Cisco Small Business serie ISA500 Integrated Security Appliance

Una soluzione integrata per l'accesso a Internet e la sicurezza per proteggere la piccola impresa

Cisco® Small Business serie ISA500 Integrated Security Appliance è una soluzione integrata per l'accesso a Internet e la sicurezza che offre un'elevata protezione dell'accesso a Internet, il supporto wireless, il supporto site-to-site e il supporto per l'accesso remoto con una vasta gamma di funzionalità UTM (Unified Threat Management). Tali funzionalità comprendono il supporto di sicurezza firewall, e-mail, Web e il controllo delle applicazioni per garantire alla piccola impresa la tranquillità derivante dalla consapevolezza di essere protetti. Ottimizzata appositamente per le piccole e medie imprese, ISA500 è una soluzione accessibile e semplice da utilizzare che può essere configurata per iniziare a proteggere la propria azienda in pochi minuti. Sfrutta la tecnologia Cisco SIO (Security Intelligence Operations), che fornisce informazioni sulle minacce globali per garantire una protezione eccezionale contro le minacce. La potenza integrata delle funzionalità di sicurezza UTM complete della soluzione ISA500, la struttura semplice da utilizzare e la capacità superiore di acquisizione delle informazioni sulle minacce garantisce maggiore protezione all'azienda e aumenta il tempo di attività e la produttività dei dipendenti, riducendo contemporaneamente al minimo i costi operativi e il rischio di interruzione delle attività aziendali.

Nella soluzione Cisco serie ISA500 viene utilizzato un approccio basato su cloud alla sicurezza e-mail e Web che consente di ridurre al minimo le attività di gestione e consente una protezione reattiva e flessibile contro le minacce. Questa funzionalità di analisi approfondita consente di aumentare la produttività dei dipendenti mediante il controllo dell'accesso al Web, la riduzione della posta indesiderata e la riduzione al minimo degli attacchi di phishing, delle intrusioni non autorizzate e di altre minacce emergenti. Nella soluzione vengono utilizzati inoltre 75 TB di dati di telemetria relativi alle minacce provenienti da 1,6 milioni di dispositivi quotidianamente gestiti da Cisco SIO per fornire un livello eccezionale di informazione sulle minacce globali e una protezione contro gli attacchi sofisticati. Questo approccio completo nei confronti della protezione dalle minacce consente di sgravare le risorse IT da attività di eliminazione di virus e pulizia di sistema dispendiose in termini di tempo.

Oltre alle numerose funzionalità già descritte, la soluzione Cisco ISA500 offre molte altre funzioni che consentono di ottimizzare il tempo di attività aziendale. Offre funzionalità di ridondanza WAN che supporta il failover, il bilanciamento del carico e il PBR (Policy Based Routing) per garantire il proseguimento delle attività aziendali quando si verificano guasti dovuti a una connessione Internet non funzionante o un guasto presso l'ISP stesso. Inoltre, nell'ambito della gamma di prodotti Cisco Small Business, la soluzione Cisco serie ISA500 è stata testata per garantirne il funzionamento con altri prodotti Cisco Small Business e il tempo di attività della soluzione nel complesso è aumentato.

La soluzione ISA500 è inoltre progettata per le aziende dinamiche di oggi. Consente ai dipendenti mobili e ai partner aziendali di connettersi in modo più protetto alle reti attraverso Internet mediante i servizi VPN IPsec (IP Security) o SSL (Secure Socket Layer). Con una soluzione Cisco serie ISA500 a protezione della propria rete, l'azienda può concentrarsi sul servizio offerto ai clienti e sulla crescita dell'azienda, invece di preoccuparsi delle problematiche di sicurezza.

Problema

Le piccole imprese necessitano di una soluzione semplice, accessibile e facile da implementare che fornisca l'accesso a Internet oltre a tutte le funzionalità di sicurezza necessarie per garantire che l'accesso a Internet venga utilizzato in modo sicuro e non comporti l'interruzione della produttività aziendale. Necessitano di un modo semplice e immediato per fornire l'accesso a Internet necessario e desiderato, ma non cercano una soluzione troppo semplicistica che le renda vulnerabili. Poiché aprono le proprie reti e le proprie applicazioni per diventare più collaborative, per supportare l'uso di dispositivi mobili e una maggiore interazione, le aziende devono fare in modo di non diventare obiettivo delle minacce alla sicurezza, quali accessi non autorizzati, virus, minacce e spyware provenienti da Internet. Di seguito viene fornita una spiegazione più dettagliata di tali problematiche e delle relative conseguenze:

- Le soluzioni composite per l'accesso a Internet e la sicurezza completa possono rivelarsi scomode e far aumentare i costi.
- Un accesso non autorizzato può comportare la perdita di dati aziendali, tempi di inattività non pianificati, instabilità delle reti e relative problematiche di responsabilità.
- I virus possono infettare le reti degli uffici, con conseguente interruzione dei servizi e perdita di ricavi.
- Le minacce provenienti da Internet possono impedire di soddisfare i requisiti normativi e di conformità.
- Le minacce via e-mail, quali spam e attacchi di phishing possono involontariamente rendere disponibili informazioni importanti e contribuire alla perdita di produttività dei dipendenti.
- Gli spyware penetrano nella propria rete e nei propri dati e potenzialmente possono comportare furto di identità e perdita di dati aziendali.
- La tecnologia e le applicazioni cloud richiedono solide funzionalità di sicurezza e crittografia per evitare di esporre le informazioni aziendali sensibili a rischi.
- Le aziende stanno sempre più aprendo le proprie reti ai clienti, ai partner e agli utenti pubblici tramite l'accesso wireless e guest, generando un potenziale per nuovi rischi di sicurezza.
- La navigazione in siti Web e di social networking non legati all'attività lavorativa e dannosi comporta una perdita di produttività, esposizione a virus e spyware e possibili problemi legali.

Soluzione

Cisco Small Business serie ISA500 Integrated Security Appliance fornisce alle piccole imprese una soluzione integrata per l'accesso a Internet protetto con funzionalità di sicurezza UTM complete supportate dall'eccezionale tecnologia SIO di Cisco che è semplice da implementare e fornisce il supporto VPN per i dipendenti mobili e distribuiti in aree geografiche diverse. Grazie al firewall basato su zone, alle funzionalità di sicurezza dei contenuti e di accesso altamente protetto, la soluzione Cisco serie ISA500 blocca le minacce prima che entrino nella rete e compromettano le attività aziendali La soluzione Cisco serie ISA500:

- **Fornisce una soluzione integrata per l'accesso a Internet e la sicurezza**
- **Protegge la propria azienda dalle minacce provenienti da Internet:** la soluzione Cisco serie ISA500 fornisce i servizi fondamentali di sicurezza perimetrale per garantire una protezione completa.
  - **Il traffico aziendale valido circola tranquillamente, mentre i visitatori indesiderati vengono bloccati:** la soluzione Cisco serie ISA500 include un firewall basato su zone che consente di applicare un controllo flessibile basato su policy sugli utenti che possono accedere alla propria rete. Supporta inoltre un'area di rete accessibile pubblicamente, nota come DMZ (Demilitarized Zone), in cui ospitare in totale sicurezza file server, server Web e altri server accessibili via Internet senza esporre la rete LAN interna dell'azienda a minacce.

- **Blocchi e filtri Web:** è possibile utilizzare la funzionalità di filtro Web e URL basata sulla reputazione per controllare l'utilizzo di Internet da parte dei dipendenti bloccando l'accesso a siti pericolosi o inappropriati. Questa funzionalità di controllo consente di ridurre al minimo le minacce alla sicurezza basate sul Web e di migliorare contemporaneamente la produttività dei dipendenti nonché di limitare il rischio di azione legale da parte di dipendenti esposti a contenuti offensivi.
- **Antivirus:** la tecnologia antivirus avanzata del gateway consente di utilizzare feed di dati aggiornati per proteggere le risorse della rete interna dagli attacchi di virus più diffusi e attivi nel punto più efficace della propria infrastruttura, ovvero il gateway Internet. Il filtraggio del traffico e-mail e Web a livello perimetrale elimina la necessità di costose attività di rimozione delle infezioni dispendiose in termini di tempo e consente di garantire la continuità delle attività aziendali.
- **Antispyware:** il blocco dello spyware più diffuso e attivo a livello di gateway ne impedisce la penetrazione nella propria rete tramite il traffico Internet (HTTP e FTP) ed e-mail, consentendo di evitare costose procedure di rimozione dello stesso spyware e di migliorare la produttività dei dipendenti.
- **Limitazione dello spam:** il solido filtro anti-spam basato sulla reputazione consente di ripristinare l'efficienza della posta elettronica in modo tale che la comunicazione con i clienti, i fornitori e i partner possa continuare senza interruzioni.
- **Antiphishing:** la funzionalità di protezione contro il furto di identità difende contro gli attacchi di phishing, di conseguenza impedendo ai dipendenti di divulgare inavvertitamente dettagli aziendali o personali che potrebbero comportare perdite finanziarie.
- **Prevenzione proattiva delle intrusioni e blocco delle comunicazioni peer-to-peer pericolose:** le funzionalità IPS (Intrusion Prevention System) della soluzione Cisco ISA500 consentono di identificare possibili intrusioni nella rete aziendale e di intervenire per bloccare l'intrusione e impedire ulteriori rischi. La soluzione Cisco serie ISA500 consente inoltre di bloccare il traffico peer-to-peer e di messaggistica istantanea, nonché di eseguire l'analisi dei protocolli per aumentare la sicurezza di rete, la produttività dei dipendenti e mantenere la rete disponibile per il traffico aziendale.
- **Inclusione della tecnologia Cisco SIO per una protezione dalle minacce impareggiabile:** la soluzione Cisco ISA500 utilizza 75 TB di dati di telemetria relativi alle minacce al giorno provenienti da Cisco SIO per fornire informazioni sulle minacce globali senza precedenti in combinazione con il sistema di difesa contro le minacce locale. Ciò consente di proteggersi contro attacchi sofisticati e fornire un approccio completo alla protezione dalle minacce.

- **Protezione contro le minacce interne e gestione del controllo degli accessi:** per consentire la protezione della propria azienda dalle minacce interne, la soluzione Cisco ISA500 fornisce un firewall basato su zone e servizi di sicurezza che includono funzionalità IPS e antivirus. Consente di proteggere gli ambienti wireless tramite un supporto protetto delle reti WLAN (Wireless LAN) con opzioni di autenticazione avanzate e gestione dell'accesso degli utenti guest.
- **Ridondanza WAN**: la soluzione Cisco ISA500 fornisce funzionalità di ridondanza WAN che supporta il failover, il bilanciamento del carico e il PBR (Policy Based Routing) per garantire il proseguimento delle attività aziendali quando si verificano guasti dovuti a una connessione Internet non funzionante o un guasto presso l'ISP stesso.
- **Accesso VPN protetto:** la soluzione Cisco serie ISA500 consente ai dipendenti remoti e mobili di stabilire in modo semplice connessioni VPN protette mediante crittografia IPsec o SSL. Una connessione VPN IPsec site-to-site è ideale per proteggere le comunicazioni tra gli uffici e fornisce un accesso completo alla rete. I dipendenti mobili possono utilizzare Cisco AnyConnect™ o il client Cisco VPN per stabilire connessioni VPN basate su SSL o IPsec con le proprie sedi principali mentre si trovano presso le sedi dei clienti, in un bar o in aeroporto.

- **Connettività wireless altamente protetta:** per fornire un accesso illimitato ai dipendenti mentre si spostano all'interno dell'ufficio, modelli selezionati di Cisco serie ISA500 supportano funzionalità di mobilità altamente protetta grazie alla connettività wireless 802.11b, g e n con crittografia WPA e autenticazione 802.11x. Il rilevamento dei punti di accesso non autorizzati consente di ridurre i rischi di utenti wireless non autorizzati e di mantenere il controllo sulla propria infrastruttura di rete.
- **Gestione basata su cloud o integrata con Cisco OnPlus e l'utilità di gestione incorporata nella soluzione ISA500:** la soluzione Cisco serie ISA500 può essere gestita mediante lo strumento Security Appliance Configuration Utility, una potente interfaccia per la gestione e il monitoraggio basata su browser semplice da utilizzare. Oltre al supporto della gestione e del monitoraggio, la Configuration Utility fornisce report sulla sicurezza e sull'utilizzo della rete per consentire agli amministratori di verificare rapidamente e facilmente le attività di sicurezza e lo stato di funzionamento della rete. Il proprio partner potrà inoltre gestire la soluzione Cisco ISA500 tramite il servizio Cisco OnPlus™. Questa piattaforma basata su cloud fornisce funzionalità di rilevamento e monitoraggio per l'intera rete della piccola impresa. Consente inoltre di delegare le attività di gestione della rete al proprio partner di fiducia per potersi concentrare sulle attività aziendali principali anziché sulla gestione della rete. Cisco OnPlus inoltre offre servizi di reporting tramite le proprie funzionalità Advanced Security Services. Grazie agli Advanced Security Services, i partner possono generare report relativi alla sicurezza, all'utilizzo della rete e allo stato dei sistemi, ad esempio eventi in cui si verifica un attacco intrusivo e l'utilizzo della larghezza di banda WAN secondo un intervallo e un orario pianificati. Tali report possono essere archiviati in formato PDF e condivisi via e-mail. Nel complesso, la soluzione Cisco ISA500 fornisce una vasta gamma di funzionalità di gestione e opzioni che forniscono l'assistenza e il supporto di rete proattivo e consentono di aumentare la disponibilità di rete e di garantire serenità all'azienda.

Vantaggi per le aziende

La soluzione Cisco serie ISA500 offre funzionalità di sicurezza e connettività che consentono di:

- **Garantire la sicurezza alla propria azienda e aumentare i tempi di attività:** applicare una soluzione di sicurezza completa per proteggere i processi aziendali più importanti, quali le transazioni commerciali, i siti Web, i servizi aziendali e la comunicazione con i clienti. Un livello di sicurezza esteso consente di rendere le proprie risorse di rete più importanti accessibili, resilienti nei confronti degli attacchi e con un maggiore tempo di attività.
- **Aumentare la produttività dei dipendenti:** migliorare la produttività dei dipendenti limitando lo spam e gli spyware e controllando l'uso inappropriato del Web. Il controllo avanzato delle applicazioni consente di ridurre al minimo l'utilizzo di applicazioni non aziendali che distolgono l'attenzione.
- **Migliorare la flessibilità aziendale:** impedire le interruzioni di applicazioni e servizi "business-critical" dovute a violazioni della sicurezza mediante l'implementazione di una soluzione completa e integrata.
- **Ridurre i rischi di responsabilità:** ridurre i rischi di responsabilità per l'azienda derivanti dalla compromissione dei dati o da controlli aziendali inadeguati mediante l'applicazione di un sistema di controllo degli accessi completo e di un sistema di protezione dalle minacce impareggiabile fornito da servizi che sfruttano completamente la tecnologia Cisco SIO. Le funzioni avanzate di riduzione e monitoraggio dei rischi consentono di rispettare in modo più efficiente le normative governative e di settore, proteggere i dati dei clienti e salvaguardare le risorse umane e altri dati aziendali sensibili.
- **Ridurre i costi IT:** sgravare le risorse di supporto IT ed evitare la procedura costosa di eliminazione delle infezioni dovute a spyware, virus, attacchi sofisticati e altro malware impedendo che si verifichino.

- **Mantenere la produttività grazie all'accesso remoto sicuro:** permettere ai dipendenti e ai partner di accedere in modo più protetto alla rete da casa, in viaggio o presso filiali con un supporto VPN integrato flessibile e semplice da utilizzare. Grazie alla funzionalità di accesso remoto altamente protetto e alla protezione efficiente dei contenuti, i dipendenti possono raggiungere le persone e gli strumenti necessari in qualsiasi momento e ovunque per lavorare in modo più efficiente e rispondere più rapidamente ai clienti e ai colleghi. I dipendenti mobili possono utilizzare il client Cisco AnyConnect per fruire di un accesso VPN intelligente sempre attivo con un livello di sicurezza coerente e sensibile al contesto, tramite un laptop o uno smartphone.
- **Migliorare l'efficienza operativa:** semplificare l'installazione e ridurre i costi di monitoraggio e di gestione continui grazie a un'interfaccia intuitiva basata su browser e a sofisticate procedure guidate di configurazione.
- **Lavorare in completa tranquillità:** ottenere i massimi vantaggi dalla propria soluzione Cisco tramite un'offerta di servizio accessibile basata su abbonamento. Il servizio di assistenza Cisco Small Business estende il supporto a livello di dispositivo a tre anni, proteggendo l'investimento grazie ad aggiornamenti del software, all'accesso al centro di assistenza Cisco Small Business e alla community di supporto e alla sostituzione dell'hardware entro il giorno lavorativo successivo.

Tali vantaggi rendono la soluzione Cisco serie ISA500 la scelta ideale per soddisfare le esigenze di sicurezza e consentire alla propria rete e ai propri dipendenti di produrre il massimo per l'azienda.

Specifiche del prodotto

Table 1. Modelli e specifiche delle appliance di sicurezza Cisco Small Business serie ISA500

Funzionalità	ISA550	ISA550W	ISA570	ISA570W
Firewall				
Velocità SPI (Stateful Packet Inspection) [1]	200 Mbps	200 Mbps	500 Mbps	500 Mbps
Firewall basato su zone	Sì	Sì	Sì	Sì
Numero massimo di connessioni	15.000	15.000	40.000	40.000
Numero massimo di regole	100	100	100	100
Sessioni al secondo (cps)	2500	2500	3000	3000
Pianificazioni	Sì	Sì	Sì	Sì
Protezione da attacchi Denial-of-Service	Sì	Sì	Sì	Sì
Velocità IPS [1]	60 Mbps	60 Mbps	90 Mbps	90 Mbps
Velocità Antivirus [1]	50 Mbps	50 Mbps	80 Mbps	80 Mbps
Velocità UTM [1]	45 Mbps	45 Mbps	75 Mbps	75 Mbps
VPN				
Velocità VPN IPsec (DES [Data Encryption Standard]/3DES [Triple DES]/AES [Advanced Encryption Standard]) [1]	75 Mbps	75 Mbps	130 Mbps	130 Mbps
Tunnel Site-to-Site VPN IPsec	25	25	100	100
Tunnel di accesso remoto VPN IPsec	10	10	75	75
Tunnel VPN SSL	10	10	50	50
Crittografia	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)
Autenticazione	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)
DPD (Dead Peer Detection) IPsec	Sì	Sì	Sì	Sì
IPsec NAT (Network Address Translation) Traversal	Sì	Sì	Sì	Sì
NetBIOS Broadcast over VPN IPsec	Sì	Sì	Sì	Sì
Pass-Through VPN	IPsec/PPTP (Point-to-Point Tunneling Protocol)/L2TP (Layer 2 Tunneling Protocol)	IPsec/PPTP/L2TP	IPsec/PPTP/L2TP	IPsec/PPTP/L2TP
Supporto client Cisco VPN	Sì	Sì	Sì	Sì
Supporto modalità client Cisco VPN	Sì	Sì	Sì	Sì
Supporto modalità di estensione di rete VPN Cisco	Sì	Sì	Sì	Sì
Supporto split tunneling VPN Cisco	Sì	Sì	Sì	Sì
Supporto client VPN SSL Cisco AnyConnect	Sì	Sì	Sì	Sì
Supporto split tunneling VPN SSL	Sì	Sì	Sì	Sì
Certificati VPN SSL	Sì	Sì	Sì	Sì
Client VPN per telelavoro (client VPN con hardware Cisco)	Sì	Sì	Sì	Sì

Funzionalità	ISA550	ISA550W	ISA570	ISA570W
L2TP Server	Sì	Sì	Sì	Sì
Servizi di sicurezza				
Sistema di prevenzione delle intrusioni (IPS)	Sì	Sì	Sì	Sì
Controllo delle applicazioni	Sì	Sì	Sì	Sì
Filtro URL Web	Sì	Sì	Sì	Sì
Protezione dalle minacce Web	Sì	Sì	Sì	Sì
Anti-Phishing	Sì	Sì	Sì	Sì
Antivirus	Sì	Sì	Sì	Sì
Anti-Spyware	Sì	Sì	Sì	Sì
Filtro anti-spam	Sì	Sì	Sì	Sì
Filtro reputazione di rete	Sì	Sì	Sì	Sì
Comunicazione				
Assegnazione di indirizzi IP	Statica, DHCP (Dynamic Host Configuration Protocol), PPPoE (Point-to-Point Protocol over Ethernet), L2TP e PPTP	Statica, DHCP, PPPoE, L2Tp, PPTP	Statica, DHCP, PPPoE, L2Tp, PPTP	Statica, DHCP, PPPoE, L2Tp, PPTP
DHCP	Server e inoltro	Server e inoltro	Server e inoltro	Server e inoltro
VLAN	16	16	16	16
Trunking (802.1Q)	Sì	Sì	Sì	Sì
NAT (Network Address Translation)	Sì	Sì	Sì	Sì
Inoltro porte	Sì	Sì	Sì	Sì
Attivazione porte	Sì	Sì	Sì	Sì
Routing	Statico, RIP (Routing Information Protocol) v1, v2	Statico, RIP v1, v2	Statico, RIP v1, v2	Statico, RIP v1, v2
DMZ	Sì	Sì	Sì	Sì
Connessione Dual WAN	Sì	Sì	Sì	Sì
Bilanciamento del carico	Simmetrico	Simmetrico	Simmetrico	Simmetrico
PBR (Policy-Based Routing) (binding del protocollo)	Sì	Sì	Sì	Sì
Failover e failback integrati e automatizzati	Sì	Sì	Sì	Sì
Bilanciamento del carico ponderato	Sì	Sì	Sì	Sì
Dynamic DNS (DDNS)	Sì	Sì	Sì	Sì
Supporto VoIP (Voice over IP)	SIP, H.323, compatibile con la maggior parte dei dispositivi gateway e di comunicazione VoIP	SIP, H.323, compatibile con la maggior parte dei dispositivi gateway e di comunicazione VoIP	SIP, H.323, compatibile con la maggior parte dei dispositivi gateway e di comunicazione VoIP	SIP, H.323, compatibile con la maggior parte dei dispositivi gateway e di comunicazione VoIP
Supporto ALG SIP	Sì	Sì	Sì	Sì
Supporto ALGP H.323	Sì	Sì	Sì	Sì
Funzionalità QoS	Sì	Sì	Sì	Sì
Accodamento basato su priorità stretta	Sì	Sì	Sì	Sì
Accodamento Round Robin ponderato	Sì	Sì	Sì	Sì
Low Latency Queuing (coda di bassa latenza)	Sì	Sì	Sì	Sì
Contrassegno DSCP	Sì	Sì	Sì	Sì

Funzionalità	ISA550	ISA550W	ISA570	ISA570W
Limitazione di velocità	Sì	Sì	Sì	Sì
VRRP (Virtual Router Redundancy Protocol)	Sì	Sì	Sì	Sì
Proxy IGMP (Internet Group Management Protocol)	Sì	Sì	Sì	Sì
Snooping IGMP	Sì	Sì	Sì	Sì
Wireless				
802.11b/g/n, 2,4 GHz, 2 x 2 MIMO (Multiple Input Multiple Output)	No	Sì	No	Sì
SSID multipli	No	4	No	4
QoS (Quality of Service) WMM (Wi-Fi Multimedia)	No	Sì	No	Sì
U-APSD (Unscheduled Automatic Power Save Delivery) (WMM-PS [WMM Power Save])	No	Sì	No	Sì
Filtro MAC	No	Sì	No	Sì
WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2-PSK (Wi-Fi Protected Access Pre-Shared Key), WPA2-ENT	No	Sì	No	Sì
BSSID (Basic Service Set Identifier) o access point virtuali	No	Sì	No	Sì
Alimentazione trasmissione regolabile dinamicamente e manualmente	No	Sì	No	Sì
Wi-Fi Protected Setup (WPS)	No	Sì	No	Sì
Accesso guest	No	Sì	No	Sì
Portale captive	No	Sì	No	Sì
Rilevamento dei punti di accesso non autorizzati	No	Sì	No	Sì
Amministrazione				
Controllo automatico del firmware per verificare la disponibilità di una nuova versione	Sì	Sì	Sì	Sì
Database utente locale	100	100	100	100
Autenticazione	Locale, RADIUS, Active Directory, LDAP (Lightweight Directory Access Protocol)	Locale, RADIUS, Active Directory, LDAP	Locale, RADIUS, Active Directory, LDAP	Locale, RADIUS, Active Directory, LDAP
Diagnostica	Ping, ricerca DNS, acquisizione pacchetti	Ping, ricerca DNS, acquisizione pacchetti	Ping, ricerca DNS, acquisizione pacchetti	Ping, ricerca DNS, acquisizione pacchetti
Protocolli di rilevamento	CDP (Cisco Discovery Protocol), Bonjour, uPnP (universal Plug and Play)	CDP (Cisco Discovery Protocol), Bonjour, uPnP	CDP (Cisco Discovery Protocol), Bonjour, uPnP	CDP (Cisco Discovery Protocol), Bonjour, uPnP
Registrazione e monitoraggio	Registro locale, syslog	Registro locale, syslog	Registro locale, syslog	Registro locale, syslog
Segnalazione dello stato	Stato di utilizzo della rete, stato del servizio di sicurezza, stato funzionamento della rete	Stato di utilizzo della rete, stato del servizio di sicurezza, stato funzionamento della rete	Stato di utilizzo della rete, stato del servizio di sicurezza, stato funzionamento della rete	Stato di utilizzo della rete, stato del servizio di sicurezza, stato funzionamento della rete
Specifiche hardware				
Interfaccia totale	7 GE	7 GE	10 GE	10 GE
Porte LAN (10/100/1000)	Fino a 6	Fino a 6	Fino a 9	Fino a 9
Porte WAN (10/100/1000)	Fino a 2	Fino a 2	Fino a 2	Fino a 2

Funzionalità	ISA550	ISA550W	ISA570	ISA570W
Porta DMZ (10/100/1000)	Fino a 4	Fino a 4	Fino a 4	Fino a 4
Porte USB 2.0	1	1	1	1
Fattore di forma	1 RU, 19 pollici montabile in rack, fissabile a parete	1 RU, 19 pollici montabile in rack, fissabile a parete	1 RU, 19 pollici montabile in rack, fissabile a parete	1 RU, 19 pollici montabile in rack, fissabile a parete
Dimensioni (L x P x A)	308 mm x 180 mm x 49 mm o 12,1 pollici x 7,1 pollici x 1,9 pollici (con gommini)	308 mm x 180 mm x 49 mm o 12,1 pollici x 7,1 pollici x 1,9 pollici (con gommini)	308 mm x 180 mm x 49 mm o 12,1 pollici x 7,1 pollici x 1,9 pollici (con gommini)	308 mm x 180 mm x 49 mm o 12,1 pollici x 7,1 pollici x 1,9 pollici (con gommini)
Peso	1,2 kg	1,3 kg	1,3 kg	1,4 kg
Interruttore di accensione On/Off	Sì	Sì	Sì	Sì
Antenne	Nessuna	2	Nessuna	2
Temperatura di funzionamento ambientale	da 0 a 40°C (da 32 a 104°F)	da 0 a 40°C (da 32 a 104°F)	da 0 a 40°C (da 32 a 104°F)	da 0 a 40°C (da 32 a 104°F)
Temperatura di conservazione	da –20 a 70°C (da –4 a 158°F)	da –20 a 70°C (da –4 a 158°F)	da –20 a 70°C (da –4 a 158°F)	da –20 a 70°C (da –4 a 158°F)
Intervallo di tensione	100–240 VCA	100–240 VCA	100–240 VCA	100–240 VCA
Frequenza di ingresso	50–60 Hz	50–60 Hz	50–60 Hz	50–60 Hz
Tensione in uscita	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V
Corrente in uscita	MAX 1,667 A	MAX 1,667 A	MAX 2,5 A	MAX 2,5 A

[1] Metodologia di test delle prestazioni: prestazioni massime basate sulla metodologia RFC 2544. Tutti i risultati sono bidirezionali aggregati. Le prestazioni reali possono variare a seconda dell'ambiente di rete e delle configurazioni.

Informazioni per l'ordinazione

Table 2. Codici prodotto e di licenza di Cisco Small Business ISA500 Integration Security Appliance

Prodotto	SKU
Cisco serie 550 Integrated Security Appliance con un anno di abbonamento ai servizi di sicurezza completi	ISA550-BUN1-K9
Cisco serie 550 Integrated Security Appliance con funzionalità wireless e un anno di abbonamento ai servizi di sicurezza completi	ISA550W-BUN1-K9
Cisco serie 570 Integrated Security Appliance con un anno di abbonamento ai servizi di sicurezza completi	ISA570-BUN1-K9
Cisco serie 570 Integrated Security Appliance con funzionalità wireless e un anno di abbonamento ai servizi di sicurezza completi	ISA570W-BUN1-K9
Cisco serie 550 Integrated Security Appliance con tre anni di abbonamento ai servizi di sicurezza completi	ISA550-BUN3-K9
Cisco serie 550 Integrated Security Appliance con funzionalità wireless e tre anni di abbonamento ai servizi di sicurezza completi	ISA550W-BUN3-K9
Cisco serie 570 Integrated Security Appliance con tre anni di abbonamento ai servizi di sicurezza completi	ISA570-BUN3-K9
Cisco serie 570 Integrated Security Appliance con funzionalità wireless e tre anni di abbonamento ai servizi di sicurezza completi	ISA570W-BUN3-K9

Licenza	SKU
Abbonamento ai servizi di sicurezza completa Cisco per la serie ISA550 – 1 anno	L-ISA550-CS-1YR=
Abbonamento ai servizi di sicurezza completa Cisco per la serie ISA570 – 1 anno	L-ISA570-CS-1YR=
Abbonamento ai servizi di sicurezza completa Cisco per la serie ISA550 – 3 anni	L-ISA550-CS-3YR=
Abbonamento ai servizi di sicurezza completa Cisco per la serie ISA570 – 3 anni	L-ISA570-CS-3YR=

Assistenza e supporto

La serie Cisco Small Business ISA500 Integrated Security Appliance è supportata dal servizio di assistenza Cisco Small Business, che offre una copertura accessibile e garantisce la tranquillità totale. Questo servizio in abbonamento accessibile, include aggiornamenti software, accesso esteso al centro di assistenza Cisco Small Business e sostituzione dell'hardware entro il giorno lavorativo successivo in base alle necessità. Fornisce assistenza basata su una community per consentire la condivisione delle conoscenze e la collaborazione con colleghi mediante forum e wiki online. Il servizio di assistenza Cisco Small Business consente di ridurre i rischi, offrire un servizio migliore ai propri colleghi e ai propri clienti in totale serenità.

Ulteriori informazioni

Per ulteriori informazioni sulle appliance di sicurezza Cisco Small Business serie ISA500, visitare il sito Web all'indirizzo www.cisco.com/go/isa500resources oppure contattare il proprio fornitore Cisco locale. Per ulteriori informazioni su Cisco OnPlus, visitare il sito Web all'indirizzo www.cisco.com/en/US/products/ps11792/index.html oppure contattare il proprio fornitore Cisco locale.

Per ulteriori informazioni sul servizio di assistenza Cisco Small Business, visitare il sito Web all'indirizzo: www.cisco.com/cisco/web/solutions/small_business/services/index.html.

Sede centrale Americhe
Cisco System, Inc.
San Jose, California

Sede centrale Asia-Pacifico
Cisco Systems (USA) Pte. Ltd.
Singapore

Sede centrale Europa
Cisco Systems International BV Amsterdam,
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito web Cisco all'indirizzo **www.cisco.com/go/offices**.

Stampato negli Stati Uniti C78-717565-00 2/13