The bridge to possible

SD-WAN: Vergleichsübersicht

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Netzwerke							
Unterstützung für herkömmliches Routing und SD-WAN auf derselben Plattform	✓ Umfassende herkömmliche Routing-Services Reibungslose Migration mit SD-WAN-relevanten Funktionen auf derselben Plattform Einheitliches Image für herkömmliches Routing und SD-WAN	✗ Kein Investitionsschutz für eine reibungslosere Migration in Bezug auf SD-WAN auf derselben Plattform Begrenzte Funktionen für herkömmliche Routing-Funktionen	✓ Für die Aktivierung von SD-WAN muss die vorhandene Infrastruktur nicht ergänzt oder geändert werden	✗ Kein Investitionsschutz für eine reibungslosere Migration in Bezug auf SD-WAN auf derselben Plattform Begrenzte Funktionen für herkömmliche Routing-Funktionen	✗ Für die Nutzung von SD-WAN ist zusätzliche neue Hardware erforderlich.	✗ Für die Aktivierung von SD-WAN muss die vorhandene Infrastruktur nicht ergänzt oder geändert werden Begrenzte Funktionen für herkömmliche Routing-Funktionen	✓ Reibungslose Migration zu SD-WAN auf derselben Plattform Vollständige herkömmliche Routing-Services verfügbar
Core-, Edge- und Cloud-SD-WAN	✓ Appliances, die in den Service-Core, den Edge und Cloud-Speicherorte integriert sind Große Auswahl an Formfaktoren mit physischen und virtuellen Angeboten	✓ Appliances, die in den Service-Core, den Edge und Cloud-Speicherorte integriert sind	✓ Appliances, die in den Service-Core, den Edge und Cloud-Speicherorte integriert sind	✓ Appliances, die in den Service-Core, den Edge und Cloud-Speicherorte integriert sind	✓ Appliances, die in den Service-Core, den Edge und Cloud-Speicherorte integriert sind	✓ Appliances, die in den Service-Core, den Edge und Cloud-Speicherorte integriert sind	✓ Appliances, die in den Service-Core, den Edge und Cloud-Speicherorte integriert sind

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Spezielle SD-WAN-Architektur	Dedizierte Komponenten auf Kontroll-, Daten- und Verwaltungsebene für Skalierbarkeit und Leistung in einer SDN-konformen Architektur Flexibilität bei der Anpassung der Architektur an die Geschäftsziele In der Cloud gehostete Bereitstellung, verwaltet vom Cisco Cloud Ops-Team	Integrierte Komponenten auf Kontroll- und Datenebene schränken die Flexibilität ein.	Ältere Firewall-basierte Architektur	Ältere kombinierte Kontroll- und Datenebenen-architektur	Dedizierte Komponenten auf Kontroll-, Daten- und Management-ebene	Integrierte Komponenten auf Kontroll- und Datenebene schränken die Flexibilität ein.	Integrierte Komponenten auf Kontroll- und Datenebene schränken die Flexibilität ein.
Echte Zero-Touch-Bereitstellung	Gegenseitig authentifizierte Multi-Faktor-Authentifizierung mit Zero-Touch-Bereitstellung für alle Komponenten One-Touch-Bereitstellung für Air-Gap-Netzwerke und MSPs	**Begrenzt** Für die Bereitstellung sind zusätzliche Authentifi-zierungsschritte erforderlich.	Mehrere Interaktionspunkte zur Aktivierung des ZTP-Prozesses Da die Lösung auf SD-WAN mit Firewall-Aktivierung basiert, sind manuelle Richtlinienkon-figurationen erforderlich.	**Begrenzt** EdgeConnect-Geräte sind vorkonfiguriert, erfordern jedoch zusätzliche Authentifizie-rungsschritte.	Mehrere Interaktionspunkte	Die ION-Geräte sind vorkonfiguriert, um sich beim Portal zu authentifizieren und Zero-Touch-Provisionierung und -Bereitstellung zu unterstützen.	**Begrenzt** Für die Bereitstellung sind zusätzliche Authentifizie-rungsschritte erforderlich.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Aktiv-aktiv-SD-WAN-Topologie mit zwei Routern	Unterstützung für Aktiv-aktiv-Netzwerke mit höherem Durchsatz und höherer Zuverlässigkeit Möglichkeit zur horizontalen Skalierung mit benutzerfreundlichen Funktionen	Aktiv-aktiv-Verbindungen werden nicht unterstützt.	**Begrenzt** Zusätzlicher WAN-Switch erforderlich, wodurch Abhängigkeiten entstehen	**Begrenzt** Ermöglicht Aktiv-aktiv-Netzwerke, erfordert jedoch einen zusätzlichen Switch, der Abhängigkeiten schafft	Aktiv-aktiv-Verbindungen werden nicht unterstützt.	Aktiv-aktiv-Verbindungen werden nicht unterstützt.	Aktiv-aktiv-Verbindungen werden unterstützt.
Advanced Routing-Protokolle für Brownfield-Integrationen	Ausdehnung erweiterter Routing-Intelligence (z. B. EIGRP, OSPF, RIP und BGP) auf Cloud-Umgebungen für schnellere, zuverlässigere Netzwerkverbindungen bei Cloud-Workloads Unterstützt dank Dual-Stack Auch Underlay-/Overlay-Routing möglich Flexible Richtlinien- und Attributunterstützung für einfache Routing-Manipulation	**Begrenzt** Unterstützung für erweiterte Routing-Protokolle wie BGP und OSP, jedoch nicht die effizienteste Pfadauswahl	Unterstützung für erweiterte Routing-Protokolle wie BGP und OSP, jedoch nicht die effizienteste Pfadauswahl	**Begrenzt** Unterstützung für erweiterte Routing-Protokolle wie BGP, aber keine Advanced Routing-Unterstützung für Protokolle wie OSPF	Unterstützung für Advanced Routing-Protokolle, einschließlich BGP und OSPF	**Begrenzt** Unterstützung für Advanced Routing-Protokolle wie BGP, aber keine Unterstützung für Protokolle wie OSPF	Unterstützung für Advanced Routing-Protokolle, einschließlich BGP und OSPF, jedoch nicht die effizienteste Pfadauswahl

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Erweiterbares Richtlinien-Framework	Die dynamische Pfadauswahl leitet kritische Anwendungen bei Netzwerkproblemen automatisch um. Mikrosegmentierung und identitätsbasiertes Richtlinienmanagement fördern die konsistente Durchsetzung von Richtlinien für mehrere Domänen und sorgen für ein einheitliches Benutzererlebnis.	**Begrenzt** Richtlinien könnten in Form von gerätebasierten Profilen übergeben werden, wären aber hinsichtlich des Traffic Engineering auf Datenebene begrenzt.	Die Richtlinien für SD-WAN und die Firewall werden separat verwaltet, was die Komplexität des Traffic Engineering und der Weitergabe zentraler Kontroll- und Datenebenenrichtlinien erhöht.	**Begrenzt** Richtlinien können im Hinblick auf geschäftliche Ziele erstellt und wiederverwendet werden, allerdings bestehen Einschränkungen bei der Mikrosegmentierung und der Durchsetzung von Richtlinien für mehrere Domänen.	**Begrenzt** Kann Traffic Engineering basierend auf anwendungssensitiven Richtlinien durchführen, aber es gibt Einschränkungen bei der Durchsetzung von Richtlinien für mehrere Domänen.	**Begrenzt** Kann Traffic Engineering basierend auf anwendungssensitiven Richtlinien durchführen, aber es gibt Einschränkungen bei der Mikrosegmentierung und bei der Durchsetzung von Richtlinien für mehrere Domänen.	Kann Traffic Engineering basierend auf Routing-Attributen, Sicherheitsrichtlinien und Anwendungsrichtlinien durchführen, aber es gibt Einschränkungen bei der Durchsetzung von Richtlinien für mehrere Domänen.
SD-WAN-/ SASE-Integration abschließen	Automatisierte Registrierung und Erstellung von IPsec-Tunneln zu Umbrella Secure Internet Gateway (SIG) mit geführten Workflows auf vManage Vollständige Integration in Cisco AnyConnect, Cisco Duo usw.	**Begrenzt** Workflows für SIG-Anbieter mit nativem SIG-Angebot noch in Arbeit	Keine geführten Workflows für SIG-Integrationen	Keine Unterstützung für Autoregistrierung oder Erstellung von IPsec-Tunneln für SASE, da sie auf Integrationen von Drittanbietern angewiesen sind.	Unterstützung für vollständige SASE-Integration	**Begrenzt** Unterstützung für vollständige SASE-Integration mit Prisma SD-WAN und Prisma Access Komplexität der API-basierten CloudBlades-Integration Keine geführten Workflows für die SIG-Integration	**Begrenzt** Unterstützung für vollständige SASE-Integration mit SD-WAN-fähiger PAN-OS NGFW und Prisma Access Keine geführten Workflows für die SIG-Integration

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
WAN-Optimierung	Bietet WAN-Optimierungs-services, einschließlich TCP-Optimierung, Eliminierung von Datenredundanz, FEC und Paketduplizierung	**Begrenzt** Bietet begrenzte WAN-Optimie-rungsservices, einschließlich FEC	**Begrenzt** Bietet begrenzte WAN-Optimie-rungsservices, einschließlich FEC	Bietet WAN-Optimieungs-services, einschließlich TCP-Optimierung, Eliminierung von Datenredundanz und FEC	**Begrenzt** Bietet begrenzte WAN-Optimie-rungsservices, einschließlich FEC	Bietet keine WAN-Optimierungs-services	**Begrenzt** Bietet begrenzte WAN-Optimier-ungsservices, einschließlich TCP-Optimierung, Paketduplizierung und FEC
Sicherheit							
Remote-Zweigstelle, lokale Sicherheits-Services	Vollständig integrierte UTM-Sicherheits-funktionen in vManage, darunter Unternehmens-Firewall mit Anwendungs-erkennung, Snort IPS, URL-Filterung, AMP Dateianalyse, Threat Grid Sandboxing, Cisco Umbrella DNS Security, SSL und Threat-Intelligence von Talos	**Begrenzt** Grundlegende Stateful Firewall	Integrierte NGFW-Funktionen mit IPS-/IDS-/ Application Control-/ AMP-Funktionen	In der SD-WAN-Konsole fehlen Sicherheit-sintegrationen.	Integrierte NGFW-Funktionen mit IPS-/IDS-/ Application-Control-/ AMP-Funktionen	**Begrenzt** Nur grundle-gende zonen-basierte Firewall Keine integrierten Sicherheits-funktionen wie IPS-/IDS-/AMP-/ URL-Filterung	Integrierte NGFW-Funktionen mit IPS-/IDS-/ Anwendung-skontrolle/AMP-/ URL-Filterung/ DNS-Sicherheits-funktionen Erfordert eine zusätzliche Lizenz

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Individueller Silicon Root of Trust	Individueller Silicon Root of Trust bei Hardware für integrierten Schutz vor grundlegenden Angriffen und Angriffen „durch die Hintertür“ Alle Cisco vEdge-Router sind mit einem werksseitig installierten TPM-Chip (Trusted Platform Module) mit signiertem Zertifikat ausgestattet. Diese integrierte Sicherheitskomponente ermöglicht die automatisierte, absolut sichere Authentifizierung von neu ins Netzwerk eingebundenen Cisco vEdge-Routern und ist extrem vorteilhaft bei Bereitstellungen im Umfang von mehreren zehntausend Endgeräten.	**Begrenzt** Kommerzielle handelsübliche Hardware mit integrierter Abwehr unbekannt	**Begrenzt** Kundenspezifische Chipkomponenten mit integrierter Abwehr unbekannt	Kommerzielle handelsübliche Hardware mit vertrauenswürdiger Lösung unbekannt	Kommerzielle handelsübliche Hardware mit vertrauenswürdiger Lösung unbekannt	Kommerzielle handelsübliche Hardware mit vertrauenswürdiger Lösung unbekannt	Kommerzielle handelsübliche Hardware mit vertrauenswürdiger Lösung unbekannt
Segmentierung	Bewährte, skalierbare MPLS-/VRF-ähnliche End-to-End-Segmentierung mit Unterstützung für Multi-Segment-Topologien und Multi-Tenant-Unterstützung	**Begrenzt** VRF-basierte Segmentierung ohne dynamische und flexible Erstellung von Multi-Segment-Topologien	**Begrenzt** Begrenzte Segmentierungsfunktionen mit komplexen VDOM-Konfigurationen ohne Erstellung dynamischer und flexibler Multi-Segment-Topologien	**Begrenzt** VRF-ähnliche Segmentierung, aber mit Routing-Einschränkungen in OSPF und Peer-Priorität	Bewährte, skalierbare MPLS-/VRF-ähnliche Segmentierung von Layer 2 bis Layer 7	**Begrenzt** Begrenzte Segmentierungsfunktionen	**Begrenzt** Bietet skalierbare VRF-ähnliche Segmentierung, aber keine flexible Erstellung von Multi-Segment-Topologien.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Traffic-Analyse verschlüsselter Daten	Möglichkeit zur Erkennung von Malware durch den Abgleich verschlüsselter SHA-Muster ohne Entschlüsselung	Keine Erkennung verschlüsselter Malware	**Begrenzt** Keine robuste ETA-Lösung für die Netzwerk-infrastruktur/-geräte	Keine Erkennung verschlüsselter Malware	Bietet Verschlüsselung für TLS-/SSL-Datenverkehr	Keine Erkennung verschlüsselter Malware	Kann Malware erkennen, indem ein- und ausgehende SSL- und SSH-Verbindungen entschlüsselt, überprüft und kontrolliert werden.
Threat-Intelligence	Weltweit anerkannte Threat-Intelligence (TALOS) mit Möglichkeit zur Bereitstellung von Incident-Response-Services	Keine Threat-Intelligence	Bietet Threat-Intelligence-Funktionen	Keine Threat-Intelligence	Bietet Threat-Intelligence und Überwachung	Keine Threat-Intelligence	Bietet Threat-Intelligence-Funktionen als Add-On
Cloud							
SaaS-Konnektivität	Die Transportunabhängigkeit bietet eine intelligente Pfadauswahl zu führenden SaaS-Anwendungen basierend auf Leistungskennzahlen und der besten Pfadauswahl, z. B. Office 365, SIG, Lastverteilung, Cisco Webex usw.	**Begrenzt** SaaS-Optimierung auf der Basis der Erstellung manueller Anwendungsregeln durch DIA-Breitbandpfade zu Co-Locations	**Begrenzt** Grundlegende SaaS-Optimierung mit manueller SLA-Erstellung für jede Anwendung	Die Transportunabhängigkeit bietet eine intelligente Pfadauswahl zu führenden SaaS-Anwendungen basierend auf Leistungskennzahlen und der besten Pfadauswahl.	**Begrenzt** Grundlegende SaaS-Optimierung mit manueller SLA-Erstellung für jede Anwendung	**Begrenzt** Grundlegende SaaS-Optimierung mit manueller Erstellung von Anwendungsregeln für jede Anwendung	**Begrenzt** Grundlegende SaaS-Optimierung mit manueller SLA-Erstellung für jede Anwendung Benötigt zusätzliche SaaS-Sicherheitsplattform für erweiterte SaaS-Optimierung

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
IaaS-Konnektivität	Geführte Workflows für die automatisierte Bereitstellung von Cisco SD-WAN Cloud OnRamp für IaaS-Verbindungen	**Begrenzt** Entweder manuelle Gateways oder gemeinsam genutzte Ressourcen Automatisierung nur mit Microsoft Azure vWAN	Manuelle Gateway-Konfiguration	**Begrenzt** Entweder manuelle Gateways oder gemeinsam genutzte Ressourcen	**Begrenzt** Entweder manuelle Gateways oder gemeinsam genutzte Ressourcen	**Begrenzt** Manuelle Gateways, gemeinsam genutzte Ressourcen oder komplexe API-Integration über CloudBlades	**Begrenzt** Entweder manuelle Gateways oder gemeinsam genutzte Ressourcen
Co-Location-Cloud-Gateways	Vereinfachte Netzwerkverwaltung dank Datenverkehrs-aggregation über Co-Location-Hubs für Cloud-Workloads mit geführten Workflows für die automatisierte Bereitstellung	**Begrenzt** Begrenzte Aggregation mit Co-Location	**Begrenzt** Begrenzte Aggregation mit Co-Location	**Begrenzt** Begrenzte Aggregation mit Co-Location	**Begrenzt** Begrenzte Aggregation mit Co-Location	**Begrenzt** Begrenzte Aggregation mit Co-Location	**Begrenzt** Begrenzte Aggregation mit Co-Location
Multicloud-Konnektivität	Geführte Workflows für die automatisierte Bereitstellung für verschiedene Cloud-Service-Provider (CSPs) wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP)	**Begrenzt** Partnerschaft mit Microsoft Azure vWAN Geführte Workflows	Begrenzte Workflows für Multicloud-Verbindungen	**Begrenzt** Manuelle Bereitstellung für verschiedene CSPs	**Begrenzt** Manuelle Bereitstellung für verschiedene CSPs	**Begrenzt** Manuelle Bereitstellung über verschiedene CSPs oder durch komplexe CloudBlades-API-Integration	**Begrenzt** Manuelle Bereitstellung für verschiedene CSPs

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Edge							
Speicher	IoT-/OT-Automatisierung mit integrierten Speicher- und Rechnerressourcen für Zweigstellen Unterstützt von der Cisco Catalyst 8200-Serie	**Begrenzt** VNFs können auf VMware SD-WAN Edge-Appliances bereitgestellt werden.	Keine Funktionen für Edge-VNF-Hosting	Keine Funktionen für Edge-VNF-Hosting	**Begrenzt** VNFs können auf Versa SD-WAN Edge-Appliances bereitgestellt werden.	Keine Funktionen für Edge-Anwendungs-hosting	Keine Funktionen für Edge-Anwendungs-hosting
Multicloud-Transparenz	Sichtbarkeit über das Internet, die Cloud und SaaS hinweg mit der nativen Integration von Cisco ThousandEyes auf kompatiblen Edge Platforms der Cisco Catalyst 8200-Serie und Catalyst 8300-Serie	**Begrenzt** Keine Funktionen für Edge-Anwendung-shosting VNFs können auf VMware SD-WAN Edge-Appliances bereitgestellt werden.	Keine Funktionen für Edge-Anwendungs-hosting	Keine Funktionen für Edge-Anwendungs-hosting	**Begrenzt** Keine Funktionen für Edge-Anwendungs-hosting VNFs können auf Versa SD-WAN Edge-Appliances bereitgestellt werden.	Transparenz über das Internet, die Cloud und SaaS mit der nativen Integration von Prisma Access ADEM	**Begrenzt** Benötigt Integration mit Prisma Access für Transparenz im Internet, in der Cloud und in SaaS über ADEM, was die Integration sehr komplex macht.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Sprachintegration	Cisco Catalyst 8000 Edge Platforms bieten umfassende Sprachservices in SD-WAN und traditionelle IOS XE-Software-Funktions-Stacks. Cisco ist der einzige SD-WAN-Anbieter, der analoge/digitale IP direkt in eine einzelne CPE integriert. Im SD-WAN-Modus verhindert die Cisco Catalyst 8300-Serie auch interne und externe Ausfälle mithilfe von SRST. Die Serie unterstützt auch weiterhin eine lange Liste traditioneller IOS XE-Sprachanwendungsfälle.	**Begrenzt** Keine Funktionen für Edge-Anwendungshosting VNFs können auf VMware SD-WAN Edge-Appliances bereitgestellt werden.	Keine Funktionen für Edge-Anwendungshosting	Keine native Sprachintegration	Keine native Sprachintegration	Keine native Sprachintegration	Keine native Sprachintegration
Erweiterte LTE-Lösungen	Erweiterte Mobilfunkfunktionen als Transportlink mit Bereitstellungsflexibilität durch integriertes Modul, Karte oder externes Gateway auf der Cisco Catalyst 8000-Serie.	Mobilfunkfunktionen als Transportlink	Mobilfunkfunktionen als Transportlink	Keine signifikante Mobilfunkunterstützung	**Begrenzt** Keine signifikante Mobilfunkunterstützung Mobilfunkunterstützung bei eingeschränktem Modell (CSG1000).	**Begrenzt** Mobilfunkunterstützung bei eingeschränktem Modell (ein ION 1200-Modell).	Unterstützt Mobilfunkfunktionen in 5G-basierter NGFW

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Industrielles SD-WAN	Robuste SD-WAN-Optionen für anspruchsvolle und industrielle Umgebungen	Keine robusten SD-WAN-Optionen	Robuste SD-WAN-Optionen	Keine robusten SD-WAN-Optionen	Keine robusten SD-WAN-Optionen	Keine robusten SD-WAN-Optionen	Robuste SD-WAN-Optionen
Wi-Fi/5G-fähig	Verwendet fortschrittliche Wireless-Frequenz- und Protokoll-technologie	Verwendet fortschrittliche Wireless-Frequenz- und Protokoll-technologie	Verwendet fortschrittliche Wireless-Frequenz- und Protokoll-technologie	Keine erweiterten Wireless-Funktionen	Verwendet fortschrittliche Wireless-Frequenz- und Protokoll-technologie	Keine erweiterten Wireless-Funktionen Abhängigkeit von Drittanbietern, um Funktionen zu aktivieren	Keine erweiterten Wireless-Funktionen Abhängigkeit von Drittanbietern, um Funktionen zu aktivieren Verfügt über 5G-fähige NGFW-Hardware
Rechenzentrums-integration (gemeinsame Richtlinien für alle Domänen)	Domänen-übergreifende Integrationen, gemeinsame QoS-Richtlinien zwischen Cisco ACI und SD-WAN Erweitern der TrustSec Security Group Tags (SGTs)/ Metadaten vom WAN über den Campus bis zum Rechenzentrum	Vereinheitlicht Rechenzent-rumsrichtlinien mit Edge-Anforderungen	Keine Rechenzent-rumsintegration Rechenzent-rumsintegration	Keine Rechenzent-rumsintegration	Keine Rechenzent-rumsintegration	Keine domänen-übergreifende Integration	Keine domänen-übergreifende Integration

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Mikrosegmentierung	Unterstützung für Mikrosegmentierung und Richtliniendurchsetzung durch skalierbare Gruppen-Tags für Benutzergruppen	**Begrenzt** Minimale Layer-2-Mikrosegmentierung und Richtliniendurchsetzung	**Begrenzt** Minimale Layer-2-Mikrosegmentierung und Richtliniendurchsetzung	Unterstützung für Mikrosegmentierung und Richtliniendurchsetzung durch skalierbare Zonen	Unterstützung für Mikrosegmentierung und Richtliniendurchsetzung durch skalierbare Zonen	Keine Mikrosegmentierung und Richtliniendurchsetzung	Unterstützung für Mikrosegmentierung und Richtliniendurchsetzung durch skalierbare Zonen

C83-743414-01 11/21