Cisco Small Business Security Appliances der Serie ISA500

Internetzugriff und Sicherheit in einer Komplettlösung für kleine und mittlere Unternehmen

Die Cisco® Small Business Integrated Security Appliances der Serie ISA500 kombinieren hoch sicheren Internet-, Wireless-, Site-to-Site- und Remote-Zugriff und ein breites Spektrum an Unified Threat Management (UTM)-Funktionen in einer umfassenden Komplettlösung für Internetzugriff und Sicherheit. Diese Funktionen umfassen neben einer Firewall auch Funktionen für E-Mail- und Websicherheit sowie Anwendungskontrolle – kleine und mittlere Unternehmen profitieren damit von umfassender Sicherheit. Die Security Appliances der Serie ISA500 wurden speziell für kleine und mittlere Unternehmen optimiert, zeichnen sich durch einen erschwinglichen Preis und eine einfache Verwendung aus und bieten dank der unkomplizierten Einrichtung innerhalb weniger Minuten umgehend Schutz für Ihr Unternehmen. Die Lösung nutzt zudem die globalen Daten zu Sicherheitsbedrohungen der Cisco Security Intelligence Operations (SIO), um einen überlegenen Schutz vor Bedrohungen zu gewährleisten. Durch die leistungsstarke Kombination aus umfangreichen UTM-Sicherheitsfunktionen, einem benutzerfreundlichen Design und der intelligenten Abwehr von Sicherheitsbedrohungen sorgen die Security Appliances der Serie ISA500 für erhöhte Sicherheit und eine gesteigerte Mitarbeiterproduktivität bei gleichzeitiger Senkung der Betriebskosten und des Risikos von Unterbrechungen des Geschäftsbetriebs.

E-Mail- und Websicherheit werden bei der Cisco Serie ISA500 anhand eines Cloud-basierten Ansatzes gewährleistet. Auf diese Weise wird nicht nur der Managementaufwand auf ein Minimum reduziert, das System ist in der Lage, schnell und flexibel auf neue Bedrohungen zu reagieren. Im Rahmen der umfassenden Sicherheitsprüfung wird der Webzugriff kontrolliert, die Anzahl von Spam-E-Mails reduziert und Phishing-Angriffe, nicht autorisierte Zugriffsversuche und neuartige Bedrohungen aus dem Netzwerk ferngehalten – Faktoren, die zu einer erhöhten Mitarbeiterproduktivität beitragen. Die Lösung nutzt überdies 75 TB an Telemetriedaten zu Bedrohungen, die täglich von 1,6 Millionen weltweit implementierten Sicherheitsgeräten an die Cisco SIO übertragen werden – damit ist ein umfassender Schutz auch vor komplexen Angriffen gewährleistet. Dieser umfassende Ansatz trägt dazu bei, dass wichtige IT-Ressourcen freigesetzt werden, da IT-Mitarbeiter deutlich weniger Zeit für das Entfernen von Viren und Systembereinigungen aufwenden müssen.

Zusätzlich zu den genannten Funktionen überzeugt die Cisco Serie ISA500 noch durch Merkmale wie WAN-Redundanz mit Unterstützung von Failover, Lastenausgleich und richtlinienbasiertem Routing, mit denen ein unterbrechungsfreier Geschäftsbetrieb auch dann gewährleistet ist, wenn die Internetverbindung ausfällt oder ein Fehler seitens des Internet Service Providers (ISP) auftritt. Als Teil des Cisco Small Business-Produktportfolios wurde die Cisco Serie ISA500 darüber hinaus auf die Kompatibilität mit anderen Cisco Small Business-Produkten getestet. Beim Einsatz in einer Gesamtlösung wird dadurch eine deutlich höhere Betriebszeit erzielt.

Die Cisco Serie ISA500 wurde mit Blick auf die dynamischen Geschäftsbedingungen der heutigen Zeit entwickelt – dank der Möglichkeit zur Einrichtung von IP Security (IPsec)- oder Secure Socket Layer (SSL)-VPNs können auch mobile Mitarbeiter oder Geschäftspartner sicher auf das Netzwerk zugreifen. Mit einer Lösung der Cisco Serie ISA500 in Ihrem Netzwerk können Sie Ihre Anstrengungen vollständig auf das Wachstum Ihres Unternehmens und die Betreuung Ihrer Kunden richten, anstatt wertvolle Zeit mit Bedenken um die Sicherheit zu vergeuden.

Herausforderung

Kleine und mittlere Unternehmen benötigen eine einfache, erschwingliche und einfach bereitzustellende Lösung, die einerseits den Zugriff auf das Internet ermöglicht und andererseits alle Sicherheitsfunktionen bietet, die für eine sichere Nutzung des Internet ohne Beeinträchtigung der geschäftlichen Produktivität erforderlich sind. Diese Unternehmen bedürfen einer einfachen Möglichkeit, im gewünschten Umfang einen Zugang zum Internet einzurichten. Zu einfach, also zu wenig ausgereift, darf diese Lösung jedoch nicht sein, damit keine Schwachstellen riskiert werden. Um die Zusammenarbeit zu optimieren und die Mobilität zu unterstützen, geben die Unternehmen ihre Netzwerke und Anwendungen zunehmend für den externen Zugriff frei. Dabei müssen sie jedoch sicherstellen, nicht zu einem leichten Ziel für Sicherheitsbedrohungen wie nicht autorisierte Zugriffe, Viren, webbasierten Angriffen und Spyware zu werden. Im Folgenden finden Sie detailliertere Beschreibungen dieser Herausforderungen und ihrer möglichen Auswirkungen:

- Multibox-Lösungen für den Internetzugriff und umfassende Sicherheit können aufwändig sein und die Kosten in die Höhe treiben.
- Nicht autorisierte Zugriffe können zum Verlust von Unternehmensdaten, zu nicht geplanten Ausfallzeiten, zu instabilen Netzwerken und zu hiermit verbundenen juristischen Konsequenzen führen.
- Viren können Unternehmensnetzwerke befallen, was zu Ausfällen und entgangenen Umsätzen führt.
- Webbasierte Bedrohungen können die Erfüllung gesetzlicher und branchenspezifischer Vorschriften beeinträchtigen.
- E-Mail-Bedrohungen, wie z. B. Spam und Phishing, können dazu führen, dass kritische Information unbeabsichtigt offengelegt werden, und die Mitarbeiterproduktivität senken.
- Anhand von Spyware können sich Angreifer Einblicke in Ihr Netzwerk und Ihre Daten verschaffen – Identitätsmissbrauch und der Verlust von Unternehmensdaten können die Folge sein.
- Cloud-Technologien und -Anwendungen setzen robuste Sicherheits- und Verschlüsselungsfunktionen voraus, um zu verhindern, dass vertrauliche Unternehmensdaten gefährdet werden.
- Unternehmen öffnen Ihre Netzwerke zunehmend für Kunden, Partner und öffentliche Benutzer, indem sie Wireless- und Gastzugriffe einrichten. Dies erhöht das Potenzial für neue Sicherheitsrisiken.
- Das Aufrufen nicht geschäftsbezogener, schädlicher Websites und sozialer Netzwerke führt zu Produktivitätsverlust, potenziellen Viren- und Spyware-Angriffen und möglichen rechtlichen Problemen.

Lösung

Die Cisco Small Business Security Appliances der Serie ISA500 bieten kleinen und mittleren Unternehmen sicheren Internetzugriff und umfassende – durch die Cisco SIO zusätzlich erweiterte – UTM-Sicherheitsfunktionen in einer umfassenden Komplettlösung, die sich durch eine einfache Bereitstellung auszeichnet und die Einrichtung von VPN-Zugriff für mobile und geografisch verteilte Mitarbeiter ermöglicht. Durch die Kombination aus zonenbasierter Firewall, Content-Sicherheit und Funktionen für den hoch sicheren Internetzugriff halten Cisco Security Appliances der Serie ISA500 Bedrohungen bereits aus dem Netzwerk fern, bevor Sie Schaden für den Geschäftsbetrieb anrichten können. Die Cisco Security Appliances der Serie ISA500 bieten:

- **Internetzugriff und Sicherheit in einer umfassenden Komplettlösung**
- **Schutz des Unternehmens vor webbasierten Bedrohungen**: Die Cisco Security Appliances der Serie ISA500 bieten wichtige Services für die Perimetersicherheit, die zum umfassenden Schutz des Netzwerks beitragen.

- **Validierter geschäftlicher Datenverkehr kann passieren, nicht autorisierte Zugriffe werden blockiert**: Die Cisco Security Appliances der Serie ISA500 bringen eine zonenbasierte Firewall zum Einsatz, mit der Zugriffe auf das Netzwerk flexibel und richtlinienbasiert kontrolliert werden können. Diese unterstützet zudem die Einrichtung eines öffentlich zugänglichen Netzwerkbereichs (DMZ), in dem Datei-, Web- und andere über das Internet zugängliche Server sicher gehostet werden können, ohne dass das interne LAN des Unternehmens Sicherheitsbedrohungen ausgesetzt ist.
- **Webblockierung und -filterung**: Zur Kontrolle der Internetnutzung der Mitarbeiter können reputationsbasierte Web- und URL-Filter verwendet werden, um Zugriffe auf schädliche oder unangemessene Websites zu blockieren. Diese fortschrittlichen Kontrollfunktionen minimieren die Risiken webbasierter Sicherheitsbedrohungen, sorgen für eine erhöhte Produktivität von Mitarbeitern und reduzieren das Risiko potenzieller rechtlicher Schritte von Mitarbeitern, die anstößigen Inhalten ausgesetzt werden könnten.
- **Antivirenfunktionen**: Die erweiterte Gateway-Antivirentechnologie nutzt kontinuierlich aktualisierte Datenfeeds, um die internen Netzwerkressourcen vor den am weitesten verbreiteten und aktivsten Virenangriffen an dem Punkt Ihrer Infrastruktur zu schützen, der für diesen Zweck am effektivsten ist: dem Internet-Gateway. Die Filterung des E-Mail- und Webverkehrs im Perimeter beseitigt die Notwendigkeit für kostspielige und zeitaufwändige Bereinigungen nach einem Virenangriff und trägt zur Geschäftskontinuität bei.
- **Antispyware**: Die Blockierung der am weitesten verbreiteten und aktivsten Spyware am Gateway verhindert, dass diese Ihr Netzwerk über Internetzugriffe (HTTP und FTP) und E-Mails erreicht. Dies vermeidet die kostspielige Entfernung von Spyware und verbessert die Mitarbeiterproduktivität.
- **Spamschutz**: Robuste, reputationsbasierte Spamfilter sorgen dafür, dass E-Mail-Funktionen weiterhin effektiv genutzt werden können – eine unterbrechungsfreie Kommunikation mit Kunden, Lieferanten und Partnern ist somit sichergestellt.
- **Anti-Phishing**: Der Schutz vor Identitätsmissbrauch dient der Abwehr von Phishing-Angriffen und verhindert, dass Mitarbeiter persönliche oder geschäftliche Daten preisgeben, die zu finanziellen Verlusten führen könnten.
- **Proaktive Blockierung von Zugriffsversuchen und Blockierung gefährlicher Peer-to-Peer-Kommunikation**: Das Intrusion Prevention System (IPS) der Cisco Serie ISA500 kann mögliche Zugriffsversuche auf das Unternehmensnetzwerk erkennen, und Maßnahmen einleiten, um den Zugriff zu verhindern und somit weiteren Risiken vorzubeugen. Darüber hinaus können die Cisco Security Appliances der Serie ISA500 den Peer-to-Peer- und Instant Messaging-Datenverkehr blockieren und mithilfe von Protokollprüfungen zur Verbesserung der Netzwerksicherheit, der Steigerung der Mitarbeiterproduktivität und der Verfügbarkeit des Netzwerks für den geschäftlichen Datenverkehr beitragen.
- **Nutzung der Cisco SIO für überragenden Schutz vor Bedrohungen**: Die Cisco Serie ISA500 nutzen die 75 TB an Telemetriedaten zu Bedrohungen, die täglich an die Cisco SIO übertragen werden, um einen überragenden Schutz vor globalen Bedrohungen zu ermöglichen, der mit lokalen Schutzfunktionen kombiniert wird. Dieser Vorgang schützt vor komplexen Angriffen und stellt somit einen umfassenden Ansatz für den Schutz vor Bedrohungen dar.

- **Schutz vor internen Bedrohungen sowie Funktionen für das Management der Zugriffskontrolle**: Zur Absicherung des Unternehmens vor internen Bedrohungen stellen die Cisco Security Appliances der Serie ISA500 zonenbasierte Firewall- und Sicherheitsservices bereit, darunter IPS und Antivirenfunktionen. So werden Wireless-Umgebungen mittels der Unterstützung für ein sicheres WLAN geschützt. Hierzu dienen robuste Authentifizierungsoptionen und das Management von Gastzugriffen.
- **WAN-Redundanz:** Die Cisco Serie ISA500 stellt WAN-Redundanz bereit. Diese unterstützt Failover, Lastenausgleich und richtlinienbasiertes Routing, damit die Geschäftsprozesse aufrechterhalten werden können, wenn die Internetverbindung ausfällt oder ein Fehler seitens des ISP auftritt.
- **Sicheren VPN-Zugriff** – Die Cisco Serie ISA500 vereinfachen die Herstellung sicherer VPN-Verbindungen mittels IPsec- oder SSL-Verschlüsselung für mobile und an anderen Standorten tätige Mitarbeiter. Ein Site-to-Site-VPN über IPsec ist ideal für die Kommunikation zwischen Zweigstellen geeignet und ermöglicht den vollständigen Netzwerkzugriff. Mobile Mitarbeiter können den Cisco AnyConnect™ oder Cisco VPN Client verwenden, um SSL- oder IPsec-basierte VPN-Verbindungen mit der Hauptniederlassung herzustellen, während sie sich z. B. vor Ort bei Kunden, in einem Café oder am Flughafen befinden.
- **Hochgradig sichere Wireless-Anbindung**:Um für Mitarbeiter, die im Gebäude unterwegs sind, uneingeschränkten Zugriff zu ermöglichen, stellen einige Modelle der Cisco Serie ISA500 hochgradig sichere Mobilität mit Wireless-Anbindung nach 802.11b, g und n mit WPA-Verschlüsselung und 802.11x-Authentifizierung bereit. Funktionen für die Erkennung von nicht autorisierten Access Points helfen, das Risiko durch nicht autorisierte Wireless-Benutzer zu reduzieren und die Kontrolle über die Netzwerkinfrastruktur zu behalten.
- **Einfaches Cloud-basiertes oder Onbox-Management mit Cisco OnPlus und dem integrierten ISA500-Managementmodul**: Die Cisco Security Appliances der Serie ISA500 können mittels des integrierten Konfigurationstools verwaltet werden. Dies ist eine leistungsfähige, dabei jedoch benutzerfreundliche browserbasierte Oberfläche für Management und Monitoring. Darüber hinaus erstellt das Konfigurationstool Berichte zur Sicherheit und zur Netzwerknutzung, sodass Administratoren schnell und einfach Sicherheitsmaßnahmen und den Status des Netzwerkbetriebs überprüfen können. Ihr Partner kann das Management der Cisco Security Appliance der Serie ISA500 auch für Sie im Rahmen des Cisco OnPlus™ Service übernehmen. Diese Cloud-basierte Plattform stellt Analyse- und Monitoring-Funktionen für das gesamte Netzwerk kleiner und mittlerer Unternehmen bereit. Darüber hinaus können Sie Netzwerkmanagementaufgaben an Ihren Partner übergeben, sodass Sie sich voll und ganz auf Ihr Kerngeschäft konzentrieren können. Cisco OnPlus stellt über die erweiterten Sicherheitsservices ebenfalls Reporting-Services bereit. Mit erweiterten Sicherheitsservices können Partner Berichte zur Sicherheit, zur Netzwerknutzung und zum Systemstatus generieren, die z. B. Informationen zu zugriffsversuchen und zur WAN-Bandbreitennutzung enthalten und zu festgelegten Zeitpunkten erstellt werden. Diese Berichte können als PDF-Dateien gespeichert und per E-Mail versendet werden. Insgesamt stellen die Cisco Security Appliances der Serie ISA500 eine Vielzahl von Managementfunktionen und -optionen bereit, die mit proaktiven Netzwerkservices und -supportleistungen die Netzwerkverfügbarkeit erhöhen und für umfassende Sicherheit sorgen.

Geschäftsvorteile

Die Cisco Serie ISA500 zeichnen sich durch umfassende Sicherheit und Verbindungsmöglichkeiten aus. Die Vorteile umfassen:

- **Sicherheit und erhöhte Betriebszeiten für Ihr Unternehmen**: Umfassende Sicherheitsfunktionen bieten Schutz für Ihre wichtigsten Geschäftsprozesse, wie Unternehmens-Shops, Websites, Services und die Kundenkommunikation. Diese Funktionen unterstützen Sie zudem dabei, den Zugriff auf wichtige Netzwerkressourcen sicherzustellen, Angriffe abzuwehren und die Verfügbarkeit zu erhöhen.
- **Erhöhte Mitarbeiterproduktivität**: Durch die Eingrenzung von Spam und Spyware und nicht geschäftsbezogener Internetnutzung erhöhen Sie die Produktivität Ihrer Mitarbeiter. Mittels der erweiterten Anwendungskontrolle können Sie die Verwendung nicht geschäftsbezogener Anwendungen verhindern, die Ihre Mitarbeiter von ihren alltäglichen Aufgaben ablenken.
- **Optimierte Ausfallsicherheit von Geschäftsprozessen**: Diese umfassende Komplettlösung für Ihre Sicherheitsinfrastruktur verhindert Ausfälle geschäftskritischer Anwendungen und Services, die durch Sicherheitsverletzungen auftreten können.
- **Geringere Haftungsrisiken**: Sie reduzieren das Haftungsrisiko für Ihr Unternehmen aufgrund beschädigter Daten oder unzureichender Unternehmenskontrollen, indem Sie eine umfassende Zugriffskontrolle implementieren und einen überragenden Schutz vor Bedrohungen bieten, der durch Services auf der Basis von Cisco SIO bereitgestellt wird. Die erweiterten Risikominimierungs- und Monitoring-Funktionen unterstützen Sie dabei, gesetzliche und branchenspezifische Vorgaben effektiver einzuhalten und Kundendaten, Mitarbeiterdaten und andere vertrauliche Unternehmensdaten zu schützen.
- **Niedrigere IT-Kosten**: Sie verringern den Aufwand für den IT-Support und vermeiden die kostspielige Behebung von Problemen, die durch Spyware, Viren, komplexe Angriffe und andere Malware verursacht werden, indem Sie diesen bereits im Vorfeld vorbeugen.
- **Gewährleistung einer produktiven Arbeit zu jeder Zeit dank sicherem Remote-Zugriff**: Ihre Mitarbeiter und Partnern können mittels der flexiblen und benutzerfreundlichen integrierten VPN-Unterstützung sicher von zu Hause, von unterwegs oder von Zweigstellen aus auf das Netzwerk zugreifen. Dank des hochsicheren Remote-Zugriffs und der robusten Content-Schutzfunktionen bleiben Ihre Mitarbeiter jederzeit und unabhängig vom Standort mit den benötigten Anwendungen und Personen in Verbindung, können effektiver arbeiten und schneller auf Anfragen von Kunden und Kollegen reagieren. Mobile Mitarbeiter erhalten über den Cisco AnyConnect Client jederzeit über eine intelligente VPN-Verbindung mit konsistenten, kontextbezogenen Sicherheitsfunktionen mit Ihrem Unternehmen in Verbindung bleiben, unabhängig davon, ob sie einen Laptop oder ein Smartphone verwenden.
- **Optimierte betriebliche Effizienz**: Die intuitive, browserbasierte Oberfläche und die intelligent strukturierten Konfigurationsassistenten vereinfachen die Installation und reduzieren den Aufwand für laufende Monitoring- und Management-Aufgaben.
- **Umfassende Absicherung**: Durch unsere kostengünstigen abonnementbasierten Serviceangebote können Sie das maximale Potenzial Ihrer Cisco Lösung ausschöpfen. Der Cisco Small Business Support Service bietet Gerätesupport für drei Jahre und schützt Ihre Investition durch Software-Upgrades und -Updates, Zugriff auf das Cisco Small Business Support Center und die Support-Community sowie Hardware-Ersatz am folgenden Geschäftstag.

Aufgrund dieser Vorteile sind die Cisco Security Appliances der Serie ISA500 die richtige Wahl für Ihre Sicherheitsanforderungen und schaffen optimale Voraussetzungen für Ihr Netzwerk und Ihre Mitarbeiter.

Spezifikationen

Table 1. Cisco Small Business Security Appliances der Serie ISA500 – Modelle und Spezifikationen

Merkmale und Funktionen	ISA550	ISA550W	ISA570	ISA570W
Firewall				
Stateful Packet Inspection-Durchsatz[1]	200 Mbit/s	200 Mbit/s	500 Mbit/s	500 Mbit/s
Zonenbasierte Firewall	Ja	Ja	Ja	Ja
Maximale Anzahl an Verbindungen	15.000	15.000	40.000	40.000
Maximale Anzahl an Regeln	100	100	100	100
Sitzungen/Sekunde (cps)	2.500	2.500	3.000	3.000
Zeitpläne	Ja	Ja	Ja	Ja
Schutz vor Denial-of-Service-Angriffen	Ja	Ja	Ja	Ja
IPS-Durchsatz[1]	60 Mbit/s	60 Mbit/s	90 Mbit/s	90 Mbit/s
AV-Durchsatz[1]	50 Mbit/s	50 Mbit/s	80 Mbit/s	80 Mbit/s
UTM-Durchsatz[1]	45 Mbit/s	45 Mbit/s	75 Mbit/s	75 Mbit/s
VPN				
IPsec-VPN-Durchsatz (Data Encryption Standard [DES]/Triple DES [3DES]/Advanced Encryption Standard [AES])[1]	75 Mbit/s	75 Mbit/s	130 Mbit/s	130 Mbit/s
Site-to-Site-IPSec-VPN-Tunnel	25	25	100	100
IPsec-VPN-Remote-Zugriffs-Tunnel	10	10	75	75
SSL-VPN-Tunnel	10	10	50	50
Verschlüsselung	DES/3DES/AES (128.192.256 Bit)	DES/3DES/AES (128.192.256 Bit)	DES/3DES/AES (128.192.256 Bit)	DES/3DES/AES (128.192.256 Bit)
Authentifizierung	MD5, SHA-1, SHA2 (256.384.512 Bit)	MD5, SHA-1, SHA2 (256.384.512 Bit)	MD5, SHA-1, SHA2 (256.384.512 Bit)	MD5, SHA-1, SHA2 (256.384.512 Bit)
IPsec Dead Peer Detection	Ja	Ja	Ja	Ja
IPsec Network Address Translation (NAT) Traversal	Ja	Ja	Ja	Ja
IPsec-NetBIOS-Broadcast über VPN	Ja	Ja	Ja	Ja
VPN-Passthrough	IPsec/Point-to-Point Tunneling Protocol (PPTP)/Layer 2 Tunneling Protocol (L2TP)	IPsec/PPTP/L2TP	IPsec/PPTP/L2TP	IPsec/PPTP/L2TP
Cisco VPN Client-Unterstützung	Ja	Ja	Ja	Ja
Cisco VPN Clientmodus-Unterstützung	Ja	Ja	Ja	Ja
Cisco VPN Network Extension-Modus-Unterstützung	Ja	Ja	Ja	Ja
Cisco VPN Split Tunneling-Unterstützung	Ja	Ja	Ja	Ja
Cisco AnyConnect SSL VPN-Client-Unterstützung	Ja	Ja	Ja	Ja
SSL VPN Split Tunneling-Unterstützung	Ja	Ja	Ja	Ja
SSL-VPN-Zertifikate	Ja	Ja	Ja	Ja

Merkmale und Funktionen	ISA550	ISA550W	ISA570	ISA570W
VPN-Client für Telearbeiter (Cisco Hardware-VPN-Client)	Ja	Ja	Ja	Ja
L2TP-Server	Ja	Ja	Ja	Ja
Sicherheitsservices				
Intrusion Prevention System (IPS)	Ja	Ja	Ja	Ja
Anwendungskontrolle	Ja	Ja	Ja	Ja
Web-URL-Filterung	Ja	Ja	Ja	Ja
Schutz vor webbasierten Bedrohungen	Ja	Ja	Ja	Ja
Anti-Phishing	Ja	Ja	Ja	Ja
Antivirus	Ja	Ja	Ja	Ja
Anti-Spyware	Ja	Ja	Ja	Ja
Spam-Filter	Ja	Ja	Ja	Ja
Netzwerkreputationsfilter	Ja	Ja	Ja	Ja
Netzwerk				
IP-Adressenzuweisung	Statisch, Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol over Ethernet (PPPoE), L2TP und PPTP	Statisch, DHCP, PPPoE, L2Tp, PPTP	Statisch, DHCP, PPPoE, L2Tp, PPTP	Statisch, DHCP, PPPoE, L2Tp, PPTP
DHCP	Server und Relay	Server und Relay	Server und Relay	Server und Relay
VLANs	16	16	16	16
Trunking (802.1q)	Ja	Ja	Ja	Ja
Network Address Translation (NAT)	Ja	Ja	Ja	Ja
Port-Weiterleitung	Ja	Ja	Ja	Ja
Port-Triggering	Ja	Ja	Ja	Ja
Routing	Statisch, Routing Information Protocol (RIP) Version 1 und 2	Statisch, RIP Version 1 und 2	Statisch, RIP Version 1 und 2	Statisch, RIP Version 1 und 2
DMZ	Ja	Ja	Ja	Ja
Dual-WAN	Ja	Ja	Ja	Ja
Lastenausgleich	Symmetrisch	Symmetrisch	Symmetrisch	Symmetrisch
Richtlinienbasiertes Routing (protokollgestützt)	Ja	Ja	Ja	Ja
Integriertes und automatisiertes Failover und Failback	Ja	Ja	Ja	Ja
Gewichteter Lastenausgleich	Ja	Ja	Ja	Ja
Dynamic DNS (DDNS)	Ja	Ja	Ja	Ja
Unterstützung für Voice-over-IP	SIP, H.323, mit den meisten VoIP-Gateway- und Kommunikationsgeräten kompatibel	SIP, H.323, mit den meisten VoIP-Gateway- und Kommunikationsgeräten kompatibel	SIP, H.323, mit den meisten VoIP-Gateway- und Kommunikationsgeräten kompatibel	SIP, H.323, mit den meisten VoIP-Gateway- und Kommunikationsgeräten kompatibel
Unterstützung für SIP ALG	Ja	Ja	Ja	Ja
Unterstützung für H.323 ALGP	Ja	Ja	Ja	Ja
QoS	Ja	Ja	Ja	Ja
Strict Priority Queuing	Ja	Ja	Ja	Ja
Weighted Round Robin Queuing	Ja	Ja	Ja	Ja
Low Latency Queuing	Ja	Ja	Ja	Ja

Merkmale und Funktionen	ISA550	ISA550W	ISA570	ISA570W
DSCP-Markierung	Ja	Ja	Ja	Ja
Ratenbegrenzung	Ja	Ja	Ja	Ja
Virtual Router Redundancy Protocol (VRRP)	Ja	Ja	Ja	Ja
Internet Group Management Protocol (IGMP)-Proxy	Ja	Ja	Ja	Ja
IGMP-Snooping	Ja	Ja	Ja	Ja
Wireless				
802.11b/g/n, 2.4 GHz, 2x2 Multiple Input Multiple Output (MIMO)	Nein	Ja	Nein	Ja
Mehrere SSIDs	Nein	4	Nein	4
Wi-Fi Multimedia (WMM) QoS	Nein	Ja	Nein	Ja
Unscheduled Automatic Power Save Delivery (U-APSD) (WMM Power Save [WMM-PS])	Nein	Ja	Nein	Ja
MAC-Filterung	Nein	Ja	Nein	Ja
Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access Pre-Shared Key (WPA2-PSK), WPA2-ENT	Nein	Ja	Nein	Ja
Basic Service Set Identifier (BSSID) oder virtuelle Access Points	Nein	Ja	Nein	Ja
Dynamisch und manuell einstellbare Übertragungsleistung	Nein	Ja	Nein	Ja
Wi-Fi Protected Setup (WPS)	Nein	Ja	Nein	Ja
Gastzugriff	Nein	Ja	Nein	Ja
Captive Portal	Nein	Ja	Nein	Ja
Erkennung von nicht autorisierten Access Points	Nein	Ja	Nein	Ja
Administration				
Automatische Prüfungen auf Verfügbarkeit neuer Firmware-Versionen	Ja	Ja	Ja	Ja
Lokale Benutzerdatenbank	100	100	100	100
Authentifizierung	Lokal, RADIUS, Active Directory, Lightweight Directory Access Protocol (LDAP)	Lokal, RADIUS, Active Directory, LDAP	Lokal, RADIUS, Active Directory, LDAP	Lokal, RADIUS, Active Directory, LDAP
Diagnose	Ping, DNS-Namensauflösung, Paketerfassung	Ping, DNS-Namensauflösung, Paketerfassung	Ping, DNS-Namensauflösung, Paketerfassung	Ping, DNS-Namensauflösung, Paketerfassung
Discovery-Protokolle	Cisco Discovery Protocol (CDP), Bonjour, Universal Plug and Play (uPnP)	Cisco Discovery Protocol (CDP), Bonjour, uPnP	Cisco Discovery Protocol (CDP), Bonjour, uPnP	Cisco Discovery Protocol (CDP), Bonjour, uPnP
Protokollierung und Monitoring	Lokales Protokoll, Syslog	Lokales Protokoll, Syslog	Lokales Protokoll, Syslog	Lokales Protokoll, Syslog
Statusberichte	Status der Netzwerknutzung, des Sicherheitsservice, des Netzwerkbetriebs	Status der Netzwerknutzung, des Sicherheitsservice, des Netzwerkbetriebs	Status der Netzwerknutzung, des Sicherheitsservice, des Netzwerkbetriebs	Status der Netzwerknutzung, des Sicherheitsservice, des Netzwerkbetriebs
Hardwarespezifikationen				
Gesamtzahl der Schnittstelle	7 GE	7 GE	10 GE	10 GE
LAN-Ports (10/100/1000)	Bis zu 6	Bis zu 6	Bis zu 9	Bis zu 9

Merkmale und Funktionen	ISA550	ISA550W	ISA570	ISA570W
WAN-Ports (10/100/1000)	Bis zu 2	Bis zu 2	Bis zu 2	Bis zu 2
DMZ-Ports (10/100/1000)	Bis zu 4	Bis zu 4	Bis zu 4	Bis zu 4
USB 2.0-Ports	1	1	1	1
Formfaktor	1 HE, 19 Zoll, Rack- und Wandmontage	1 HE, 19 Zoll, Rack- und Wandmontage	1 HE, 19 Zoll, Rack- und Wandmontage	1 HE, 19 Zoll, Rack- und Wandmontage
Abmessungen (B x T x H)	308 mm x 180 mm x 49 mm (mit Gummischeiben)	308 mm x 180 mm x 49 mm (mit Gummischeiben)	308 mm x 180 mm x 49 mm (mit Gummischeiben)	308 mm x 180 mm x 49 mm (mit Gummischeiben)
Gewicht	1,2 kg	1,3 kg	1,3 kg	1,4 kg
Ein-/Aus-Schalter	Ja	Ja	Ja	Ja
Antennen	Keine	2	Keine	2
Umgebungstemperatur – Betrieb	0 bis 40 °C	0 bis 40 °C	0 bis 40 °C	0 bis 40 °C
Lagertemperatur	-20 bis 70 °C	-20 bis 70 °C	-20 bis 70 °C	-20 bis 70 °C
Spannungsbereich	100-240 V (Wechselstrom)	100-240 V (Wechselstrom)	100-240 V (Wechselstrom)	100-240 V (Wechselstrom)
Eingangsfrequenz	50-60 Hz	50-60 Hz	50-60 Hz	50-60 Hz
Ausgangsspannung	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V
Ausgangsstrom	Max. 1,667 A	Max. 1,667 A	Max. 2,5 A	Max. 2,5 A

[1] Leistungstestmethode: Maximale Leistung basierend auf RFC 2544. Bei allen Ergebnissen handelt es sich um bidirektionale Gesamtwerte. Die tatsächliche Leistung ist von der Netzwerkumgebung und den Konfigurationen abhängig.

Bestellungen

Table 2. Cisco Small Business Integrated Security Appliance der Serie ISA500 - Produkt- und Lizenz-Teilenummern

Produkt	SKU
Cisco Integrated Security Appliance 550 mit einjährigem umfassenden Sicherheitsabonnement	ISA550-BUN1-K9
Cisco Integrated Security Appliance 550 mit Wireless-Funktionalität und einjährigem umfassenden Sicherheitsabonnement	ISA550W-BUN1-K9
Cisco Integrated Security Appliance 570 mit einjährigem umfassenden Sicherheitsabonnement	ISA570-BUN1-K9
Cisco Integrated Security Appliance 570 mit Wireless-Funktionalität und einjährigem umfassenden Sicherheitsabonnement	ISA570W-BUN1-K9
Cisco Integrated Security Appliance 550 mit dreijährigem umfassenden Sicherheitsabonnement	ISA550-BUN3-K9
Cisco Integrated Security Appliance 550 mit Wireless-Funktionalität und dreijährigem umfassenden Sicherheitsabonnement	ISA550W-BUN3-K9
Cisco Integrated Security Appliance 570 mit dreijährigem umfassenden Sicherheitsabonnement	ISA570-BUN3-K9
Cisco Integrated Security Appliance 570 mit Wireless-Funktionalität und dreijährigem umfassenden Sicherheitsabonnement	ISA570W-BUN3-K9

Lizenz	SKU
Umfassendes Sicherheitsabonnement von Cisco für die Serie ISA550 – 1 Jahr	L-ISA550-CS-1YR=
Umfassendes Sicherheitsabonnement von Cisco für die Serie ISA570 – 1 Jahr	L-ISA570-CS-1YR=
Umfassendes Sicherheitsabonnement von Cisco für die Serie ISA550 – 3 Jahre	L-ISA550-CS-3YR=
Umfassendes Sicherheitsabonnement von Cisco für die Serie ISA570 – 3 Jahre	L-ISA570-CS-3YR=

Service und Support

Die Cisco Small Business Security Appliances der Serie ISA500 werden durch den Cisco Small Business Support Service unterstützt, der eine kostengünstige Abdeckung bietet. Dieser im Abonnement bereitgestellte kostengünstige Service beinhaltet Software-Upgrades und Updates, erweiterten Zugriff auf das Cisco Small Business Support Center und – falls erforderlich – Hardware-Ersatz am folgenden Geschäftstag. Sie erhalten zudem Zugriff auf unsere umfangreiche Support-Community, auf der Sie Ihre Kenntnisse weitergeben und sich mit Branchenkollegen über Onlineforen und Wikis austauschen können. Der Cisco Small Business Support Service unterstützt Sie dabei, Risiken zu reduzieren und Ihre Serviceleistungen für Kollegen und Kunden zu verbessern.

Weitere Informationen

Weitere Informationen zu Cisco Small Business Integrated Security Appliances der Serie ISA500 erhalten Sie unter www.cisco.com/go/isa500resources oder bei Ihrem Cisco Händler vor Ort. Weitere Informationen zu Cisco OnPlus erhalten Sie unter www.cisco.com/en/US/products/ps11792/index.html oder bei Ihrem Cisco Händler vor Ort.

Weitere Informationen zum Cisco Small Business Support Service finden Sie unter www.cisco.com/cisco/web/solutions/small_business/services/index.html.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco System, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices**.

Gedruckt in den USA C78-717565-00 2/13