GUIDA ALL'AMMINISTRAZIONE

Router VPN multifunzione Cisco RV130

Router VPN multifunzione wireless Cisco RV130W

Aggiornato: dicembre 2016

78-21401-01

Sommario

1

Introduzione

Nella pagina **Introduzione** vengono visualizzate alcune comuni attività di configurazione del dispositivo. Fare clic sui collegamenti di questa pagina Web per passare alla pagina di configurazione pertinente.

Questa pagina viene visualizzata a ogni avvio del Device Manager. Per evitare che venga visualizzata, selezionare **Non visualizzare all'avvio**.

Impostazioni iniziali

Modifica password amministratore predefinita	Visualizza la pagina **Utenti**, in cui è possibile modificare la password dell'amministratore e configurare un account ospite. Vedere la sezione **Configurazione degli account utente**.
Avvia installazione guidata	Avvia la procedura di installazione guidata. Seguire le istruzioni visualizzate.
Configura impostazioni WAN	Apre la pagina **Configurazione Internet** in cui è possibile modificare i parametri. Ad esempio, il nome host del dispositivo. Vedere la sezione **Configurazione delle connessioni alla WAN cablata**.
Configura impostazioni LAN	Apre la pagina **Configurazione LAN** in cui è possibile modificare i parametri LAN. Ad esempio, l'indirizzo IP di gestione. Vedere la sezione **Configurazione delle impostazioni LAN**.
Configura impostazioni wireless	Apre la pagina **Impostazioni di base** in cui è possibile gestire la radio. Vedere la sezione Configurazione delle reti wireless.

Accesso rapido

Aggiorna firmware router	Apre la pagina **Aggiornamento firmware/lingua** in cui è possibile aggiornare il firmware o il pacchetto lingua del dispositivo. Vedere la sezione **Aggiornamento del firmware o modifica della lingua**.
Aggiungi client VPN	Apre la pagina **Server PPTP** in cui è possibile impostare e gestire i tunnel VPN. Vedere la sezione **Configurazione PPTP**.
Configura accesso gestione remota	Apre la pagina **Impostazioni di base** in cui è possibile abilitare le funzionalità di base del dispositivo. Vedere la sezione **Configurazione delle impostazioni firewall di base**.

Stato dispositivo

Riepilogo di sistema	Visualizza la pagina **Riepilogo di sistema** che mostra lo stato del firmware, lo stato della configurazione IPv4 e IPv6 e lo stato delle funzioni wireless e del firewall sul dispositivo. Vedere la sezione **Visualizzazione del riepilogo di sistema**.
Stato wireless	Visualizza la pagina **Statistiche wireless** che mostra lo stato della radio. Vedere la sezione **Visualizzazione delle statistiche wireless**.
Stato VPN	Visualizza la pagina **Server VPN IPsec** che elenca le VPN gestite da questo dispositivo. Vedere la sezione **Visualizzazione dello stato di connessione VPN IPsec sito a sito**.

Altre risorse

Assistenza	Fare clic per aprire la pagina dell'assistenza Cisco.
Forum	Fare clic per visitare i forum online dell'assistenza Cisco.

Collegamento alla rete wireless

Per collegare un dispositivo client, ad esempio un computer, alla rete wireless, occorre configurare la connessione wireless sul dispositivo client utilizzando le informazioni di protezione wireless che sono state configurate per il router mediante la procedura di installazione guidata.

I seguenti passaggi sono forniti a titolo esemplificativo: potrebbe essere necessario configurare il dispositivo in modo diverso. Per istruzioni specifiche, consultare la documentazione relativa al dispositivo client.

PASSAGGIO 1 Aprire la finestra con le impostazioni della connessione wireless o il programma del dispositivo.

Sul computer potrebbe essere installato un programma software speciale per gestire le connessioni wireless; in alternativa, è possibile visualizzare le connessioni wireless nel Pannello di controllo della finestra **Connessioni di rete** o **Rete e Internet** (la posizione varia a seconda del sistema operativo).

PASSAGGIO 2 Immettere il nome della propria rete (SSID) specificato durante la procedura guidata.

PASSAGGIO 3 Scegliere il tipo di crittografia e immettere la chiave di protezione definita nella procedura guidata.

Se non è stata attivata la protezione (sconsigliato), lasciare vuoti i campi relativi alla crittografia wireless configurati con il tipo di protezione e la frase chiave.

PASSAGGIO 4 Verificare la connessione wireless e salvare le impostazioni.

2

Visualizzazione dello stato del dispositivo

Per garantire che le statistiche e i dati vengano aggiornati di frequente nelle pagine relative allo stato, scegliere una frequenza di aggiornamento dall'elenco a discesa **Frequenza aggiornamento**.

Visualizzazione del Dashboard

Selezionare **Stato** > **Dashboard** per visualizzare un'istantanea della configurazione del dispositivo dell'utente. La pagina Dashboard mostra le seguenti informazioni relative al dispositivo: versione del firmware, utilizzo della CPU e della memoria, impostazioni di registrazione degli errori, LAN, WAN, wireless, VPN IPSec sito a sito e impostazioni del server PPTP VPN.

Per modificare le impostazioni visualizzate, fare clic sul collegamento **dettagli** per accedere alla pagina di configurazione della sezione. Per ulteriori informazioni sulla gestione delle impostazioni visualizzate nella pagina **Dashboard**, consultare:

- **Configurazione delle impostazioni di log**
- **Configurazione della VPN IPsec sito a sito di base**
- **Configurazione delle impostazioni LAN**
- **Configurazione delle connessioni alla WAN cablata**
- **Configurazione delle impostazioni wireless di base**

Dall'elenco a discesa **Frequenza di aggiornamento** scegliere la frequenza con cui si desidera aggiornare i valori di parametri e statistiche più recenti sul dashboard.

Facendo clic su **Mostra vista pannello**, la pagina Dashboard mostra una vista interattiva del pannello posteriore del dispositivo. Per visualizzare le informazioni di connessione per una porta, passare il cursore del mouse sopra l'immagine della porta corrispondente.

Visualizzazione del riepilogo di sistema

Selezionare **Stato** > **Riepilogo di sistema** per visualizzare i dettagli relativi alle proprietà del dispositivo, alle impostazioni di rete attraverso le modalità di indirizzo IP e alle impostazioni di firewall, wireless e VPN. Fare clic su **Aggiorna** per visualizzare le informazioni più recenti.

Fare clic sul collegamento sottolineato per accedere alla relativa finestra di configurazione. Ad esempio, per modificare l'indirizzo IP della LAN, fare clic su **IP LAN**. Viene visualizzata la finestra di configurazione LAN.

Nella pagina **Riepilogo di sistema** vengono visualizzate le seguenti informazioni:

Informazioni di sistema

- **Versione firmware**: la versione corrente del software installato sul dispositivo.
- **Checksum Firmware MD5**: l'algoritmo message-digest utilizzato per verificare l'integrità dei file.
- **Impostazioni locali**: la lingua installata sul router.
- **Versione lingua**: versione del pacchetto della lingua installato. La versione del pacchetto lingua deve essere compatibile con il software attualmente installato. In alcuni casi, è possibile utilizzare un pacchetto lingua precedente con un'immagine del firmware più recente. Il router controlla la versione del pacchetto lingua verificandone la compatibilità con la versione corrente del firmware.
- **Checksum lingua MD5**: il checksum MD5 del pacchetto lingua.
- **Modello CPU**: il chipset della CPU in uso.
- **Numero di serie**: il numero di serie del dispositivo.
- **Tempo di attività sistema**: il tempo di attività del sistema.
- **Ora corrente**: ora del giorno.
- **ID prodotto e versione**: ID del prodotto e ID della versione del dispositivo.

Configurazione IPv4

- **IP LAN**: indirizzo IP LAN del dispositivo.
- **IP WAN**: indirizzo IP WAN del dispositivo. Per rilasciare l'indirizzo IP attuale e ottenerne uno nuovo, selezionare **Rilascia** o **Rinnova**.

- **Gateway**: l'indirizzo IP del gateway a cui è connesso il router (ad esempio, il modem via cavo).
- **Modalità**: visualizza **Gateway** se il NAT è attivo o **Router**.
- **DNS 1**: indirizzo IP del server DNS primario della porta WAN.
- **DNS 2**: indirizzo IP del server DNS secondario della porta WAN.
- **DDNS**: indica se il DNS dinamico è attivato o disattivato.

Configurazione IPv6

- **IP LAN**: indirizzo IP LAN del dispositivo.
- **IP WAN**: indirizzo IP WAN del dispositivo.
- **Gateway**: l'indirizzo IP del gateway a cui è connesso il dispositivo (ad esempio, il modem via cavo).
- **NTP**: il server NTP (nome host o indirizzo IPv6).
- **Delegazione prefisso**: il prefisso restituito dal dispositivo all'ISP, che viene fornito agli indirizzi IPv6 sul dispositivo.
- **DNS 1**: l'indirizzo IP del server DNS primario.
- **DNS 2**: l'indirizzo IP del server DNS secondario.

Riepilogo wireless

Visualizza il nome pubblico e le impostazioni di sicurezza per le reti wireless configurate sulla pagina **Wireless > Impostazioni di base**. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni wireless di base**.

Stato impostazione firewall

Visualizza le impostazioni DoS, delle richieste WAN e della gestione remota configurate sulla pagina **Firewall > Impostazioni di base**. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni firewall di base**.

Stato impostazione VPN

Visualizza le connessioni IPsec e PPTP VPN disponibili e gli utenti connessi per ogni tipo di VPN.

- **Collegamenti IPsec disponibili**: il numero di collegamenti VPN IPsec disponibili.

- **Collegamenti PPTP VPN disponibili**: il numero di collegamenti PPTP VPN disponibili.
- **Utenti IPsec connessi**: il numero di utenti VPN IPsec connessi.
- **Utenti PPTP VPN connessi**: il numero di utenti PPTP VPN connessi.

Per ulteriori informazioni sulla configurazione delle connessioni server VPN e degli account utente, consultare **Configurazione della VPN IPsec sito a sito di base** e **Configurazione PPTP**.

Visualizzazione dei servizi TCP/IP attivi

Selezionare **Stato > Servizi TCP/IP attivi** per visualizzare le connessioni IPv4 e IPv6 TCP/IP attive sul dispositivo dell'utente. La sezione **Elenco servizi attivi** per IPv4 e IPv6 visualizza i protocolli e i servizi attivi sul dispositivo.

Visualizzazione delle statistiche wireless

Selezionare **Stato > Statistiche wireless** per visualizzare i dati statistici wireless della radio del dispositivo. Nel campo **Frequenza di aggiornamento**, scegliere la frequenza con cui si desidera visualizzare le statistiche più recenti sul dashboard.

Per mostrare i byte in kilobyte (KB) e i dati numerici in formato arrotondato, selezionare la casella **Mostra dati statistici semplificati** e fare clic su **Salva**. Per impostazione predefinita, i dati byte sono visualizzati in byte mentre gli altri dati numerici in formato esteso.

Per ripristinare i contatori delle statistiche wireless, fare clic su **Azzera conteggio**. I contatori vengono azzerati al riavvio del dispositivo.

Visualizzazione dello stato Captive Portal

Selezionare **Stato > Captive Portal** per visualizzare le informazioni relative agli utenti Captive Portal connessi. Per ulteriori informazioni sulla configurazione dei Captive Portal sul dispositivo, leggere **Configurazione di Captive Portal**.

Visualizzazione dello stato di connessione VPN IPsec sito a sito

Selezionare **Stato > VPN IPsec sito a sito** per visualizzare lo stato di connessione dei criteri VPN IPsec sito a sito attivi sul dispositivo. Per ulteriori informazioni sulla configurazione dei criteri VPN, consultare **Configurazione della VPN IPsec sito a sito di base**.

Per modificare la frequenza con cui visualizzare lo stato di connessione più recente e in tempo reale, selezionare la frequenza di aggiornamento dall'elenco a discesa **Frequenza di aggiornamento**.

Per impostazione predefinita, i dati byte sono visualizzati in byte mentre gli altri dati numerici in formato esteso. Per mostrare i byte in kilobyte (KB) e i dati numerici in formato arrotondato, selezionare la casella **Mostra dati statistici semplificati** e fare clic su **Salva**.

Per terminare una connessione VPN attiva, fare clic su **Disconnetti**.

Visualizzazione dello stato del server VPN IPsec

Selezionare **Stato > Server VPN IPsec** per visualizzare un elenco delle connessioni VPN IPsec e la durata della connessione. Per ulteriori informazioni sulla configurazione delle connessioni VPN IPsec, consultare **Configurazione del server VPN IPsec**.

Visualizzazione del server PPTP

Selezionare **Stato > Server PPTP** per visualizzare un elenco delle connessioni VPN PPTP, la durata delle connessioni e le azioni che è possibile eseguire per queste connessioni. Per ulteriori informazioni sulla configurazione delle connessioni PPTP VPN, consultare **Configurazione PPTP**.

Visualizzazione dei registri

Scegliere **Stato > Visualizza registri**. Fare clic su **Aggiorna registri**, per visualizzare le voci di registro più recenti.

Per filtrare i registri o specificare la gravità dei registri da visualizzare, selezionare le caselle accanto al tipo di registro e fare clic su **Vai**. Tutti i tipi di registri sopra un tipo di registro selezionato vengono inclusi automaticamente e non è possibile deselezionarli. Ad esempio, facendo clic sulla casella di controllo **Errore**, verranno inclusi automaticamente anche i registri Emergenza, Allarme e Critico.

I livelli di gravità degli eventi sono elencati dalla gravità maggiore a quella minore, come indicato di seguito:

- **Emergenza**: il sistema non è utilizzabile.
- **Allarme**: si richiede di eseguire un'azione.
- **Critico**: il sistema è in una condizione critica.
- **Errore**: il sistema è in una condizione di errore.
- **Avviso**: è stato generato un avviso di sistema.
- **Notifica**: il sistema funziona correttamente, ma è stata generata una notifica di sistema.
- **Informativo**: informazioni sul dispositivo.
- **Debug**: fornisce informazioni dettagliate su un evento.

Per eliminare tutte le voci della finestra dei registri, fare clic su **Cancella registri**.

Per salvare tutti i messaggi dei registri dal dispositivo sul disco rigido locale, fare clic su **Salva registri**.

Per specificare il numero di voci da visualizzare per ogni pagina, selezionare un numero dal menu a discesa.

Per spostarsi tra le pagine dei registri, utilizzare i pulsanti di esplorazione.

Visualizzazione dei dispositivi connessi

La pagina **Dispositivi connessi** visualizza le informazioni relative ai dispositivi client attivi connessi al router. Per visualizzare i dispositivi connessi, selezionare **Stato** > **Dispositivi connessi**.

Per specificare i tipi di interfacce da visualizzare, selezionare un valore dal menu a discesa **Filtro**.

- **Tutti**: tutti i dispositivi collegati al router.
- **Wireless**: tutti i dispositivi collegati attraverso un'interfaccia wireless.
- **Cablati**: tutti i dispositivi collegati al router attraverso le porte Ethernet.
- **WDS**: tutti dispositivi WDS (Wireless Distribution System) connessi al router.

La tabella **ARP IPv4** visualizza le informazioni dagli altri router che hanno risposto alla richiesta ARP (Address Resolution Protocol) del dispositivo. Se un dispositivo non risponde alla richiesta, viene rimosso dall'elenco.

La tabella **NDP IPv6** visualizza tutti i dispositivi NDP (Neighbor Discovery Protocol, protocollo di rilevamento adiacente) IPv6 connessi al collegamento locale del dispositivo.

Visualizzazione delle statistiche delle porte

Nella pagina **Statistiche porte** vengono visualizzate le statistiche dettagliate dell'attività delle porte.

Per visualizzare le statistiche dell'interfaccia, selezionare **Stato > Statistiche dell'interfaccia**.

Per aggiornare la pagina a intervalli regolari, selezionare la frequenza desiderata dall'elenco a discesa **Frequenza di aggiornamento**.

Per mostrare i byte in kilobyte (KB) e i dati numerici in formato arrotondato, selezionare la casella **Mostra dati statistici semplificati** e fare clic su **Salva**. Per impostazione predefinita, i dati byte sono visualizzati in byte mentre gli altri dati numerici in formato esteso.

Per ripristinare i contatori delle statistiche delle porte, fare clic su **Azzera conteggio**.

Nella pagina **Statistiche porte** vengono visualizzate le informazioni seguenti:

Interfaccia	Nome dell'interfaccia di rete.
Pacchetto	Numero di pacchetti ricevuti/inviati.
Byte	Numero di byte di informazioni ricevuti/inviati al secondo.
Errori	Numero di errori di pacchetto ricevuti/inviati.
Persi	Numero di pacchetti ricevuti/inviati che sono stati persi.
Multicast	Il numero di pacchetti multicast inviati tramite questa radio.
Collisioni	Numero di collisioni di segnale che si sono verificate su questa porta. Una collisione si verifica quando la porta tenta di inviare dati contemporaneamente ad una porta su un altro router o computer connesso alla stessa porta.

Visualizzazione dello stato della rete mobile

Le statistiche della rete mobile 3G/4G e dei dispositivi mobili (chiavette) configurati sul dispositivo.

Per visualizzare lo stato della rete mobile, selezionare **Stato > Rete mobile**. Vengono visualizzate le seguenti informazioni:

- **Connessione**: il dispositivo connesso alla rete ospite.
- **Indirizzo IP Internet**: l'indirizzo IP assegnato al dispositivo USB.
- **Subnet Mask**: subnet mask del dispositivo USB.
- **Gateway predefinito**: indirizzo IP del gateway predefinito.
- **Tempo di attività della connessione**: il tempo di attività della connessione.
- **Utilizzo della sessione corrente**: volume dei dati ricevuti (Rx) e trasmessi (Tx) sulla connessione mobile.
- **Utilizzo mensile**: utilizzo della larghezza di banda e dati scaricati mensilmente.
- **Produttore**: nome del produttore della scheda.
- **Modello scheda**: numero del modello della scheda.

- **Firmware scheda**: versione del firmware della scheda.
- **Stato SIM**: stato della scheda SIM.
- **IMS**: identificativo univoco associato agli utenti telefonici mobili della rete GSM, UMTS o LTE.
- **Gestore**: gestore della rete mobile.
- **Tipo di servizio**: tipo di servizio a cui si accede.
- **Intensità del segnale**: intensità del segnale della rete wireless mobile.
- **Stato scheda**: stato della scheda dati.

3

Configurazione della rete

Configurazione delle connessioni alla WAN cablata

La configurazione delle proprietà WAN per una rete IPv4 varia a seconda del tipo di connessione Internet di cui si dispone.

Configurazione DHCP (configurazione automatica)

Se il provider di servizi Internet (ISP) utilizza il protocollo DHCP (Dynamic Host Control Protocol) per assegnare un indirizzo IP, si riceve un indirizzo IP generato dinamicamente a ogni accesso.

Per configurare le impostazioni WAN DHCP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **WAN**.

PASSAGGIO 2 Dall'elenco a discesa **Tipo di connessione Internet**, selezionare **Configurazione automatica - DHCP**.

PASSAGGIO 3 Dall'elenco a discesa **Origine Server DNS**, selezionare uno dei seguenti modi per configurare l'indirizzo server DNS:

- Se si dispone già di indirizzi server DNS dal proprio ISP, selezionare **Utilizza questi server DNS** e immettere gli indirizzi primari e secondari.
- Se non si dispone di indirizzi server DNS dall'ISP, selezionare **Ottieni dinamicamente da ISP**.
- Per utilizzare i server DNS forniti da OpenDNS (208.67.222.222, 208.67.220.220) per risolvere gli indirizzi Web, selezionare **Usa OpenDNS**.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione dell'indirizzo IP statico

Se l'ISP ha assegnato un indirizzo IP permanente, attenersi alla seguente procedura per configurare le impostazioni WAN:

PASSAGGIO 1 Scegliere **Networking** > **WAN**.

PASSAGGIO 2 Dal menu a discesa **Tipo di connessione Internet**, selezionare **IP statico**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IP Internet	L'indirizzo IP della porta WAN.
Subnet mask	La subnet mask della porta WAN.
Origine server DNS	L'indirizzo del server DNS. Se si dispone già di indirizzi server DNS dal proprio ISP, selezionare **Utilizza questi server DNS** e immettere gli indirizzi primari e secondari nei campi **DNS statico 1** e **DNS statico 2**. Per utilizzare i server DNS forniti da OpenDNS (208.67.222.222, 208.67.220.220) per risolvere gli indirizzi Web, selezionare **Usa OpenDNS**.
Gateway predefinito	Indirizzo IP del gateway predefinito.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione PPPoE

Per configurare le impostazioni PPPoE (Point-to-Point Protocol over Ethernet), attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **WAN**.

PASSAGGIO 2 Dal menu a discesa **Tipo di connessione Internet**, selezionare **PPPoE**.

PASSAGGIO 3 Selezionare un profilo PPPoE o fare clic su **Configura profilo** per creare un nuovo profilo.

PASSAGGIO 4 Sulla pagina Profili PPPoE, immettere le seguenti informazioni (se necessario, contattare l'ISP per ottenere le informazioni di accesso PPPoE):

Nome profilo	Un nome univoco per il profilo PPPoE.
Nome utente	Il nome utente assegnato dall'ISP.
Password	La password assegnata dall'ISP.
Origine server DNS	L'indirizzo server DNS. Se si dispone già di indirizzi server DNS dal proprio ISP, selezionare **Utilizza questi server DNS** e immettere gli indirizzi primari e secondari. In caso contrario, selezionare **Ottieni dinamicamente da ISP**. Per utilizzare i server DNS forniti da OpenDNS (208.67.222.222, 208.67.220.220) per risolvere gli indirizzi Web, selezionare **Usa OpenDNS**.
Connessione su richiesta	Selezionare questa opzione se l'ISP calcola i costi sulla base della durata dei collegamenti. Se si seleziona questa opzione, la connessione Internet è attiva solo in presenza di traffico. Se la connessione rimane inattiva, vale a dire in assenza di flusso di traffico, la connessione viene chiusa. Se si fa clic su **Connessione su richiesta**, immettere il numero di minuti dopo i quali la connessione viene chiusa nel campo **Tempo massimo di inattività**.
Mantieni connessione attiva	Se si seleziona questa opzione, la connessione Internet rimane sempre attiva. Nel campo per il periodo di richiamata, immettere il numero di secondi trascorsi i quali il dispositivo tenta di riconnettersi dopo una disconnessione.

Tipo di autenticazione	**Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato. Il dispositivo restituisce le credenziali di autenticazione con il tipo di protezione inviato dal server. **PAP**: protocollo PAP (Password Authentication Protocol) utilizzato dal protocollo Point-to-Point per connettersi all'ISP. **CHAP**: il protocollo CHAP (Challenge Handshake Authentication Protocol) richiede che il client e il server debbano conoscere il testo non criptato della chiave segreta per l'utilizzo dei servizi dell'ISP. **MS-CHAP o MS-CHAPv2**: la versione Microsoft del protocollo CHAP utilizzata per accedere ai servizi dell'ISP.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione PPTP

Per configurare le impostazioni PPTP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **WAN**.

PASSAGGIO 2 Dal menu a discesa **Tipo di connessione Internet**, selezionare **PPTP**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IP Internet	L'indirizzo IP della porta WAN.
Subnet mask	La subnet mask della porta WAN.
Gateway predefinito	Indirizzo IP del gateway predefinito.
Server PPTP	L'indirizzo IP del server PPTP (Point-To-Point Tunneling Protocol).
Nome utente	Il nome utente assegnato dall'ISP.
Password	La password assegnata dall'ISP.

Connessione su richiesta	Selezionare questa opzione se l'ISP calcola i costi sulla base della durata dei collegamenti. Se si seleziona questa opzione, la connessione Internet è attiva solo in presenza di traffico. Se la connessione rimane inattiva, vale a dire in assenza di flusso di traffico, la connessione viene chiusa. Se si fa clic su **Connessione su richiesta**, immettere il numero di minuti dopo i quali la connessione viene chiusa nel campo **Tempo massimo di inattività**.
Mantieni connessione attiva	Se si seleziona questa opzione, la connessione Internet rimane sempre attiva. Nel campo **Periodo di richiamata**, immettere il numero di secondi trascorsi i quali il dispositivo tenta di riconnettersi dopo una disconnessione.
Tipo di autenticazione	Scegliere il tipo di autenticazione: **Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato. Il dispositivo restituisce le credenziali di autenticazione con il tipo di protezione inviato in precedenza dal server. **PAP**: il dispositivo utilizza il protocollo PAP (Password Authentication Protocol) per connettersi all'ISP. **CHAP**: il dispositivo utilizza il protocollo CHAP (Challenge Handshake Authentication Protocol) per connettersi all'ISP. **MS-CHAP o MS-CHAPv2**: il dispositivo utilizza il protocollo MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) per la connessione all'ISP.
Nome servizio	Immettere un nome per il nuovo servizio PPTP.
Crittografia MPPE	Selezionare la casella di controllo **Attiva** per abilitare la crittografia MPPE (Microsoft Point-to-Point Encryption) per la connessione PPTP.

Origine server DNS	L'indirizzo server DNS. Se si dispone già di indirizzi server DNS dal proprio ISP, selezionare **Utilizza questi server DNS** e immettere gli indirizzi primari e secondari nei campi **DNS statico 1** e **DNS statico 2**. Per ottenere gli indirizzi dei server DNS dall'ISP, selezionare **Ottieni dinamicamente da ISP**. Per utilizzare i server DNS forniti da OpenDNS (208.67.222.222, 208.67.220.220) per risolvere gli indirizzi Web, selezionare **Usa OpenDNS**.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione L2TP

Per configurare le impostazioni L2TP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **WAN**.

PASSAGGIO 2 Dal menu a discesa **Tipo di connessione Internet**, selezionare **L2TP**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IP Internet	L'indirizzo IP della porta WAN.
Subnet mask	La subnet mask della porta WAN.
Gateway predefinito	L'indirizzo IP del gateway predefinito.
Server L2TP	L'indirizzo IP del server L2TP.
Versione	La versione L2TP che si desidera utilizzare. Se si utilizza la versione 3, inserire l'ID del fornitore e l'ID del circuito virtuale.
Lunghezza cookie	La dimensione del cookie nel pacchetto di dati L2TP v3, che identifica la sessione L2TP.

ID fornitore	L'ID del fornitore contenuto nel formato di codifica AVP per L2TP. Per utilizzare i valori di attributo adottati da IETF nell'AVP, selezionare Standard. Per implementare le estensioni L2TP di Cisco e i valori di attributo privati, selezionare Cisco.
ID circuito virtuale	L'identificatore del circuito di Livello 2 su cui vengono trasportati i pacchetti di dati L2TP. Questa informazione è obbligatoria se si seleziona Cisco come **ID fornitore** per L2TP v3.
Nome utente	Immettere il nome utente assegnato dall'ISP.
Password	Immettere la password assegnata dall'ISP.
Connessione su richiesta	Selezionare questa opzione se l'ISP calcola i costi sulla base della durata dei collegamenti. Se si seleziona questa opzione, la connessione Internet è attiva solo in presenza di traffico. Se la connessione rimane inattiva, vale a dire in assenza di flusso di traffico, la connessione viene chiusa. Se si fa clic su **Connessione su richiesta**, immettere il numero di minuti dopo i quali la connessione viene chiusa nel campo **Tempo massimo di inattività**.
Mantieni connessione attiva	Se si seleziona questa opzione, la connessione Internet rimane sempre attiva. Nel campo per il periodo di richiamata, immettere il numero di secondi trascorsi i quali il dispositivo tenta di riconnettersi dopo una disconnessione.

Tipo di autenticazione	**Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato. Il dispositivo restituisce le credenziali di autenticazione con il tipo di protezione inviato dal server. **PAP**: il protocollo PAP (Password Authentication Protocol) viene utilizzato per connettersi all'ISP. **CHAP**: il protocollo CHAP (Challenge Handshake Authentication Protocol) viene utilizzato per connettersi all'ISP. **MS-CHAP o MS-CHAPv2**: il protocollo MS- CHAP (Microsoft Challenge Handshake Authentication Protocol) viene utilizzato per connettersi all'ISP.
Nome servizio	Immettere un nome per il nuovo servizio L2TP.
Crittografia MPPE	Selezionare **Attiva** per abilitare la crittografia MPPE (Microsoft Point-to-Point Encryption) per la connessione L2TP.
Origine server DNS	L'indirizzo server DNS. Se si dispone già di indirizzi server DNS dal proprio ISP, selezionare **Utilizza questi server DNS** e immettere gli indirizzi primari e secondari nei campi **Server DNS primario** e **Server DNS secondario**. Per ottenere gli indirizzi server DNS dall'ISP, selezionare **Ottieni dinamicamente da ISP**. Per utilizzare i server DNS forniti da OpenDNS (208.67.222.222, 208.67.220.220) per risolvere gli indirizzi Web, selezionare **Usa OpenDNS**.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle impostazioni di rete opzionali

Per configurare le impostazioni opzionali, attenersi alla seguente procedura:

PASSAGGIO 1 In **Impostazioni facoltative**, configurare le seguenti opzioni:

MTU	La MTU (Maximum Transmission Unit) indica la dimensione del pacchetto più grande che è possibile inviare tramite la rete. A meno che l'ISP non faccia richiesta di modifica, Cisco consiglia di selezionare l'opzione **Auto**. Le dimensioni predefinite della MTU sono di 1500 byte. Se l'ISP richiede un'impostazione MTU personalizzata, selezionare **Manuale** e immettere le dimensioni MTU.
Dimensioni	Le dimensioni MTU personalizzate. Il valore MTU predefinito per reti Ethernet è solitamente 1500 byte. Per le connessioni PPPoE questo valore è di 1492 byte.
VLAN senza tag	Selezionare la casella per attivare il tag VLAN. Se la casella è attivata (impostazione predefinita), tutto il traffico sarà contrassegnato con un ID VLAN. Tutto il traffico sul dispositivo utilizza per impostazione predefinita la VLAN 1, la VLAN predefinita senza tag. Tutto il traffico non presenta alcun tag se la VLAN senza tag non viene disattivata e non vengono modificati l'ID VLAN del traffico senza tag o l'ID VLAN.
ID VLAN senza tag	Un numero da 1 a 4094 per l'ID VLAN senza tag. Il valore predefinito è 1. Quando viene inoltrato alla rete, il traffico sulla VLAN specificato in questo campo non presenta un tag con un ID VLAN. VLAN 1 è la VLAN senza tag predefinita.

VLAN gestione access point	La VLAN associata all'indirizzo IP utilizzato per accedere al dispositivo, quando è configurato come access point. Se si creano VLAN aggiuntive, per motivi di sicurezza, selezionare un valore corrispondente alla VLAN configurata sugli altri switch della rete. Potrebbe essere necessario modificare la VLAN di gestione per limitare l'accesso a Device Manager.

PASSAGGIO 2 Fare clic su **Salva**.

Configurazione di una rete mobile

Selezionare **Rete > WAN > Rete mobile** per configurare il dispositivo in modo che si connetta al modem USB mobile a banda larga connesso alla sua interfaccia USB.

Configurazione delle impostazioni della rete mobile globali

Per configurare le impostazioni globali dei dispositivi USB supportati:

PASSAGGIO 1 Collegare il modem USB. Se il modem è supportato, verrà automaticamente rilevato e visualizzato nella pagina Rete mobile.

PASSAGGIO 2 Selezionare la modalità di connessione **Automatica** o **Manuale** Il ripristino della connessione Ethernet funziona soltanto se la modalità di connessione è automatica.

- Per consentire al modem di stabilire automaticamente una connessione, selezionare la modalità **Auto**. Se si seleziona Auto, impostare un tempo per **Connetti su richiesta** oppure selezionare **Mantieni connessione attiva**. Connetti su richiesta conclude la connessione Internet dopo il periodo di inattività specificato nel campo **Tempo massimo di inattività**.

  Se la connessione Internet viene interrotta per inattività il modem stabilirà nuovamente una connessione non appena l'utente proverà ad accedere a Internet. Nel campo **Tempo di inattività massimo**, immettere il numero di minuti che devono trascorrere prima che la connessione Internet venga interrotta. Selezionare **Mantieni connessione attiva**, per mantenere sempre attiva la connessione.

- Per eseguire manualmente la disconnessione e la connessione del modem, selezionare la modalità **Manuale**.

Il dispositivo visualizza lo stato attuale della connessione del modem, che comprende inizializzazione, connessione, disconnessione o disconnesso.

PASSAGGIO 3 Verificare che il campo **Stato scheda** della scheda mobile sia impostato su **Connesso**.

Configurazione manuale delle impostazioni di rete mobile

Per modificare i parametri di rete mobile nell'area **Configurazione della rete mobile**, fare clic sul pulsante di opzione **Manuale**. Il dispositivo rileva automaticamente i modem supportati ed elenca i corretti parametri di configurazione. Per annullare i parametri globali, selezionare **Manuale**.

PASSAGGIO 1 Inserire le informazioni nei seguenti campi:

Campo	Descrizione
APN (Access Point Name)	La rete Internet a cui è connesso il dispositivo mobile. Inserire il nome dell'access point fornito dal provider della rete mobile. Se non si conosce il nome dell'access point, contattare il provider.
Numero di composizione	Il numero di composizione fornito dal service provider della rete mobile per la connessione Internet.
Nome utente Password	Il nome utente e la password forniti dal provider della rete mobile.
Verifica SIM	Attivazione o disattivazione del controllo della scheda SIM.
PIN della SIM	Il codice PIN associato alla scheda SIM. Il campo viene visualizzato soltanto per le schede SIM GSM. Il PIN della SIM può essere modificato sia in modalità manuale che automatica.
Nome server	Il nome del server per la connessione a Internet (se fornito dal provider).

Campo	Descrizione
Autenticazione	L'autenticazione utilizzata dal provider. Questo valore può essere modificato scegliendo il tipo di autenticazione dall'elenco a discesa. L'impostazione predefinita è Auto. Se non si conosce il tipo di autenticazione da usare, selezionare Auto.
Tipo di servizio	Il tipo di connessione ai servizi dati mobili più diffuso in base al segnale di servizio della zona. Se nella postazione attuale è disponibile un solo servizio dati mobile, è possibile limitare l'opzione preferita riducendo i tempi di configurazione della connessione. La prima selezione cerca un servizio HSPDA/3G/UMTS e passa automaticamente in GPRS, se disponibile.
Servizio LTE	Impostazione del servizio LTE (Long-term Evolution). **Automatico** consente di scegliere un segnale in base al segnale di servizio della zona. **Solo 4G** ricerca solo segnali 4G. **Solo 3G** ricerca soltanto i segnali 3G.

PASSAGGIO 2 Fare clic su **Salva** per salvare le impostazioni.

Impostazione limite larghezza di banda

Il dispositivo esegue il monitoraggio dell'attività dati di collegamento di rete mobile e invia una notifica al raggiungimento di una determinata soglia.

Per abilitare o disabilitare "Tracciamento limite larghezza di banda" e impostare i limiti:

PASSAGGIO 1 Selezionare **Abilitato** o **Disabilitato**.

PASSAGGIO 2 Selezionare la data di rinnovo mensile dall'elenco a discesa per indicare il giorno del mese in cui vengono reimpostati i limiti della larghezza di banda.

PASSAGGIO 3 Nel campo **Limite mensile larghezza di banda**, inserire la quantità massima di dati in megabyte che è possibile trasferire prima che il dispositivo intraprenda azioni, come l'invio di un'e-mail a un amministratore.

Impostazione e-mail

Una volta raggiunto il limite della larghezza di banda, è possibile inviare un'e-mail all'amministratore. Per impostare l'indirizzo di e-mail di destinazione, vedere la sezione **Configurazione invio dei registri tramite e-mail**.

Dopo aver selezionato la casella, un'e-mail verrà inviata:

- Quando l'utilizzo della rete mobile supera una percentuale prestabilita.
- Quando il dispositivo esegue il failover sul percorso di backup e avvia il ripristino.
- A ogni intervallo specificato in cui un collegamento di rete mobile è attivo.

Impostazione di failover e ripristino

Anche se sono disponibili collegamento di rete mobile o Ethernet, per stabilire un collegamento WAN è possibile utilizzare una sola connessione alla volta. In caso di problemi con una connessione WAN, il dispositivo tenterà di eseguire la connessione con un'altra interfaccia. Questa funzionalità si chiama Failover. Al ripristino della connessione principale WAN, verrà ripristinato il percorso originario e terminata la connessione di backup. Questa funzione si chiama Ripristino.

PASSAGGIO 1 Selezionare **Networking > WAN > Failover e ripristino**, per visualizzare la finestra di Failover e ripristino.

PASSAGGIO 2 Selezionare **Attiva Failover a WAN 3G** per attivare collegamento di rete mobile e impostarlo su failover dal collegamento Ethernet. Quando il collegamento WAN Ethernet non è attivo, il dispositivo tenta di attivare il collegamento di rete mobile sull'interfaccia USB. Se il failover non è abilitato, il collegamento di rete mobile sarà sempre disattivato.

PASSAGGIO 3 Selezionare **Abilita ripristino WAN Ethernet** per consentire al collegamento di tornare al collegamento Ethernet, abbandonando il collegamento di rete mobile. La modalità di connessione **WAN > Rete mobile** deve essere impostata su Auto per utilizzare la funzionalità di ripristino della connessione WAN Ethernet.

PASSAGGIO 4 Nel campo **Intervallo controllo failover,** inserire il tempo (in secondi), trascorso il quale il dispositivo deve tentare di rilevare la connessione fisica o la presenza di traffico del collegamento di rete mobile. Se il collegamento è inattivo, a questo intervallo il dispositivo tenterà di eseguire un ping verso la destinazione. Se il pacchetto di ping non riceve risposta, il dispositivo considererà interrotto il collegamento e proverà a utilizzare l'interfaccia WAN Ethernet.

PASSAGGIO 5 Nel campo **Intervallo controllo ripristino,** inserire il tempo (in secondi), trascorso il quale il dispositivo deve tentare di rilevare la connessione fisica o la presenza di traffico del collegamento WAN Ethernet. Se il collegamento è inattivo, a questo intervallo il dispositivo tenterà di eseguire un ping verso la destinazione. In caso di risposta al pacchetto ping, il dispositivo considererà attivo il collegamento e tenterà di disabilitare il collegamento alla rete mobile per poi abilitare la WAN Ethernet.

PASSAGGIO 6 Fare clic su **Tornare immediatamente a Ethernet quando disponibile.** o fare clic su **Tornare a Ethernet in un intervallo di tempo specifico** e inserire l'intervallo di tempo relativo.

PASSAGGIO 7 Nel campo **Sito convalida connessione**, selezionare il sito da cui eseguire la convalida del failover. Utilizzare il gateway dell'hop successivo (per impostazione predefinita il dispositivo esegue il ping sul gateway predefinito) o selezionare un sito personalizzato e inserire l'indirizzo IPv4 o IPv6 del sito.

PASSAGGIO 8 Fare clic su **Salva** per salvare le impostazioni.

La tabella "Interfaccia WAN" visualizza lo stato della WAN Ethernet e di collegamento di rete mobile su Internet. Per visualizzare i dettagli della porta, fare clic sul collegamento ipertestuale **Stato**.

Configurazione delle impostazioni LAN

Le impostazioni DHCP e TCP/IP predefinite funzionano per la maggior parte delle applicazioni. Se si desidera impostare un altro PC della rete come server DHCP o se si desidera configurare manualmente le impostazioni di rete di tutti i dispositivi, disattivare il DHCP.

Inoltre, invece di utilizzare un server DNS, che esegue la mappatura dei nomi di dominio Internet, come www.cisco.com, a numeri IP, è possibile utilizzare un server WINS (Windows Internet Naming Service). Un server WINS è l'equivalente di un server DNS, ma utilizza il protocollo NetBIOS per risolvere i nomi degli host. Il dispositivo include l'indirizzo IP del server WINS nella configurazione DHCP che invia ai client DHCP.

Quando il dispositivo è connesso ad un modem o a un altro dispositivo con una rete configurata sulla stessa sottorete (192.168.1.x), cambia automaticamente la sottorete LAN in una sottorete casuale basata su 10.x.x.x in modo da evitare conflitti con la sottorete sul lato WAN del router .

Modifica dell'indirizzo IP di gestione dispositivo

L'indirizzo IP per la gestione del dispositivo locale del dispositivo è statico ed è 192.168.1.1 per impostazione predefinita.

Per modificare l'indirizzo IP di gestione del dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **Configurazione LAN**.

PASSAGGIO 2 Nella sezione **IPv4**, immettere le seguenti informazioni:

VLAN	Numero della rete VLAN.
Indirizzo IP locale	Indirizzo IP LAN del dispositivo. Verificare che l'indirizzo IP non sia utilizzato da un altro dispositivo.
Subnet mask	La subnet mask dell'indirizzo IP locale. La subnet mask predefinita è 255.255.255.0.

PASSAGGIO 3 Fare clic su **Salva**.

Dopo avere modificato l'indirizzo IP del dispositivo, il PC non è più in grado di visualizzare il Device Manager.

Per visualizzare il Device Manager, eseguire una delle seguenti operazioni:

- Se sul router è configurato DHCP, rilasciare e rinnovare l'indirizzo IP del PC.
- Assegnare un indirizzo manuale al PC. L'indirizzo deve trovarsi nella stessa sottorete del dispositivo. Ad esempio, se si modifica l'indirizzo IP del dispositivo in 10.0.0.1, assegnare al PC un indirizzo IP nell'intervallo compreso tra 10.0.0.2 e 10.0.0.255.

Aprire una finestra del browser e immettere il nuovo indirizzo IP per collegarsi nuovamente al dispositivo.

Configurazione del server DHCP

Per impostazione predefinita, il dispositivo agisce da server DHCP per gli host della WLAN (Wireless LAN) o LAN cablata. Il dispositivo può assegnare indirizzi IP e server DNS.

Una volta abilitato DHCP, il dispositivo assegna indirizzi IP ai dispositivi di rete della LAN da un pool di indirizzi IPv4. Il dispositivo testa ogni indirizzo prima che venga assegnato per evitare la presenza di indirizzi duplicati sulla LAN.

Il pool di indirizzi IP predefinito va da 192.168.1.100 a 192.168.1.149. Per impostare un indirizzo IP statico su un dispositivo di rete, utilizzare un indirizzo IP non compreso nel pool. Ad esempio, supponendo che il pool DHCP sia impostato con i parametri predefiniti, è possibile utilizzare gli indirizzi IP statici compresi fra 192.168.1.2 e 192.168.1.99 per evitare conflitti con il pool di indirizzi IP DHCP.

Per configurare le impostazioni DHCP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **Configurazione LAN**.

PASSAGGIO 2 (Opzionale) Selezionare la VLAN da modificare dall'elenco a discesa.

PASSAGGIO 3 Nel campo **Server DHCP**, selezionare una delle seguenti opzioni:

Attiva	Consente al dispositivo di agire come server DHCP sulla rete.
Disattiva	Disabilita DHCP sul dispositivo per configurare manualmente gli indirizzi IP di tutti i dispositivi di rete.
Inoltro DHCP	Inoltra gli indirizzi IP assegnati da un altro server DHCP ai dispositivi di rete.

Se il server DHCP del dispositivo è abilitato, inserire queste informazioni:

Indirizzo IP iniziale	Il primo indirizzo presente nel pool di indirizzi IP. Qualsiasi client DHCP che accederà alla LAN riceverà un indirizzo IP estratto da questo intervallo.
Numero massimo di utenti DHCP	Il numero massimo di client DHCP.

Intervallo indirizzi IP	(Solo lettura) L'intervallo di indirizzi IP disponibili per i client DHCP.
Durata lease client	La durata (in ore) del lease degli indirizzi IP ai client.
DNS statico 1	Indirizzo IP del server DNS primario.
DNS statico 2	Indirizzo IP del server DNS secondario.
DNS statico 3	Indirizzo IP del server DNS terziario.
WINS	Indirizzo IP del server WINS primario.

PASSAGGIO 4 Se è stata selezionata l'opzione **Inoltro DHCP**, immettere l'indirizzo del gateway di inoltro nel campo **Server DHCP remoto**. Il gateway di inoltro trasmette messaggi di DHCP ai dispositivi di rete, compresi quelli presenti su altre sottoreti.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione delle VLAN

Una VLAN (Virtual LAN) è un gruppo di punti terminali di una rete, associati per funzione o altre caratteristiche condivise. A differenza delle LAN, che hanno solitamente un fondamento geografico, le VLAN possono raggruppare punti terminali senza tenere in considerazione la posizione fisica delle apparecchiature degli utenti.

Il dispositivo dispone di una VLAN predefinita (VLAN 1) che non può essere eliminata. È possibile creare fino a quattro ulteriori VLAN sul dispositivo.

Per creare una VLAN, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **Appartenenza VLAN**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Immettere le seguenti informazioni:

ID VLAN	L'ID VLAN numerico per assegnare i punti terminali dell'appartenenza VLAN. Immettere un numero compreso tra 3 e 4094. L'ID VLAN 1 è riservato alla VLAN predefinita, che viene utilizzata per i frame senza tag ricevuti sull'interfaccia.
Descrizione	Una descrizione che identifica la VLAN.
Porta 1 **Porta 2** **Porta 3** **Porta 4**	È possibile associare le VLAN sul dispositivo alle porte LAN del dispositivo. Per impostazione predefinita, tutte le porte LAN appartengono alla VLAN1. È possibile modificare queste porte per associarle ad altre VLAN. Scegliere il tipo di frame in uscita per ciascuna porta: **Senza tag**: l'interfaccia è un membro senza tag della VLAN. I frame della VLAN vengono inviati senza tag alla porta VLAN. **Con tag**: la porta è un membro con tag della VLAN. I frame della VLAN vengono inviati con tag alla porta VLAN. **Escluso**: la porta al momento non è un membro della VLAN. Questa è l'impostazione predefinita per tutte le porte quando viene creata la VLAN.

PASSAGGIO 4 Fare clic su **Salva**.

Per modificare le impostazioni di una VLAN, selezionare la VLAN e fare clic su **Modifica**. Per eliminare una VLAN selezionata, fare clic su **Elimina**. Fare clic su **Salva** per applicare le modifiche.

Configurazione di DHCP statico

È possibile configurare il dispositivo in modo da assegnare un indirizzo IP specifico ad un dispositivo con un indirizzo MAC specifico.

Per configurare DHCP statico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **DHCP statico**.

PASSAGGIO 2 Dal menu a discesa **VLAN**, selezionare un numero di VLAN.

PASSAGGIO 3 Fare clic su **Aggiungi riga**.

PASSAGGIO 4 Immettere le seguenti informazioni:

Descrizione	La descrizione del client.
Indirizzo IP	L'indirizzo IP che si desidera assegnare al dispositivo client. L'indirizzo IP assegnato deve essere esterno al pool di indirizzi DHCP. Nell'assegnazione statica di DHCP, il server DHCP assegna lo stesso IP all'indirizzo MAC definito ogni volta che questo dispositivo client viene connesso alla rete. Il server DHCP assegna l'indirizzo IP riservato quando il dispositivo client che utilizza l'indirizzo MAC corrispondente richiede un indirizzo IP.
Indirizzo MAC	L'indirizzo MAC del dispositivo client. Il formato dell'indirizzo MAC è XX:XX:XX:XX:XX:XX in cui X è un numero da 0 a 9 (inclusi) o una lettera compresa tra la A e la F (incluse).

Per modificare le impostazioni di un client DHCP statico, selezionare il client e fare clic su **Modifica**. Per eliminare un DHCP statico selezionato, fare clic su **Elimina**. Fare clic su **Salva** per applicare le modifiche.

Visualizzazione dei client DHCP in leasing

È possibile visualizzare un elenco di tutti i punti terminali su una rete (identificati da nome host, indirizzo IP o MAC) e vedere gli indirizzi IP assegnati loro dal server DHCP. Viene visualizzata anche la VLAN dei punti terminali.

Per visualizzare i client DHCP, selezionare **Networking** > **LAN** > **Client DHCP in leasing**.

Per ogni VLAN definita sul dispositivo, una tabella mostra un elenco dei client associati alla VLAN.

Per assegnare un indirizzo IP statico a uno dei dispositivi connessi:

PASSAGGIO 1 Nella riga dei dispositivi collegati, selezionare la casella **Aggiungi al DHCP statico**.

PASSAGGIO 2 Fare clic su **Salva**.

Il server DHCP sul router assegna sempre l'indirizzo IP mostrato quando il dispositivo richiede un indirizzo IP.

Configurazione di un host DMZ

Il dispositivo supporta zone demilitarizzate (DMZ). Una zona demilitarizzata o DMZ è una sottorete aperta al pubblico, ma che si trova dietro al firewall. Una rete DMZ consente di reindirizzare i pacchetti che arrivano all'indirizzo IP della porta WAN ad un indirizzo IP specifico della LAN.

Si consiglia di posizionare gli host che devono essere esposti alla WAN, ad esempio il server Web o di posta, nella rete DMZ. È possibile configurare le regole del firewall per consentire l'accesso a servizi e a porte specifiche nella rete DMZ sia dalla LAN che dalla WAN. Nel caso di attacchi su uno qualsiasi dei nodi DMZ, la LAN non è necessariamente vulnerabile.

È necessario configurare un indirizzo IP fisso (statico) per l'endpoint designato come host DMZ. È necessario assegnare all'host DMZ un indirizzo IP, che si deve trovare nella stessa sottorete dell'indirizzo IP del router ma non può essere identico all'indirizzo IP assegnato all'interfaccia LAN di questo gateway.

Per configurare la rete DMZ, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **Hosting DMZ**.

PASSAGGIO 2 Selezionare la casella **Attiva** per attivare la DMZ sulla rete.

PASSAGGIO 3 Dal menu a discesa **VLAN**, selezionare l'ID della VLAN sulla quale è attivato DMZ.

PASSAGGIO 4 Nel campo **Indirizzo IP host,** immettere l'indirizzo IP dell'host DMZ. L'host DMZ è il punto terminale che riceve i pacchetti reindirizzati.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione RSTP

RSTP (Rapid Spanning Tree Protocol) è un protocollo di rete che previene i loop nella rete e riconfigura dinamicamente i canali fisici che devono inoltrare i frame. Per configurare il protocollo RTSP (Rapid Spanning Tree Protocol), attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **LAN** > **RSTP**.

PASSAGGIO 2 Immettere le seguenti informazioni:

Priorità di sistema	Selezionare la priorità di sistema dal menu a discesa. È possibile selezionare una priorità di sistema compresa tra 0 e 61440 con incrementi di 4096. I valori validi sono 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 e 61440. Più bassa è la priorità di sistema, più probabilità ci sono che il router diventi la radice dello spanning tree. L'impostazione predefinita è **327688**.
Hello Time	Il tempo di attesa costituisce il periodo di tempo atteso dalla radice dello spanning tree prima di inviare messaggi di saluto. Immettere un numero compreso tra 1 e 10. Il valore predefinito è **2**.
Tempo massimo	Il tempo massimo rappresenta il periodo di tempo atteso dal router per ricevere un messaggio di saluto. Se si raggiunge il tempo massimo, il router tenta di modificare lo spanning tree. Immettere un numero compreso tra 6 e 40. Il valore predefinito è **20**.

Ritardo reindirizzamento	Il ritardo di reindirizzamento è l'intervallo dopo il quale un'interfaccia passa da condizione di blocco a reindirizzamento. Immettere un numero compreso tra 4 e 30. Il valore predefinito è **15**.
Forza versione	Selezionare la versione del protocollo predefinito da utilizzare. Selezionare **Normale** (utilizzo di RSTP) o **Compatibile** (compatibile con il vecchio STP). L'impostazione predefinita è **Normale**.

PASSAGGIO 3 Nella **tabella delle impostazioni**, configurare le seguenti impostazioni:

Attiva protocollo	Selezionare questa opzione per attivare RSTP sulla porta associata. RSTP è disattivato per impostazione predefinita.
Edge	Selezionare questa opzione per specificare che la porta associata è una porta edge (stazione terminale). Deselezionare questa opzione per specificare che la porta associata è un collegamento (bridge) a un altro dispositivo STP. L'opzione Edge per la porta è attiva per impostazione predefinita.
Costo del percorso	Immettere il costo di percorso RSTP per le porte designate. Utilizzare 0 per il valore predefinito (il dispositivo determina automaticamente il valore del percorso). È anche possibile immettere un numero compreso tra 2 e 200000000.

PASSAGGIO 4 Fare clic su **Salva**.

Gestione delle porte

È possibile configurare le impostazioni di velocità e di controllo del flusso delle porte LAN del dispositivo.

Per configurare la velocità e il controllo del flusso delle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **Gestione porte**.

PASSAGGIO 2 Configurare le informazioni seguenti:

Porta	Il numero della porta.
Collegamento	La velocità della porta. Se alla porta non sono collegati dispositivi, in questo campo viene mostrato **Disattivato**.
Modalità	Selezionare dal menu a discesa una delle seguenti quattro velocità di porta: • **Negoziazione automatica**: il dispositivo e il dispositivo connesso scelgono una velocità comune. • **10Mbps Half**: 10 Mbps in entrambe le direzioni, ma solo una direzione alla volta. • **10Mbps Full**: 10 Mbps in entrambe le direzioni simultaneamente. • **100Mbps Half**: 100 Mbps in entrambe le direzioni, ma solo una direzione alla volta. • **100Mbps Full**: 100 Mbps in entrambe le direzioni simultaneamente.
Frame jumbo	Attivare Frame jumbo sul dispositivo per inviare frame all'interno della LAN contenenti fino a 9.000 byte di dati per frame. Un frame Ethernet standard contiene 1.500 byte di dati.
Controllo flusso	Selezionare questa opzione per attivare il controllo di flusso per la porta. Il controllo di flusso è il processo di gestione della frequenza di trasmissione dati tra due nodi per prevenire che un trasmettitore veloce trasmetta più velocemente di quanto possa ricevere un ricevitore lento. Fornisce un meccanismo che permette al ricevitore di controllare la velocità di trasmissione, in modo che il nodo di ricezione non venga sopraffatto con dati dal nodo di trasmissione.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione di Link Aggregation

Utilizzare la pagina Link Aggregation per raggruppare più collegamenti Ethernet in un singolo canale logico. I gruppi di Link Aggregation migliorano la convenienza del dispositivo a livello di costo aumentando la larghezza di banda senza dover richiedere aggiornamenti di hardware, inoltre facilitano il reindirizzamento in caso di una singola porta o guasto del cavo.

Per assegnare le porte a un gruppo di Link Aggregation, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking > LAN > Link Aggregation**. La sezione **Stato delle porte** visualizza la modalità associata a ciascuna porta sul dispositivo e lo stato.

PASSAGGIO 2 Nella sezione **Tabella impostazioni Link Aggregation**, selezionare la casella per ogni porta da includere nel gruppo.

PASSAGGIO 3 Fare clic su **Salva**.

Clonazione dell'indirizzo MAC

A volte può essere necessario impostare lo stesso indirizzo MAC per la porta WAN del dispositivo e il PC o un indirizzo MAC identico a un altro indirizzo MAC. Questa procedura viene denominata clonazione dell'indirizzo MAC.

Ad esempio, alcuni ISP registrano l'indirizzo MAC della scheda del computer durante l'installazione del servizio. Se si posiziona un router dietro al modem via cavo o DSL, l'indirizzo MAC della porta WAN del dispositivo non viene riconosciuto dall'ISP.

In questo caso, per configurare il dispositivo affinché venga riconosciuto dall'ISP, è possibile clonare l'indirizzo MAC della porta WAN in modo che sia identico a quello del computer.

Per configurare un clone di indirizzo MAC, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Clona indirizzo MAC**.

PASSAGGIO 2 Nel campo **Clona indirizzo MAC**, selezionare **Attiva**.

PASSAGGIO 3 Per impostare l'indirizzo MAC della porta WAN del dispositivo, attenersi alla seguente procedura:

- Per utilizzare l'indirizzo MAC del PC come indirizzo MAC della porta WAN, fare clic su **Clona indirizzo MAC del PC**.
- Per specificare un indirizzo MAC diverso, immettere l'indirizzo desiderato nel campo **Indirizzo MAC**.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione del routing

Utilizzare la pagina Routing per configurare la modalità operativa e altre opzioni di routing per il dispositivo.

Configurazione della modalità operativa

Per configurare la modalità operativa del dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Routing**.

PASSAGGIO 2 Nel campo **Modalità operativa,** selezionare una delle seguenti opzioni:

Gateway	Per impostare il dispositivo come gateway. (Consigliato) Mantenere questa impostazione predefinita se il dispositivo ospita la connessione di rete a Internet e svolge le funzioni di routing.
Router	(Solo per utenti avanzati) Fare clic su questo pulsante per impostare il dispositivo come router. Selezionare questa opzione se il dispositivo si trova su una rete con altri router. Se si attiva la modalità router, la funzionalità NAT (Network Address Translation) viene disattivata sul dispositivo.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione del routing dinamico

Il protocollo RIP (Routing Information Protocol) è un protocollo IGP (Interior Gateway Protocol) utilizzato comunemente nelle reti interne. Questo protocollo consente al router di scambiare automaticamente le informazioni di routing con altri router; consente, inoltre, di regolare in modo dinamico le tabelle di routing e adattarsi alle modifiche della rete.

Il routing dinamico (RIP) consente al dispositivo di regolarsi automaticamente alle modifiche fisiche nella disposizione della rete e scambiare le tabelle di routing con gli altri router.

Il router determina il percorso dei pacchetti di rete con il minor numero di hop tra l'origine e la destinazione.

NOTA La funzione RIP è disattivata per impostazione predefinita sul dispositivo.

Per configurare il routing dinamico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Routing**.

PASSAGGIO 2 Configurare le seguenti impostazioni:

RIP	Selezionare **Attiva** per attivare RIP. Questo consente al dispositivo di utilizzare la funzione RIP per il routing del traffico.
Versione pacchetto RIP Invia	Sezionare la versione pacchetto RIP Invia (**RIPv1** o **RIPv2**). La versione di RIP utilizzata per inviare gli aggiornamenti di routing agli altri router della rete dipende dalle impostazioni di configurazione degli altri router. RIPv2 è compatibile all'indietro con RIPv1.
Versione pacchetto RIP Ricevi	Scegliere la versione pacchetto RIP Ricevi.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione del routing Inter-VLAN

Per consentire a una stazione terminale in una VLAN di comunicare con una stazione terminale in un'altra VLAN, selezionare la casella di controllo **Attivazione routing inter-VLAN**.

Configurazione del routing statico

È possibile configurare i percorsi statici per indirizzare i pacchetti alla rete di destinazione. Un percorso statico è un percorso predeterminato che un pacchetto deve percorrere per raggiungere un host o una rete specifica.

Alcuni ISP richiedono percorsi statici invece dei protocolli di routing dinamico per creare la tabella di routing. I percorsi statici non richiedono risorse della CPU per lo scambio di informazioni di routing con un router paritetico.

È inoltre possibile utilizzare i percorsi statici per raggiungere i router paritetici che non supportano i protocolli di routing dinamico. I percorsi statici possono essere utilizzati insieme a quelli dinamici. Il dispositivo supporta fino a 30 percorsi statici.

Fare attenzione a non introdurre loop di routing nella rete.

Per configurare il routing statico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Routing**.

PASSAGGIO 2 Dal menu a discesa **Voci percorso**, selezionare una voce percorso.

Per eliminare una voce percorso, fare clic su **Elimina voce**.

PASSAGGIO 3 Configurare le impostazioni seguenti per la voce percorso selezionata:

Immettere il nome del percorso	Immettere il nome del percorso.
IP LAN destinazione	Immettere l'indirizzo IP della LAN di destinazione.
Subnet mask	Immettere la subnet mask della rete di destinazione.
Gateway	Immettere l'indirizzo IP del gateway utilizzato per questo percorso.

Interfaccia	Selezionare l'interfaccia alla quale sono inviati i pacchetti per questo percorso: • **LAN e wireless**: fare clic su questo pulsante per indirizzare i pacchetti verso la rete LAN e wireless. • **Internet (WAN)**: fare clic su questo pulsante per indirizzare i pacchetti verso la rete Internet (WAN).

PASSAGGIO 4 Fare clic su **Salva**.

Visualizzazione della tabella di routing

Nella tabella di routing sono contenute le informazioni sulla topologia della rete presente.

Per visualizzare le informazioni di routing della rete, fare clic su **Networking** > **Tabella di routing** e scegliere una delle seguenti opzioni:

- **Mostra tabella routing IPv4**: la tabella di routing viene visualizzata con i campi configurati nelle pagine **Networking** > **Routing**.
- **Mostra tabella routing IPv6**: la tabella di routing viene visualizzata con i campi configurati nella pagina **Networking** > **IPv6**.

Configurazione di DNS dinamico

DDNS (Dynamic DNS) è un servizio Internet che consente di localizzare i router che dispongono di IP pubblici variabili utilizzando i nomi di dominio Internet. Per utilizzare il servizio DDNS è necessario creare un account con un fornitore di servizi DDNS, ad esempio DynDNS.com, TZO.com, 3322.org o noip.com.

Il router notifica ai server del servizio DNS dinamico i cambiamenti dell'indirizzo IP WAN, in modo da permettere l'accesso ai servizi pubblici della rete tramite il nome di dominio.

Per configurare il servizio DDNS, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **DNS dinamico**.

PASSAGGIO 2 Scegliere l'**Intervallo di aggiornamento** dall'elenco a discesa.

PASSAGGIO 3 La sezione **Tabella servizi DDNS** indica i servizi DDNS che è possibile attivare sul dispositivo.

PASSAGGIO 4 Selezionare la casella di controllo dei servizi che si desidera attivare e fare clic su **Modifica**.

PASSAGGIO 5 Selezionare la casella di controllo **Attiva** per attivare il servizio.

PASSAGGIO 6 Configurare le informazioni seguenti:

Nome utente/indirizzo e-mail	Il nome utente dell'account DDNS o l'indirizzo e-mail utilizzati per creare l'account DDNS.
Password	Password per l'account DDNS.
Nome dominio/host	Il nome host del server DDNS o il nome del dominio utilizzato per accedere alla rete.
Indirizzo IP Internet	(Solo lettura) L'indirizzo IP Internet del dispositivo.
Stato	(Solo lettura) Indica se l'aggiornamento del servizio DDNS è stato completato correttamente o se l'invio al server DDNS delle informazioni di aggiornamento dell'account non è riuscito.

PASSAGGIO 7 Fare clic su **Test configurazione**, per testare la configurazione DDNS.

PASSAGGIO 8 Fare clic su **Salva**.

Configurazione della modalità IP

Le proprietà di configurazione della WAN possono essere definite sia per reti IPv4 che per reti IPv6. In queste pagine è possibile immettere informazioni relative alla connessione Internet e altri parametri.

Per selezionare una modalità IP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **Modalità IP**.

PASSAGGIO 2 Dal menu a discesa **Modalità IP**, selezionare una delle seguenti opzioni:

LAN:IPv4, WAN:IPv4	Per utilizzare IPv4 sulle porte LAN e WAN.
LAN:IPv6, WAN:IPv4	Per utilizzare IPv6 sulle porte LAN e IPv4 sulle porte WAN.
LAN:IPv6, WAN:IPv6	Per utilizzare IPv6 sulle porte LAN e WAN.
LAN:IPv4+IPv6, WAN:IPv4	Per utilizzare IPv4 e IPv6 sulle porte LAN e IPv4 sulle porte WAN.
LAN:IPv4+IPV6, WAN:IPv4+IPv6	Per utilizzare IPv4 e IPv6 sulle porte LAN e WAN.
LAN:IPv4, WAN:IPv6	Per utilizzare IPv4 sulle porte LAN e IPv6 sulle porte WAN.

PASSAGGIO 3 (Opzionale) Se si sta utilizzando il tunneling 6to4, che permette la trasmissione di pacchetti IPv6 su una rete IPv4, procedere come segue:

a. Fare clic su **Mostra voce DNS 6to4 statico**.

b. Nei campi **Dominio** e **IP**, immettere fino a cinque mappature dominio-IP.

La funzione di tunneling 6to4 viene solitamente utilizzata quando un sito o un utente finale desidera connettersi a Internet IPv6 utilizzando la rete IPv4 esistente.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione di IPv6

IPv6 (Internet Protocol version 6) è la versione del protocollo Internet (IP) designata a sostituire IPv4. La configurazione delle proprietà WAN per una rete IPv6 varia a seconda del tipo di connessione Internet di cui si dispone.

Configurazione della connessione WAN IPv6

È possibile configurare il dispositivo per agire da client DHCPv6 dell'ISP per questa WAN o utilizzare un indirizzo IPv6 statico fornito dall'ISP.

Per configurare le impostazioni IPv6 WAN sul dispositivo, è necessario impostare prima la modalità IP su una delle seguenti modalità:

- LAN:IPv6, WAN:IPv6
- LAN:IPv4+IPv6, WAN:IPv4
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

Per ottenere istruzioni sulle modalità di configurazione della modalità IP, vedere la sezione **Configurazione della modalità IP**.

Configurazione SLAAC

Per assegnare automaticamente un indirizzo basato su prefisso IPv6, configurare il dispositivo in modo che utilizzi la SLAAC (configurazione automatica indirizzo stateless) per l'assegnazione dell'indirizzo client IPv6.

Per utilizzare SLAAC, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione WAN IPv6**.

PASSAGGIO 2 Nel campo **Tipo di connessione WAN**, selezionare SLAAC. Per DHCP "stateless" non è necessario un server DHCPv6 presso l'ISP. Al contrario, un messaggio di rilevamento ICMPv6 avrà origine dal dispositivo e verrà utilizzato per la configurazione automatica.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione di DHCPv6

Se l'ISP fornisce un indirizzo dinamico, configurare il dispositivo come client DHCPv6.

Per configurare il dispositivo come client DHCPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione WAN IPv6**.

PASSAGGIO 2 Nel campo **Tipo di connessione WAN**, selezionare **Configurazione automatica - DHCPv6**. Il gateway si connette al server DHCPv6 dell'ISP per ottenere un indirizzo in lease.

PASSAGGIO 3 Per automatizzare l'assegnazione di prefissi al dispositivo (client DHCP), selezionare il pulsante di opzione **Attivazione delegazione prefisso**.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione di un indirizzo IPv6 WAN statico

Se l'ISP assegna un indirizzo fisso per l'accesso alla WAN, configurare il dispositivo per l'utilizzo di un indirizzo IPv6 statico.

Per configurare un indirizzo IPv6 statico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione WAN IPv6**.

PASSAGGIO 2 Nel campo **Tipo di connessione WAN**, selezionare **IPv6 statico**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Indirizzo IPv6	Indirizzo IPv6 della porta WAN.
Lunghezza prefisso IPv6	Lunghezza di prefisso IPv6 (di solito definita dall'ISP). La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Tutti gli host della sottorete utilizzano lo stesso prefisso. Ad esempio, nell'indirizzo IPv6 `2001:0DB8:AC10:FE01::` il prefisso è `2001`.
Gateway IPv6 predefinito	Indirizzo IPv6 del gateway predefinito. Di solito si tratta dell'indirizzo IP del server presso l'ISP.
DNS statico 1	Indirizzo IP del server DNS IPv6 primario.
DNS statico 2	Indirizzo IP del server DNS IPv6 secondario.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle impostazioni PPPoE IPv6

È possibile utilizzare IPv4 PPPoE, IPv6 PPPoE o entrambi. Se utilizzano entrambi, le impostazioni IPv6 WAN PPPoE devono corrispondere a quelle IPv4 WAN PPPoE. Se non corrispondono, verrà visualizzato un messaggio che richiede di impostare il protocollo IPv6 in modo che corrisponda a quello IPv4. Leggere **Configurazione PPPoE**.

Per configurare le impostazioni IPv6 PPPoE, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione WAN IPv6**.

PASSAGGIO 2 Nel campo **Tipo di connessione WAN**, scegliere **IPv6 PPPoE**.

PASSAGGIO 3 Immettere le seguenti informazioni (se necessario, contattare l'ISP per ottenere le informazioni di accesso PPPoE):

Nome utente	Nome utente assegnato dall'ISP.
Password	Password assegnata dall'ISP.
Connessione su richiesta	Se l'ISP calcola i costi sulla base della durata dei collegamenti, selezionare il pulsante di opzione. Se si seleziona questa opzione, la connessione Internet sarà attiva solo in presenza di traffico. Se la connessione rimane inattiva, vale a dire in assenza di flusso di traffico, la connessione viene chiusa. Nel campo **Tempo massimo di inattività**, inserire il numero di minuti trascorsi senza che venga rilevato traffico sul collegamento prima che quest'ultimo venga interrotto.
Mantieni connessione attiva	Mantiene attivo il collegamento WAN inviando un messaggio di mantenimento della connessione attiva attraverso la porta. Nel campo per il periodo di richiamata, immettere il numero di secondi trascorsi i quali il dispositivo tenta di riconnettersi dopo una disconnessione.

Tipo di autenticazione	Tipi di autenticazione: **Negoziazione automatica**: il server invia una richiesta di configurazione specificando l'algoritmo di protezione impostato sul server. Il dispositivo risponde con le proprie credenziali di autenticazione, tra cui il tipo di protezione inviato in precedenza dal server. **PAP**: utilizzo del protocollo PAP (Password Authentication Protocol) per connettersi all'ISP. **CHAP**: utilizzo del protocollo CHAP (Challenge Handshake Authentication Protocol) per connettersi all'ISP. **MS-CHAP or MS-CHAPv2**: utilizzo del protocollo MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) per connettersi all'ISP.
Nome servizio	Nome che potrebbe essere richiesto dall'ISP per eseguire l'accesso al server PPPoE.
MTU	La MTU (Maximum Transmission Unit) indica la dimensione del pacchetto più grande che è possibile inviare tramite la rete. A meno che l'ISP non faccia richiesta di modifica, Cisco consiglia di selezionare l'opzione **Auto**. Il valore di MTU standard per le reti Ethernet è di 1500 byte. Per le connessioni PPPoE questo valore è di 1492 byte. Se l'ISP richiede un'impostazione MTU personalizzata, selezionare **Manuale.**
Dimensioni	Dimensione MTU. Se l'ISP richiede un'impostazione MTU personalizzata, immettere le dimensioni MTU.
Modalità indirizzi	Modalità indirizzi statici o dinamici. Se si seleziona l'opzione statica, immettere l'indirizzo IPv6 nel campo successivo.
Lunghezza prefisso IPv6	Lunghezza prefisso IPv6.
Gateway IPv6 predefinito	Indirizzo IP del gateway IPv6 predefinito.
DNS statico 1	Indirizzo IP del server DNS primario.
DNS statico 2	Indirizzo IP del server DNS secondario.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle connessioni LAN IPv6

Nella modalità IPv6 il server DHCP LAN è attivato per impostazione predefinita (analogamente alla modalità IPv4). Il server DHCPv6 assegna gli indirizzi IPv6 dai pool di indirizzi configurati che utilizzano la lunghezza di prefisso IPv6 assegnata alla LAN.

Per configurare le impostazioni IPv6 LAN sul dispositivo, è necessario impostare prima la modalità IP su una delle seguenti modalità.

- LAN:IPv6, WAN:IPv4
- LAN:IPv6, WAN:IPv6
- LAN:IPv4+IPv6, WAN:IPv4
- LAN:IPv4+IPv6, WAN:IPv4+IPv6

Per ulteriori informazioni su come impostare la modalità IP, vedere la sezione **Configurazione della modalità IP**.

Per configurare le impostazioni LAN IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Configurazione LAN IPv6**.

PASSAGGIO 2 Immettere le seguenti informazioni per configurare l'indirizzo IPv6 LAN:

Indirizzo IPv6	Immettere l'indirizzo IPv6 del dispositivo. L'indirizzo IPv6 predefinito del gateway è fec0::1 (or FEC0:0000:0000:0000:0000:0000:0000:0001). È possibile modificare questo indirizzo IPv6 a 128 bit in base ai requisiti di rete.
Lunghezza prefisso IPv6	Immettere la lunghezza del prefisso IPv6. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Il prefisso è lungo 64 bit per impostazione predefinita. Tutti gli host della rete hanno bit iniziali identici per l'indirizzo IPv6; in questo campo viene impostato il numero di bit iniziali comuni degli indirizzi di rete.

PASSAGGIO 3 Fare clic su **Salva** o continuare la configurazione delle impostazioni LAN DHCP IPv6.

PASSAGGIO 4 Immettere le seguenti informazioni per configurare le impostazioni DHCPv6:

Stato DHCP	Selezionare questa opzione per attivare il server DHCPv6. Se l'opzione è attivata, il dispositivo assegna un indirizzo IP nell'intervallo specificato, con l'aggiunta di informazioni specifiche, a qualsiasi punto terminale LAN che richiede indirizzi DHCP.
Nome dominio	(Opzionale) Nome di dominio del server DHCPv6.
Preferenza server	Livello di preferenza per il server DHCP. I messaggi di annuncio DHCP con il valore di preferenza server più alto rispetto a un host LAN sono preferiti rispetto ad altri messaggi di annuncio server DHCP. L'impostazione predefinita è 255.
DNS statico 1	Indirizzo IPv6 del server DNS primario sulla rete IPv6 dell'ISP.
DNS statico 2	Indirizzo IPv6 del server DNS secondario sulla rete IPv6 dell'ISP.
Durata lease client	Durata (in secondi) del lease degli indirizzi IPv6 ai punti terminali della LAN.

PASSAGGIO 5 Selezionare **Networking** > **IPv6** > **Configurazione LAN IPv6**.

PASSAGGIO 6 Nella **Tabella pool indirizzi IPv6**, fare clic su **Aggiungi riga**.

PASSAGGIO 7 Immettere le informazioni seguenti:

Indirizzo iniziale	Indirizzo IPv6 iniziale del pool.
Indirizzo finale	Indirizzo IPv6 finale del pool.
Lunghezza prefisso IPv6	Lunghezza del prefisso che definisce il numero di bit iniziali comuni negli indirizzi di rete.

PASSAGGIO 8 Fare clic su **Salva**.

Per modificare le impostazioni di un pool, selezionare il pool e fare clic su **Modifica**. Per eliminare un pool selezionato, fare clic su **Elimina**. Fare clic su **Salva** per applicare le modifiche.

Configurazione del routing statico IPv6

È possibile configurare i percorsi statici per indirizzare i pacchetti alla rete di destinazione. Un percorso statico è un percorso predeterminato che un pacchetto deve percorrere per raggiungere un host o una rete specifica.

Alcuni ISP richiedono percorsi statici invece dei protocolli di routing dinamico per creare la tabella di routing. I percorsi statici non richiedono risorse della CPU per lo scambio di informazioni di routing con un router paritetico.

È inoltre possibile utilizzare i percorsi statici per raggiungere i router paritetici che non supportano i protocolli di routing dinamico. I percorsi statici possono essere utilizzati insieme a quelli dinamici. Fare attenzione a non introdurre loop di routing nella rete.

Per creare un percorso statico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking**> **IPv6** > **IPv6 Routing statico**.

PASSAGGIO 2 Nell'elenco dei percorsi statici, fare clic su **Aggiungi riga**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Nome	Nome percorso.
Destinazione	Indirizzo IPv6 dell'host o della rete di destinazione per il percorso.
Lunghezza prefisso	Numero di bit prefisso nell'indirizzo IPv6 che definisce la sottorete di destinazione.
Gateway	Indirizzo IPv6 del gateway attraverso il quale è possibile raggiungere l'host o la rete di destinazione.
Interfaccia	Interfaccia del percorso: **LAN**, **WAN** o **6to4**.
Metrica	Priorità del percorso. Selezionare un valore tra 2 e 15. Se esistono più percorsi per la stessa destinazione, verrà utilizzato il percorso con il costo più basso.

Attivo	Selezionare questa opzione per attivare il percorso. Quando si aggiunge un percorso non attivo, questo viene elencato nella tabella dei percorsi, ma non viene utilizzato dal dispositivo. Può essere utile inserire un percorso inattivo se quest'ultimo non è disponibile al momento dell'aggiunta. Quando la rete diventa disponibile, è possibile attivare il percorso.

PASSAGGIO 4 Fare clic su **Salva**.

Per modificare le impostazioni di un percorso, selezionare il percorso e fare clic su **Modifica**. Per eliminare un percorso selezionato, fare clic su **Elimina**. Fare clic su **Salva** per applicare le modifiche.

Configurazione del routing (RIPng)

RIPng (RIP Next Generation) è un protocollo di routing basato sull'algoritmo del vettore di distanza-(D-V). Il protocollo RIPng utilizza i pacchetti UDP per scambiare informazioni di routing attraverso la porta 521.

Il protocollo RIPng utilizza il numero di hop per misurare la distanza da una destinazione. Il numero di hop viene definito metrica o costo. Il numero di hop da un router a una rete connessa direttamente è 0. Il numero di hop tra due router connessi direttamente è 1. Se il numero di hop è maggiore o uguale a 16, la rete o l'host di destinazione non è raggiungibile.

L'aggiornamento di routing viene inviato ogni 30 secondi per impostazione predefinita. Se il router non riceve aggiornamenti di routing da un dispositivo adiacente dopo 180 secondi, i percorsi appresi dal dispositivo adiacente sono considerati non raggiungibili. Se dopo altri 240 secondi non si ricevono aggiornamenti di routing, il router rimuove questi percorsi dalla tabella di routing.

Sul dispositivo, il protocollo RIPng è disattivato per impostazione predefinita.

Per configurare il protocollo RIPng, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Routing (RIPng)**.

PASSAGGIO 2 Selezionare **Attiva**.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione del tunneling

Il tunneling IPv6-to-IPv4 (tunneling 6-to-4) consente la trasmissione di pacchetti IPv6 su una rete IPv4. Il tunneling IPv4-to-IPv6 (tunneling 4-to-6) consente la trasmissione di pacchetti IPv4 su una rete IPv6.

Tunneling 6to4

6Il tunneling 6-to-4 viene solitamente utilizzato quando un sito o un utente finale desidera connettersi a Internet IPv6 utilizzando la rete IPv4 esistente.

Per configurare il tunneling 6-to-4, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **IPv6** > **Tunneling**.

PASSAGGIO 2 Nel campo **Tunneling 6to4**, selezionare **Attiva**.

PASSAGGIO 3 Selezionare il tipo di tunneling:

- **6to4**
- **6RD** (implementazione rapida)
- **ISATAP** (Intra-Site Automatic Tunnel Addressing Protocol). Selezionare **Automatico** o **Manuale**.

PASSAGGIO 4 Per il tunneling 6RD, scegliere **Automatico** o **Manuale**. Se è stata selezionata l'opzione **Manuale**, immettere le informazioni seguenti:

- **Prefisso IPv6**
- **Lunghezza prefisso IPv6**
- **Inoltro bordo**
- **Lunghezza maschera IPv4**

PASSAGGIO 5 Per il tunneling ISATAP, scegliere **Automatico** o **Manuale**. Se è stata selezionata l'opzione **Manuale**, immettere le informazioni seguenti:

- **Prefisso IPv6**
- **Lunghezza prefisso IPv6**

PASSAGGIO 6 Fare clic su **Salva**.

Tunneling 4to6

Per configurare il tunneling 4to6, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **IPv6** > **Tunneling**.

PASSAGGIO 2 Nel campo **Tunneling 4to6**, selezionare la casella **Attiva**.

PASSAGGIO 3 Immettere l'indirizzo IPv6 WAN locale nel dispositivo.

PASSAGGIO 4 Immettere l'indirizzo IPv6 remoto o l'indirizzo IP dell'endpoint remoto.

PASSAGGIO 5 Fare clic su **Salva**.

Visualizzazione dello stato del tunnel IPv6

Per visualizzare lo stato del tunnel IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Networking** > **IPv6** > **Stato tunnel IPv6**.

PASSAGGIO 2 Fare clic su **Aggiorna** per visualizzare le informazioni più recenti.

In questa pagina vengono visualizzate informazioni relative alla configurazione automatica del tunnel tramite interfaccia WAN dedicata. Nella tabella vengono mostrati il nome del tunnel e l'indirizzo IPv6 creati sul dispositivo.

Configurazione dell'annuncio router

Il Router Advertisement Daemon (RADVD) sul dispositivo ascolta le sollecitazioni del router sulla LAN IPv6 e risponde con annunci del router come richiesto. Si tratta di una configurazione automatica IPv6 stateless e il dispositivo distribuisce prefissi IPv6 a tutti i nodi presenti sulla rete.

Per configurare RADVD, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **IPv6** > **Annuncio router**.

PASSAGGIO 2 Immettere le informazioni seguenti:

Stato RADVD	Selezionare **Attiva** per attivare RADVD.
Modalità annuncio	Selezionare una delle seguenti modalità: **Multicast non richiesto**: inviare annunci del router (RA) a tutte le interfacce che appartengono al gruppo multicast. **Solo Unicast**: includere solo gli annunci relativi a indirizzi IPv6 noti (gli RA vengono inviati all'interfaccia appartenente esclusivamente a indirizzi noti).
Intervallo annuncio	Intervallo di annuncio (4-1800) per **Multicast non richiesto**. Il valore predefinito è 30. L'intervallo di annuncio è un valore casuale tra l'intervallo di annuncio router minimo (MinRtrAdvInterval) e l'intervallo di annuncio router massimo (MaxRtrAdvInterval). MinRtrAdvInterval = 0,33 * MaxRtrAdvInterval
Flag RA	Selezionare **Gestito** per utilizzare il protocollo stateful/gestito per la configurazione automatica degli indirizzi. Selezionare **Altro** per utilizzare il protocollo stateful/gestito di un'altra configurazione automatica di informazioni non relative a indirizzi.

Preferenza router	Selezionare dal menu a discesa **basso**, **medio** o **alto**. L'impostazione predefinita è medio. La preferenza router fornisce una metrica di preferenza per i router predefiniti. I valori basso, medio e alto vengono segnalati nei bit inutilizzati dei messaggi RA. Questa estensione è compatibile all'indietro, sia per i router (impostazione del valore di preferenza router) che per gli host (interpretazione del valore di preferenza router). Questi valori sono ignorati dagli host che non implementano la preferenza router. Si tratta di una funzione utile se nella LAN sono presenti altri dispositivi abilitati per RADVD.
MTU	Dimensione MTU (0 oppure da 1280 a 1500). L'impostazione predefinita è 1500 byte. La MTU (Maximum Transmission Unit) indica la dimensione del pacchetto più grande che è possibile inviare tramite la rete. Il valore MTU viene utilizzato negli RA per garantire che tutti i nodi della rete utilizzino lo stesso valore MTU quando il valore MTU della LAN non è noto.
Durata router	Valore di durata del router, ovvero la durata, in secondi, dei messaggi di annuncio sul percorso. L'impostazione predefinita è 3600 secondi.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione dei prefissi annuncio

Per configurare i prefissi annuncio RADVD disponibili, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Networking** > **IPv6** > **Prefissi annuncio**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Immettere le informazioni seguenti:

Tipo di prefisso IPv6	Scegliere uno dei tipi seguenti: **6to4**: consente la trasmissione di pacchetti IPv6 su una rete IPv4. Viene solitamente utilizzato quando un sito o un utente finale desidera connettersi a Internet IPv6 utilizzando la rete IPv4 esistente. **Globale/Locale**: un indirizzo IPv6 univoco localmente che può essere utilizzato su reti IPv6 private oppure un indirizzo Internet IPv6 univoco a livello globale.
ID SLA	Se si seleziona **6to4** come tipo di prefisso IPv6, immettere l'ID SLA (Site-Level Aggregation Identifier). L'ID SLA nel prefisso di indirizzo 6to4 viene impostato sull'ID dell'interfaccia sulla quale sono inviati gli annunci.
Prefisso IPv6	Se si seleziona **Globale/Locale** come tipo di prefisso IPv6, immettere il prefisso IPv6. Il prefisso IPv6 specifica l'indirizzo di rete IPv6.
Lunghezza prefisso IPv6	Se si seleziona **Globale/Locale** come tipo di prefisso IPv6, immettere la lunghezza del prefisso. La variabile di lunghezza del prefisso è un valore decimale che indica il numero di bit di ordine superiore adiacenti dell'indirizzo che costituiscono la porzione di rete dell'indirizzo.
Durata prefisso	Durata del prefisso, ovvero l'intervallo di tempo durante il quale il router che effettua la richiesta è autorizzato a utilizzare il prefisso.

PASSAGGIO 4 Fare clic su **Salva**.

4

Configurazione delle reti wireless

Sicurezza per reti wireless

Le reti wireless sono comode e semplici da installare. Ma poiché le reti wireless utilizzano le onde radio per l'invio delle informazioni, sono più vulnerabili agli attacchi di intrusi rispetto alle tradizionali reti cablate.

Suggerimenti per la protezione delle reti wireless

Pur non essendo possibile impedire fisicamente ad altri utenti di connettersi alla propria rete wireless, è possibile adottare le seguenti precauzioni per rendere la rete più sicura:

- Modificare il nome di rete wireless o il SSID predefinito.

  I dispositivi wireless sono dotati di un nome di rete wireless o SSID predefinito. Si tratta del nome della rete wireless e può essere costituito da un massimo di 32 caratteri.

  Per proteggere la rete, modificare il nome di rete predefinito con un nome univoco che permetta di distinguere la rete wireless da altre reti wireless circostanti.

  Quando si sceglie un nome, non utilizzare informazioni personali, dato che queste informazioni potrebbero essere visibili a chiunque cerchi reti wireless.

- Modificare la password predefinita.

  Per modificare le impostazioni di prodotti wireless, come access point, router e gateway, viene chiesto di immettere una password. Questi dispositivi sono dotati di una password predefinita. La password predefinita è spesso **cisco**.

  Gli hacker conoscono questi valori predefiniti e possono provare ad utilizzarli per accedere al dispositivo wireless in questione e modificare le impostazioni della rete corrispondente. Per impedire l'accesso non autorizzato, personalizzare la password del dispositivo applicandone una più complessa.

- Attivare il filtro degli indirizzi MAC.

  I router e gateway Cisco offrono la possibilità di attivare il filtro degli indirizzi MAC. L'indirizzo MAC è una serie univoca di numeri e lettere assegnata a ciascun dispositivo di rete.

  Se il filtro degli indirizzi MAC è attivo, l'accesso alla rete wireless è consentito solo ai dispositivi wireless con indirizzi MAC specifici. Ad esempio, è possibile specificare l'indirizzo MAC di ogni computer della rete in modo che solo quei computer possano accedere alla rete wireless.

- Attivare la crittografia.

  La crittografia protegge i dati trasmessi su una rete wireless. WPA/WPA2 (Wi-Fi Protected Access) e WEP (Wired Equivalency Privacy) offrono diversi livelli di protezione per la comunicazione wireless. Attualmente, i dispositivi con certificazione Wi-Fi devono supportare WPA2, ma non hanno l'obbligo di supportare WEP.

  Una rete crittografata con WPA/WPA2 è più sicura di una rete crittografata con WEP, poiché WPA/WPA2 utilizza la crittografia con chiavi dinamiche.

  Per proteggere le informazioni durante la trasmissione sulle onde radio, attivare il livello massimo di crittografia supportato dalle proprie apparecchiature di rete.

  WEP è uno standard di crittografia meno recente e può essere l'unica opzione disponibile su alcuni dispositivi obsoleti che non supportano lo standard WPA.

- Tenere i router, gli access point o i gateway distanti dalle pareti esterne e dalle finestre.

- Quando non sono in uso (ad esempio di notte o durante le vacanze), spegnere i router, gli access point o i gateway.

- Utilizzare sempre frasi chiave con almeno otto caratteri di lunghezza. Combinare lettere e numeri per evitare l'utilizzo di parole standard che possono essere trovate in un dizionario.

Linee guida generali per la sicurezza di rete

La protezione della rete wireless non serve a nulla se la rete sottostante non è sicura. Cisco consiglia di adottare le seguenti precauzioni:

- Proteggere mediante password tutti i computer della rete e i singoli file contenenti informazioni riservate.

- Modificare le password a intervalli regolari.

- Installare software antivirus e software firewall personale.
- Disattivare la condivisione dei file (peer-to-peer) per impedire l'utilizzo della condivisione dei file da parte delle applicazioni senza autorizzazione.

Reti wireless sul dispositivo

Il dispositivo fornisce quattro reti wireless virtuali, ovvero quattro SSID (Service Set Identifier): ciscosb1, ciscosb2, ciscosb3 e ciscosb4. Si tratta dei nomi predefiniti o SSID per queste reti, tuttavia è possibile modificarli e sostituirli con nomi più significativi. In questa tabella sono riportate le impostazioni predefinite di queste reti:

Nome SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Attivata	Sì	No	No	No
Trasmissione SSID	Attivata	Disattivata	Disattivata	Disattivata
Modalità di protezione	Disattivata[1]	Disattivata	Disattivata	Disattivata
Filtro MAC	Disattivata	Disattivata	Disattivata	Disattivata
VLAN	1	1	1	1
Isolamento wireless con SSID	Disattivata	Disattivata	Disattivata	Disattivata
WMM	Attivata	Attivata	Attivata	Attivata
Pulsante hardware WPS	Attivata	Disattivata	Disattivata	Disattivata

1. Nell'Installazione guidata, selezionare Protezione massima o Protezione elevata per proteggere il dispositivo dall'accesso non autorizzato.

Configurazione delle impostazioni wireless di base

Selezionare **Wireless** > **Impostazioni di base** per configurare le impostazioni wireless di base.

Per configurare le impostazioni di base wireless, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Wireless** > **Impostazioni di base**.

PASSAGGIO 2 Nel campo **Radio**, selezionare la casella **Attiva** per attivare la radio wireless. Per impostazione predefinita è attivata una sola rete wireless, **ciscosb1**.

PASSAGGIO 3 Nel campo **Modalità rete wireless**, selezionare una delle opzioni seguenti dal menu a discesa:-

Combinazione B/G/N	Selezionare questa opzione se la rete è composta da dispositivi Wireless-N, Wireless-B e Wireless-G. Questa è l'impostazione predefinita (consigliata).
Solo B	Selezionare questa opzione se la rete è composta solo da dispositivi Wireless-B.
Solo G	Selezionare questa opzione se la rete è composta solo da dispositivi Wireless-G.
Solo N	Selezionare questa opzione se la rete è composta solo da dispositivi Wireless-N.
Combinazione B/G	Selezionare questa opzione se la rete è composta da dispositivi Wireless-B e Wireless-G.
Combinazione G/N	Selezionare questa opzione se la rete è composta da dispositivi Wireless-G e Wireless-N.

PASSAGGIO 4 Se si sceglie **Combinazione B/G/N**, **Solo N** o **Combinazione G/N** nel campo **Selezione banda wireless**, selezionare la larghezza di banda della rete (**20 MHz** or **20/40 MHz**). Se è stata selezionata l'opzione Solo N, sulla rete è necessario utilizzare la protezione WPA2. Vedere la sezione **Configurazione della modalità di protezione**.

PASSAGGIO 5 Nel campo **Canale wireless**, selezionare il canale wireless dal menu a discesa.

PASSAGGIO 6 Nel campo **VLAN di gestione AP**, selezionare **VLAN 1** se si utilizzano le impostazioni predefinite.

Se si creano VLAN aggiuntive, selezionare un valore corrispondente alla VLAN configurata sugli altri switch della rete. Questo viene fatto per motivi di sicurezza. Potrebbe essere necessario modificare la VLAN di gestione per limitare l'accesso a Device Manager.

PASSAGGIO 7 (Opzionale) Nel campo **U-APSD (risparmio energia WMM)**, selezionare **Attiva** per attivare la funzione U-APSD (Unscheduled Automatic Power Save Delivery), denominata anche risparmio energia WMM, che permette alla radio di conservare energia.

U-APSD è un sistema di risparmio energetico ottimizzato per applicazioni in tempo reale, come VoIP, con trasferimento di dati full-duplex su WLAN. Con la classificazione del traffico IP in uscita come dati Voce, questi tipi di applicazioni possono aumentare la durata della batteria di circa il 25% riducendo al minimo i ritardi di trasmissione.

PASSAGGIO 8 (Opzionale) Configurare le impostazioni delle quattro reti wireless (vedere la sezione **Modifica delle impostazioni della rete wireless**).

PASSAGGIO 9 Fare clic su **Salva**.

Modifica delle impostazioni della rete wireless

La **Tabella wireless** nella pagina **Impostazioni di base** elenca le impostazioni delle quattro reti wireless supportate sul dispositivo.

Per configurare le impostazioni della rete wireless, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare la casella delle reti da configurare.

PASSAGGIO 2 Fare clic su **Modifica**.

PASSAGGIO 3 Configurare le seguenti impostazioni:

Attiva SSID	Selezionare **Attiva** per attivare la rete.
Nome SSID	Immettere il nome della rete.

Trasmissione SSID	Selezionare questa casella per attivare la trasmissione di SSID. Se il broadcast SSID è attivo, il router wireless dichiara la sua disponibilità ai dispositivi dotati di wireless nel raggio del router.
Modalità di protezione	Vedere la sezione **Configurazione della modalità di protezione**.
Filtro MAC	Vedere la sezione **Configurazione del filtro MAC**.
VLAN	Selezionare la VLAN associata alla rete.
Isolamento wireless con SSID	Selezionare questa casella per attivare l'isolamento wireless all'interno della rete SSID.
WMM (Wi-Fi Multimedia)	Selezionare questa casella per attivare WMM.
Max client associati	Il numero massimo di client che possono essere connessi alla rete wireless selezionata. Immettere un numero compreso tra 1 e 64.
WPS	Selezionare questa casella per mappare a questa rete il pulsante WPS del dispositivo sul pannello frontale.
Profilo portale	Vedere la sezione **Configurazione di Captive Portal**.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione della modalità di protezione

È possibile configurare una delle seguenti modalità di protezione per le reti wireless:

Configurazione WEP

La modalità di protezione WEP offre una protezione debole, con un metodo di crittografia di base non sicuro come WPA. La protezione WEP potrebbe essere necessaria nel caso in cui i dispositivi di rete non supportino WPA.

NOTA Se non è necessario utilizzare la protezione WEP, si consiglia l'utilizzo della protezione WPA2. Se si utilizza la modalità solo wireless N, è necessario utilizzare WPA2.

Per configurare la modalità di protezione WEP, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Wireless** > **Impostazioni di base**. Nella **Tabella wireless**, selezionare la casella corrispondente alla rete che si desidera configurare.

PASSAGGIO 2 Fare clic su **Modifica modalità protezione**. Verrà visualizzata la pagina **Impostazioni di protezione**.

PASSAGGIO 3 Nel campo **Seleziona SSID**, selezionare l'identificatore SSID per il quale si desidera configurare le impostazioni di protezione.

PASSAGGIO 4 Dal menu **Modalità di protezione**, scegliere **WEP**.

PASSAGGIO 5 Nel campo **Tipo di autenticazione**, selezionare una delle seguenti opzioni:

- **Sistema aperto**: questa è l'opzione predefinita.
- **Chiave condivisa**: selezionare questa opzione se consigliato dall'amministratore di rete. Se non si è sicuri, selezionare l'opzione predefinita.

In entrambi i casi, il client wireless deve fornire la chiave condivisa corretta (password) per accedere alla rete wireless.

PASSAGGIO 6 Nel campo **Crittografia**, selezionare il tipo di crittografia:

- **10/64 bit (10 cifre esadecimali):** fornisce una chiave a 40 bit.
- **26/128 bit (26 cifre esadecimali)**: fornisce una chiave a 104 bit, che offre una migliore crittografia rendendo la chiave più difficile da decifrare. Si consiglia la crittografia a 128 bit.

PASSAGGIO 7 (Opzionale) Nel campo **Frase chiave** immettere una frase alfanumerica (per garantire una sicurezza ottimale deve essere più lunga di otto caratteri) e fare clic su **Genera chiave** per generare quattro chiavi WEP univoche nei campi **chiave WEP**.

Se si desidera utilizzare una chiave personale, immetterla direttamente nel campo **Chiave 1** (opzione consigliata). La lunghezza della chiave deve essere di 5 caratteri ASCII (o 10 caratteri esadecimali) per WEP a 64 bit e 13 caratteri ASCII (o 26 caratteri esadecimali) per WEP a 128 bit. I caratteri esadecimali validi sono quelli compresi tra 0 e 9 e tra A e F.

PASSAGGIO 8 Nel campo **Chiave TX**, selezionare la chiave da utilizzare come chiave condivisa che verrà utilizzata dai dispositivi per accedere alla rete wireless.

PASSAGGIO 9 Fare clic su **Salva** per salvare le impostazioni.

PASSAGGIO 10 Fare clic su **Indietro** per tornare alla pagina **Impostazioni di base**.

Configurazione di WPA Personal, WPA2 Personal e Combinazione WPA2-Personal

Le modalità di protezione WPA Personal, WPA2 Personal e Combinazione WPA2-Personal offrono una protezione potente in sostituzione di WEP.

- **WPA Personal**: WPA fa parte dello standard di protezione wireless (802.11i) standardizzato dalla Wi-Fi Alliance e progettato come misura intermedia per la sostituzione di WEP durante la preparazione dello standard 802.11i. WPA Personal supporta il protocollo TKIP (Temporal Key Integrity Protocol) e la crittografia AES (Advanced Encryption Standard).
- **WPA2 Personal**: (opzione consigliata) WPA2 è l'implementazione dello standard di protezione specificato nello standard finale 802.11i. WPA2 supporta la crittografia AES e questa opzione utilizza la chiave precondivisa PSK per l'autenticazione.
- **Combinazione WPA2-Personal**: consente ad entrambi i client WPA e WPA2 di connettersi simultaneamente tramite l'autenticazione PSK.

L'autenticazione personale corrisponde alla chiave PSK, ovvero una frase chiave alfanumerica condivisa con il peer wireless.

Per configurare la modalità di protezione WPA Personal, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella della rete da configurare.

PASSAGGIO 2 Fare clic su **Modifica modalità protezione**. Verrà visualizzata la pagina **Impostazioni di protezione**.

PASSAGGIO 3 Nel campo **Seleziona SSID**, selezionare l'identificatore SSID per il quale si desidera configurare le impostazioni di protezione.

PASSAGGIO 4 Dal menu **Modalità di protezione**, selezionare una delle tre opzioni WPA Personal.

PASSAGGIO 5 (Solo WPA Personal) Nel campo **Crittografia**, selezionare una delle seguenti opzioni:

- **TKIP/AES**: selezionare **TKIP/AES** per garantire la compatibilità con i dispositivi wireless meno recenti che non supportano AES.
- **AES**: questa è l'opzione più sicura.

PASSAGGIO 6 Nel campo **Chiave di protezione**, immettere una frase alfanumerica (8-63 caratteri ASCII o 64 caratteri esadecimali). L'indicatore di complessità della password indica il grado di sicurezza offerto dalla password: inferiore al minimo, debole, buona, molto buona o sicura. Consigliamo l'uso di una chiave di sicurezza che risulti sicura sull'indicatore di complessità.

PASSAGGIO 7 Per mostrare la chiave di sicurezza inserita selezionare la casella **Password in chiaro**.

PASSAGGIO 8 Nel campo **Rinnovo chiave**, immettere l'intervallo temporale (600-7200 secondi) tra i rinnovi della chiave. Il valore predefinito è 3600.

PASSAGGIO 9 Fare clic su **Salva** per salvare le impostazioni. Fare clic su **Indietro** per tornare alla pagina **Impostazioni di base**.

Configurazione di WPA Enterprise, WPA2 Enterprise e Combinazione WPA2-Enterprise

Le modalità di protezione WPA Enterprise, WPA2 Enterprise e Combinazione WPA2-Enterprise consentono di utilizzare l'autenticazione server RADIUS.

- **WPA Enterprise**: consente l'utilizzo di WPA con l'autenticazione server RADIUS.
- **WPA2 Enterprise**: consente l'utilizzo di WPA2 con l'autenticazione server RADIUS.

- **Combinazione WPA2-Enteprise**: consente ad entrambi i client WPA e WPA2 di connettersi simultaneamente tramite l'autenticazione RADIUS.

Per configurare la modalità di protezione WPA Enteprise, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella della rete da configurare.

PASSAGGIO 2 Fare clic su **Modifica modalità protezione**.

PASSAGGIO 3 Nel campo **Seleziona SSID**, selezionare l'identificatore SSID per il quale si desidera configurare le impostazioni di protezione.

PASSAGGIO 4 Dal menu **Modalità di protezione**, selezionare una delle tre opzioni WPA Enteprise.

PASSAGGIO 5 (Solo WPA Enterprise) Nel campo **Crittografia**, selezionare una delle seguenti opzioni:

- **TKIP/AES**: selezionare **TKIP/AES** per garantire la compatibilità con i dispositivi wireless meno recenti che non supportano AES.
- **AES**: questa è l'opzione più sicura.

PASSAGGIO 6 Nel campo **Server RADIUS**, immettere l'indirizzo IP del server RADIUS.

PASSAGGIO 7 Nel campo **Porta RADIUS**, immettere la porta utilizzata per accedere al server RADIUS.

PASSAGGIO 8 Nel campo **Chiave condivisa**, immettere una frase alfanumerica.

PASSAGGIO 9 Nel campo **Rinnovo chiave**, immettere l'intervallo temporale (600-7200 secondi) tra i rinnovi della chiave. Il valore predefinito è 3600.

PASSAGGIO 10 Fare clic su **Salva** per salvare le impostazioni.

PASSAGGIO 11 Fare clic su **Indietro** per tornare alla pagina **Impostazioni di base**.

Configurazione del filtro MAC

È possibile utilizzare il filtro MAC per consentire o negare l'accesso alla rete wireless sulla base dell'indirizzo MAC (hardware) del dispositivo richiedente. Ad esempio, è possibile immettere gli indirizzi MAC di una serie di computer e consentire solo a quei computer di accedere alla rete. È possibile configurare il filtro MAC per ciascuna rete o SSID.

Per configurare il filtraggio MAC, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella della rete da configurare.

PASSAGGIO 2 Fare clic su **Modifica filtro MAC**. Viene visualizzata la pagina del **Filtro MAC wireless**.

PASSAGGIO 3 Nel campo **Modifica filtro MAC**, selezionare la casella **Attiva** per attivare il filtro MAC per questo SSID.

PASSAGGIO 4 Nel campo **Controllo connessione**, selezionare il tipo di accesso alla rete wireless:

- **Impedire l'accesso alla rete wireless ai PC elencati di seguito**: selezionare questa opzione per impedire che i dispositivi con gli indirizzi MAC elencati nella **Tabella indirizzi MAC** accedano alla rete wireless. Questa è l'opzione predefinita.
- **Consenti**: selezionare questa opzione per consentire ai dispositivi con gli indirizzi MAC elencati nella **Tabella indirizzi MAC** di accedere alla rete wireless.

PASSAGGIO 5 Per mostrare i computer e gli altri dispositivi della rete wireless, fare clic su **Mostra elenco client**.

PASSAGGIO 6 Nel campo **Salva nell'elenco filtri indirizzo MAC** selezionare la casella per inserire il dispositivo nell'elenco di dispositivi da aggiungere alla **Tabella indirizzi MAC**.

PASSAGGIO 7 Fare clic su **Aggiungi a MAC** per aggiungere i dispositivi selezionati della **Tabella elenco client** alla **Tabella indirizzi MAC**.

PASSAGGIO 8 Fare clic su **Salva** per salvare le impostazioni.

PASSAGGIO 9 Fare clic su **Indietro** per tornare alla pagina **Impostazioni di base**.

Configurazione dell'opzione Ora accesso

Per proteggere ulteriormente la rete, è possibile limitare l'accesso specificando gli orari di accesso.

Per configurare l'opzione Ora accesso, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella wireless** (**Wireless** > **Impostazioni di base**), selezionare la casella della rete da configurare.

PASSAGGIO 2 Fare clic su **Ora accesso**. Viene visualizzata la pagina **Ora accesso**.

PASSAGGIO 3 Nel campo **Tempo attività** , selezionare la casella **Attiva** per attivare l'opzione Ora accesso.

PASSAGGIO 4 Nei campi **Ora di inizio** e **Ora di fine**, specificare gli orari del giorno durante i quali è possibile accedere alla rete.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione delle impostazioni wireless avanzate

Le impostazioni wireless avanzate devono essere regolate solo da un amministratore esperto; se le impostazioni non sono corrette, si potrebbe notare una riduzione delle prestazioni wireless.

Per configurare le impostazioni wireless avanzate, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Wireless** > **Impostazioni avanzate**. Viene visualizzata la pagina Impostazioni avanzate.

PASSAGGIO 2 Configurare le impostazioni seguenti:

Burst frame	Attivare questa opzione per incrementare le prestazioni delle reti wireless, a seconda del produttore dei prodotti wireless. Se non si è sicuri di come utilizzare questa opzione, mantenere l'impostazione predefinita (attivato).

Nessuna conferma WMM	L'attivazione dell'opzione Nessuna conferma WMM consente di ottenere un throughput più efficiente, ma frequenze di errore maggiori in un ambiente di frequenza radio (RF) rumoroso. Per impostazione predefinita, questa impostazione è disattivata.
Velocità di base	L'impostazione della velocità di base non è la velocità di trasmissione, ma una serie di velocità di trasmissione sulla piattaforma Services Ready. Il dispositivo dichiara la propria velocità di base agli altri dispositivi wireless della rete affinché conoscano le velocità di trasmissione utilizzate. La piattaforma Services Ready dichiara inoltre che verrà selezionata automaticamente la velocità di trasmissione più adatta. L'impostazione predefinita è Predefinito, quando il dispositivo può trasmettere a tutte le velocità standard wireless (1 Mb/s, 2 Mb/s, 5,5 Mb/s, 11 Mb/s, 18 Mb/s, 24 Mb/s, 36 Mb/s, 48 Mb/s e 54 Mb/s). Oltre alle velocità di trasmissione B e G, il dispositivo supporta le velocità N. Le altre opzioni disponibili sono 1-2 Mbps, da utilizzare con dispositivi con tecnologia wireless meno recente, e Tutte, quando il dispositivo può trasmettere a tutte le velocità wireless. La velocità di trasmissione di base non corrisponde alla velocità di trasmissione dei dati effettiva. Per specificare la velocità di trasmissione dei dati del dispositivo, configurare l'impostazione Velocità di trasmissione.
Velocità di trasmissione	Impostare la velocità di trasmissione dei dati in base alla velocità della rete wireless. È possibile scegliere tra varie velocità di trasmissione oppure selezionare l'opzione **Auto** affinché il dispositivo utilizzi automaticamente la massima velocità di trasmissione possibile attivando la funzione di fallback automatico. La funzione di fallback automatico consente di negoziare la migliore velocità di connessione possibile tra il dispositivo e un client wireless. L'impostazione predefinita è Auto.

Velocità di trasmissione N	La velocità di trasmissione dei dati deve essere impostata in base alla velocità della rete wireless N. È possibile scegliere tra varie velocità di trasmissione oppure selezionare l'opzione **Auto** affinché il dispositivo utilizzi automaticamente la massima velocità di trasmissione possibile e attivare la funzione di fallback automatico. La funzione di fallback automatico consente di negoziare la migliore velocità di connessione possibile tra il dispositivo e un client wireless. L'impostazione predefinita è Auto.
Modalità di protezione CTS	Il dispositivo utilizza automaticamente la modalità di protezione CTS (Clear-To-Send) nel caso si verifichino problemi gravi relativamente ai prodotti Wireless-G e Wireless-N che non siano in grado di comunicare con il dispositivo in ambienti in cui è presente notevole traffico 802.11b. Questa funzione migliora la capacità di ricezione delle trasmissioni Wireless-G e Wireless-N del dispositivo, ma ne compromette significativamente le prestazioni. L'impostazione predefinita è Auto.
Intervallo beacon	Questo valore indica l'intervallo di frequenza del beacon. Un beacon è un pacchetto trasmesso dal dispositivo per sincronizzare la rete wireless. Immettere un valore compreso tra 40 e 3.500 millisecondi. Il valore predefinito è 100.
Intervallo DTIM	Questo valore, compreso tra 1 e 255, indica l'intervallo di invio dei messaggi DTIM (Delivery Traffic Indication Message). Il campo DTIM viene utilizzato per eseguire il conto alla rovescia per indicare ai client la disponibilità della successiva finestra di ascolto di messaggi broadcast e multicast. Quando il dispositivo ha raccolto messaggi broadcast o multicast destinati ai client associati, invia un messaggio DTIM con un valore di intervallo DTIM. In questo modo i client ricevono il beacon e si preparano a ricevere i messaggi broadcast e multicast. Il valore predefinito è 1.

Soglia di frammentazione	Questo valore indica la dimensione massima di un pacchetto prima che i dati vengano suddivisi in più pacchetti. Se si verifica un elevato numero di errori relativi ai pacchetti, è consigliabile incrementare leggermente il valore della soglia di frammentazione. Un valore della soglia di frammentazione troppo basso potrebbe infatti compromettere le prestazioni della rete. Si consiglia di apportare solo riduzioni di lieve entità al valore predefinito. Nella maggior parte dei casi è opportuno non modificare il valore predefinito di 2346.
Soglia RTS	Se si riscontra un flusso di dati inconsistente, immettere solo riduzioni di lieve entità. Si consiglia il valore predefinito di 2347. Se la dimensione di un pacchetto di rete è inferiore alla soglia RTS (Request to Send) impostata, il meccanismo RTS/CTS (Request to Send) non viene attivato. La piattaforma Services Ready invia frame RTS a una data stazione ricevente e negozia l'invio di un frame di dati. Dopo avere ricevuto un pacchetto RTS, la stazione wireless risponde con un frame CTS per autorizzare l'avvio della trasmissione.

PASSAGGIO 3 Fare clic su **Salva**.

Rilevamento di access point non autorizzati

Un AP non autorizzato è un access point che è stato installato su una rete sicura senza l'autorizzazione esplicita di un amministratore di sistema. Gli AP non autorizzati rappresentano una minaccia per la sicurezza poiché chiunque abbia accesso alla postazione può installare un AP wireless che consenta l'accesso alla rete da parti non autorizzate.

Utilizzare la pagina di rilevamento AP non autorizzato per consentire al proprio dispositivo di visualizzare informazioni su tutti gli AP rilevati dal dispositivo nei pressi della rete. Nel caso in cui l'access point indicato come non autorizzato è in realtà un access point legittimo, è possibile aggiungerlo alla **Tabella AP autorizzati**. Selezionare la frequenza di aggiornamento per assicurarsi che la pagina di Rilevamento AP non autorizzato visualizzi sempre le informazioni più recenti.

Per attivare il rilevamento di AP non autorizzati, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Wireless > AP non autorizzato**.

PASSAGGIO 2 Fare clic sul pulsante di opzione **Rilevamento AP non autorizzato attivo**.

PASSAGGIO 3 Fare clic su **Salva**.

Per autorizzare gli access point rilevati, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella AP non autorizzati rilevati**, selezionare la casella degli access point che si desidera autorizzare.

PASSAGGIO 2 Fare clic su **Autorizza**.

Per aggiungere un access point alla tabella AP autorizzati, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Aggiungi riga**.

PASSAGGIO 2 Inserire l'indirizzo MAC dell'access point che si desidera autorizzare.

PASSAGGIO 3 Inserire il SSID o il nome che identifica la rete wireless.

PASSAGGIO 4 Scegliere la modalità di protezione associata all'access point.

PASSAGGIO 5 Selezionare TKIP (Temporal Key Integrity Protocol) o CCMP (Counter Cipher Mode Protocol) come algoritmo di crittografia associato all'access point.

PASSAGGIO 6 Selezionare server RADIUS o PSK (Pre-Shared Key) per autenticare l'access point.

PASSAGGIO 7 Selezionare la modalità di rete wireless utilizzata dall'access point.

PASSAGGIO 8 Scegliere la frequenza radio utilizzata dalll'access point.

PASSAGGIO 9 Fare clic su **Salva**.

Importazione degli elenchi di AP autorizzati

È possibile importare un elenco di access point utilizzando un file CSV. Utilizzare i valori riportati di seguito come riferimento quando si crea un file CSV.

Campo	Valori
Protezione	• 0 — Aperto • 1 — WEP • 2 — WPA-Personal • 3 — WPA-Enterprise • 4 — WPA2-Personal • 5 — WPA2-Enterprise
Modalità di rete	• 0 — Solo B • 1 — Solo G • 2 — Solo N • 3 — Combinazione BG • 4 — Combinazione GN • 5 — Combinazione BGN

Campo	Valori
Canale	• 0 — Auto • 1 — 2.412 • 2 — 2.417 • 3 — 2.422 • 4 — 2.427 • 5 — 2.432 • 6 — 2.437 • 7 — 2.442 • 8 — 2.447 • 9 — 2.452 • 10 — 2.457 • 11 — 2.462
Crittografia	• 2 — TKIP • 4 — CCMP
Autenticazione	• 2 — PSK • 1 — RADIUS

Assicurarsi che il contenuto del file CSV venga disposto come illustrato nel seguente esempio:

BSSID	Protezione	Crittografia	Autenticazione	Rete wireless	Canale	SSID
00:1C:10:CE:44:48	4	2	2	3	1	Auth_Guest

Per importare un elenco di AP autorizzati:

PASSAGGIO 1 Fare clic su **Unisci** per aggiungere un elenco di access point che si desidera importare agli access point visualizzati nella **Tabella AP autorizzati**. Fare clic su **Sostituisci** per sostituire gli AP nella tabella con gli AP nell'elenco che si desidera importare.

PASSAGGIO 2 Fare clic su **Sfoglia** per individuare il file che si desidera importare.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione di WDS

Un WDS (Wireless Distribution System) è un sistema che consente l'interconnessione wireless degli access point di una rete. Consente l'espansione di una rete wireless tramite access point multipli senza la necessità di fornire una backbone cablata per collegarli.

Per stabilire un collegamento WDS, il dispositivo e altri peer WDS remoti devono essere configurati sulla stessa modalità di rete wireless, canale wireless, selezione di banda wireless e tipo di crittografia (nessuno o WEP).

È possibile configurare WDS nella modalità Bridge, in cui gli AP agiscono da collegamento comune tra più AP, o nella modalità Ripetitore, in cui un AP si collega a due AP senza una connessione cablata alla LAN, ripetendo i segnali utilizzando la connessione wireless.

WDS è supportato solo sui SSID 1.

Per configurare WDS nella modalità Bridge, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Wireless** > **WDS**.

PASSAGGIO 2 Per attivare WDS, selezionare la casella **Attiva.**

PASSAGGIO 3 Selezionare il pulsante di opzione **WDS Bridge**.

PASSAGGIO 4 Nella sezione **Indirizzo MAC bridge wireless remoto**, immettere l'indirizzo MAC per gli access point (fino a un massimo di quattro) da utilizzare come bridge nei campi **MAC 1**, **MAC 2**, **MAC 3** e **MAC 4**.

PASSAGGIO 5 Fare clic su **Salva**.

Per configurare WDS nella modalità Ripetitore, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Wireless** > **WDS**.

PASSAGGIO 2 Selezionare la casella **WDS**.

PASSAGGIO 3 Selezionare la modalità Ripetitore. Se si seleziona l'opzione **Consenti ripetizione del segnale wireless da un ripetitore**, inserire gli indirizzi MAC degli access point (fino a un massimo di tre) da utilizzare come ripetitori nei campi **MAC 1**, **MAC 2** e **MAC 3**.

PASSAGGIO 4 Se si seleziona **Ripeti segnale wireless di un access point remoto**:

- Inserire l'indirizzo MAC di un access point wireless nel campo **MAC**.
- Fare clic su **Mostra reti disponibili** per visualizzare la **Tabella reti disponibili.** Fare clic su **Connetti** per aggiungere l'indirizzo MAC dell'access point selezionato al campo **MAC**.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione di WPS

Configurare WPS in modo da consentire a tutti i dispositivi compatibili di connettersi alla rete wireless in maniera semplice e sicura. Fare riferimento al dispositivo client o alla relativa documentazione per ulteriori istruzioni su come configurare WPS sul dispositivo client.

Per configurare WPS:

PASSAGGIO 1 Scegliere **Wireless** > **WPS**. Viene visualizzata la pagina Wi-Fi Protected Setup.

PASSAGGIO 2 Selezionare l'opzione SSID dal menu a discesa.

PASSAGGIO 3 Configurare il WPS sui dispositivi client in uno dei seguenti tre modi:

a. Fare clic o premere il pulsante WPS sul dispositivo client, quindi fare clic sull'icona WPS di questa pagina.

b. Inserire il numero PIN WPS del client e fare clic su **Registra**.

c. Il dispositivo client richiede un numero PIN di questo router: utilizzare quello indicato.

Stato PIN dispositivo: stato del PIN del dispositivo WPA.

PIN dispositivo: identifica il PIN di un dispositivo che sta cercando di connettersi.

Validità PIN: la validità della chiave. Alla scadenza viene negoziata una nuova chiave.

Al termine della configurazione del WPS, nella parte inferiore della pagina **WPS** appaiono le seguenti informazioni: Stato Wi-Fi Protected Setup, Nome rete (SSID), Protezione, Crittografia.

Configurazione di Captive Portal

Utilizzare la funzionalità di Captive Portal per fornire l'accesso autenticato e controllato a Internet e alle proprie risorse di rete, senza compromettere la sicurezza. Un Captive Portal visualizza una pagina web speciale per autenticare i client prima che possano utilizzare Internet. È possibile configurare la verifica Captive Portal in modo da consentire l'accesso sia agli utenti ospiti che agli utenti di rete autenticati.

Configurare le istanze Captive Portal per ciascuna rete wireless virtuale sul dispositivo, associandole al profilo portale.

Creazione di profili Captive Portal

Per creare un profilo Captive Portal, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Wireless > Captive Portal > Profilo portale.** Nella sezione **Tabella profilo portale**, fare clic su **Aggiungi riga**. Per modificare il profilo del portale fornito sul dispositivo, selezionare la casella **Default_Portal_Profile** e fare clic su **Modifica**.

PASSAGGIO 2 Immettere un nome per il proprio profilo Captive Portal.

PASSAGGIO 3 Scegliere se si desidera utilizzare il profilo per autenticare gli utenti ospite o gli utenti sulla propria rete.

PASSAGGIO 4 Per reindirizzare gli utenti a un URL dopo l'autenticazione, attivare **URL reindirizzamento automatico**, quindi immettere il nome dominio completo valido o l'indirizzo IP nel campo **Reindirizza URL**. Ad esempio, includere http:// nell'URL.

PASSAGGIO 5 Nel campo **Timeout sessione**, specificare il numero di minuti in cui il dispositivo manterrà aperta una sessione di autenticazione con il client wireless associato. Il valore predefinito è di 60 minuti.

PASSAGGIO 6 Selezionare un colore per il font del testo che si desidera visualizzare sulla pagina.

PASSAGGIO 7 Specificare il testo che si desidera visualizzare, ad esempio il nome dell'organizzazione, il testo dell'etichetta per i campi nome utente e password e l'etichetta sul pulsante di accesso.

PASSAGGIO 8 Immettere il testo di Copyright associato alla propria azienda.

PASSAGGIO 9 Nei campi **Errore 1** ed **Errore 2**, immettere i messaggi di errore che si desidera mostrare ai client in caso di accesso non riuscito e quando si supera il numero massimo di connessioni.

PASSAGGIO 10 Per utilizzare una casella di controllo che consenta agli utenti di accettare i termini di utilizzo prima di continuare, attivare **Contratto**. Il testo nel campo **Testo contratto** verrà visualizzato come etichetta della casella di controllo.

PASSAGGIO 11 Inserire i termini di accettazione che si desidera mostrare agli utenti nel campo **Criteri di utilizzo**.

PASSAGGIO 12 Nella sezione **Carica file**, selezionare i file da caricare per il logo dell'azienda e i file sfondo corrispondenti al branding della propria azienda. Salvare il profilo.

Per visualizzare in anteprima il profilo, scegliere **Captive Portal > Anteprima pagina del portale**, quindi selezionare il profilo dall'elenco a discesa **Profilo portale**.

Configurazione delle istanze di Captive Portal

Per configurare l'istanza Captive Portale del dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Wireless > Impostazioni di base**.

PASSAGGIO 2 Nella sezione **Tabella Wireless**, selezionare la casella **Attiva** per il SSID per il quale si desidera configurare un Captive Portal. Fare clic su **Modifica**.

PASSAGGIO 3 Selezionare un profilo portale per il SSID.

È possibile creare fino a quattro Captive Portal utilizzando SSID per il proprio dispositivo. Per creare un nuovo profilo portale, selezionare **Creare un nuovo profilo portale** dall'elenco a discesa. Scegliere Default_Portal_Profile per utilizzare il profilo portale fornito sul proprio dispositivo.

PASSAGGIO 4 Selezionare la casella **Attiva** per abilitare il Captive Portal per il SSID.

PASSAGGIO 5 Salvare le istanze Captive Portal.

Creazione degli account utente Captive Portal.

Per creare un account utente Captive Portal, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Wireless > Captive Portal > Account utente**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Immettere il nome utente e la password. Immettere nuovamente la password per verificarla.

Si consiglia di utilizzare una combinazione di lettere maiuscole e minuscole, numeri e simboli e di non includere nella password parole presenti in dizionari di qualsiasi lingua. La password può essere composta da un massimo di 64 caratteri.

PASSAGGIO 4 Nel campo **Tempo di accesso (minuti)**, specificare la durata della sessione di autenticazione.

PASSAGGIO 5 Per importare nomi utente e password da un file .CSV, fare clic su **Importa**. Viene visualizzata la pagina **Amministrazione > Utenti**. Nella sezione **Importa nome utente e password**, fare clic su **Sfoglia** per individuare il file, quindi fare clic su **Importa**. Per ulteriori informazioni, vedere la sezione **Importazione degli account utente**.

PASSAGGIO 6 Salvare gli account utente.

Configurazione della modalità del dispositivo

È possibile configurare il dispositivo per lavorare nelle seguenti modalità:

- **Router**: per agire da router wireless.
- **AP (access point)**: per fornire connessioni wireless ai client e capacità Wi-Fi estendendo reti cablate esistenti. Tutte le porte LAN vengono disabilitate quando il dispositivo funge da access point.

  Assicurarsi di configurare le informazioni VLAN di gestione AP sulla pagina **Networking > WAN > Configurazione WAN**. Per ulteriori informazioni, vedere la sezione **Configurazione delle impostazioni opzionali**.

Per selezionare la modalità del dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Wireless > Modalità dispositivo**, quindi scegliere la modalità in base alla quale eseguire il dispositivo.

PASSAGGIO 2 Fare clic su **Salva**.

5

Configurazione del firewall

Funzioni del firewall

La rete può essere protetta creando e applicando regole che il dispositivo utilizza per bloccare e consentire il traffico Internet in ingresso e in uscita in maniera selettiva. Successivamente si specificano i dispositivi a cui vengono applicate le regole e come applicarle. Per questa operazione è necessario definire quanto segue:

- Tipi di servizi o traffico che il router dovrebbe consentire o bloccare. Ad esempio, esplorazione del Web, VoIP e altri servizi standard e servizi personalizzati definiti dall'utente.
- La direzione del traffico specificando l'origine e la destinazione del traffico stesso; a tal fine si specifica la "zona di origine" (LAN/WAN/DMZ) e la "zona di destinazione" (LAN/WAN/DMZ).
- Le pianificazioni in base alle quali il router deve applicare le regole.
- Le parole chiave, nel nome di dominio o nell'URL di una pagina Web, che il router deve bloccare o consentire.
- Le regole per consentire o bloccare il traffico Internet in ingresso e uscita per servizi specifici in base ad una determinata pianificazione.
- Gli indirizzi MAC dei dispositivi il cui accesso in ingresso alla rete deve essere bloccato dal router.
- I trigger di porta che segnalano al router di consentire o bloccare l'accesso a servizi specifici come definiti dal numero di porta.
- I rapporti e gli avvisi che il router deve inviare.

Ad esempio, è possibile stabilire dei criteri di accesso limitato basati sull'ora del giorno, sugli indirizzi Web e su parole chiave Web. È possibile bloccare l'accesso a Internet da parte di applicazioni e servizi della LAN, come chat room o giochi. È possibile impedire l'accesso proveniente dalla WAN o dalla rete DMZ pubblica a gruppi specifici di PC della rete.

Le regole per il traffico in ingresso (da WAN a LAN/DMZ) limitano l'accesso al traffico in ingresso della rete, consentendo in modo selettivo solo ad alcuni utenti esterni specifici di accedere a risorse locali specifiche. Per impostazione predefinita ogni accesso alla LAN sicura dal lato WAN non sicuro viene bloccato, ad eccezione delle risposte alle richieste provenienti dalla LAN o da DMZ. Per consentire ai dispositivi esterni l'accesso ai servizi della LAN sicura, è necessario creare una regola del firewall per ciascun servizio.

Se si desidera consentire il traffico in ingresso, l'indirizzo IP della porta WAN del router deve essere reso pubblico. Questa operazione viene denominata "esposizione dell'host". Il metodo di esposizione dell'host dipende dalla configurazione delle porte WAN; per il dispositivo è possibile utilizzare l'indirizzo IP se alla porta WAN viene assegnato un indirizzo statico oppure è possibile utilizzare un nome DDNS (DNS dinamico) se l'indirizzo WAN è dinamico.

Le regole per il traffico in uscita (da LAN/DMZ a WAN) limitano il traffico in uscita dalla rete, consentendo in modo selettivo solo ad alcuni utenti locali specifici di accedere a risorse esterne specifiche. La regola predefinita per il traffico in uscita consente l'accesso dalle zone sicure (LAN) alla rete DMZ pubblica o alla WAN non sicura. Per impedire agli host sulla LAN sicura di accedere ai servizi esterni (WAN non sicura) è necessario creare una regola firewall per ciascun servizio.

Configurazione delle impostazioni firewall di base

Per configurare le impostazioni firewall di base, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Impostazioni di base**.

PASSAGGIO 2 Configurare le seguenti impostazioni firewall:

Protezione spoofing dell'indirizzo IP	Per proteggere la rete dallo spoofing dell'indirizzo IP, selezionare la casella di controllo **Attiva**.
Protezione DoS	Selezionare **Attiva** per attivare la protezione Denial of Service.
Blocco richiesta WAN	Blocca le richieste ping inviate dalla WAN al dispositivo.

Accesso Web LAN/VPN	Selezionare il tipo di accesso Web che può essere utilizzato per collegarsi al firewall: HTTP o HTTPS (HTTP protetto).
Gestione remota **Accesso remoto** **Aggiornamento remoto** **Indirizzo IP remoto consentito** **Porta di gestione remota**	Vedere la sezione **Configurazione della gestione remota**.
Multicast Passthrough IPv4 (proxy IGMP)	Selezionare **Attiva** per attivare il passtrough multicast per l'IPv4.
Multicast Passthrough IPv6 (proxy IGMP)	Selezionare **Attiva** per attivare il passtrough multicast per l'IPv6.
SIP ALG	Per consentire al traffico SIP (Session Initiation Protocol) di attraversare il firewall, selezionare la casella di controllo **SIP ALG**. Il dispositivo supporta un massimo di 256 sessioni.
UPnP **Consenti agli utenti di configurare** **Consenti agli utenti di disabilitare l'accesso Internet**	Vedere la sezione **Configurazione di Universal Plug and Play**.
Blocca Java	Selezionare questa opzione per bloccare l'esecuzione degli applet Java. Gli applet Java sono piccoli programmi integrati nelle pagine Web che attivano la funzionalità dinamica della pagina. Un applet pericoloso può essere utilizzato per compromettere o infettare i computer. L'attivazione di questa impostazione blocca il download degli applet Java. Fare clic su **Auto** per bloccare automaticamente Java oppure fare clic su **Manuale** e immettere una porta specifica sulla quale bloccare Java.

Blocca cookie	Selezionare questa opzione per bloccare i cookie. I cookie vengono utilizzati per memorizzare informazioni relative alla sessione da parte di siti Web che solitamente richiedono l'accesso. Tuttavia, diversi siti Web utilizzano i cookie per tenere traccia delle informazioni e delle abitudini di navigazione di un utente. L'attivazione di questa opzione impedisce ai siti Web di creare cookie. Molti siti Web richiedono l'accettazione di cookie per consentire un accesso regolare al sito. Il blocco dei cookie può provocare un funzionamento non corretto dei siti Web. Fare clic su **Auto** per bloccare automaticamente i cookie oppure fare clic su **Manuale** e immettere una porta specifica sulla quale bloccare i cookie.
Blocca ActiveX	Selezionare questa opzione per bloccare i contenuti ActiveX. In modo analogo agli applet Java, i controlli ActiveX vengono installati su un computer Windows quando si esegue Internet Explorer. Un controllo ActiveX pericoloso può essere utilizzato per compromettere o infettare i computer. L'attivazione di questa impostazione blocca il download degli applet ActiveX. Fare clic su **Auto** per bloccare automaticamente ActiveX oppure fare clic su **Manuale** e immettere una porta specifica sulla quale bloccare ActiveX.

Blocca proxy	Selezionare questa opzione per bloccare i server proxy. Un server proxy (o semplicemente proxy) consente ai computer di connettersi ad altri computer tramite il proxy aggirando in questo modo alcune regole del firewall. Ad esempio, se le connessioni ad indirizzi IP specifici sono bloccate da una regola del firewall, le richieste possono essere indirizzate tramite un proxy che non viene bloccato dalla regola, rendendo quindi inefficace la limitazione. L'attivazione di questa funzione blocca i server proxy. Fare clic su **Auto** per bloccare automaticamente i server proxy oppure fare clic su **Manuale** e immettere una porta specifica sulla quale bloccare i server proxy.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione della gestione remota

È possibile attivare la gestione remota per consentire l'accesso al dispositivo da una rete WAN remota.

Per configurare la gestione remota, definire le impostazioni seguenti nella pagina **Impostazioni di base**:

Gestione remota	Selezionare **Attiva** per attivare la gestione remota.
Accesso remoto	Selezionare il tipo di accesso Web che può essere utilizzato per collegarsi al firewall: HTTP o HTTPS (HTTP protetto).
Aggiornamento remoto	Per attivare gli aggiornamenti remoti del dispositivo, selezionare **Attiva**.

Indirizzo IP remoto consentito	Fare clic su **Qualsiasi indirizzo IP** per consentire la gestione remota da qualsiasi indirizzo IP oppure immettere un indirizzo IP specifico nel campo dell'indirizzo.
Porta di gestione remota	Immettere la porta sulla quale è consentito l'accesso remoto. La porta predefinita è 443. Se si accede da remoto al router, è necessario inserire la porta di gestione remota nell'indirizzo IP. Ad esempio: **https://<ip-remoto>:<porta-remota>**, o **https://168.10.1.11:443**

ATTENZIONE Quando la gestione remota viene attivata, il router diventa accessibile a chiunque conosca il suo indirizzo IP. Dato che un utente WAN malintenzionato potrebbe riconfigurare il dispositivo e utilizzarlo in modo improprio, si consiglia vivamente di modificare la password dell'amministratore e qualsiasi eventuale password ospite prima di continuare.

Configurazione di Universal Plug and Play

Universal Plug and Play (UPnP) consente il rilevamento automatico dei dispositivi che possono comunicare con il dispositivo.

Per configurare UPnP, definire le impostazioni seguenti nella pagina **Impostazioni di base**:

UPnP	Selezionare **Attiva** per attivare UPnP.
Consenti agli utenti di configurare	Selezionare questa casella per consentire l'impostazione di regole di mappatura porta UPnP agli utenti che dispongono di computer con supporto UPnP o altri dispositivi con abilitazione UPnP. Se questa opzione viene disattivata, il dispositivo non consente all'applicazione di aggiungere la regola di reindirizzamento.
Consenti agli utenti di disabilitare l'accesso Internet	Selezionare questa casella per consentire agli utenti di disattivare l'accesso a Internet.

Gestione delle pianificazioni del firewall

È possibile creare pianificazioni per applicare le regole del firewall in giorni oppure in orari specifici.

Aggiunta o modifica di una pianificazione del firewall

Per creare o modificare una pianificazione, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Firewall** > **Gestione pianificazioni**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Nel campo **Nome**, immettere un nome univoco per la pianificazione. Questo nome viene visualizzato nell'elenco **Seleziona programma** nella pagina Configurazione regola firewall (vedere la sezione **Configurazione delle regole di accesso**).

PASSAGGIO 4 Nella sezione **Giorni pianificati**, selezionare se si desidera applicare la pianificazione a tutti i giorni o solo a giorni specifici. Se si seleziona **Giorni specifici**, selezionare la casella vicino ai giorni che si desidera includere nella pianificazione.

PASSAGGIO 5 Nella sezione **Ora del giorno pianificata**, selezionare l'ora del giorno in cui applicare la pianificazione. Se si seleziona **Orari specifici**, immettere gli orari di inizio e fine.

PASSAGGIO 6 Fare clic su **Salva**.

Configurazione della gestione servizi

Quando si crea una regola per il firewall è possibile specificare un servizio che viene controllato dalla regola. È possibile selezionare i tipi di servizio più comuni, oltre a poter creare servizi personalizzati.

La pagina della **Gestione servizio** consente di creare servizi personalizzati per i quali definire regole del firewall. Il nuovo servizio definito appare nell'elenco dei **servizi personalizzati disponibili**.

Per creare un servizio personalizzato, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Firewall** > **Gestione servizi**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Nel campo **Nome servizio**, immettere in nome del servizio per l'identificazione e la gestione.

PASSAGGIO 4 Nel campo **Protocollo**, selezionare dal menu a discesa il protocollo Layer 4 utilizzato dal servizio:

- **TCP**
- **UDP**
- **TCP e UDP**
- **ICMP**

PASSAGGIO 5 Nel campo **Porta iniziale**, immettere la prima porta TCP o UDP dell'intervallo utilizzato dal servizio.

PASSAGGIO 6 Nel campo **Porta finale**, immettere l'ultima porta TCP o UDP dell'intervallo utilizzato dal servizio.

PASSAGGIO 7 Fare clic su **Salva**.

Per modificare una voce, selezionarla e fare clic su **Modifica**. Effettuare le modifiche quindi fare clic su **Salva**.

Configurazione delle regole di accesso

Configurazione del criterio predefinito in uscita

La pagina **Regole di accesso** consente la configurazione dei criteri predefiniti di uscita per il traffico indirizzato dalla rete sicura (LAN) alla rete non sicura (WAN dedicata/opzionale).

Il criterio predefinito per il traffico in ingresso proveniente dalla zona non sicura alla zona sicura è Blocca sempre e non può essere modificato.

NOTA I criteri di accesso a Internet annullano le regole di accesso quando entrambi sono configurati sul dispositivo.

Per configurare il criterio predefinito in uscita, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Firewall** > **Regole di accesso**.

PASSAGGIO 2 Selezionare **Consenti** o **Nega**.

Nota: per configurare un firewall IPv6 accertarsi che sul dispositivo sia abilitato il supporto per IPv6. Vedere la sezione **Configurazione di IPv6**.

PASSAGGIO 3 Fare clic su **Salva**.

Riordinamento delle regole di accesso

L'ordine di visualizzazione delle regole di accesso nella tabella corrispondente indica l'ordine in cui tali regole vengono applicate. È possibile assegnare un nuovo ordine alla tabella se si desidera che alcune regole vengano applicate prima di altre, Ad esempio, è possibile applicare una regola che consenta certi tipi di traffico prima di bloccarne altri.

Per riordinare le regole di accesso, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Firewall** > **Regole di accesso**.

PASSAGGIO 2 Fare clic su **Riordina**.

PASSAGGIO 3 Selezionare la casella di controllo nella riga della regola da spostare in alto o in basso, quindi fare clic sulla freccia corrispondente per spostare la regola in alto o in basso, oppure selezionare la posizione desiderata per la regola nell'elenco a discesa e fare clic su **Sposta in**.

PASSAGGIO 4 Fare clic su **Salva**.

Aggiunta di regole di accesso

Tutte le regole di accesso configurate per il dispositivo sono disponibili nella **Tabella regole di accesso**. Questo elenco mostra anche se la regola è abilitata (attiva) e fornisce un riepilogo della zona "da/a", dei servizi e degli utenti coinvolti dalla regola.

Per creare una regola di accesso, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Firewall** > **Regole di accesso**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Nel campo **Tipo di connessione**, selezionare l'origine del traffico:

- **Uscita (LAN > WAN)**: selezionare questa opzione per creare una regola per il traffico in uscita.

- **Ingresso (LAN > WAN)**: selezionare questa opzione per creare una regola per il traffico in entrata.
- **Ingresso (WAN > DMZ)**: selezionare questa opzione per creare una regola per il traffico in entrata.

PASSAGGIO 4 Dall'elenco a discesa **Azione** scegliere l'azione:

- **Blocca sempre**: blocca sempre il tipo di traffico selezionato.
- **Consenti sempre**: consente sempre il tipo di traffico selezionato.
- **Blocca per pianificazione**: blocca il tipo di traffico selezionato in base a una pianificazione.
- **Consente per pianificazione**: consente il tipo di traffico selezionato in base a una pianificazione.

PASSAGGIO 5 Dal menu a discesa **Servizi**, selezionare il servizio da consentire o bloccare per questa regola. Selezionare **Tutto il traffico** per consentire l'applicazione della regola a tutte le applicazioni e servizi oppure selezionare un'applicazione singola da bloccare:

- DNS (Domain Name System, DNS), UDP o TCP
- FTP (File Transfer Protocol)
- HTTP (Hyptertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- TFTP (Trivial File Transfer Protocol)
- IMAP (Internet Message Access Protocol)
- NNTP (Network News Transport Protocol)
- POP3 (Post Office Protocol)
- SNMP (Simple Network Management Protocol)
- SMTP (Simple Mail Transfer Protocol)
- Telnet
- STRMWORKS
- TACACS (Terminal Access Controller Access-Control System)
- Telnet (comando)

- Telnet Secondary
- Telnet SSL
- Voce (SIP)

PASSAGGIO 6 Nel campo **IP di origine**, selezionare gli utenti ai quali verranno applicate le regole del firewall:

- **Qualsiasi**: la regola viene applicata al traffico proveniente da qualsiasi host della rete locale.
- **Indirizzo singolo**: la regola viene applicata al traffico proveniente da un indirizzo IP specifico della rete locale. Immettere l'indirizzo nel campo **Inizio**.
- **Intervallo di indirizzi**: la regola viene applicata al traffico proveniente da un indirizzo IP che si trova in un intervallo di indirizzi IP. Immettere l'indirizzo IP iniziale nel campo **Inizio** e l'indirizzo IP finale nel campo **Fine**.

PASSAGGIO 7 Nel campo **Registro**, specificare se i pacchetti per questa regola devono essere registrati.

Per registrare i dettagli di tutti i pacchetti che soddisfano questa regola, selezionare **Sempre** dal menu a discesa. Ad esempio, se una regola in uscita per una pianificazione è stata contrassegnata come **Blocca sempre**, per ogni pacchetto che tenta di effettuare una connessione in uscita per quel servizio, nel registro viene registrato un messaggio riportante l'indirizzo dell'origine e quello di destinazione, oltre ad altre informazioni, per il pacchetto.

L'attivazione della registrazione può generare un volume significativo di messaggi di registro ed è consigliabile utilizzarla solo a fini di debug.

Selezionare **Mai** per disattivare la registrazione.

Nota: quando il traffico scorre dalla LAN o DMZ verso la WAN, il sistema richiede la riscrittura dell'indirizzo IP di origine o di destinazione dei pacchetti IP in ingresso quando passano dal firewall.

PASSAGGIO 8 Nel campo **Stato regola**, selezionare la casella per attivare la nuova regola di accesso.

PASSAGGIO 9 Fare clic su **Salva**.

Creazione di un criterio di accesso a Internet

Il dispositivo supporta diverse opzioni per bloccare l'accesso a Internet. È possibile bloccare tutto il traffico Internet, bloccare il traffico Internet di certi PC o punti terminali o bloccare l'accesso a Internet specificando parole chiave da bloccare. Se le parole chiave si trovano nel nome del sito, ad esempio nell'URL del sito Web oppure nel nome del newsgroup, il sito viene bloccato.

Aggiunta o modifica di un criterio di accesso a Internet

Per creare un criterio di accesso a Internet, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Criterio di accesso Internet**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Seleziona la casella di controllo **Attivazione stato**.

PASSAGGIO 4 Immettere il nome del criterio per l'identificazione e la gestione.

PASSAGGIO 5 Dal menu a discesa **Azione**, scegliere il tipo di limitazione di accesso necessario:

- **Blocca sempre**: blocca sempre il traffico Internet. Questa opzione consente di bloccare il traffico Internet da e verso tutti i punti terminali. Se si desidera bloccare tutto il traffico, pur consentendo ad alcuni punti terminali di ricevere traffico Internet, vedere il passaggio 7.
- **Consenti sempre**: consente sempre il traffico Internet. È possibile perfezionare questa opzione per bloccare punti terminali specifici dal traffico Internet; vedere il passaggio 7. Inoltre, è possibile consentire il traffico Internet tranne che per alcuni siti Web; vedere il passaggio 8.
- **Blocca per pianificazione**: blocca il traffico Internet in base a una pianificazione (ad esempio, per bloccare il traffico Internet durante le ore lavorative della settimana, pur consentendo la navigazione dopo le ore lavorative e nei weekend).
- **Consenti per pianificazione**: consente il traffico Internet in base a una pianificazione.

Se si seleziona **Blocca in base a pianificazione** oppure **Consenti in base a pianificazione**, fare clic su **Configura pianificazioni** per creare una pianificazione. Vedere la sezione **Gestione delle pianificazioni del firewall**.

PASSAGGIO 6 Selezionare una pianificazione dal menu a discesa.

PASSAGGIO 7 (Opzionale) Applicare il criterio di accesso a PC specifici per consentire o bloccare il traffico proveniente da dispositivi specifici:

a. Nella tabella **Applica il criterio di accesso ai seguenti PC** fare clic su **Aggiungi riga**.

b. Dal menu a discesa **Tipo**, selezionare il tipo di identificazione del PC, ovvero in base all'indirizzo MAC o l'indirizzo IP o fornendo un intervallo di indirizzi IP.

c. Nel campo **Valore** immettere le informazioni seguenti, a seconda dell'opzione selezionata nel passaggio precedente:

- L'indirizzo MAC (xx:xx:xx:xx:xx:xx) del PC al quale si applica il criterio.
- L'indirizzo IP del PC al quale si applica il criterio.
- L'indirizzo iniziale e quello finale dell'intervallo di indirizzi da bloccare, ad esempio, 192.168.1.2-192.168.10,253.

PASSAGGIO 8 Per bloccare il traffico da siti Web specifici, attenersi alla seguente procedura:

a. Nella tabella **Nome dominio sito Web e parola chiave**, fare clic su **Aggiungi riga**.

b. Dal menu a discesa **Tipo**, selezionare come bloccare un sito Web (specificando il nome dominio o una parola chiave che appare nell'URL).

c. Nel campo **Valore**, immettere l'URL o la parola chiave utilizzata per bloccare il sito Web.

Ad esempio, per bloccare l'URL esempio.com, selezionare **Indirizzo URL** dal menu a discesa e immettere **esempio.com** nel campo **Valore**. Per bloccare un URL che contiene la parola chiave “esempio”, selezionare **Parola chiave** dal menu a discesa e immettere **esempio** nel campo **Valore**.

PASSAGGIO 9 Fare clic su **Salva**.

Configurazione di NAT (Network Address Translation) uno-a-uno

Utilizzare la pagina NAT uno-a-uno per associare gli indirizzi IP locali dietro il firewall agli indirizzi IP globali. NAT uno-a-uno consente di visualizzare con indirizzi IP pubblici i sistemi dietro un firewall che sono configurati con un indirizzo IP privato.

Per aggiungere una regola NAT uno-a-uno:

PASSAGGIO 1 Selezionare **Firewall > NAT uno-a-uno**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Nel campo **Inizio intervallo privato**, inserire l'indirizzo IP di partenza nell'intervallo di indirizzi IP (LAN) privati.

PASSAGGIO 4 Nel campo **Inizio intervallo pubblico**, inserire l'indirizzo IP di partenza nell'intervallo di indirizzi IP (WAN) pubblici.

PASSAGGIO 5 In **Lunghezza intervallo**, inserire il numero di indirizzi IP pubblici da associare a indirizzi privati.

PASSAGGIO 6 Nel campo **Servizio**, scegliere il servizio a cui viene applicata la regola. I servizi per NAT statico consentono di configurare i servizi accettati dall'indirizzo IP privato (LAN) nell'inviare il traffico verso il corrispondente indirizzo IP pubblico. I servizi configurati sugli indirizzi IP privati dell'intervallo vengono accettati quando è disponibile traffico sull'indirizzo IP pubblico corrispondente.

PASSAGGIO 7 Fare clic su **Salva**.

Configurazione del reindirizzamento delle porte

Il reindirizzamento delle porte viene utilizzato per instradare il traffico proveniente da Internet da una porta sulla WAN a un'altra porta sulla LAN. Sono disponibili servizi comuni oppure è possibile definire un servizio personalizzato con relative porte da reindirizzare.

Le pagine **Regole reindirizzamento porta singola** e **Regole reindirizzamento intervallo porte** elencano tutte le regole di reindirizzamento porte disponibili per il dispositivo e permettono di configurare tali regole.

NOTA Il reindirizzamento delle porte non è adeguato per i server della LAN perché prima dell'apertura delle porte in ingresso è necessario che il dispositivo LAN stabilisca una connessione in uscita.

Per il corretto funzionamento di alcune applicazioni è necessario che i dati vengano ricevuti su una porta specifica o un intervallo di porte quando i dispositivi esterni si collegano. Il router deve inviare tutti i dati in ingresso per l'applicazione alla porta o all'intervallo di porte richiesto.

Il gateway dispone di un elenco di applicazioni e giochi comuni con porte in ingresso e in uscita corrispondenti da aprire. È anche possibile specificare una regola di reindirizzamento porte definendo il tipo di traffico (TCP o UDP) e l'intervallo di porte in ingresso e in uscita da aprire se abilitate.

Configurazione reindirizzamento porta singola

Per aggiungere una regola di reindirizzamento porta singola, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Reindirizzamento porta singola**. Viene visualizzato un elenco predefinito di applicazioni.

PASSAGGIO 2 Nel campo **Applicazione**, immettere il nome dell'applicazione per la quale configurare il reindirizzamento porte.

PASSAGGIO 3 Nel campo **Porta esterna**, immettere il numero di porta che attiva la regola quando viene effettuata una richiesta di connessione dal traffico in uscita.

PASSAGGIO 4 Nel campo **Porta interna**, immettere il numero di porta utilizzata dal sistema remoto per rispondere alla richiesta ricevuta.

PASSAGGIO 5 Nel menu a discesa **Interfaccia**, selezionare **Entrambi (Ethernet e 3G)**, **Ethernet** o **3G**.

PASSAGGIO 6 Dal menu a discesa **Protocollo**, selezionare un protocollo (**TCP**, **UDP** o **TCP** e **UDP**).

PASSAGGIO 7 Nel campo **Indirizzo IP**, immettere l'indirizzo IP dell'host lato LAN al quale viene inoltrato lo specifico traffico IP. Ad esempio, è possibile inoltrare il traffico HTTP alla porta 80 dell'indirizzo di un server Web lato LAN.

PASSAGGIO 8 Nel campo **Attiva**, selezionare la casella **Attiva** per attivare la regola.

PASSAGGIO 9 Fare clic su **Salva**.

Configurazione reindirizzamento intervallo porte

Per aggiungere una regola di reindirizzamento di un intervallo di porte, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Reindirizzamento intervallo porte**.

PASSAGGIO 2 Nel campo **Applicazione**, immettere il nome dell'applicazione per la quale configurare il reindirizzamento porte.

PASSAGGIO 3 Nel campo **Porta esterna**, specificare il numero di porta che attiverà la regola quando viene effettuata una richiesta di connessione dal traffico in uscita.

PASSAGGIO 4 Nel campo **Inizio**, specificare il numero di porta iniziale dell'intervallo di porte da reindirizzare.

PASSAGGIO 5 Nel campo **Fine**, specificare il numero di porta finale dell'intervallo di porte da reindirizzare.

PASSAGGIO 6 Nel menu a discesa **Interfaccia**, selezionare **Entrambi (Ethernet e 3G)**, **Ethernet** o **3G**.

PASSAGGIO 7 Dal menu a discesa **Protocollo**, selezionare un protocollo (**TCP**, **UDP** o **TCP** e **UDP**).

PASSAGGIO 8 Nel campo **Indirizzo IP**, immettere l'indirizzo IP dell'host lato LAN al quale viene inoltrato lo specifico traffico IP.

PASSAGGIO 9 Nel campo **Attiva**, selezionare la casella **Attiva** per attivare la regola.

PASSAGGIO 10 Fare clic su **Salva**.

Configurazione attivazione intervallo di porte

L'attivazione delle porte consente ai dispositivi della LAN o DMZ di richiedere il reindirizzamento di una o più porte verso tali dispositivi. L'attivazione delle porte attende la richiesta di uscita dalla LAN/DMZ su una delle porte in uscita definite, quindi apre la porta in ingresso per il tipo di traffico specificato.

L'attivazione delle porte è una forma di reindirizzamento porte dinamico durante la trasmissione di dati da parte di un'applicazione attraverso porte aperte in uscita o in entrata. L'attivazione delle porte apre una porta in ingresso per un tipo specifico di traffico su una porta in uscita definita. L'attivazione delle porte è più flessibile del reindirizzamento porte statico (disponibile quando si definiscono le regole del firewall) dato che una regola non deve fare riferimento a un indirizzo o a un intervallo IP LAN specifico. Le porte, inoltre, non vengono lasciate aperte se non sono in uso, fornendo di conseguenza un livello di sicurezza che il reindirizzamento porte non consente.

NOTA L'attivazione delle porte non è adeguato per i server della LAN visto che il dispositivo LAN dispone di una dipendenza che stabilisce una connessione in uscita prima dell'apertura delle porte in ingresso.

Per il corretto funzionamento di alcune applicazioni è necessario che i dati vengano ricevuti su una porta specifica o un intervallo di porte quando i dispositivi esterni si collegano. Il router deve inviare tutti i dati in ingresso per l'applicazione alla porta o all'intervallo di porte richiesto. Il gateway dispone di un elenco di applicazioni e giochi comuni con porte in ingresso e in uscita corrispondenti da aprire. È anche possibile specificare una regola di attivazione delle porte definendo il tipo di traffico (TCP o UDP) e l'intervallo di porte in ingresso e in uscita da aprire se abilitate.

Per aggiungere una regola di attivazione delle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Firewall** > **Attivazione intervallo di porte**.

PASSAGGIO 2 Nel campo **Applicazione**, immettere il nome dell'applicazione per la quale configurare il reindirizzamento porte.

PASSAGGIO 3 Nei campi **Intervalli attivati**, specificare il numero di porta o intervallo di porte che attiverà questa regola quando viene effettuata una richiesta di connessione dal traffico in uscita. Se la connessione in uscita utilizza solo una porta, immettere lo stesso numero di porta in entrambi campi.

PASSAGGIO 4 Nei campi **Intervalli reindirizzati**, immettere il numero di porta o l'intervallo di porte utilizzato dal sistema remoto per rispondere alla richiesta ricevuta. Se la connessione in ingresso utilizza solo una porta, immettere lo stesso numero di porta in entrambi campi.

PASSAGGIO 5 Nel menu a discesa **Interfaccia**, selezionare **Entrambi (Ethernet e 3G)**, **Ethernet** o **3G**.

PASSAGGIO 6 Nel campo **Attiva**, selezionare la casella **Attiva** per attivare la regola.

PASSAGGIO 7 Fare clic su **Salva**.

6

Configurazione VPN

Tipi di tunnel VPN

È possibile configurare la VPN sul proprio dispositivo per avere un canale di comunicazione protetto o un tunnel tra:

- Due router gateway
- Un dispositivo client remoto e un router gateway

Configurazione della VPN IPsec sito a sito di base

Il dispositivo supporta la funzionalità VPN IPsec sito a sito per un tunnel VPN gateway a gateway singolo. Dopo aver configurato le impostazioni VPN di base, è possibile connettersi in modo sicuro a un altro router abilitato per la VPN. Ad esempio, è possibile configurare il dispositivo di un sito di una filiale per connetterlo a un router che collega i tunnel VPN sito a sito al sito aziendale, in modo che il sito della filiale abbia l'accesso protetto alla rete aziendale.

Per configurare le impostazioni VPN di base per una connessione IPsec sito a sito, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **VPN > VPN IPsec sito a sito > Impostazioni VPN di base**.

PASSAGGIO 2 Nel campo **Nuovo nome connessione**, immettere il nome del tunnel VPN.

PASSAGGIO 3 Nel campo **Chiave pre-condivisa**, immettere la chiave pre-condivisa, o la password, che verrà scambiata tra due router. Il numero di caratteri deve essere compreso tra 8 e 49.

PASSAGGIO 4 Nel campo **Informazioni endpoint**, immettere le seguenti informazioni:

- **Endpoint remoto**: selezionare se il router al quale il dispositivo si connette viene identificato dal suo indirizzo IP o da un nome di dominio completo valido. Ad esempio, un indirizzo IP come 192.168.1.1 oppure un nome di dominio completo come cisco.com.
- **Indirizzo IP (Internet) WAN remoto**: immettere l'indirizzo IP pubblico o il nome di dominio dell'endpoint remoto.
- **Indirizzo IP (Internet) WAN locale**: immettere l'indirizzo IP pubblico o il nome di dominio del dispositivo.

PASSAGGIO 5 Nei campi **Accessibilità remota connessione protetta**, immettere le seguenti informazioni:

- **Indirizzo IP (rete locale) LAN remoto**: l'indirizzo (LAN) della rete privata dell'endpoint remoto. Si tratta dell'indirizzo IP della rete interna al sito remoto.
- **Subnet mask LAN remota**: la subnet mask (LAN) della rete privata dell'endpoint remoto.
- **Indirizzo IP (rete locale) LAN locale**: l'indirizzo (LAN) della rete privata appartenente alla rete locale. Si tratta dell'indirizzo IP della rete interna sul dispositivo.
- **Subnet mask (rete locale) LAN locale**: la subnet mask (LAN) della rete privata appartenente alla rete locale.

Nota: gli indirizzi IP LAN e WAN remoti non possono coesistere nella stessa sottorete. Ad esempio, un indirizzo IP LAN remoto di 192.168.1.100 e un indirizzo IP LAN locale di 192.168.1.115 causano un conflitto quando il traffico viene indirizzato sulla VPN. Il terzo ottetto deve essere differente affinché gli indirizzi IP siano su sottoreti diverse. Ad esempio, un indirizzo IP LAN remoto di 192.168.1.100 e un indirizzo IP LAN locale di 192.168.2.100 sono accettabili.

PASSAGGIO 6 Fare clic su **Salva**.

Visualizzazione dei valori predefiniti

Fai clic su **Visualizza impostazioni predefinite** per visualizzare i valori predefiniti utilizzati nelle impostazioni VPN di base. Questi valori sono proposti da VPNC e presumono l'utilizzo di una chiave pre-condivisa o di una password, conosciuta dal dispositivo e dall'endpoint remoto.

Configurazione dei parametri avanzati della VPN IPsec sito a sito

I parametri VPN avanzati come IKE e altri criteri VPN controllano il modo in cui il dispositivo avvia e riceve le connessioni VPN.

Per configurare i parametri VPN avanzati, selezionare **VPN > VPN IPsec sito a sito > Impostazione VPN avanzata**.

Gestione dei criteri IKE

Il protocollo IKE (Internet Key Exchange) consente lo scambio dinamico di chiavi fra due host IPsec. È possibile creare i criteri IKE per definire i parametri di sicurezza da utilizzare durante lo scambio di dati con il router remoto tramite la connessione VPN IPsec. Ad esempio, è possibile creare i criteri IKE per definire i parametri per l'autenticazione dei peer e gli algoritmi di crittografia. Assicurarsi che la crittografia, l'autenticazione e i parametri di gruppo nei criteri VPN siano compatibili con le impostazioni del router remoto.

Per aggiungere in criterio IKE**:**

PASSAGGIO 1 Sulla pagina **Impostazione VPN avanzata**, fare clic su **Aggiungi riga**.

PASSAGGIO 2 Immettere un nome univoco che identifichi il criterio IKE per identificare e gestire il criterio facilmente.

PASSAGGIO 3 Nel campo **Modalità di scambio**, selezionare una delle seguenti modalità per il criterio:

- **Principale**: consente di negoziare il tunnel con una protezione di livello superiore, ma a una minore velocità.
- **Aggressiva**: stabilisce una connessione più veloce, ma con un livello di protezione inferiore.

PASSAGGIO 4 Nei campi **Identificatore locale** e **Identificatore remoto**, indicare se si desidera identificare il proprio dispositivo e il router tramite indirizzo IP effettivo o indirizzo IP pubblico. Se si seleziona l'indirizzo IP, immettere l'indirizzo IP effettivo del dispositivo e del router remoto.

PASSAGGIO 5 Nella sezione **Parametri SA IKE**, configurare i parametri per definire la potenza e la modalità per la negoziazione della SA (Security Association) tra il proprio dispositivo e il router remoto:

a. Nel campo **Algoritmo di crittografia**, selezionare l'algoritmo per crittografare i dati.

b. Nel campo **Algoritmo di autenticazione**, specificare l'algoritmo di autenticazione per l'intestazione VPN. Assicurarsi che l'algoritmo di autenticazione sia configurato in maniera identica su entrambi i lati del tunnel VPN.

c. Nel campo **Chiave pre-condivisa**, immettere la chiave o la password. Assicurarsi che la chiave non contenga le doppie virgolette (").

d. Nel campo **Gruppo Diffie-Hellman (DH)**, specificare l'algoritmo del gruppo DH utilizzato durante lo scambio delle chiavi precondivise. Il gruppo DH imposta la potenza dell'algoritmo in termini di bit. Assicurarsi che il gruppo DH sia configurato in maniera identica su entrambi i lati del criterio IKE.

e. Nel campo **Durata SA**, immettere l'intervallo in secondi passato il quale la SA (Security Association) non sarà più valida.

f. Per attivare la funzione **DPD (Dead Peer Detection)**, selezionare la casella **Attiva**. La funzione DPD viene utilizzata per rilevare se un peer è attivo. Se il peer viene rilevato come inattivo, il dispositivo elimina la SA (Security Association) IPsec e IKE. Se è stata attivata la funzione, immettere anche queste impostazioni:

- **Ritardo DPD**: l'intervallo in secondi che intercorre tra messaggi DPD R-U-THERE consecutivi. I messaggi DPD R-U-THERE vengono inviati solo quando il traffico IPsec è inattivo.
- **Timeout DPD**: il tempo massimo di attesa del dispositivo per ottenere una risposta al messaggio DPD prima di considerare il peer inattivo.

PASSAGGIO 6 Fare clic su **Salva**.

NOTA Se è già stata configurata una connessione VPN, non è possibile aggiungerne un'altra senza prima eliminare quella esistente.

Gestione dei criteri VPN

NOTA Prima di creare un criterio VPN automatico, assicurarsi di creare un criterio IKE in base al quale si desidera creare il criterio VPN automatico.

Per gestire i criteri VPN, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **VPN > VPN IPsec sito a sito > Impostazioni VPN avanzata**. Fare clic su **Aggiungi riga**.

PASSAGGIO 2 Nella sezione **Aggiungi/Modifica configurazione criterio VPN Configurazione**:

a. Nel campo **Nome criterio**, inserire un nome univoco che identifichi il criterio.

b. Nel campo **Tipo di criterio**, scegliere una delle seguenti opzioni:

- **Criterio automatico**: alcuni parametri del tunnel VPN vengono generati automaticamente. Tale operazione richiede l'utilizzo del protocollo IKE (Internet Key Exchange) per le negoziazioni tra i due endpoint della VPN.
- **Criterio manuale**: tutti i parametri (comprese le chiavi) di un tunnel VPN vengono inserite manualmente per ciascun endpoint. In questa operazione non viene coinvolto alcun server o organizzazione di terze parti.

c. **Endpoint remoto**: selezionare il tipo di identificatore da fornire al gateway nell'endpoint remoto: **Indirizzo IP** o **FQDN** (nome di dominio completo). Immettere l'indirizzo IP o l'FQDN.

PASSAGGIO 3 Nelle sezioni **Selezione traffico locale** e **Selezione traffico remoto**:

- Nei campi **IP Locale e IP remoto**, indicare quanti endpoint faranno parte del criterio VPN:
  - **Singolo**: limita il criterio a un unico host. Nel campo **Indirizzo IP**, immettere l'indirizzo IP dell'host che farà parte della VPN.
  - **Sottorete**: consente a un'intera sottorete di connettersi alla rete VPN. Inserire l'indirizzo di rete nel campo **Indirizzo IP**, quindi immettere la subnet mask nel campo **Subnet Mask**. Immettere l'indirizzo IP di rete della sottorete nel campo **Indirizzo IP**. Immettere la subnet mask, ad esempio 255.255.255.0, nel campo **Subnet mask**. Nel campo viene visualizzato automaticamente l'indirizzo di sottorete predefinito in base all'indirizzo IP.

NOTA Non utilizzare sottoreti sovrapposte per i selettori del traffico locale o remoto. L'utilizzo di queste sottoreti richiederebbe l'aggiunta di percorsi statici sul router e sugli host da utilizzare. Ad esempio, evitare:

Selettore del traffico locale: 192.168.1.0/24

Selettore del traffico remoto: 192.168.0.0/16

PASSAGGIO 4 Per un tipo di criterio **manuale**, immettere le impostazioni nella sezione **Parametri criterio manuale**:

- **SPI in arrivo, SPI in uscita**: immettere un valore esadecimale di lunghezza compresa tra 3 e 8 caratteri (ad esempio 0x1234). L'indice SPI (Security Parameter Index) identifica l'associazione di protezione (Security Association, SA) dei flussi di traffico in entrata e in uscita.
- **Algoritmo di crittografia manuale**: selezionare l'algoritmo utilizzato per crittografare i dati.
- **Chiave ingresso, chiave uscita**: immettere la chiave di crittografia del criterio in arrivo e in uscita. La lunghezza della chiave dipende dall'algoritmo di crittografia selezionato:
  - DES, 8 caratteri
  - 3DES, 24 caratteri
  - AES-128, 16 caratteri
  - AES-192, 24 caratteri
  - AES-256, 32 caratteri
- **Algoritmo di integrità manuale**: selezionare l'algoritmo utilizzato per verificare l'integrità dei dati.
- **Chiave ingresso, chiave uscita**: immettere la chiave di integrità (per l'ESP con modalità di integrità) per il criterio in ingresso e in uscita. La lunghezza della chiave dipende dall'algoritmo scelto:
  - MD5, 16 caratteri
  - SHA-1, 20 caratteri
  - SHA2-256, 32 caratteri

PASSAGGIO 5 Per un tipo di criterio **automatico**, immettere le impostazioni nella sezione **Parametri criterio automatico**.

- **Durata SA**: immettere la durata della SA (Security Association) in secondi. Una volta trascorso il numero di secondi specificato, la SA (Security Association) viene rinegoziata. Il valore predefinito è 3.600 secondi. Il valore minimo è 300 secondi.
- **Algoritmo di crittografia**: selezionare l'algoritmo utilizzato per crittografare i dati.
- **Algoritmo di integrità**: selezionare l'algoritmo utilizzato per verificare l'integrità dei dati.

- **Gruppo chiave PFS**: selezionare la casella **Attiva** per attivare la PFS (Perfect Forward Secrecy), in modo da migliorare la protezione. Seppur lento, questo protocollo aiuta a impedire gli ascolti indesiderati garantendo l'esecuzione di uno scambio Diffie-Hellman per ogni negoziazione di fase 2.
- **Gruppo DH:** specificare l'algoritmo del gruppo DH utilizzato durante lo scambio di una chiave precondivisa. Il gruppo DH imposta la potenza dell'algoritmo in termini di bit. Assicurarsi che il gruppo DH sia configurato in maniera identica su entrambi i lati del criterio IKE.
- **Seleziona il criterio IKE**: scegliere il criterio IKE che definirà le caratteristiche della negoziazione SA.

PASSAGGIO 6 Fare clic su **Salva**.

Configurazione del server VPN IPsec

Utilizzando la VPN IPsec viene abilitato l'accesso remoto alle risorse aziendali stabilendo un tunnel crittografato attraverso Internet. Il dispositivo supporta i seguenti client VPN IPsec:

- TheGreenBow
- ShrewSoft

Configurazione del server VPN IPsec

Per configurare il server VPN IPsec:

PASSAGGIO 1 Selezionare **VPN > Server VPN IPsec > Impostazione**.

PASSAGGIO 2 Selezionare la casella di controllo **Attivazione del server**.

PASSAGGIO 3 Nella sezione **Fase1**, configurare le impostazioni per autenticare i due endpoint VPN a vicenda e negoziare l'associazione di protezione (SA) IKE in modo che venga configurato un canale protetto per la negoziazione delle SA nella Fase 2.

a. Nel campo **Chiave pre-condivisa**, immettere la chiave pre-condivisa, o la password, che verrà scambiata tra il proprio dispositivo e l'endpoint remoto. La lunghezza della password deve essere compresa tra 8 e 49 caratteri.

b. Nel campo **Modalità di scambio**, selezionare una delle seguenti modalità per la connessione VPN IPsec:

- **Principale**: consente di negoziare il tunnel con una protezione di livello superiore, ma a una minore velocità.
- **Aggressiva**: stabilisce una connessione più veloce, ma con un livello di protezione inferiore.

c. Scegliere l'**Algoritmo di crittografia** per crittografare i dati, quindi scegliere l'**Algoritmo di autenticazione** per l'intestazione VPN. Assicurarsi che l'algoritmo di autenticazione sia configurato allo stesso modo sul dispositivo e sull'endpoint remoto.

d. Nel campo **Gruppo Diffie-Hellman (DH)**, specificare l'algoritmo del gruppo DH utilizzato durante lo scambio delle chiavi precondivise, il quale imposta la potenza dell'algoritmo in termini di bit. Assicurarsi che il Gruppo DH sia configurato allo stesso modo sul dispositivo e sull'endpoint remoto.

e. Nel campo **IKE Durata SA**, inserire il numero di secondi trascorsi i quali la SA per la connessione VPN viene rinegoziata.

PASSAGGIO 4 Nella sezione **Configurazione fase 2**, impostare i parametri per la negoziazione della SA IPsec per il tunnel IPsec:

a. Nel campo **IP locale** , indicare quanti endpoint faranno parte dei criteri VPN:

- **Singolo**: limita il criterio a un unico host. Nel campo **Indirizzo IP**, immettere l'indirizzo IP dell'host che farà parte della VPN.

- **Sottorete**: consente a un'intera sottorete di connettersi alla rete VPN. Inserire l'indirizzo di rete nel campo **Indirizzo IP**, quindi immettere la subnet mask nel campo **Subnet Mask**. Immettere l'indirizzo IP di rete della sottorete nel campo **Indirizzo IP**. Immettere la subnet mask, ad esempio 255.255.255.0, nel campo **Subnet mask**. Nel campo viene visualizzato automaticamente l'indirizzo di sottorete predefinito in base all'indirizzo IP.

b. Nel campo **Durata SA IPsec** , inserire il numero di secondi trascorsi i quali la SA IPsec per la connessione VPN viene rinegoziata.

c. Scegliere l'**Algoritmo di crittografia** per crittografare i dati, quindi scegliere l'**Algoritmo di autenticazione** per l'intestazione VPN. Assicurarsi che l'algoritmo di autenticazione sia configurato allo stesso modo sul dispositivo e sull'endpoint remoto.

d. Per creare una connessione VPN IPsec più sicura, selezionare la casella di controllo **Abilita gruppo chiave PFS**, garantendo un nuovo scambio di chiave Diffie-Hellman nella fase 2. Perfect Forward Secrecy (PFS) aggiunge un livello di sicurezza proteggendo i dati tramite una nuova chiave, qualora la chiave DH generata nella fase 1 venga compromessa durante il transito. Accertarsi che entrambi gli endpoint IPsec abbiano l'opzione PFS abilitata.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione degli account utente VPN IPsec

PASSAGGIO 1 Selezionare **VPN > Server VPN IPsec > Utente**.

PASSAGGIO 2 Fare clic su **Aggiungi riga**.

PASSAGGIO 3 Immettere il nome utente e la password.

Si consiglia di utilizzare una combinazione di lettere maiuscole e minuscole, numeri e simboli e di non includere nella password parole presenti in dizionari di qualsiasi lingua. La password può essere composta da un massimo di 64 caratteri.

PASSAGGIO 4 Per importare nomi utente e password da un file .CSV, fare clic su **Importa**. Viene visualizzata la pagina **Amministrazione > Utenti**. Nella sezione **Importa nome utente e password**, fare clic su **Sfoglia** per individuare il file, quindi fare clic su **Importa**.

PASSAGGIO 5 Salvare gli account utente.

Configurazione PPTP

PPTP (Point to Point Tunneling Protocol) è un protocollo di rete che consente il trasferimento sicuro di dati da un client remoto a una rete aziendale creando una connessione VPN sicura attraverso reti pubbliche, quali Internet.

Configurazione di un server PPTP

Per configurare il server PPTP VPN:

PASSAGGIO 1 Selezionare **VPN** > **Server PPTP**.

PASSAGGIO 2 Nella sezione **Configurazione server PPTP**, configurare le impostazioni PPTP VPN:

a. Selezionare la casella di controllo **Attivazione del server PPTP**.

b. Immettere l'indirizzo IP del server PPTP.

c. Immettere l'intervallo di indirizzi IP dei client PPTP.

d. Per crittografare i dati che vengono trasmessi tramite connessione PPTP VPN, selezionare la casella di controllo **Attivazione crittografia MPPE**.

PASSAGGIO 3 Fare clic su **Salva**.

Creazione e gestione degli utenti PPTP

Per creare e abilitare utenti PPTP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **VPN > Server PPTP**. Nella **Tabella Account utente PPTP**, fare clic su **Aggiungi riga**.

PASSAGGIO 2 Inserire il nome utente e la password che verranno usati per autenticare l'utente PPTP. Inserire valori compresi tra i 4 e i 32 caratteri di lunghezza.

PASSAGGIO 3 Selezionare la casella di controllo **Attiva** per attivare l'utente.

PASSAGGIO 4 Per importare nomi utente e password da un file .CSV, fare clic su **Importa**. Viene visualizzata la pagina **Amministrazione > Utenti**. Nella sezione **Importa nome utente e password**, fare clic su **Sfoglia** per individuare il file, quindi fare clic su **Importa**.

PASSAGGIO 5 Salvare gli account utente.

Configurazione del passthrough VPN

Il passthrough VPN consente il passaggio del traffico VPN generato dai client VPN attraverso il dispositivo.

Per configurare il passthrough VPN, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **VPN** > **Passthrough VPN**.

PASSAGGIO 2 Selezionare la casella di controllo **Attiva**, per scegliere il tipo di traffico il cui passaggio attraverso il dispositivo è consentito.

PASSAGGIO 3 Fare clic su **Salva**.

Certificato SSL

Cisco RV130/RV130W supporta l'autenticazione di certificato per VPN IPsec. Il certificato SSL (Secure Socket Layer) offr la crittografia dei dati e autentica il server prima che venga stabilita la sessione SSL.

Per gestire il certificato SSL, fare clic su **VPN > Certificato SSL.**

- **Tabella certificati affidabili (certificato CA)**
  - Fare clic su **Carica** per accedere alla pagina **Certificati**. Fare clic su **Sfoglia** per selezionare un certificato attendibile dal disco rigido locale, quindi fare clic su **Importa**.
- **Certificati automatici attivi**
  - Fare clic su **Carica** per accedere alla pagina **Certificati**. Fare clic su **Sfoglia** per selezionare un certificato automatico attivo dal disco rigido locale, quindi fare clic su **Importa**.
- **Richiesta certificati automatici**

  Un certificato automatico viene rilasciato da una CA per identificare il dispositivo dell'utente (oppure autofirmato se non si desidera la protezione dell'identità di una CA). Per richiedere un certificato automatico firmato da una CA, è possibile generare una richiesta di firma del certificato dal gateway immettendo i parametri di identificazione e inviandoli alla CA per la firma. Una volta firmato, il certificato attendibile della CA e quello firmato

dalla CA vengono caricati per attivare il certificato automatico che consente di convalidare l'identità di questo gateway. Il certificato automatico viene quindi utilizzato nelle connessioni IPsec con i peer per convalidare l'autenticità del gateway.

- **Genera certificato**: per generare una richiesta di certificato SSL, fare clic su **Genera certificato** che permette di visualizzare una nuova pagina di richiesta per le informazioni relative al certificato.

  Nome: immettere il nome del nuovo certificato.

  Oggetto: rispettare il formato 'CN=xxx' ('CN' scritto in maiuscolo).

  Algoritmo hash: selezionare l'algoritmo hash appropriato dall'elenco a discesa.

  Algoritmo firma: selezionare l'algoritmo firma appropriato dall'elenco a discesa.

  Lunghezza chiave firma: selezionare la lunghezza chiave firma appropriata dall'elenco a discesa.

  Indirizzo IP (opzionale): immettere l'indirizzo IP del router.

  Nome di dominio (opzionale): immettere il nome di dominio del router.

  Indirizzo e-mail (opzionale): immettere l'indirizzo e-mail dei richiedenti.

  - **Esporta per amministratore**: esportare le richieste di certificato nel disco rigido locale.

- **Esporta certificato**: per scaricare il certificato del router, fare clic sul pulsante **Esporta per client**.

Fare clic su **Salva** per salvare la configurazione, oppure su **Annulla** per ripristinare le impostazioni.

Installazione guidata VPN

Per utilizzare la procedura di installazione guidata VPN, attenersi alla procedura seguente:

PASSAGGIO 1 Fare clic su **VPN > Installazione guidata VPN**.

PASSAGGIO 2 Verrà visualizzata la finestra dell'installazione guidata. Attenersi alle istruzioni visualizzate sullo schermo per configurare il dispositivo.

7

Configurazione della Qualità del servizio (QoS)

QoS assegna la priorità ad applicazioni, utenti o flussi di dati, oppure garantisce un determinato livello di prestazioni per un flusso di dati. Tali garanzie sono importanti in caso di capacità di rete insufficiente. Ad esempio per le applicazioni multimediali in streaming in tempo reale, come voice-over-IP, giochi online e IPTV, che richiedono una velocità di dati fissa e avvertono notevolmente qualsiasi ritardo, nonché per le reti limitate in termini di capacità.

Configurazione della gestione della larghezza di banda

È possibile utilizzare la funzione di gestione della larghezza di banda del dispositivo per gestire la larghezza di banda del traffico dalla rete sicura (LAN) alla rete non sicura (WAN).

Configurazione della larghezza di banda

È possibile limitare la larghezza di banda per ridurre la velocità con cui il dispositivo trasmette i dati. Inoltre è possibile utilizzare un profilo della larghezza di banda per limitare il traffico in uscita ed evitare che gli utenti della LAN consumino tutta la larghezza di banda del collegamento Internet.

Per impostare la larghezza di banda upstream e downstream, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **QoS** > **Gestione larghezza di banda**.

PASSAGGIO 2 Nel campo **Gestione larghezza di banda**, selezionare **Attiva**. La larghezza di banda massima fornita dall'ISP viene visualizzata nella sezione **Larghezza di banda**.

PASSAGGIO 3 Nella **Tabella larghezza di banda**, immettere le seguenti informazioni per l'interfaccia WAN:

Upstream	La larghezza di banda (kb/s) utilizzata per inviare i dati su Internet.
Downstream	La larghezza di banda (kb/s) utilizzata per ricevere i dati da Internet (si applica solo alla VLAN predefinita).

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione della priorità della larghezza di banda

Nella **Tabella priorità larghezza di banda**, è possibile assegnare priorità ai servizi per gestire l'utilizzo della larghezza di banda.

Per configurare la priorità della larghezza di banda, attenersi alla seguente procedura:

PASSAGGIO 1 Nella **Tabella priorità larghezza di banda**, fare clic su **Aggiungi riga**.

PASSAGGIO 2 Inserire le informazioni nei seguenti campi:

Attiva	Selezionare questa opzione per attivare la gestione della larghezza di banda per il servizio.
Direzione	Scegliere se impostare la priorità per il traffico in entrata o in uscita.
Categoria	Scegliere se impostare la priorità della larghezza di banda per servizio, VLAN/SSID, IP di origine (traffico in entrata) o IP di destinazione (traffico in uscita).
Servizio	Selezionare il servizio a cui assegnare la priorità.
VLAN/SSID	Selezionare la VLAN o il SSID per cui si desidera impostare la priorità.
Indirizzo IP	Se si seleziona IP di origine o IP di destinazione nel campo **Categoria**, immettere l'indirizzo IP e la subnet mask del punto di origine o di destinazione.
Subnet mask	

Priorità	Impostare la priorità (**bassa**, **media** o **alta**) per la categoria selezionata.
Contrassegnazione	Spuntare la casella per attivare la contrassegnazione sul DSCP (Differentiated Services Code Point). Se si attiva questa funzione, la priorità del traffico di rete della LAN viene assegnata in base alla mappatura della coda DSCP nella pagina **Impostazioni DSCP**.
DSCP	Immettere il valore di contrassegnazione per i pacchetti su questa rete.

PASSAGGIO 3 Fare clic su **Salva**.

Per modificare le impostazioni di una voce della tabella, selezionare la relativa casella e fare clic su **Modifica**. Una volta terminate le modifiche, fare clic su **Salva**.

Per eliminare una voce dalla tabella, selezionare la relativa casella e fare clic su **Elimina**. Fare clic su **Salva**.

Per aggiungere una nuova definizione del servizio, fare clic sul pulsante **Gestione servizio**. È possibile definire un nuovo servizio da utilizzare per tutte le definizioni del firewall e QoS. Vedere la sezione **Configurazione della gestione servizi**.

Configurazione delle impostazioni di QoS basato su porta

È possibile configurare le impostazioni QoS per ciascuna porta del dispositivo. Il supporta quattro code di priorità che permettono di assegnare una priorità al traffico per ciascuna porta.

Per configurare le impostazioni di QoS per le porte del dispositivo, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **QoS** > **Impostazioni QoS basato su porta**.

PASSAGGIO 2 Per ciascuna porta della tabella **Impostazioni QoS basato su porta**, immettere le informazioni seguenti:

Modalità Trust	Selezionare una delle seguenti opzioni dal menu a discesa: • **Porta**: abilita le impostazioni QoS basato su porta. È possibile impostare la priorità del traffico per una determinata porta. La priorità della coda di traffico è compresa fra 1 (valore più basso) e 3 (valore più alto). • **DSCP**: DSCP (Differentiated Services Code Point). Se si attiva questa funzione, la priorità del traffico di rete della LAN viene assegnata in base alla mappatura della coda DSCP nella pagina **Impostazioni DSCP**. • **CoS**: classe di servizio.
Coda reindirizzamento traffico predefinita per dispositivi non attendibili	Selezionare un livello di priorità per il traffico in uscita (da 1 a 3).

PASSAGGIO 3 Fare clic su **Salva**.

Per ripristinare le impostazioni predefinite di QoS basato su porta, fare clic su **Ripristina predefiniti** e salvare le modifiche.

Configurazione delle impostazioni CoS

Utilizzare il collegamento alla pagina Impostazioni QoS basato su porta per mappare le impostazioni di priorità CoS alla coda QoS.

Per associare le impostazioni di priorità CoS alla coda di reindirizzamento del traffico, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **QoS** > **Impostazioni CoS**.

PASSAGGIO 2 Per ciascun livello di priorità CoS nella **tabella delle impostazioni CoS**, selezionare un valore di priorità dal menu a discesa **Coda reindirizzamento traffico**.

Questi valori contrassegnano i tipi di traffico con priorità di traffico maggiore o minore a seconda del tipo di traffico.

PASSAGGIO 3 Fare clic su **Salva**.

Per ripristinare le impostazioni predefinite di QoS basato su porta, fare clic su **Ripristina predefiniti** e su **Salva**.

Configurazione delle impostazioni DSCP

Utilizzare la pagina **Impostazioni DSCP** per configurare la mappatura della coda DSCP a QoS.

Per configurare la mappatura della coda DSCP a QoS, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **QoS** > **Impostazioni DSCP**.

PASSAGGIO 2 Scegliere se elencare solo i valori RFC o tutti i valori DSCP nella **tabella delle impostazioni DSCP** facendo clic sul pulsante appropriato.

PASSAGGIO 3 Per ciascun valore DSCP nella **tabella delle impostazioni DSCP**, selezionare un livello di priorità dal menu a discesa **Coda**.

Viene quindi eseguita la mappatura del valore DSCP al valore della coda QoS selezionata.

PASSAGGIO 4 Fare clic su **Salva**.

Per ripristinare le impostazioni DSCP predefinite, fare clic su **Ripristina predefiniti**, quindi su **Salva**.

8

Gestione del dispositivo

Impostazione delle proprietà del dispositivo

Assegnare un nome e un nome dominio al dispositivo per garantire che venga facilmente identificato da altri dispositivi.

Per configurare le proprietà del dispositivo:

PASSAGGIO 1 Selezionare **Amministrazione> Proprietà del dispositivo**.

PASSAGGIO 2 Nel campo **Nome host**, inserire un nome per identificare il dispositivo in maniera univoca sulla propria rete. Ad esempio, RTR141.

PASSAGGIO 3 Nel campo **Nome dominio**, inserire il nome del dominio nel quale è collocato il dispositivo. Ad esempio, abcbusiness.com. Se non si conosce il nome del dominio della propria organizzazione, contattare l'amministratore di rete.

PASSAGGIO 4 Salvare le modifiche.

Impostazione della complessità password

È possibile impostare un requisito minimo di complessità richiesto per le modifiche della password.

Per configurare le impostazioni di complessità password, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Complessità password**.

PASSAGGIO 2 Nel campo **Impostazioni complessità password**, selezionare **Attiva**.

PASSAGGIO 3 Configurare le impostazioni di complessità password.

Lunghezza minima password	Immettere la lunghezza minima della password (0-64 caratteri).
Numero minimo classi di caratteri	Immettere un numero che rappresenti una delle seguenti classi di carattere: • Lettere maiuscole • Lettere minuscole • Numeri • Caratteri speciali disponibili su una tastiera standard Per impostazione predefinita, le password devono contenere caratteri di almeno tre di queste classi.
La nuova password deve essere diversa da quella attuale	Selezionare **Attiva** per impedire che la nuova password sia uguale a quella corrente.
Scadenza password	Selezionare **Attiva** per impostare la scadenza delle password dopo un determinato periodo.
Durata password	Immettere il numero di giorni massimo della durata della password (1-365). Il valore predefinito è 180 giorni.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione degli account utente

Il dispositivo supporta due account utente per le impostazioni di amministrazione e visualizzazione: un utente amministrativo (nome utente e password predefiniti: cisco) e un utente ospite (nome utente predefinito: guest).

L'account ospite ha l'accesso in sola lettura. È possibile impostare e modificare il nome utente e la password per entrambi gli account.

Per configurare gli account utente, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Utenti**.

PASSAGGIO 2 Nel campo **Attivazione account**, selezionare le caselle per gli account che si desidera attivare. (l'account amministratore deve essere attivo).

PASSAGGIO 3 (Opzionale) Per modificare l'account amministratore, sotto **Impostazione account amministratore** selezionare **Modifica impostazioni amministratore**. Per modificare l'account ospite, sotto Impostazioni ospite selezionare **Modifica impostazioni ospite**. Immettere le seguenti informazioni:

Nuovo nome utente	Immettere un nuovo nome utente.
Vecchia password	Immettere la password corrente.
Nuova password	Immettere la nuova password. Si consiglia di utilizzare una combinazione di lettere maiuscole e minuscole, numeri e simboli e di non includere nella password parole presenti in dizionari di qualsiasi lingua. La password può essere composta da un massimo di 64 caratteri.
Digita di nuovo la nuova password	Immettere di nuovo la nuova password.

PASSAGGIO 4 Fare clic su **Salva**.

Importazione degli account utente

È possibile importare diversi utenti contemporaneamente utilizzando un file CSV.

Assicurarsi che i dati del file CSV vengano disposti come illustrato nella seguente tabella:

TIPO	NOME UTENTE	PASSWORD
Amministratore	Ammin123	Ammin123
Ospite	Ospite123	Ospite123

TIPO	NOME UTENTE	PASSWORD	ATTIVA
PPTP	pptp-user-1	12345678	enable
PPTP	pptp-user-2	345123678	disable

TIPO	NOME UTENTE	PASSWORD
VPNServer	vpn-user-1	12345678
VPNServer	vpn-user-2	33245678

TIPO	NOME UTENTE	PASSWORD	ACCESS_TIME
rete ospite	guestnet-user-1	12345678	1440
rete ospite	guestnet-user-2	33245678	60

NOTA I nomi delle colonne fanno distinzione tra maiuscole e minuscole. Non modificare l'ordine o i nomi delle colonne.

Per importare gli account utente da un file CSV:

PASSAGGIO 1 Nel campo **Importa nome utente e password**, fare clic su **Sfoglia**.

PASSAGGIO 2 Selezionare il file e fare clic su **Apri**.

PASSAGGIO 3 Fare clic su **Importa**.

Impostazione dell'intervallo di timeout della sessione

L'intervallo di timeout è il numero massimo di minuti di inattività dopo il quale la sessione del Device Manager viene terminata. L'intervallo di timeout può essere configurato per gli account Amministratore e Ospite.

Per configurare il timeout della sessione, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministratore** > **Timeout sessione**.

PASSAGGIO 2 Nel campo **Timeout inattività amministratore**, immettere il numero, in minuti, dopo il quale la sessione verrà terminata per inattività. Scegliere **Mai** per consentire all'amministratore di rimanere sempre connesso.

PASSAGGIO 3 Nel campo **Timeout inattività ospite**, immettere il numero, in minuti, dopo il quale la sessione verrà terminata per inattività. Scegliere **Mai** per consentire all'amministratore di rimanere sempre connesso.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione di SNMP (Simple Network Management Protocol)

SNMP (Simple Network Management Protocol) consente di monitorare e gestire il router da un manager SNMP. SNMP fornisce un mezzo remoto per monitorare e controllare i dispositivi di rete e per gestire configurazioni, raccolta di statistiche, prestazioni e sicurezza.

Configurazione delle informazioni di sistema SNMP

NOTA Prima di usare SNMP, installare il software SNMP sul computer. Il dispositivo supporta solo SNMPv3 per la gestione SNMP e SNNPv1/2/3 per i messaggi trap SNMP.

Per attivare SNMP, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **SNMP**.

PASSAGGIO 2 Selezionare **Attiva** per attivare SNMP.

PASSAGGIO 3 Selezionare **Attiva** per abilitare l'opzione **Consenti l'accesso utente tramite Internet** o **Consenti l'accesso utente tramite VPN**.

PASSAGGIO 4 Selezionare la versione SNMP nel campo **Modalità**.

PASSAGGIO 5 Immettere le informazioni seguenti:

SysContact	Immettere il nome della persona da contattare per questo dispositivo. Ad esempio, l'amministratore di rete.
SysLocation	Immettere la descrizione della posizione fisica del dispositivo. Ad esempio, Rack 2, quarto piano.
SysName	Immettere un nome che consenta di identificare il dispositivo facilmente. Ad esempio, RTR 141.

PASSAGGIO 6 Fare clic su **Salva**.

Modifica degli utenti SNMPv3

È possibile configurare i parametri SNMPv3 per i due account utente predefiniti del dispositivo (Amministratore e Ospite).

Per configurare le impostazioni SNMPv3, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **SNMP**.

PASSAGGIO 2 Nella sezione **Configurazione utente SNMPv3**, configurare le seguenti impostazioni:

Nome utente	Selezionare l'account da configurare (**admin** o **ospite**).
Privilegio d'accesso	Visualizza i privilegi di accesso dell'account utente selezionato.
Livello di protezione	Selezionare il livello di protezione SNMPv3: **Nessuna autenticazione e nessun privilegio**: non richiede autenticazione e privacy. **Autenticazione e nessun privilegio**: invia solo l'algoritmo di autenticazione e la password. **Autenticazione e privilegio**: invia l'algoritmo di autenticazione/privacy e la password.

Server algoritmo autenticazione	Selezionare il tipo di algoritmo di autenticazione (**MD5** o **SHA**).
Password di autenticazione	Immettere la password di autenticazione.
Algoritmo di privacy	Selezionare il tipo di algoritmo di privacy (**DES** o **AES**).
Password privacy	Immettere la password di privacy.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione dei trap SNMP

I campi della sezione **Configurazione trap SNMP** consentono di configurare un agente SNMP al quale il dispositivo invia i messaggi di trap (notifiche).

Per configurare i trap, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **SNMP**.

PASSAGGIO 2 Nella sezione **Configurazione trap**, configurare le seguenti impostazioni:

Indirizzo IP	Immettere l'indirizzo IP del manager SNMP o dell'agente trap.
Porta	Immettere la porta trap SNMP dell'indirizzo IP al quale verranno inviati i messaggi trap.
Comunità	Immettere la stringa della comunità alla quale appartiene l'agente. La maggior parte degli agenti è configurata per l'ascolto dei trap nella comunità Pubblica.
Versione SNMP	Selezionare la versione SNMP: **v1**, **v2c** o **v3**.
Livello di gravità trap SNMP	Scegliere il livello di gravità in base al quale il dispositivo deve inviare messaggi trap.

PASSAGGIO 3 Fare clic su **Salva**.

Utilizzo degli strumenti di diagnostica

Il dispositivo mette a disposizione diversi strumenti di diagnostica per la risoluzione dei problemi di rete.

- **Strumenti di rete**
- **Configurazione del mirroring delle porte**

Strumenti di rete

Utilizzare gli strumenti di rete per risolvere gli errori di rete.

Utilizzo di PING

È possibile utilizzare l'utilità Ping per testare la connettività tra il router e un altro dispositivo della rete. Lo strumento Ping può anche essere utilizzato per testare la connessione a Internet eseguendo il ping di un nome di dominio valido, ad esempio www.cisco.com.

Per utilizzare il PING, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Diagnostica** > **Strumenti di rete**.

PASSAGGIO 2 Nel campo **Indirizzo IP/Nome dominio**, immettere l'indirizzo IP o un nome di dominio valido, ad esempio www.cisco.com, sul quale effettuare il ping.

PASSAGGIO 3 Fare clic su **Ping**. Vengono visualizzati i risultati del ping, che indicano se il dispositivo è raggiungibile.

Utilizzo di Traceroute

L'utilità Traceroute visualizza tutti i router presenti tra l'indirizzo IP di destinazione e il router. Il router visualizza fino a 30 hop (router intermedi) tra il router e la destinazione.

Per utilizzare Traceroute, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Diagnostica** > **Strumenti di rete**.

PASSAGGIO 2 Nel campo **Indirizzo IP/Nome dominio**, immettere l'indirizzo IP da tracciare.

PASSAGGIO 3 Fare clic su **Traceroute**. Vengono visualizzati i risultati di Traceroute.

Esecuzione di una ricerca DNS

È possibile utilizzare lo strumento di ricerca per trovare l'indirizzo IP di un host, ad esempio un server Web, FTP o di posta, su Internet.

Per recuperare l'indirizzo IP di un server Web, FTP, di posta o qualsiasi altro server su Internet, digitare il nome Internet nella casella di testo e fare clic su **Ricerca**. Se la voce host o di dominio esiste, verrà restituita una risposta con l'indirizzo IP. Il messaggio "Host sconosciuto" indica che il nome Internet specificato non esiste.

Per utilizzare lo strumento di ricerca, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Diagnostica** > **Strumenti di rete**.

PASSAGGIO 2 Nel campo **Nome Internet**, immettere il nome Internet dell'host.

PASSAGGIO 3 Fare clic su **Ricerca**. Vengono visualizzati i risultati di nslookup.

Configurazione del mirroring delle porte

La funzione di mirroring delle porte monitora il traffico di rete mediante l'invio di copie dei pacchetti in ingresso e in uscita a una porta di monitoraggio. È possibile utilizzare il mirroring delle porte come strumento diagnostico o di debug, soprattutto quando si cerca di difendersi da un attacco o si esamina il traffico utente da LAN a WAN per vedere se gli utenti accedono a informazioni o siti Web ai quali non dovrebbero accedere.

Per evitare problemi con il mirroring delle porte, l'host LAN deve utilizzare un indirizzo IP statico. Se non viene configurato un indirizzo IP statico per l'host LAN, i lease DHCP possono scadere per l'host LAN e provocare errori di mirroring della porta.

Per configurare il mirroring delle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Diagnostica** > **Mirroring delle porte**.

PASSAGGIO 2 Nel campo **Origine mirroring**, selezionare le porte su cui eseguire il mirroring.

PASSAGGIO 3 Dal menu a discesa **Porta di mirroring**, selezionare una porta di mirroring. Se si utilizza una porta per il mirroring, non usarla per altri tipi di traffico.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle impostazioni di log ed e-mail

Configurare i log per monitorare le attività associate all'integrità e al livello di prestazioni del dispositivo.

Configurazione delle impostazioni di log

Per configurare la registrazione, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Registrazione** > **Impostazioni registro**.

PASSAGGIO 2 Nel campo **Modalità registro**, selezionare la casella di controllo **Attiva**.

PASSAGGIO 3 Selezionare la casella di controllo **Attivazione avviso tramite e-mail** per configurare il dispositivo in modo che invii avvisi a un indirizzo e-mail specifico in caso di eventi o comportamenti che possano influire su prestazioni, funzionamento e sicurezza del dispositivo o a scopo di debug. Selezionare la casella appropriata per attivare gli avvisi tramite e-mail per i seguenti eventi:

WAN attivo/inattivo	Invia un avviso tramite e-mail quando il collegamento WAN è inattivo e invia un'altra e-mail quando il collegamento è nuovamente attivo.
Tunnel VPN IPsec sito a sito attivo/inattivo	Invia un'e-mail quando il tunnel VPN IPsec sito a sito è inattivo e invia un'ulteriore e-mail quando il tunnel è nuovamente attivo.
Sovraccarico della CPU	Invia un'e-mail di avviso quando l'utilizzo della CPU è superiore alla soglia e invia un'ulteriore e-mail quando rientra nuovamente nei valori normali.
Avvio del sistema	Invia un avviso tramite e-mail all'avvio del dispositivo.

Nuovo firmware disponibile	Invia un avviso tramite e-mail quando è disponibile un nuovo firmware per il dispositivo.

PASSAGGIO 4 Fare clic su **Aggiungi riga**.

PASSAGGIO 5 Configurare le seguenti impostazioni:

Server di log remoto	Immettere l'indirizzo IP del server di log in cui vengono gestiti i registri.
Gravità log per log locale ed e-mail	Scegliere il livello di gravità dell'evento in base al quale si desidera mantenere i registri e inviarli a un indirizzo e-mail specifico. Tutti i tipi di log con un livello di gravità più alto rispetto al tipo di log selezionato vengono automaticamente inclusi e non è possibile escluderli. Ad esempio, se si selezionano i log errore, verranno selezionati anche i log emergenza, allarme e critici. I livelli di gravità degli eventi sono elencati dalla gravità maggiore alla minore: • **Emergenza**: il sistema non è utilizzabile. • **Allarme**: è necessaria un'azione. • **Critico**: il sistema è in una condizione critica. • **Errore**: il sistema è in una condizione di errore. • **Avviso**: è stato generato un avviso di sistema. • **Notifica**: il sistema funziona correttamente, ma è stata generata una notifica di sistema. • **Informazioni**: informazioni sul dispositivo. • **Debug**: informazioni dettagliate sugli eventi. Scegliendo questo livello di gravità dei log si genera un lungo elenco di log e ciò non è consigliabile durante le normali operazioni del router.
Attiva	Per attivare queste impostazioni di registrazione, selezionare questa casella.

PASSAGGIO 6 Fare clic su **Salva**.

PASSAGGIO 7 Fare clic su **Visualizza log** per visualizzare la tabella dei log di sistema.

Per modificare una voce nella **Tabella impostazioni registro**, selezionare la voce e fare clic su **Modifica**. Effettuare le modifiche quindi fare clic su **Salva**.

Configurazione invio dei registri tramite e-mail

È possibile configurare il dispositivo in modo da inviare i registri tramite e-mail. Si consiglia di impostare un account e-mail separato per l'invio e la ricezione di registri.

Per prima cosa è necessario configurare la gravità dei registri da acquisire; vedere la sezione **Configurazione delle impostazioni di log**.

Per configurare l'invio dei registri tramite e-mail, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Registrazione** > **Impostazioni e-mail**.

PASSAGGIO 2 Per attivare l'invio degli eventi di registro tramite e-mail, selezionare **Attiva**.

Viene visualizzata la gravità minima del registro e-mail per i registri da acquisire. Per modificarla, fare clic su **Configura gravità**.

PASSAGGIO 3 Configurare le seguenti impostazioni:

Indirizzo server e-mail	Immettere l'indirizzo del server SMTP. Si tratta del server di posta associato all'account e-mail configurato (ad esempio mail.nomeazienda.it).
Porta server e-mail	Immettere la porta del server SMTP. Se il provider della posta elettronica richiede una porta speciale per le e-mail, inserirla qui. Altrimenti lasciare l'impostazione predefinita, 25.
Indirizzo e-mail risposta	Inserire l'indirizzo e-mail di risposta al quale il dispositivo invierà messaggi nel caso non fosse possibile inviare i registri dal router all'indirizzo e-mail di destinazione.

Invia a indirizzo e-mail (1)	Immettere l'indirizzo e-mail a cui inviare i registri (ad esempio, registri@nomeazienda.it).
Invia a indirizzo e-mail (2) (opzionale)	
Invia a indirizzo e-mail (3) (opzionale)	
Crittografia e-mail	Selezionare SSL o TSL come metodo di crittografia e-mail. Selezionare Disattiva se non si desidera utilizzare un metodo di crittografia e-mail.
Autenticazione con server SMTP	Se il server (di posta) SMTP richiede l'autenticazione per accettare i collegamenti, selezionare il tipo di autenticazione dal menu a discesa: **Nessuno**, **ACCESSO**, **NORMALE** e **CRAM-MD5**.
Nome utente autenticazione e-mail	Immettere il nome utente di autenticazione e-mail (ad esempio, registri@nomeazienda.it).
Password autenticazione e-mail	Inserire la password di autenticazione e-mail (ad esempio, la password utilizzata per accedere all'account e-mail configurato come destinatario dei registri).
Test autenticazione e-mail	Fare clic su **Test** per testare l'autenticazione e-mail.

PASSAGGIO 4 Nella sezione **Invia registri tramite e-mail in base a pianificazione**, configurare le seguenti impostazioni:

Unità	Selezionare l'unità di tempo dei registri (**Mai**, **Ogni ora**, **Ogni giorno** o **Ogni settimana**). Se si seleziona **Mai**, i registri non vengono inviati.
Giorno	Se si sceglie un programma settimanale per l'invio dei registri, selezionare il giorno della settimana in cui inviare i registri.

Ora	Se si sceglie un programma quotidiano o settimanale per l'invio dei registri, selezionare l'ora del giorno in cui inviare i registri.

PASSAGGIO 5 Fare clic su **Salva**.

Configurazione di Bonjour

Bonjour è un protocollo di annuncio di servizio e di rilevamento. Sul dispositivo, Bonjour pubblicizza solo i servizi di default configurati sul dispositivo quando Bonjour è abilitato.

Per abilitare Bonjour, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Bonjour**.

PASSAGGIO 2 Selezionare **Attiva** per attivare Bonjour.

PASSAGGIO 3 Per attivare Bonjour per una VLAN elencata nella **Tabella controlli interfaccia Bonjour**, selezionare la casella **Attiva Bonjour** corrispondente.

È possibile attivare Bonjour su VLAN specifiche. L'attivazione di Bonjour su una VLAN consente ai dispositivi presenti sulla VLAN di rilevare i servizi Bonjour disponibili sul router, come HTTP/HTTPS.

Ad esempio, se una VLAN è configurata con un ID di 2, i dispositivi e gli host presenti sulla VLAN 2 non possono rilevare i servizi Bonjour in esecuzione sul router a meno che Bonjour non sia abilitato per VLAN 2.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione delle impostazioni di data e ora

È possibile configurare il fuso orario, scegliere se regolare o meno l'ora legale e definire il server NTP (Network Time Protocol) da utilizzare per sincronizzare la data e l'ora. Il router ottiene le informazioni relative alla data e all'ora dal server NTP.

Per configurare le impostazioni di NTP e dell'ora, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Impostazioni ora**. Viene indicata l'ora corrente.

PASSAGGIO 2 Inserire le informazioni nei seguenti campi:

Fuso orario	Selezionare il proprio fuso orario in relazione all'ora di Greenwich (GMT).
Regola per l'ora legale	Se applicabile alla propria area geografica, selezionare la casella **Regola per l'ora legale**. Questa casella di controllo diventa non disponibile se si fa clic su **Manuale** nel campo **Imposta data e ora**.
Modalità Ora legale	Se si seleziona **Per data**, immettere la data specifica in cui avviare la modalità Ora legale. Se si seleziona **Ricorrente**, immettere il mese, la settimana, il giorno della settimana e l'ora in cui avviare la modalità Ora legale. Immettere le informazioni appropriate nei campi **da** e **a**.
Differenza ora legale	Selezionare dal menu a discesa lo scostamento dall'ora UTC (Coordinated Universal Time).
Imposta data e ora	Scegliere se si desidera che la data e l'ora sul dispositivo vengano impostate manualmente o automaticamente. Se si seleziona **Manuale**, inserire la data e l'ora nei campi **Inserire data e ora**.
Server NTP	Per utilizzare i server NTP predefiniti, fare clic sul pulsante **Usa predefinito**. Per utilizzare un server NTP specifico, fare clic su **Server NTP definito dall'utente** e immettere il nome di dominio completo o l'indirizzo IP dei server NTP nei due campi disponibili.

PASSAGGIO 3 Fare clic su **Salva**.

Backup e ripristino del sistema

È possibile effettuare un backup delle impostazioni di configurazione personalizzate per un ripristino successivo oppure effettuare il ripristino da un backup precedente dalla pagina **Amministrazione > Impostazioni backup/ ripristino**.

Se il firewall funziona come da configurazione, è possibile eseguire un backup per un ripristino successivo. Durante il backup le impostazioni vengono salvate come file su un PC. È possibile ripristinare le impostazioni del firewall da questo file.

ATTENZIONE Durante l'operazione di ripristino non tentare di connettersi online, spegnere il firewall, spegnere il PC oppure utilizzare il firewall prima che sia stata completata l'operazione. L'operazione dovrebbe durare circa un minuto. Quando la spia di test si spegne, attendere ancora qualche secondo prima di utilizzare il firewall.

Backup delle impostazioni di configurazione

Per eseguire il backup o il ripristino della configurazione, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Impostazioni backup/ripristino**.

PASSAGGIO 2 Selezionare la configurazione di cui effettuare il backup o da cancellare:

Configurazione iniziale	Selezionare questa opzione per scaricare la configurazione iniziale. La configurazione iniziale è la configurazione più recente utilizzata dal dispositivo. Se la configurazione iniziale del router è stata persa, utilizzare questa pagina per copiare la configurazione di backup nella configurazione iniziale e mantenere intatte tutte le informazioni della configurazione precedente. Per facilitare la distribuzione è possibile scaricare la configurazione iniziale su altre unità RV130/RV130W.
Configurazione mirror	Selezionare questa opzione se si desidera che il dispositivo esegua il backup della configurazione iniziale dopo 24 ore di funzionamento senza modifiche della configurazione iniziale.
Configurazione di backup	Selezionare questa opzione per effettuare il backup delle impostazioni di configurazione correnti.

PASSAGGIO 3 Per scaricare un file di backup basato sull'opzione di configurazione selezionata, fare clic su **Download**.

Il file (startup.cfg, mirror.cfg o backup.cfg) viene scaricato per impostazione predefinita nella cartella predefinita Download, ad esempio C:\Documents and Settings\Administrator\Documenti\Download\.

PASSAGGIO 4 Per cancellare la configurazione selezionata, fare clic su **Cancella**.

Ripristino delle impostazioni di configurazione

Per ripristinare un file di configurazione salvato in precedenza:

PASSAGGIO 1 Selezionare **Amministrazione** > **Impostazioni backup/ripristino**.

PASSAGGIO 2 Nel campo Caricamento configurazione, selezionare la configurazione da caricare (**Configurazione iniziale** o **Configurazione di backup**).

PASSAGGIO 3 Fare clic su **Sfoglia** per selezionare il file.

PASSAGGIO 4 Selezionare il file e fare clic su **Apri**.

PASSAGGIO 5 Fare clic su **Avvia caricamento**.

Il dispositivo carica il file di configurazione e utilizza le impostazioni contenute per aggiornare la configurazione iniziale. Quindi, il dispositivo viene riavviato e utilizza la nuova configurazione.

Copia delle impostazioni di configurazione

Copiare la configurazione iniziale nella configurazione di backup per garantire la disponibilità di una copia di backup nel caso l'utente dimenticasse il nome utente e la password, impedendo l'accesso a Device Manager. Per tornare al Device Manager, ripristinare le impostazioni di fabbrica del dispositivo.

La configurazione di backup rimane in memoria e permette di copiare le informazioni di backup nella configurazione iniziale ripristinando tutte le impostazioni.

Per copiare una configurazione, ad esempio una configurazione iniziale nella configurazione di backup, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Impostazioni backup/ripristino**.

PASSAGGIO 2 Nel campo **Copia**, selezionare le configurazioni di origine e di destinazione dal menu a discesa.

PASSAGGIO 3 Fare clic su **Avvia copia**.

Generazione di una chiave di crittografia

Il router consente di generare una chiave di crittografia per la protezione dei file di backup.

Per generare una chiave di crittografia, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Impostazioni backup/ripristino**.

PASSAGGIO 2 Fare clic su **Mostra impostazioni avanzate**.

PASSAGGIO 3 Nella casella, immettere il seed utilizzato per generare la chiave.

PASSAGGIO 4 Fare clic su **Salva**.

Aggiornamento del firmware o modifica della lingua

L'aggiornamento a una nuova versione del firmware o la modifica della lingua del router vengono eseguiti dalla pagina **Amministrazione** > **Aggiornamento firmware/lingua**.

ATTENZIONE Durante l'aggiornamento del firmware, non tentare di connettersi online, spegnere l'unità, spegnere il PC oppure interrompere il processo in qualsiasi modo prima che sia stata completata l'operazione. Il processo richiede circa un minuto, incluso il riavvio. L'interruzione del processo di aggiornamento in punti specifici di scrittura della memoria flash può danneggiarla e rendere il router inutilizzabile.

Aggiornamento del firmware

Per aggiornare il router con una nuova versione del firmware, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Aggiornamento firmware/lingua**.

PASSAGGIO 2 (Opzionale) Fare clic su **Download** per scaricare l'ultima versione del firmware.

PASSAGGIO 3 Nel campo **Tipo di file**, fare clic sul pulsante di scelta **Immagine firmware**.

PASSAGGIO 4 Fare clic su **Sfoglia** per individuare e selezionare il firmware scaricato.

PASSAGGIO 5 (Opzionale) Per ripristinare le impostazioni di fabbrica del dispositivo dopo avere aggiornato il firmware, selezionare **Ripristinare tutte le configurazioni/ impostazioni di fabbrica**.

ATTENZIONE Il ripristino delle impostazioni predefinite del dispositivo elimina tutte le impostazioni di configurazione.

PASSAGGIO 6 Fare clic su **Avvia aggiornamento**.

Dopo la convalida, la nuova immagine firmware viene scritta nella memoria flash e il router viene riavviato automaticamente con il nuovo firmware.

PASSAGGIO 7 Scegliere **Stato** > **Riepilogo di sistema** per accertarsi che sul router sia stata installata la nuova versione firmware.

Modifica della lingua

Per modificare la lingua sul dispositivo:

PASSAGGIO 1 Selezionare **Amministrazione** > **Aggiornamento firmware/lingua**.

PASSAGGIO 2 Nel campo **Tipo di file**, fare clic sul pulsante di scelta **File di lingua**.

PASSAGGIO 3 Fare clic su **Sfoglia** per individuare e selezionare il file della lingua.

PASSAGGIO 4 (Opzionale) Per ripristinare i parametri di configurazione predefiniti del dispositivo, selezionare **Ripristina tutte le impostazioni/configurazioni predefinite**.

PASSAGGIO 5 Fare clic su **Avvia aggiornamento**.

Riavvio del dispositivo

Per riavviare il router, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Amministrazione** > **Riavvia**.

PASSAGGIO 2 Fare clic su **Riavvia**.

Ripristino delle impostazioni di fabbrica

ATTENZIONE Durante l'operazione di ripristino non tentare di connettersi online, spegnere il router, spegnere il PC oppure utilizzare il router prima che sia stata completata l'operazione. L'operazione dovrebbe durare circa un minuto. Quando la spia di test si spegne, attendere ancora qualche secondo prima di utilizzare il router.

Per ripristinare le impostazioni di fabbrica del router, attenersi alla seguente procedura:

PASSAGGIO 1 Scegliere **Amministrazione** > **Ripristina impostazioni di fabbrica**.

PASSAGGIO 2 Fare clic su **Predefinito**.

9

Filtro del traffico Web

Il filtro del traffico Web è una funzione del router che consente di gestire l'accesso a siti internet inappropriati. Può migliorare una rete già protetta e promuovere la produttività sul luogo di lavoro controllando le richieste di accesso a internet di un client per determinare se consentire o rifiutare l'accesso a un particolare sito.

L'amministratore può disporre di linee guida per la protezione generale della rete, l'internet delle cose e/o regole che desidera implementare su una rete personalizzata per un particolare reparto. L'amministratore può creare regole programmate personalizzate e associarle a elenchi eccezioni consentendo l'accesso a siti internet specifici a utenti specifici in orari particolari, per esempio.

Configurazione del filtro del traffico Web

Lo scopo di questa sezione è illustrare la configurazione del filtro del traffico Web sul router e sottolineare l'importanza di questa funzione. Per attivare e configurare il filtro del traffico Web sul router, eseguire questa procedura:

PASSAGGIO 1 Fare clic su **Filtro del traffico Web**.

PASSAGGIO 2 Nella sezione Filtro del traffico Web, selezionare una delle seguenti opzioni:

- **Sempre attivo**: il filtro del traffico Web è sempre attivato
- **Pianificato**: consente di impostare un programma di implementazione del filtro
- **Sempre inattivo**: consente di disattivare il filtro

NOTA Come impostazione predefinita, il filtro del traffico Web è impostato su Sempre inattivo.

PASSAGGIO 3 Nella sezione Reputazione Web, selezionare **Attiva** per attivare il filtro in base alla categoria di applicazione del filtro selezionata.

PASSAGGIO 4 Fare clic su Categorie e selezionare una delle seguenti opzioni per gestire e applicare i filtri.

- **Bassa**: le categorie Contenuto per adulti e Sicurezza sono attivate. Selezionare e verificare le opzioni disponibili per personalizzare il filtro.
- **Media**: le categorie Contenuto per adulti, Illegale/Discutibile e Sicurezza sono attivate. Selezionare e verificare le opzioni disponibili per personalizzare il filtro.
- **Alta**: le categorie Contenuto per adulti, Business/Investimenti, Intrattenimento, Illegale/Discutibile, Risorse IT, Stile di vita/Cultura e Sicurezza sono attivate. Selezionare e verificare le opzioni disponibili per personalizzare il filtro.
- **Personalizzata**: per il filtro del traffico Web personalizzato non sono presenti opzioni predefinite.

PASSAGGIO 5 Fare clic su **Salva** e **Indietro** per tornare alla pagina del filtro e continuare la configurazione.

PASSAGGIO 6 Selezionare **Attiva filtro HTTPS** per applicare un filtro ai contenuti in base all'indirizzo IP anziché all'URL. I siti internet con HTTP o HTTPS protetto saranno accessibili. Per bloccare i siti internet indipendentemente dalla presenza di un URL protetto, non selezionare **Attiva filtro HTTPS**.

NOTA Il filtro HTTPS si basa sull'indirizzo IP del server Web anziché sull'URL perché l'URL è crittografato. Spesso, diversi siti internet utilizzano lo stesso indirizzo IP del server Web. In questo caso, il router non bloccherà la pagina se esistono diverse categorie di sito internet associate a tale indirizzo IP. Tuttavia, il router bloccherà la pagina nel caso di un indirizzo IP che ospita contenuto per adulti o di un indirizzo IP noto per ospitare o distribuire malware.

PASSAGGIO 7 Se si seleziona **Pianificato** come opzione per l'applicazione del filtro del traffico Web, viene visualizzata la tabella pianificazioni. Sotto la tabella pianificazioni, fare clic su **Aggiungi riga** per creare una regola o un criterio pianificato da implementare.

PASSAGGIO 8 Nella tabella di programmazione, immettere un nome e una descrizione nei relativi campi.

PASSAGGIO 9 Quindi, selezionare il giorno o i giorni della settimana in cui si desidera attivare il filtro.

PASSAGGIO 10 In seguito, utilizzando l'orologio a 24 ore, immettere l'ora in cui la regola entra in vigore.

PASSAGGIO 11 Infine, selezionare **Attiva** per attivare la regola pianificata.

NOTA Non esiste un limite al numero di regole da implementare.

PASSAGGIO 12 Fare clic su **Salva**.

PASSAGGIO 13 (Facoltativo). Creare un elenco per consentire, negare o escludere siti internet/contenuti nel processo di applicazione del filtro. Scegliere il tipo tra una delle seguenti opzioni:

- **Lista bianca**: fare clic su **Aggiungi riga**, selezionare **Nome dominio** o **Parola chiave** dall'elenco a discesa. Quindi, immettere un valore per identificare questo criterio.
- **Lista nera**: fare clic su **Aggiungi riga**, selezionare **Nome dominio** o **Parola chiave** dall'elenco a discesa. Quindi, immettere un valore per identificare questo criterio.
- **Lista degli indirizzi da escludere**: fare clic su **Aggiungi riga**, selezionare **Nome dominio** o **Parola chiave** dall'elenco a discesa. Quindi, immettere un valore per identificare questo criterio.

PASSAGGIO 14 Per modificare o eliminare un criterio di applicazione del filtro del traffico Web, selezionare il criterio dall'elenco e fare clic su **Modifica** o **Elimina.**

PASSAGGIO 15 Fare clic su **Salva**.

A

Risorse aggiuntive

Assistenza	
Community di assistenza Cisco	www.cisco.com/go/smallbizsupport
Assistenza e risorse Cisco	www.cisco.com/go/smallbizhelp
Contatti per il servizio di assistenza telefonica	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Download del firmware Cisco	www.cisco.com/cisco/software/navigator.html?i=!ch Selezionare un collegamento per scaricare il firmware. Dati di accesso non richiesti.
Richieste open source di Cisco	www.cisco.com/go/smallbiz_opensource_request
Cisco Partner Central (richiede l'immissione di dati di accesso da parte dei partner)	www.cisco.com/web/partners/sell/smb
Documentazione relativa al prodotto	
Router VPN multifunzione wireless Cisco RV130/RV130W	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html

Per i risultati relativi a EU Lot 26, visitare il sito www.cisco.com/go/eu-lot26-results.