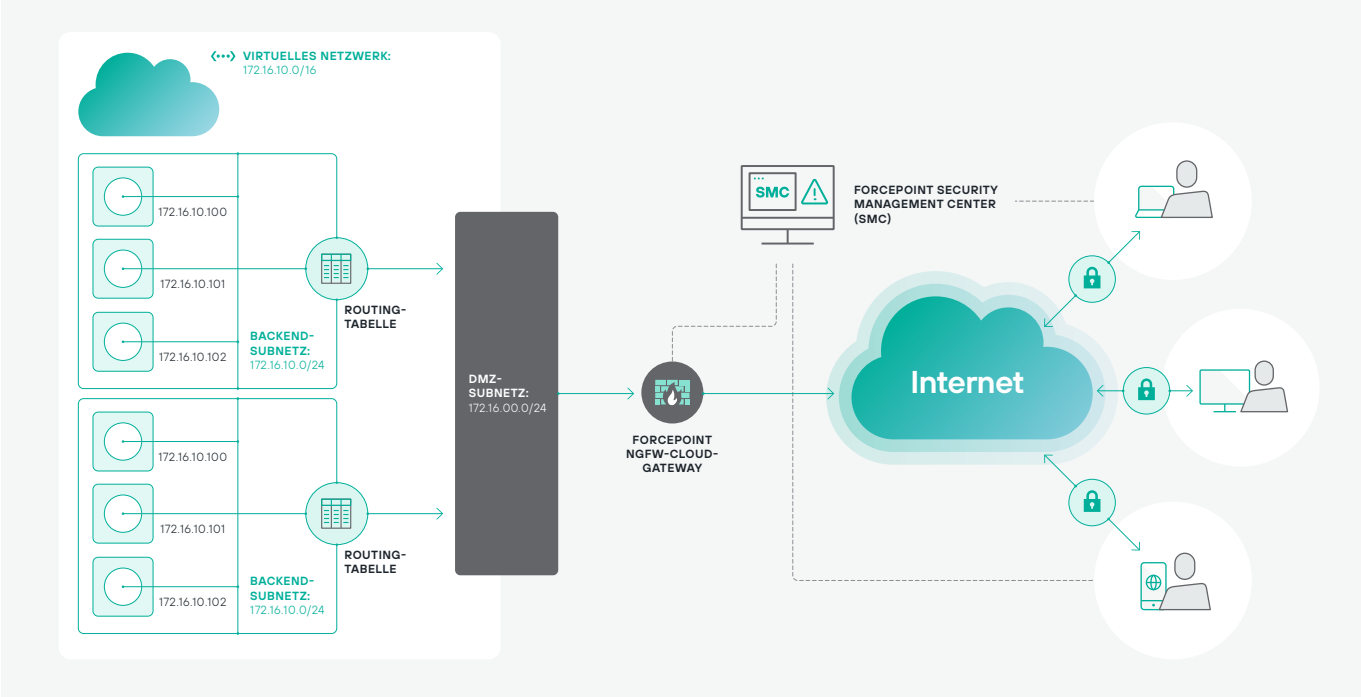
→ Erstellt eine SD-WAN-Schicht, die verwendet werden kann, um Datenverkehr zwischen Standorten über den Azure Virtual WAN-Backbone zu leiten.
→ Ermöglicht es Administratoren, redundante VPN-Tunnel in jeder NGFW-Engine zu erstellen, die vom SMC durch die Verwendung des IPsec-Standards kontrolliert wird.
→ Lässt eine Verbindung von VPN-Tunneln in jeder NGFW-Engine zu bestimmten Azure Virtual WAN-Regionen zu.

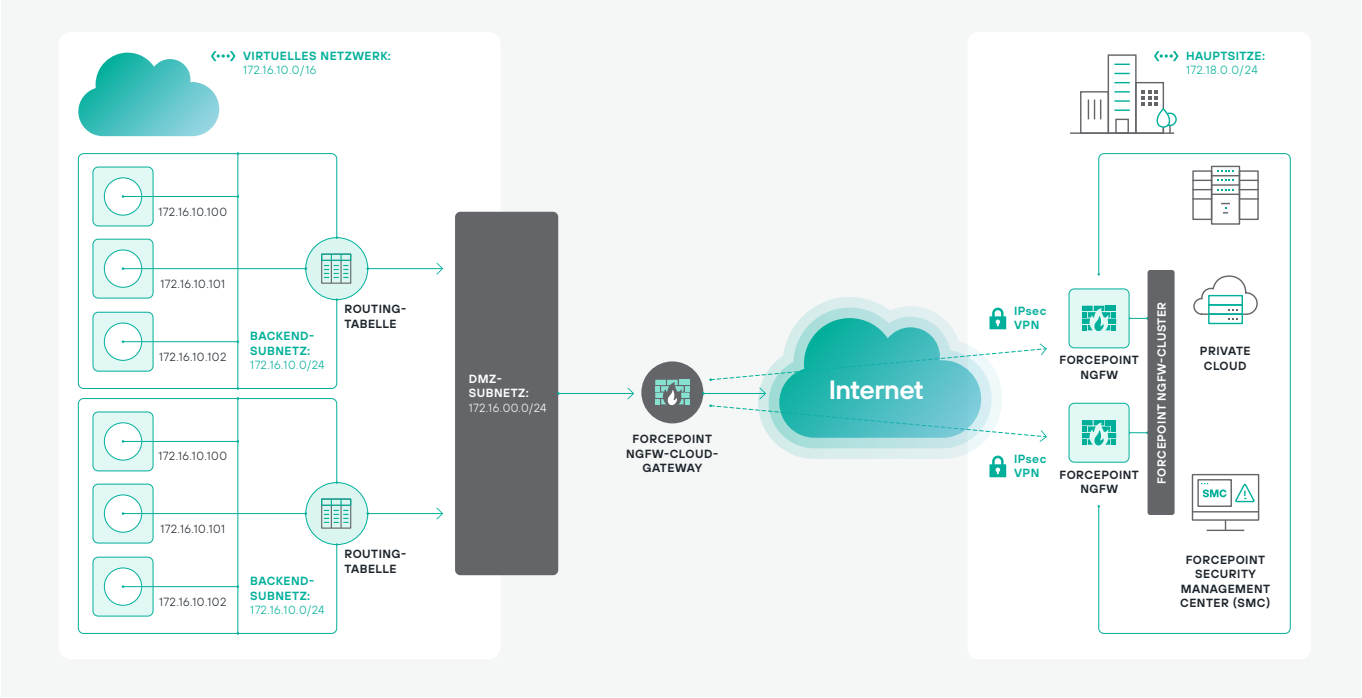


Konnektivität für Unternehmensrechenzentren

Physische und virtuelle Forcepoint NGFW-Gateways verbinden Ihre lokalen Rechenzentren im Unternehmen mit den virtuellen Rechenzentren in der Azure-Cloud. Für diesen Zweck ist Folgendes möglich:

- → Einfaches Erstellen von VPN-Verbindungen (eine oder mehrere) zwischen Ihrem Rechenzentrumsnetzwerk und Ihrer Software-VPN-Appliance von Forcepoint, die in Ihrem virtuellen Azure-Netzwerk ausgeführt wird.
- → Verwalten und Kontrollieren aller Forcepoint-Firewalls – softwarebasiert oder physisch – an beiden Enden der VPN-Verbindungen über das SMC.
- → Im Hinblick auf die Geschäftskontinuität im Bereich des Hauptsitzes der VPN-Verbindungen können Sie auch einen Cluster von physischen Firewalls für eine Ausfallsicherung verwenden.





VNET-zu-VNET-Routing zwischen Regionen

Erstellen Sie sichere VPN-Tunnel zwischen zwei oder mehreren Software-VPN-Appliances von Forcepoint, um virtuelle Netzwerke in mehreren Azure-Cloud-Regionen zu verbinden oder darüber hinaus. Für diesen Zweck ist Folgendes möglich:

→ Verwalten, Kontrollieren und Einsetzen von Sicherheitsrichtlinien an beiden Enden der VPN-Verbindung mit Forcepoint SMC.