370111

GUIDA ALL'AMMINISTRAZIONE

Cisco
Router VPN Dual WAN Gigabit RV320/RV325

Pubblicato per la prima volta ad agosto 2014
Ultimo aggiornamento: agosto 2017

78-21281-01B0

Sommario

Sommario

Sommario

1

Introduzione

Grazie per avere scelto Cisco RV32x. In questo capitolo vengono fornite le informazioni per iniziare a utilizzare il dispositivo.

Utilizzo della finestra Introduzione

Le impostazioni predefinite sono sufficienti per molte piccole imprese. La rete o il provider di servizi Internet (ISP) potrebbero richiedere una modifica delle impostazioni. Per utilizzare l'interfaccia Web, è necessario un PC con Internet Explorer (versione 6 e successiva), Firefox o Safari (per Mac).

Per avviare l'interfaccia Web, attenersi alla seguente procedura:

PASSAGGIO 1 Collegare un PC a una porta LAN numerata del dispositivo. Se il PC funge da client DHCP, gli viene assegnato un indirizzo IP nell'intervallo 192.168.1.x.

PASSAGGIO 2 Avviare un browser Web.

PASSAGGIO 3 Nella barra degli indirizzi, immettere l'indirizzo IP predefinito del dispositivo, **192.168.1.1**. È possibile che nel browser venga visualizzato un messaggio in cui si informa che il sito Web non è attendibile. Accedere al sito Web.

PASSAGGIO 4 Quando viene visualizzata la pagina di accesso, immettere il nome utente predefinito **cisco** e la password predefinita **cisco** (caratteri minuscoli).

PASSAGGIO 5 Fare clic su **Login**. Viene visualizzata la pagina **Riepilogo di sistema**. Controllare l'**attività della porta** per vedere se la connessione WAN è attivata. Se non è attivata, procedere con il passaggio successivo.

PASSAGGIO 6 Per utilizzare la procedura guidata per configurare la connessione Internet, fare clic su **Installazione guidata** nella pagina Riepilogo di sistema. In alternativa, fare clic su **Procedura guidata** nel riquadro di spostamento, quindi fare clic su **Avvia ora** nella sezione Configurazione di base. Seguire le istruzioni visualizzate.

Se nel browser Web viene visualizzato un messaggio di avviso relativo alle finestre a comparsa, consentire il contenuto bloccato.

PASSAGGIO 7 Per configurare le altre impostazioni, utilizzare i collegamenti nel riquadro di spostamento.

Suggerimenti per la risoluzione dei problemi

In caso di problemi con la connessione a Internet e all'interfaccia Web, verificare gli elementi seguenti:

- Assicurarsi che nel browser Web non sia attiva la modalità Non in linea.
- Controllare le impostazioni di connessione alla rete LAN per la scheda Ethernet. Il PC deve ottenere un indirizzo IP tramite DHCP. In alternativa, il PC può avere un indirizzo IP statico nell'intervallo 192.168.1.x con il gateway predefinito impostato su 192.168.1.1 (indirizzo IP predefinito del dispositivo).
- Assicurarsi di aver configurato le impostazioni corrette nella procedura guidata di configurazione della connessione Internet.
- Spegnere il modem e il dispositivo per reimpostarli. Quindi, accendere il modem e lasciarlo inattivo per circa due minuti. Accendere poi il dispositivo. Ora si dovrebbe ricevere un indirizzo IP WAN.
- Se si utilizza un modem DSL, contattare l'ISP per impostare la modalità bridge sul modem DSL.

Funzioni dell'interfaccia utente

L'interfaccia utente è stata concepita per agevolare la configurazione e la gestione del dispositivo.

Navigazione

I moduli principali dell'interfaccia Web sono indicati dai pulsanti nel riquadro di spostamento di sinistra. Fare clic su un pulsante per visualizzare ulteriori opzioni. Per aprire una pagina, fare clic su un'opzione.

Finestre a comparsa

Alcuni collegamenti e pulsanti consentono di visualizzare finestre a comparsa con ulteriori informazioni o le relative pagine di configurazione. Se nel browser Web viene visualizzato un messaggio di avviso relativo alle finestre a comparsa, consentire il contenuto bloccato.

Guida

Per visualizzare le informazioni sulla pagina di configurazione selezionata, fare clic su **Guida** nell'angolo superiore destro dell'interfaccia Web. Se nel browser Web viene visualizzato un messaggio di avviso relativo alle finestre a comparsa, consentire il contenuto bloccato.

Disconnessione

Per uscire dall'interfaccia Web, fare clic su **Esci** nell'angolo superiore destro della finestra interfaccia Web. Viene visualizzata la pagina di accesso.

2

Procedura guidata

Dalla pagina Procedura guidata, è possibile avviare la procedura guidata Configurazione di base che fornisce istruzioni passo per passo per la configurazione iniziale del dispositivo e la procedura guidata Configurazione regola di accesso che consente di configurare i criteri di protezione per la rete.

Per accedere a questa pagina, selezionare **Procedura guidata** nel riquadro di spostamento.

Configurazione di base

Utilizzare la procedura guidata Configurazione di base per modificare il numero di porte WAN o per configurare la connessione Internet.

Fare clic su **Avvia ora** per eseguire la procedura guidata Configurazione di base. Per proseguire, attenersi alle istruzioni visualizzate. Fare riferimento alle informazioni fornite dal proprio ISP per specificare le impostazioni di connessione.

Configurazione regola di accesso

Utilizzare la procedura guidata Configurazione regola di accesso per creare le regole di accesso al firewall. Fare clic su **Avvia ora** per eseguire la procedura guidata Configurazione regola di accesso. La procedura guidata fornisce le informazioni sulle regole predefinite per questo dispositivo. Per proseguire, attenersi alle istruzioni visualizzate.

3

Riepilogo di sistema

Nella finestra Riepilogo di sistema, vengono visualizzate informazioni sulla situazione corrente delle connessioni del dispositivo, lo stato, le impostazioni e i log.

Informazioni di sistema

Descrizioni delle informazioni di sistema:

- **Numero di serie**: il numero di serie del dispositivo.
- **Versione firmware**: il numero di versione del firmware installato.
- **VID PID**: il numero di versione dell'hardware.
- **Checksum MD5**: un valore utilizzato per la convalida dei file.
- **IPv4/Subnet mask LAN**: l'indirizzo IP di gestione IPv4 e la subnet mask del dispositivo.
- **IPv6/Prefisso LAN**: l'indirizzo IP di gestione IPv6 e il prefisso.
- **Modalità di lavoro**: controlla il comportamento del dispositivo in relazione alla connessione WAN. Se il dispositivo ospita una connessione Internet WAN, è selezionata la modalità Gateway. La modalità Router, invece, è selezionata se il dispositivo si trova su una rete senza connessione WAN oppure se si utilizza un altro dispositivo per stabilire la connessione WAN. Per modificare questo parametro, fare clic su **Modalità di lavoro**. Viene visualizzata la finestra Routing avanzato.
- **Tempo di attività del sistema**: il numero di giorni, ore, minuti e secondi in cui il dispositivo è rimasto attivo.

Configurazione (procedura guidata)

Per accedere alla procedura guidata di impostazione della connessione Internet e seguire le istruzioni fornite, fare clic su **Installazione guidata** per avviare la procedura **Procedura guidata**.

Attività delle porte

Nella pagina Attività porte vengono identificate le interfacce delle porte e viene mostrato lo stato di ogni porta:

- **ID porta**: l'etichetta della porta.
- **Interfaccia**: il tipo di interfaccia: LAN, WAN o DMZ. Se sono presenti più interfacce WAN, viene aggiunto un numero alla fine del nome, ad esempio WAN1 o WAN2.
- **Stato**: lo stato della porta: disattivata (rosso), attivata (nero) o connessa (verde). Il valore Stato è un collegamento ipertestuale.

IPv4 e IPv6

Nella sezione IPv4 o IPv6 vengono mostrate le statistiche di ogni porta WAN. La scheda IPv6 è disponibile se nella pagina **Configurazione della rete** è stato attivato l'IP dual-stack.

Informazioni WAN

Vengono fornite le informazioni WAN seguenti:

- **Indirizzo IP**: l'indirizzo IP pubblico dell'interfaccia.
- **Gateway predefinito**: il gateway predefinito dell'interfaccia.
- **DNS**: l'indirizzo IP del server DNS dell'interfaccia.
- **DNS dinamico**: le impostazioni DDNS della porta: attivato o disattivato.

Stato protezione

In questa sezione viene mostrato lo stato delle funzioni di protezione:

- **SPI (Stateful Packet Inspection)**: lo stato del firewall: attivo (verde) o non attivo (rosso). Monitora lo stato delle connessioni di rete, come flussi TCP e comunicazioni UDP. Il firewall riconosce pacchetti accettabili per diversi tipi di connessioni. Vengono accettati soltanto i pacchetti che corrispondono a una connessione attiva nota; gli altri vengono rifiutati.
- **DoS (Denial of Service)**: lo stato del filtro DoS: attivo (verde) o non attivo (rosso). Un attacco DoS ha lo scopo di rendere inutilizzabili un computer o le risorse di rete.
- **Blocco richiesta WAN**: le porte di rete vengono *nascoste* ai dispositivi Internet; in questo modo gli utenti esterni non possono accedere alla rete ed è possibile impedire che altri utenti Internet possano rilevare la rete o eseguire il ping. Lo stato è attivo (verde) o non attivo (rosso). Blocco richiesta WAN
- **Gestione remota**: indica se è consentita o meno una connessione remota per la gestione del dispositivo. Attivo (verde) indica che la gestione remota è consentita. Non attivo (rosso) indica che la gestione remota non è consentita.
- **Regola di accesso**: il numero di regole di accesso impostate.

Per visualizzare informazioni dettagliate sulla funzione di protezione, fare clic sul relativo pulsante.

Stato dell'impostazione VPN

In questa sezione viene mostrato lo stato dei tunnel VPN:

- **Tunnel VPN in uso**: i tunnel VPN utilizzati.
- **Tunnel VPN disponibili**: i tunnel VPN disponibili.
- **Tunnel EasyVPN in uso**: i tunnel EasyVPN utilizzati.
- **Tunnel EasyVPN disponibili**: i tunnel EasyVPN disponibili.

- **Tunnel PPTP in uso**: i tunnel PPTP (Point-to-Point Tunneling Protocol) utilizzati. PPTP è un metodo utilizzato per l'implementazione di reti private virtuali. PPTP utilizza un canale di controllo su TCP e un tunnel GRE (Generic Routing Encapsulation) per incapsulare i pacchetti PPP.
- **Tunnel PPTP disponibili**: i tunnel PPTP disponibili.

Stato dell'impostazione dei log

In questa sezione viene mostrato lo stato dei log:

- **Server Syslog**: stato di syslog: attivo (verde) o non attivo (rosso).
- **Log e-mail**: stato del log e-mail: attivo (verde) o non attivo (rosso).

4

Configurazione

Nella pagina Configurazione vengono mostrate le impostazioni di configurazione sul router. Utilizzare la pagina Configurazione > Rete per configurare reti LAN, WAN (Internet), DMZ e così via.

Configurazione della rete

Per accedere alla pagina Rete, fare clic su Configurazione > Rete.

Per alcuni ISP è necessario assegnare un nome host e un nome di dominio per identificare il dispositivo. Vengono forniti valori predefiniti, che è possibile modificare in base alle necessità:

- **Nome host**: mantenere l'impostazione predefinita o immettere un nome host specificato dall'ISP.
- **Nome dominio**: mantenere l'impostazione predefinita o immettere un nome di dominio specificato dall'ISP.

Modalità IP

Selezionare il tipo di indirizzamento da utilizzare sulle reti:

- **Solo IPv4**: solo indirizzamento IPv4.
- **IP dual-stack**: indirizzamento IPv4 e IPv6. Dopo aver salvato i parametri, è possibile configurare sia indirizzi IPv4 che IPv6 per reti LAN, WAN e DMZ.

Aggiunta o modifica di una rete IPv4

Per impostazione predefinita è configurata una sottorete LAN IPv4 (192.168.1.1). Una sottorete è generalmente sufficiente per la maggior parte delle piccole aziende. Se l'indirizzo IP di origine di un dispositivo LAN corrisponde a una sottorete non consentita in maniera esplicita, il firewall nega l'accesso. È possibile consentire il traffico da altre sottoreti e utilizzare il dispositivo come un router periferico che fornisce connettività Internet a una rete.

PASSAGGIO 1 Fare clic sulla scheda **IPv4** per visualizzare la Tabella sottoreti multiple.

PASSAGGIO 2 Per aggiungere una sottorete, fare clic su **Aggiungi**. Nelle colonne vengono visualizzati i campi Indirizzo IP e Subnet mask. Dopo aver fatto clic su **Salva**, è possibile modificare la sottorete per renderla parte di una VLAN, gestire gli indirizzi IP attraverso il server DHCP o impostare i parametri del server TFTP.

PASSAGGIO 3 Immettere l'indirizzo IP e la subnet mask del dispositivo nei rispettivi campi.

PASSAGGIO 4 Per salvare le modifiche, fare clic su **Salva** oppure fare clic su **Annulla** per annullarle.

Per modificare una sottorete, selezionare la sottorete IPv4 da modificare e fare clic su **Modifica**. Nella sezione **Configurazione di DHCP** viene descritto il processo di modifica dei parametri della sottorete.

Modifica del prefisso dell'indirizzo IPv6

Se è stato attivato l'IP dual-stack come modalità IP, è possibile configurare il prefisso IPv6.

Per configurare il prefisso IPv6, fare clic sulla scheda **IPv6**, selezionare il prefisso IPv6, quindi fare clic su **Modifica**. L'indirizzo IP predefinito è fc00::1 e la lunghezza predefinita del prefisso è di 7 caratteri. La scheda IPv6 è disponibile soltanto se è stato attivato l'**IP dual-stack** nella tabella **Modalità IP**. Viene visualizzata la finestra **Configurazione di DHCP**.

Impostazioni della porta WAN

Nella tabella delle impostazioni WAN vengono visualizzati l'interfaccia, ad esempio USB1, WAN1 o WAN2, e il tipo di connessione. È possibile modificare le impostazioni delle interfacce.

NOTA Se si esegue IPv6, selezionare la scheda **IPv6** prima di selezionare l'interfaccia WAN da configurare. In caso contrario, i parametri IPv6 non vengono visualizzati nella finestra **Impostazioni connessione WAN**.

Per configurare le impostazioni della connessione WAN, selezionare un'interfaccia WAN e fare clic su **Modifica**. Viene visualizzata la finestra **Impostazioni connessione WAN**.

Selezionare un'opzione dal menu a discesa **Tipo di connessione WAN** e modificare i parametri correlati come descritto in queste sezioni:

Assegnazione automatica dell'indirizzo IP

Selezionare questa opzione se l'ISP assegna un indirizzo IP dinamico al dispositivo. Questo tipo di connessione è diffusa soprattutto fra gli utenti che utilizzano un modem via cavo. L'ISP assegna l'indirizzo IP del dispositivo per questa porta, inclusi gli indirizzi IP del server DNS.

Per specificare un server DNS, selezionare **Utilizza gli indirizzi server DNS seguenti** e immettere un indirizzo IP nel campo **Server DNS 1**. Se si desidera, è possibile immettere un secondo server DNS. In questo caso, viene utilizzato il primo server DNS disponibile.

Per impostare automaticamente le dimensioni dell'unità massima di trasmissione (**MTU**, Maximum Transfer Unit), selezionare **Automatico**. In caso contrario, per impostare manualmente le dimensioni della **MTU**, selezionare **Manuale** e immettere la dimensione desiderata, ovvero le dimensioni massime (in byte) dell'unità di dati protocollo che il livello può trasmettere.

Per configurare i parametri IPv6, selezionare **Attiva**. Il processo client DHCPv6 e le richieste di delega del prefisso attraverso l'interfaccia selezionata sono attivati. Utilizzare questa opzione se l'ISP è in grado di inviare prefissi LAN utilizzando DHCPv6. Se l'ISP non supporta questa opzione, configurare manualmente un prefisso LAN:

NOTA Se DHCP-PD è attivato, l'indirizzamento IPv6 LAN manuale è disattivato. Se DHCP-PD è disattivato, l'indirizzamento IPv6 LAN manuale è attivato.

- **Indirizzo IPv6 LAN**: il prefisso IPv6 globale assegnato dall'ISP ai dispositivi LAN dell'utente, se applicabile. Per ulteriori informazioni, rivolgersi all'ISP.

- **Lunghezza prefisso**: la lunghezza del prefisso IPv6. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Tutti gli host della rete hanno bit iniziali identici nell'indirizzo IPv6. Immettere il numero di bit iniziali comuni negli indirizzi di rete. La lunghezza predefinita del prefisso è 64.
- **Assegnazione prefisso LAN**:
  - **Senza azioni**: non fornisce un indirizzo IPv6 stateless o stateful per PC lato LAN.
  - **Configura automaticamente su RA**: fornisce un indirizzo IPv6 *stateless* per PC lato LAN.
  - **Configura automaticamente su DHCPv6**: fornisce un indirizzo IPv6 *stateful* per PC lato LAN.
  - Configura automaticamente su RA e DHCPv6: fornisce indirizzi IPv6 stateless e stateful per PC lato LAN.

IP statico

Selezionare questa opzione se l'ISP ha assegnato all'account un indirizzo IP permanente. Immettere le impostazioni fornite dall'ISP:

- **Specifica indirizzo IP WAN**: l'indirizzo IP assegnato dall'ISP all'account.
- **Subnet mask (IPv4)**: la subnet mask.
- **Indirizzo gateway predefinito**: l'indirizzo IP del gateway predefinito.

Per specificare un server DNS; immettere un indirizzo IP nel campo **Server DNS 1**. Se si desidera, è possibile immettere un secondo server DNS. In questo caso, viene utilizzato il primo server DNS disponibile.

Per impostare automaticamente le dimensioni dell'unità massima di trasmissione (**MTU**, Maximum Transfer Unit), selezionare **Automatico**. In caso contrario, per impostare manualmente le dimensioni della **MTU**, selezionare **Manuale** e immettere la dimensione desiderata, ovvero le dimensioni massime (in byte) dell'unità di dati protocollo che il livello può trasmettere.

Per configurare i parametri IPv6:

- **Indirizzo IPv6 LAN**: il prefisso IPv6 globale assegnato dall'ISP ai dispositivi LAN dell'utente, se applicabile. Per ulteriori informazioni, rivolgersi all'ISP.

- **Lunghezza prefisso**: la lunghezza del prefisso IPv6. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Tutti gli host della rete hanno bit iniziali identici nell'indirizzo IPv6. Immettere il numero di bit iniziali comuni negli indirizzi di rete. La lunghezza predefinita del prefisso è 64.
- **Assegnazione prefisso LAN**
  - **Senza azioni**: non fornisce un indirizzo IPv6 stateless o stateful per PC lato LAN.
  - **Configura automaticamente su RA**: fornisce un indirizzo IPv6 *stateless* per PC lato LAN.
  - **Configura automaticamente su DHCPv6**: fornisce un indirizzo IPv6 *stateful* per PC lato LAN.
  - **Configura automaticamente su RA e DHCPv6**: fornisce indirizzi IPv6 stateless e stateful per PC lato LAN.

PPPoE

Selezionare questa opzione se l'ISP utilizza il protocollo PPPoE (Point to Point Protocol over Ethernet) per stabilire le connessioni Internet (tipico delle linee DSL). Quindi, immettere le impostazioni fornite dall'ISP:

- **Nome utente** e **Password**: il nome utente e la password dell'account ISP. Il numero massimo di caratteri per ciascuna voce è 255.
- **Nome servizio**: una serie di servizi forniti dall'ISP identificati dal nome di servizio.
- **Timer connessione**: la connessione viene interrotta dopo un periodo di inattività.
  - **Connessione su richiesta**: se questa funzionalità è attiva, il dispositivo stabilisce automaticamente la connessione. Se si attiva questa funzionalità, immettere un valore nel campo **Tempo di inattività massimo**, ovvero il numero di minuti di inattività trascorsi i quali la connessione verrà interrotta. L'impostazione predefinita è 5 minuti.
  - **Mantieni connessione attiva**: garantisce che il router sia sempre connesso a Internet. Se questa funzionalità è selezionata, il router mantiene la connessione attiva inviando periodicamente alcuni pacchetti di dati. Questa opzione mantiene la connessione sempre attiva, anche quando il collegamento rimane inattivo per periodi prolungati. Se si attiva questa funzionalità, immettere un valore nel campo **Frequenza di riconnessione** per specificare la frequenza con

cui il router controlla la connessione Internet. L'impostazione predefinita è 30 secondi.

- **Utilizza gli indirizzi server DNS seguenti**: attiva la ricezione di informazioni sulla connessione da server DNS.
- **Server DNS 1** e **Server DNS 2**: l'indirizzo IP dei server DNS. Se si desidera, è possibile immettere un secondo server DNS. In questo caso, viene utilizzato il primo server DNS disponibile.
- **MTU**: dimensioni dell'unità massima di trasmissione (**MTU**). Selezionare **Automatico** per impostare automaticamente le dimensioni. In caso contrario, per impostare manualmente le dimensioni della **MTU**, selezionare **Manuale** e immettere la dimensione desiderata, ovvero le dimensioni massime (in byte) dell'unità di dati protocollo che il livello può trasmettere.

Per configurare i parametri IPv6, selezionare **Attiva**. Il processo client DHCPv6 e le richieste di delega del prefisso attraverso l'interfaccia selezionata sono attivati. Utilizzare questa opzione se l'ISP è in grado di inviare prefissi LAN utilizzando DHCPv6. Se l'ISP non supporta questa opzione, configurare manualmente un prefisso LAN:

NOTA Se DHCP-PD è attivato, l'indirizzamento IPv6 LAN manuale è disattivato. Se DHCP-PD è disattivato, l'indirizzamento IPv6 LAN manuale è attivato.

- **Indirizzo IPv6 LAN**: il prefisso IPv6 globale assegnato dall'ISP ai dispositivi LAN dell'utente, se applicabile. Per ulteriori informazioni, rivolgersi all'ISP.
- **Lunghezza prefisso**: la lunghezza del prefisso IPv6. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Tutti gli host della rete hanno bit iniziali identici nell'indirizzo IPv6. Immettere il numero di bit iniziali comuni negli indirizzi di rete. La lunghezza predefinita del prefisso è 64.
- **Assegnazione prefisso LAN**:
  - **Senza azioni**: non fornisce un indirizzo IPv6 stateless o stateful per PC lato LAN.
  - **Configura automaticamente su RA**: fornisce un indirizzo IPv6 *stateless* per PC lato LAN.
  - **Configura automaticamente su DHCPv6**: fornisce un indirizzo IPv6 *stateful* per PC lato LAN.
  - **Configura automaticamente su RA e DHCPv6**: fornisce indirizzi IPv6 stateless e stateful per PC lato LAN.

PPTP (IPv4)

Selezionare questa opzione se richiesto dall'ISP. PPTP (Point-to-Point Tunneling Protocol) è un servizio utilizzato in Europa e Israele.

- **Specifica indirizzo IP WAN**: l'indirizzo IP assegnato dall'ISP all'account.
- **Subnet mask (IPv4)**: la subnet mask assegnata all'account.
- **Indirizzo gateway predefinito**: l'indirizzo IP del gateway predefinito.
- **Nome utente** e **Password**: il nome utente e la password dell'account ISP. Il numero massimo di caratteri è 60.
- **Timer connessione**: la connessione viene interrotta dopo un periodo di inattività.
  - **Connessione su richiesta**: se questa funzionalità è attiva, il dispositivo stabilisce automaticamente la connessione. Se si attiva questa funzionalità, immettere un valore nel campo **Tempo di inattività massimo**, ovvero il numero di minuti di inattività trascorsi i quali la connessione verrà interrotta. L'impostazione predefinita è 5 minuti.
  - **Mantieni connessione attiva**: garantisce che il router sia sempre connesso a Internet. Se questa funzionalità è selezionata, il router mantiene la connessione attiva inviando periodicamente alcuni pacchetti di dati. Questa opzione mantiene la connessione sempre attiva, anche quando il collegamento rimane inattivo per periodi prolungati. Se si attiva questa funzionalità, immettere un valore nel campo **Frequenza di riconnessione** per specificare la frequenza con cui il router controlla la connessione Internet. L'impostazione predefinita è 30 secondi.
- **MTU**: dimensioni dell'unità massima di trasmissione (**MTU**). Selezionare **Automatico** per impostare automaticamente le dimensioni. In caso contrario, per impostare manualmente le dimensioni della **MTU**, selezionare **Manuale** e immettere la dimensione desiderata, ovvero le dimensioni massime (in byte) dell'unità di dati protocollo che il livello può trasmettere.

Bridge trasparente (IPv4)

Selezionare questa opzione se si utilizza il router per connettere due segmenti di rete. È possibile impostare una sola interfaccia WAN come bridge trasparente.

- **Specifica indirizzo IP WAN**: l'indirizzo IP esterno assegnato dall'ISP all'account.
- **Subnet mask**: la subnet mask specificata dall'ISP.

- **Indirizzo gateway predefinito**: l'indirizzo IP del gateway predefinito.
- **Server DNS 1** e **Server DNS 2**: gli indirizzi IP dei server DNS. Se si desidera, è possibile immettere un secondo server DNS. In questo caso, viene utilizzato il primo server DNS disponibile.
- **Intervallo IP LAN interno**: l'intervallo IP LAN interno con bridge. La WAN e la LAN del bridge trasparente devono essere sulla stessa sottorete.
- **MTU**: dimensioni dell'unità massima di trasmissione (**MTU**). Selezionare **Automatico** per impostare automaticamente le dimensioni. In caso contrario, per impostare manualmente le dimensioni della **MTU**, selezionare **Manuale** e immettere la dimensione desiderata, ovvero le dimensioni massime (in byte) dell'unità di dati protocollo che il livello può trasmettere.

Configurazione automatica dell'indirizzo stateless (IPv6)

Selezionare questa opzione se l'ISP utilizza le richieste e gli annunci router IPv6, se gli host della rete apprendono la rete alla quale sono connessi e se, successivamente, possono configurare automaticamente un ID host su tale rete.

Per specificare un server DNS; immettere un indirizzo IP nel campo **Server DNS 1**. Se si desidera, è possibile immettere un secondo server DNS. In questo caso, viene utilizzato il primo server DNS disponibile.

Per impostare automaticamente le dimensioni dell'unità massima di trasmissione (**MTU**, Maximum Transfer Unit), selezionare **Automatico**. In caso contrario, per impostare manualmente le dimensioni della **MTU**, selezionare **Manuale** e immettere la dimensione desiderata, ovvero le dimensioni massime (in byte) dell'unità di dati protocollo che il livello può trasmettere.

Per configurare i parametri IPv6:

- **Indirizzo IPv6 LAN**: il prefisso IPv6 globale assegnato dall'ISP ai dispositivi LAN dell'utente, se applicabile. Per ulteriori informazioni, rivolgersi all'ISP.
- **Lunghezza prefisso**: la lunghezza del prefisso IPv6. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Tutti gli host della rete hanno bit iniziali identici nell'indirizzo IPv6. Immettere il numero di bit iniziali comuni negli indirizzi di rete. La lunghezza predefinita del prefisso è 64.
- **Assegnazione prefisso LAN**:
  - **Senza azioni**: non fornisce un indirizzo IPv6 stateless o stateful per PC lato LAN.

- **Configura automaticamente su RA**: fornisce un indirizzo IPv6 *stateless* per PC lato LAN.
- **Configura automaticamente su DHCPv6**: fornisce un indirizzo IPv6 *stateful* per PC lato LAN.
- **Configura automaticamente su RA e DHCPv6**: fornisce indirizzi IPv6 stateless e stateful per PC lato LAN.

IPv6 nel tunnel IPv4 (IPv6)

Selezionare questa opzione se l'ISP utilizza IPv6 nel tunnel IPv4 per stabilire le connessioni Internet.

È necessario immettere un indirizzo **IP statico** IPv4. Quindi, immettere le impostazioni fornite dall'ISP:

- **Indirizzo IPv6 locale**: l'indirizzo IPv6 locale dell'account ISP.
- **Indirizzo IPv4 remoto**: l'indirizzo IPv4 remoto dell'account ISP.
- **Indirizzo IPv6 remoto**: l'indirizzo IPv6 remoto dell'account ISP.
- **Server DNS 1** e **Server DNS 2**: gli indirizzi IP dei server DNS. Se si desidera, è possibile immettere un secondo server DNS. In questo caso, viene utilizzato il primo server DNS disponibile.
- **Indirizzo IPv6 LAN**: il prefisso IPv6 globale assegnato dall'ISP ai dispositivi LAN dell'utente, se applicabile. Per ulteriori informazioni, rivolgersi all'ISP.
- **Lunghezza prefisso**: la lunghezza del prefisso IPv6. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Tutti gli host della rete hanno bit iniziali identici nell'indirizzo IPv6. Immettere il numero di bit iniziali comuni negli indirizzi di rete. La lunghezza predefinita del prefisso è 64.
- **Assegnazione prefisso LAN**
  - **Senza azioni**: non fornisce un indirizzo IPv6 stateless o stateful per PC lato LAN.
  - **Configura automaticamente su RA**: fornisce un indirizzo IPv6 *stateless* per PC lato LAN.
  - **Configura automaticamente su DHCPv6**: fornisce un indirizzo IPv6 *stateful* per PC lato LAN.
  - **Configura automaticamente su RA e DHCPv6**: fornisce indirizzi IPv6 stateless e stateful per PC lato LAN.

Tunnel 6to4 (IPv6)

Selezionare questa opzione per stabilire un tunnel automatico in una rete IPv4 (o una reale connessione Internet IPv4) su due reti IPv6 indipendenti. Immettere i parametri seguenti.

Indirizzo IPv4 di inoltro: consente a un host 6to4 di comunicare con l'Internet IPv6 nativo. È necessario che sia disponibile un gateway IPv6 predefinito impostato su un indirizzo 6to4 che contenga un indirizzo IPv4 di un router di inoltro 6to4. Per evitare la configurazione manuale da parte degli utenti, è stato assegnato l'indirizzo anycast `192.88.99.1` per l'invio di pacchetti a un router di inoltro 6to4.

- **Server DNS 1** e **Server DNS 2**: gli indirizzi IP dei server DNS. Se si desidera, è possibile immettere un secondo server DNS. In questo caso, viene utilizzato il primo server DNS disponibile.
- **Indirizzo IPv6 LAN**: il prefisso IPv6 globale assegnato dall'ISP ai dispositivi LAN dell'utente, se applicabile. Per ulteriori informazioni, rivolgersi all'ISP.
- **Lunghezza prefisso**: la lunghezza del prefisso IPv6. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Tutti gli host della rete hanno bit iniziali identici nell'indirizzo IPv6. Immettere il numero di bit iniziali comuni negli indirizzi di rete. La lunghezza predefinita del prefisso è 64.
- **Assegnazione prefisso LAN**
  - **Senza azioni**: non fornisce un indirizzo IPv6 stateless o stateful per PC lato LAN.
  - **Configura automaticamente su RA**: fornisce un indirizzo IPv6 *stateless* per PC lato LAN.
  - **Configura automaticamente su DHCPv6**: fornisce un indirizzo IPv6 *stateful* per PC lato LAN.
  - **Configura automaticamente su RA e DHCPv6**: fornisce indirizzi IPv6 stateless e stateful per PC lato LAN.

Tunnel di implementazione rapida IPv6 (6rd) (IPv6)

Selezionare questa opzione se l'ISP utilizza tunnel di implementazione rapida IPv6 (6rd) per stabilire le connessioni Internet. Immettere le impostazioni fornite dall'ISP.

- **Modalità configurazione 6rd**:

  - **Manuale**: impostare manualmente il prefisso 6rd, l'indirizzo IPv4 di inoltro e la lunghezza della maschera IPv4 indicati dall'ISP.
  - **Auto (DHCP)**: utilizzare DHCP (Option 212) per ottenere il prefisso 6rd, l'indirizzo IPv4 di inoltro e la lunghezza della maschera IPv4.
- **Prefisso 6rd**: prefisso 6rd per l'account ISP.
- **Indirizzo IPv4 di inoltro**: l'indirizzo IPv4 di inoltro dell'account ISP.
- **Lunghezza maschera IPv4**: la lunghezza della subnet mask IPv4 6rd dell'account ISP. Il valore utilizzato di solito è 0.
- **Server DNS 1** e **Server DNS 2**: gli indirizzi IP dei server DNS. Se si desidera, è possibile immettere un secondo server DNS. In questo caso, viene utilizzato il primo server DNS disponibile.
- **Indirizzo IPv6 LAN**: il prefisso IPv6 globale assegnato dall'ISP ai dispositivi LAN dell'utente, se applicabile. Per ulteriori informazioni, rivolgersi all'ISP.
- **Lunghezza prefisso**: la lunghezza del prefisso IPv6. La rete IPv6 (sottorete) viene identificata dai bit iniziali dell'indirizzo denominati prefisso. Tutti gli host della rete hanno bit iniziali identici nell'indirizzo IPv6. Immettere il numero di bit iniziali comuni negli indirizzi di rete. La lunghezza predefinita del prefisso è 64.
- **Assegnazione prefisso LAN**
  - **Senza azioni**: non fornisce un indirizzo IPv6 stateless o stateful per PC lato LAN.
  - **Configura automaticamente su RA**: fornisce un indirizzo IPv6 *stateless* per PC lato LAN.
  - **Configura automaticamente su DHCPv6**: fornisce un indirizzo IPv6 *stateful* per PC lato LAN.
  - **Configura automaticamente su RA e DHCPv6**: fornisce indirizzi IPv6 stateless e stateful per PC lato LAN.

Impostazioni della porta USB1 o USB2

La configurazione della porta USB consente di gestire la connessione tra il dispositivo e la chiavetta USB. Consente, inoltre, di gestire il failover della porta WAN (ridondanza). Per alcune chiavi USB le credenziali vengono configurate automaticamente. Per altre, come la chiave Verizon UML290VW 4G, è necessaria la configurazione manuale. Per ulteriori informazioni, consultare la documentazione del produttore della chiave.

Connessione 3G/4G

Per stabilire una connessione 3G o 4G, specificare i parametri seguenti:

- **Codice PIN** e **Conferma codice PIN**: il codice PIN associato alla scheda SIM. Questo campo viene visualizzato soltanto per le schede SIM GSM.
- **Nome dell'Access Point**: la rete Internet a cui è connesso il dispositivo mobile. Immettere 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 da comporre fornito dal provider di servizi della rete mobile per la connessione Internet.
- **Nome utente** e **Password**: il nome utente e la password forniti dal provider di servizi della rete mobile.
- **Attiva DNS**: selezionare questa casella per attivare DNS.
- **Server DNS (obbligatorio)** e **Server DNS (facoltativo)**: gli indirizzi IP dei server DNS. Se si desidera, è possibile immettere un secondo server DNS. In questo caso, viene utilizzato il primo server DNS disponibile.
- **MTU**: dimensioni dell'unità massima di trasmissione (**MTU**). Selezionare **Automatico** per impostare automaticamente le dimensioni. In caso contrario, per impostare manualmente le dimensioni della **MTU**, selezionare **Manuale** e immettere la dimensione desiderata, ovvero le dimensioni massime (in byte) dell'unità di dati protocollo che il livello può trasmettere.

Impostazione di failover e ripristino

Anche se potrebbero essere disponibili Ethernet e il collegamento di rete mobile, 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 la connessione di backup verrà abbandonata. Questa funzionalità si chiama *ripristino*.

PASSAGGIO 1 Per visualizzare la finestra Failover e ripristino, fare clic su Configurazione > **Rete**.

PASSAGGIO 2 Selezionare una porta USB e fare clic su **Modifica**. Viene visualizzata la finestra Rete.

PASSAGGIO 3 Fare clic sulla scheda Failover USB e immettere le seguenti informazioni:

- **Modalità operativa**: quando un collegamento WAN Ethernet viene interrotto, il dispositivo tenta di attivare il collegamento di rete mobile sull'interfaccia USB. Configurare il comportamento di failover:
  - Hot Standby failover 3G/4G: in caso di interruzione della connessione sulla porta WAN Ethernet, il traffico WAN viene reindirizzato sul collegamento USB 3G/4G. La chiave USB è alimentata quando non è attiva.
  - Hot Standby failover 3G/4G: in caso di interruzione della connessione sulla porta WAN Ethernet, il traffico WAN viene reindirizzato sul collegamento USB 3G/4G. La chiave USB non è alimentata quando non è attiva.
  - Modalità primaria: il collegamento 3G/4G è utilizzato come connessione WAN primaria.
- **Qualità del segnale**: indica l'intensità del segnale tra la chiave USB 3G/4G e l'access point. Fare clic su **Aggiorna** per aggiornare i dati.

PASSAGGIO 4 Per impedire eccedenze di dati, selezionare un valore nel campo **Conteggio addebito**. **Traffico (KB)** monitora il volume di dati inviati o ricevuti (in kilobyte) sul collegamento USB. **Tempo (min)** conteggia i minuti durante i quali la connessione 3G/4G è attiva.

- Se si seleziona Traffico (KB), immettere le seguenti informazioni:
  - **Tariffa**: costo di un determinato volume di dati, espresso in dollari.

- **Addebito aggiuntivo**: costo per KB di dati (espresso in dollari) oltre un determinato volume.
- **Interrompi connessione...**: selezionare questa opzione per attivare l'interruzione della connessione quando viene superato il volume specificato.

▪ Se si seleziona Tempo (min), immettere le seguenti informazioni:

- **Tariffa**: costo per un determinato periodo di tempo, espresso in dollari.
- **Addebito aggiuntivo**: costo in dollari se viene superato il periodo di tempo stabilito.
- **Interrompi connessione...**: selezionare questa opzione per attivare l'interruzione della connessione quando viene superato il tempo specificato.

Viene visualizzata la finestra:

- **Durata precedente cumulativa**: periodo di tempo durante il quale la connessione 3G/4G è stata attiva dal momento del ripristino.
- **Durata corrente cumulativa**: periodo di tempo trascorso da quando il dispositivo ha attivato una connessione 3G/4G.
- **Addebito**: costo stimato della connessione a partire dall'azzeramento dei contatori.

PASSAGGIO 5 Impostare le opzioni di **Diagnostica**:

- **Riavvia il conteggio**: selezionare questa opzione e immettere il giorno del mese in cui dovranno essere azzerati i contatori. Se il valore è maggiore del numero di giorni nel mese, ad esempio 31 in un mese di 30, i contatori vengono azzerati l'ultimo giorno del mese.
- **Verifica automatica giornaliera**: selezionare questa opzione e immettere l'ora del giorno (formato a 24 ore) in cui testare la connessione. La verifica automatica è considerata riuscita se il dispositivo ottiene un indirizzo IP dal provider di servizi. Gli errori vengono inviati al log.
- **Verifica automatica del log**: selezionare questa opzione per registrare l'attività della verifica automatica. Tutti i risultati del test vengono inviati al log.

PASSAGGIO 6 Fare clic su Salva per salvare le impostazioni.

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

Per configurare la rete DMZ, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Configurazione** > **Rete** e fare clic su **Attiva DMZ**. Viene visualizzato un messaggio.

PASSAGGIO 2 Fare clic su **Sì** per accettare la modifica.

PASSAGGIO 3 Selezionare l'interfaccia DMZ nelle tabella **Impostazioni DMZ** e fare clic su **Modifica**. Viene visualizzata la finestra **Modifica connessione DMZ**.

PASSAGGIO 4 Selezionare **Sottorete** per identificare una sottorete per i servizi DMZ, quindi immettere un indirizzo IP DMZ e la subnet mask nei rispettivi campi. In alternativa, selezionare **Intervallo** per riservare un gruppo di indirizzi IP della stessa sottorete per i servizi DMZ e immettere l'intervallo di indirizzi IP.

PASSAGGIO 5 Fare clic su **Salva**.

Password

Il nome utente e la password consentono l'accesso al dispositivo in modalità di amministrazione. Il nome utente predefinito è **cisco** La password predefinita è **cisco**. È possibile modificare il nome utente e la password predefiniti. Si raccomanda vivamente di modificare la password predefinita scegliendone una complessa.

Per accedere alla pagina Password, fare clic su **Configurazione > Password**.

Se nella pagina **Impostazioni generali** (Firewall) è stata attivata la gestione remota, è *necessario* modificare la password.

ATTENZIONE Se si perde o si dimentica la password non è possibile recuperarla. In questi casi, è necessario ripristinare le impostazioni predefinite di fabbrica del dispositivo eliminando tutte le modifiche alla configurazione. Se si accede al dispositivo da remoto e si ripristinano le impostazioni predefinite di fabbrica del dispositivo, sarà possibile accedere al dispositivo solo dopo aver stabilito un collegamento locale cablato sulla stessa sottorete.

Una volta modificato il nome utente o la password, l'utente viene disconnesso. Effettuare l'accesso a dispositivo con le nuove credenziali.

Per modificare il nome utente o la password:

PASSAGGIO 1 Scegliere **Impostazione**>**Password**.

PASSAGGIO 2 Inserire il nuovo nome utente nel campo **Nome utente**. Per mantenere il nome utente corrente, lasciare il campo vuoto.

PASSAGGIO 3 Inserire la password corrente nel campo **Vecchia password**. Questa operazione è obbligatoria se si intende modificare il nome utente mantenendo la password attuale.

NOTA Se si intende modificare il nome utente mantenendo la password attuale, lasciare vuoti i campi **Nuova password** e **Conferma nuova password**.

PASSAGGIO 4 Inserire la nuova password per dispositivo nel campo **Nuova password**. Utilizzare una combinazione di caratteri alfanumerici e simboli. La password non può includere spazi. Dopodiché, inserire di nuovo la nuova password nel campo **Conferma nuova password**. Controllare che le due password corrispondano.

PASSAGGIO 5 Selezionare Attiva per attivare le impostazioni di complessità della password:.

Per configurare le impostazioni di complessità della password:

PASSAGGIO 1 Nel campo **Impostazioni complessità password**, selezionare **Attiva**.

PASSAGGIO 2 Configurare le impostazioni nei seguenti campi:

Lunghezza minima password	Immettere la lunghezza minima della password (0-64 caratteri). Per impostazione predefinita, le password devono contenere almeno 8 caratteri.
Numero minimo classi di caratteri	Immettere il numero di classi da includere nella password. Per impostazione predefinita, le password devono contenere caratteri di almeno tre di queste categorie. ▪ Lettere maiuscole ▪ Lettere minuscole ▪ Numeri ▪ Caratteri speciali disponibili su una tastiera standard
La nuova password deve essere diversa da quella attuale	Selezionare **Attiva** se si desidera che la nuova password sia diversa da quella corrente.
Misuratore complessità password	Misuratore complessità indica la complessità della password in base alle regole di complessità. Le opzioni sono rosso (inaccettabile), giallo (accettabile) e verde (complessa)..
Durata password	Immettere il numero di giorni massimo della durata della password (1-365). La durata predefinita è 180 giorni.

PASSAGGIO 3 Nel campo Timeout sessione inserire il numero di minuti trascorsi i quali la sessione scade. Salvare le modifiche

PASSAGGIO 4 Fare clic su **Salva**.

Ora

Il tempo è un fattore critico per un dispositivo di rete. La funzione Ora inserisce correttamente data e ora nel log di sistema e nei messaggi di errore e sincronizza il trasferimento dei dati con altri dispositivi di rete.

È possibile configurare il fuso orario, scegliere se impostare 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 accedere alla pagina Ora, fare clic su **Configurazione > Ora**.

Per configurare le impostazioni NTP e dell'ora, selezionare **Configurazione** > **Ora**.

- **Fuso orario**: selezionare il fuso orario in relazione all'ora di Greenwich (GMT).
- **Ora legale**: attivare o disattivare la regolazione in base all'ora legale. Immettere la data di inizio nel campo **Da** e la data di fine nel campo **A**.
- **Imposta data e ora**: **Automatico** attiva il server NTP. Se si seleziona l'opzione Automatico, immettere il nome o l'indirizzo IP completo del server NTP. **Manuale** attiva l'impostazione della data e dell'ora locale e utilizza l'orologio del dispositivo per gestire l'ora. Se è stata selezionata l'opzione **Manuale**, immettere la data e l'ora nei rispettivi campi.

Host DMZ

La funzione Host DMZ consente di esporre un host della LAN su Internet per utilizzare determinati servizi, ad esempio giochi online o videoconferenze. È possibile impostare regole del firewall per limitare l'accesso all'host DMZ da Internet.

Per accedere alla pagina Host DMZ, fare clic su **Configurazione > Host DMZ**.

Per configurare un host DMZ, immettere un indirizzo nel campo **Indirizzo IP privato DMZ** e fare clic su **Salva**.

Reindirizzamento (porta)

Il reindirizzamento della porta consente l'accesso pubblico a servizi su dispositivi di rete sulla LAN aprendo una porta specifica o un intervallo di porte per un servizio, ad esempio FTP. L'attivazione delle porte apre un intervallo di porte per servizi, come i giochi online, che utilizzano porte alternative per comunicare tra server e host LAN.

Per accedere alla pagina di reindirizzamento della porta, fare clic su **Configurazione > Reindirizzamento**.

Configurazione del reindirizzamento della porta

Il dispositivo inoltra le richieste di servizi sulla rete da parte degli utenti ai server in base ai parametri di reindirizzamento della porta. Se le richieste riguardano servizi non specificati, l'accesso viene negato. Ad esempio, se il numero di porta 80 (HTTP) viene inoltrato all'indirizzo IP 192.168.1.2, tutte le richieste HTTP sull'interfaccia vengono inoltrate a 192.168.1.2. Tutto il traffico rimanente viene rifiutato, a meno che sia consentito in maniera esplicita da un'altra voce.

Utilizzare questa funzione per definire un server Web o un server FTP. Accertarsi di immettere un indirizzo IP valido. Per eseguire un server Internet, potrebbe essere necessario utilizzare un indirizzo IP statico. Per una maggiore sicurezza, gli utenti esterni possono comunicare con il server ma non possono collegarsi ad altri dispositivi di rete.

Per aggiungere o modificare un servizio nella tabella, attenersi alla seguente procedura:

PASSAGGIO 1 Per aggiungere un servizio, fare clic su **Aggiungi** nella tabella Reindirizzamento intervallo porte.

Per modificare un servizio, selezionare la riga desiderata e fare clic su **Modifica**.

È possibile modificare i campi.

PASSAGGIO 2 Impostare le seguenti opzioni:

- Selezionare un'opzione dall'elenco a discesa **Servizio**. Se il servizio desiderato non compare nell'elenco, è possibile seguire le istruzioni della sezione **Aggiunta o modifica del nome di un servizio** per aggiungerlo.
- Inserire l'indirizzo del server nel campo **Indirizzo IP**.
- Selezionare l'**interfaccia**.

- Selezionare lo **stato**. Selezionare la casella per attivare il servizio. Deselezionarla per disattivare il servizio.

PASSAGGIO 3 Fare clic su **Salva**.

Aggiunta o modifica del nome di un servizio

Per aggiungere o modificare una voce nell'elenco dei servizi, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione servizio**. Se nel browser Web viene visualizzato un messaggio relativo alle finestre a comparsa, consentire il contenuto bloccato.

PASSAGGIO 2 Per aggiungere un servizio, fare clic su **Aggiungi** nella tabella Gestione servizio.

Per modificare un servizio, selezionare la riga desiderata e fare clic su **Modifica**.

È possibile modificare i campi. Se nel browser Web viene visualizzato un messaggio relativo alle finestre a comparsa, consentire il contenuto bloccato.

PASSAGGIO 3 Nell'elenco è possibile inserire fino a 30 servizi.

- **Nome servizio**: una breve descrizione.
- **Protocollo**: il protocollo richiesto. Fare riferimento alla documentazione del servizio per il quale si sta effettuando l'hosting.
- **Intervallo porte**: l'intervallo dei numeri di porta riservati a questo servizio.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione dell'attivazione delle porte

L'attivazione delle porte consente al dispositivo di monitorare i dati in uscita per determinati numeri di porta. L'indirizzo IP del client che ha inviato i dati corrispondenti viene memorizzato nel dispositivo. Quando i dati richiesti vengono restituiti al dispositivo, vengono trasmessi al client corretto utilizzando le regole di associazione degli indirizzi IP e delle porte.

Alcune applicazioni o giochi Internet utilizzano porte atipiche per comunicare tra il server e l'host LAN. Per utilizzare queste applicazioni, immettere la porta di attivazione (in uscita) e la porta in ingresso alternativa nella tabella Attivazione porte.

Per aggiungere o modificare il nome di un'applicazione nella tabella, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare la scheda **Configurazione** > **Reindirizzamento**.

PASSAGGIO 2 Per aggiungere il nome di un'applicazione, fare clic su **Aggiungi** nella tabella Reindirizzamento intervallo porte.

Per modificare il nome di un'applicazione, selezionare la riga desiderata e fare clic su **Modifica**. È possibile modificare i campi.

Se nel browser Web viene visualizzato un messaggio relativo alle finestre a comparsa, consentire il contenuto bloccato.

PASSAGGIO 3 Impostare le seguenti opzioni:

- **Nome applicazione**: il nome dell'applicazione.
- **Intervallo porte attivate**: il numero di porta iniziale e quello finale dell'intervallo di porte attivate. Per ulteriori informazioni, fare riferimento alla documentazione dell'applicazione.
- **Intervallo porte in ingresso**: il numero di porta iniziale e quello finale dell'intervallo di porte in ingresso. Per ulteriori informazioni, fare riferimento alla documentazione dell'applicazione.

PASSAGGIO 4 Fare clic su **Salva**.

Eliminazione di una voce della tabella

Per eliminare una voce dalla tabella, selezionare la voce desiderata e fare clic su **Elimina**.

Traduzione dell'indirizzo porta

La tecnica PAT (Port Address Translation, traduzione dell'indirizzo porta) è un'estensione di NAT (Network Address Translation) che consente di associare più dispositivi su una LAN a un singolo indirizzo IP pubblico per conservare gli indirizzi IP.

Il metodo PAT è simile al reindirizzamento delle porte; l'unica differenza consiste nel fatto che un pacchetto in ingresso con porta di destinazione (porta esterna) viene tradotto in una porta di destinazione differente del pacchetto (una porta interna). Il provider di servizi Internet (ISP) assegna un singolo indirizzo IP al dispositivo periferico. Quando un computer accede a Internet, il dispositivo assegna al client un numero di porta che viene aggiunto all'indirizzo IP interno fornendo al computer un indirizzo IP univoco.

Se un altro computer accede a Internet, il dispositivo assegna lo stesso indirizzo IP pubblico, ma con un numero di porta diverso. Sebbene entrambi i computer condividano lo stesso indirizzo IP pubblico, il dispositivo sa a quale computer inviare i pacchetti poiché utilizza i numeri di porta per assegnare ai pacchetti l'indirizzo IP interno univoco dei computer.

Per accedere a questa pagina, selezionare **Configurazione** > **Traduzione dell'indirizzo porta**.

Per aggiungere o modificare l'opzione PAT, attenersi alla seguente procedura:

PASSAGGIO 1 Per aggiungere un servizio, fare clic su **Aggiungi** nella tabella Traduzione dell'indirizzo porta.

Per modificare un servizio, selezionare la riga desiderata e fare clic su **Modifica**. È possibile modificare i campi.

Se nel browser Web viene visualizzato un messaggio relativo alle finestre a comparsa, consentire il contenuto bloccato.

PASSAGGIO 2 Selezionare un'opzione dall'elenco a discesa **Servizio**. È possibile immettere fino a un massimo di 30 servizi. Se il servizio desiderato non compare nell'elenco, è possibile seguire le istruzioni della sezione **Aggiunta o modifica del nome di un servizio** per aggiungerlo.

PASSAGGIO 3 Immettere l'indirizzo IP o il nome del dispositivo di rete che ospita il servizio.

PASSAGGIO 4 Fare clic su **Salva**.

Aggiunta o modifica del nome di un servizio

Per aggiungere o modificare una voce nell'elenco dei servizi, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Gestione servizio**. Se nel browser Web viene visualizzato un messaggio relativo alle finestre a comparsa, consentire il contenuto bloccato.

PASSAGGIO 2 Per aggiungere un servizio, fare clic su **Aggiungi** nella tabella Gestione servizio.

Per modificare un servizio, selezionare la riga desiderata e fare clic su **Modifica**. È possibile modificare i campi.

Se nel browser Web viene visualizzato un messaggio relativo alle finestre a comparsa, consentire il contenuto bloccato.

PASSAGGIO 3 Nell'elenco è possibile inserire fino a 30 servizi.

- **Nome servizio**: una breve descrizione.
- **Protocollo**: il protocollo richiesto. Fare riferimento alla documentazione del servizio per il quale si sta effettuando l'hosting.
- **Porta esterna**: il numero della porta esterna.
- **Porta interna**: il numero della porta interna.

PASSAGGIO 4 Fare clic su **Salva**.

Configurazione di NAT uno-a-uno

Il metodo NAT uno-a-uno crea una relazione che associa un indirizzo IP WAN valido a indirizzi IP LAN nascosti dalla WAN (Internet) da NAT. Ciò protegge i dispositivi LAN da rilevamenti e attacchi.

Per ottenere risultati ottimali, riservare gli indirizzi IP per le risorse interne che si desidera raggiungere attraverso il metodo NAT uno-a-uno.

È possibile associare un singolo indirizzo IP LAN o un intervallo di indirizzi IP a un intervallo esterno di indirizzi IP WAN di pari lunghezza, ad esempio tre indirizzi interni e tre indirizzi esterni. Il primo indirizzo interno è associato al primo indirizzo esterno, il secondo indirizzo IP interno è associato al secondo indirizzo esterno e così via.

Per accedere alla configurazione di NAT uno-a-uno, selezionare **Configurazione** > **NAT uno-a-uno** nel riquadro di spostamento.

Per attivare questa funzione, selezionare la casella **Attiva**.

Per aggiungere una voce all'elenco, fare clic su **Aggiungi** e inserire le seguenti informazioni:

- **Inizio intervallo privato**: l'indirizzo iniziale dell'intervallo di indirizzi IP interni che si desidera associare all'intervallo pubblico. Non includere nell'intervallo l'indirizzo IP di gestione del router.
- **Inizio intervallo pubblico**: l'indirizzo iniziale dell'intervallo di indirizzi IP pubblici forniti dall'ISP. Non includere nell'intervallo l'indirizzo IP WAN del router.
- **Lunghezza intervallo**: il numero di indirizzi IP nell'intervallo. La lunghezza dell'intervallo non può superare il numero di indirizzi IP validi. Per associare un singolo indirizzo, immettere 1.

Per modificare una voce, selezionare la voce desiderata e fare clic su **Modifica**. Nei campi di testo vengono visualizzate le informazioni disponibili. Effettuare le modifiche, quindi fare clic su **Salva**.

Clonazione degli indirizzi MAC

Alcuni ISP richiedono la registrazione di un indirizzo MAC (il codice a 12 cifre di identificazione univoca assegnato a ogni dispositivo di rete). Se in precedenza è stato registrato un indirizzo MAC diverso per il dispositivo presso l'ISP, è possibile selezionare questa funzionalità per clonare l'indirizzo sul dispositivo. Altrimenti è necessario contattare l'ISP per modificare l'indirizzo MAC registrato.

NOTA Se la funzionalità Clona indirizzo MAC è attiva, il mirroring delle porte non funziona.

Per accedere alla clonazione dell'indirizzo MAC, selezionare **Configurazione** > **Clona indirizzo MAC** nel riquadro di spostamento.

Per clonare un indirizzo MAC, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic sul pulsante di scelta **Interfaccia**.

PASSAGGIO 2 Fare clic su **Modifica** per visualizzare la pagina Modifica clone indirizzo MAC.

- **Indirizzo MAC definito dall'utente per la WAN**: fare clic sul pulsante di scelta e immettere le 12 cifre dell'indirizzo MAC registrato presso l'ISP.
- **Indirizzo MAC da questo PC**: fare clic per utilizzare l'indirizzo MAC del computer come indirizzo MAC clone per il dispositivo.

PASSAGGIO 3 Fare clic su **Salva**.

DNS Dinamico

Il servizio DDNS (Dynamic Domain Name System) assegna un nome di dominio fisso a un indirizzo IP WAN dinamico, in modo da poter effettuare l'hosting del proprio server Web, FTP o altro tipo di TCP/IP sulla LAN. Selezionare questa funzionalità per configurare le interfacce WAN con le informazioni DDNS.

Prima di configurare il servizio DNS dinamico sul router, si consiglia di visitare il sito www.dyndns.org e di registrare un nome di dominio. Il servizio è fornito da DynDNS.org. Gli utenti in Cina devono visitare il sito www.3322.org per effettuare la registrazione.

Per accedere a DDNS, selezionare **Configurazione > DNS dinamico** nel riquadro di spostamento.

Dopo aver selezionato un'interfaccia e aver fatto clic su **Modifica**, viene visualizzata la pagina Modifica configurazione DNS dinamico.

Per modificare il servizio DDNS, attenersi alla seguente procedura:

PASSAGGIO 1 Dall'elenco **Servizio DDNS**, scegliere il servizio.

PASSAGGIO 2 Immettere le informazioni dell'account:

- **Nome utente**: il nome utente per l'account DDNS. Se non è stato registrato un nome host, fare clic su **Registra** per accedere al sito Web DynDNS.com, dove è possibile iscriversi gratuitamente al servizio DNS dinamico.
- **Password**: la password per l'account DDNS.
- **Nome host**: il nome host registrato presso il provider DDNS. Ad esempio, se il nome host è *myhouse.dyndns.org*, immettere *myhouse* nel primo campo, *dyndns* nel secondo campo e *org* nell'ultimo campo.

- **Periodo di aggiornamento**: immettere il numero di ore in cui viene eseguito l'aggiornamento della configurazione del DNS dinamico. Per impostazione predefinita, tale numero è 360.

Vengono visualizzate le seguenti informazioni di sola lettura:

- **Indirizzo IP Internet**: l'indirizzo IP WAN per l'interfaccia.
- **Stato**: lo stato di DDNS. Se le informazioni sullo stato indicano un errore, accertarsi di aver immesso correttamente le informazioni dell'account associato al servizio DDNS.

PASSAGGIO 3 Fare clic su **Salva**.

Routing avanzato

Questa funzionalità attiva il routing dinamico e aggiunge percorsi statici alla tabella di routing per IPv4 e IPv6.

Per visualizzare la tabella di routing, fare clic su **Visualizza tabella di routing**. Fare clic su **Aggiorna** per aggiornare i dati. Fare clic su **Chiudi** per chiudere la finestra a comparsa.

Configurazione del routing dinamico

Il routing dinamico costruisce automaticamente le tabelle di routing in base alle informazioni dei protocolli di routing; ciò consente alla rete di agire in modo quasi autonomo nell'evitare errori di rete e blocchi.

Per configurare il routing dinamico IPv4 utilizzando il protocollo RIP (Routing Information Protocol), fare clic sulla scheda **IPv4**.

Per configurare il routing dinamico IPv6 utilizzando il protocollo RIPng (Routing Information Protocol) di prossima generazione, fare clic sulla scheda **IPv6**.

Configurazione del routing dinamico IPv4

PASSAGGIO 1 Scegliere la modalità di funzionamento:

- **Gateway**: selezionare questa modalità se il dispositivo ospita la connessione di rete a Internet. Questa è l'impostazione predefinita.
- **Router**: selezionare questa modalità se il dispositivo è su una rete con altri router e un altro dispositivo è il gateway di rete a Internet o questa rete non è connessa a Internet. In modalità Router, la connettività Internet è disponibile per i dispositivi di rete solo se è presente un altro router che funziona da gateway. Dal momento che la protezione firewall è fornita dal gateway, disattivare il firewall del dispositivo.

PASSAGGIO 2 Attivare il protocollo **RIP** per consentire al dispositivo di scambiare automaticamente le informazioni di routing con altri router e di regolare dinamicamente le tabelle di routing per adattarsi alle modifiche della rete. Il RIP è disattivato per impostazione predefinita. Se si attiva questa funzione, configurare anche le seguenti impostazioni:

- **Ricezione versioni RIP**: selezionare il protocollo RIP per la ricezione dei dati di rete: **Nessuno**, **RIPv1**, **RIPv2** o **Sia RIP v1 che v2**.

  RIPv1 è una versione di routing basata su classe. Non include informazioni di sottorete e, pertanto, non supporta subnet mask a lunghezza variabile (VLSM). RIPv1 non presenta nemmeno il supporto per l'autenticazione del router ed è quindi vulnerabile agli attacchi. **RIPv2** include una subnet mask e supporta la sicurezza di autenticazione mediante password.

- **Trasmissione versioni RIP**: selezionare il protocollo RIP per la trasmissione dei dati di rete: **Nessuno**, **RIPv1**, **RIPv2 - Broadcast** o **RIPv2 - Multicast**.

  RIPv2 - Broadcast (consigliato) trasmette i dati nell'intera sottorete. **RIPv2 - Multicast** invia dati a indirizzi multicast. RIPv2 - Multicast contribuisce anche a evitare carichi non necessari tramite il multicasting di tabelle di routing a router adiacenti invece della trasmissione all'intera rete.

PASSAGGIO 3 Fare clic su **Salva**.

Configurazione del routing dinamico IPv6

La scheda IPv6 è disponibile se è stato attivato l'IP dual-stack nella pagina Configurazione > Rete.

Per attivare RIPng, selezionare la casella **RIPng**.

Configurazione del routing statico

Il routing statico può essere configurato per IPv4 o IPv6. Si tratta di percorsi che vengono mantenuti nella tabella di routing. È possibile immettere massimo 30 percorsi.

Per configurare un percorso statico, fare clic su **Aggiungi** o selezionare una voce e fare clic su **Modifica**:

- **IP destinazione**: l'indirizzo di sottorete del segmento della LAN remota. Per i domini IP di Classe C, l'indirizzo di rete è rappresentato dai primi tre campi dell'indirizzo IP della rete LAN di destinazione. L'ultimo campo è zero.
- **Subnet mask (solo IPv4)**: la subnet mask utilizzata nel dominio IP della rete LAN di destinazione. Per i domini IP di Classe C la subnet mask è generalmente 255.255.255.0.
- **Lunghezza prefisso (solo IPv6)**: lunghezza del prefisso IPv6.
- **Gateway predefinito**: l'indirizzo IP del router dell'ultima risorsa.
- **Numero di hop**: il numero massimo di nodi o hop che un pacchetto attraversa prima di essere eliminato; il numero massimo è 15 hop. Un nodo è qualsiasi dispositivo della rete, ad esempio uno switch o un router.
- **Interfaccia**: l'interfaccia da utilizzare per il percorso.

Per eliminare una voce dall'elenco, selezionare la voce desiderata, quindi fare clic su **Elimina**.

Per visualizzare i dati attuali, fare clic su **Visualizza tabella di routing**. Viene visualizzato l'elenco delle voci della tabella di routing. È possibile fare clic su **Aggiorna** per aggiornare i dati oppure su **Chiudi** per chiudere la finestra a comparsa.

Bilanciamento del carico in arrivo

Il bilanciamento del carico in arrivo distribuisce il traffico in ingresso in maniera equa tra tutte le porte WAN per sfruttare al massimo la larghezza di banda. Impedisce anche una distribuzione non equa e la congestione del traffico.

Per attivare e configurare il bilanciamento del carico in arrivo, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Attiva bilanciamento del carico in arrivo**.

PASSAGGIO 2 Immettere le informazioni sul nome di dominio:

- **Nome dominio**: il nome di dominio assegnato dal provider del servizio DNS.
- **TTL** (Durata): l'intervallo di tempo per le richieste DNS (secondi, 0~65535). Un intervallo lungo incide sul tempo di aggiornamento. Un intervallo più breve aumenta il carico del sistema, ma la precisione del bilanciamento del carico in arrivo è maggiore. È possibile regolare questo parametro per garantire prestazioni di rete ottimali.
- **Amministratore**: l'indirizzo e-mail dell'amministratore.

PASSAGGIO 3 Immettere i parametri del **server DNS**:

- **Server nome**: il server DNS che traduce il nome di dominio.
- **Interfaccia**: l'interfaccia WAN corrispondente al server nome. Il sistema mostra gli indirizzi IP WAN acquisiti e attivati.

PASSAGGIO 4 Immettere il nome host che fornisce i servizi, ad esempio il server di posta o il server FTP, nel campo **Nome** (Record) **Host** e selezionare l'interfaccia **IP WAN** di distribuzione del traffico in ingresso.

PASSAGGIO 5 Immettere l'**alias** che assegna vari nomi a un host che potrebbe fornire vari servizi e la **destinazione**, un nome di dominio Record A esistente.

PASSAGGIO 6 Fare clic su **Impostazioni SPF** per aggiungere testo SPF. SPF (Sender Policy Framework) è un sistema di convalida della posta elettronica che blocca lo spam rilevando lo spoofing della posta elettronica (una vulnerabilità comune) attraverso la verifica degli indirizzi IP di origine. La configurazione di questo campo non è obbligatoria. Per ulteriori informazioni, visitare il sito http://www.openspf.org/Tools#wizard?mydomain=&x=35&y=6.

PASSAGGIO 7 Immettere i parametri del **server di posta**:

- **Nome host**: il nome (senza nome di dominio) dell'host di posta.
- **Peso**: l'ordine degli host di posta. A numeri bassi corrisponde una priorità più alta.
- **Server di posta**: il nome del server che viene salvato nel Record A o il nome di un server di posta esterno.

PASSAGGIO 8 Fare clic su **Salva**.

Aggiornamento del dispositivo USB

È possibile utilizzare questo dispositivo di rete per aggiornare il firmware del dispositivo USB.

Per l'aggiornamento di un dispositivo USB collegato a una porta USB, individuare il file da caricare da un PC sul dispositivo USB e fare clic su **Aggiorna**.

5

DHCP

DHCP (Dynamic Host Configuration Protocol) è un protocollo di rete utilizzato per configurare i dispositivi di rete per la comunicazione su una rete IP. Un client DHCP utilizza il protocollo DHCP per acquisire da un server DHCP informazioni di configurazione, come l'indirizzo IP, il percorso predefinito e uno o più indirizzi server DNS. Queste informazioni vengono poi utilizzate dal client DHCP per configurare il proprio host. Una volta completato il processo di configurazione, l'host è in grado di comunicare su Internet.

Sul server DHCP viene gestito un database di indirizzi IP disponibili e di informazioni sulla configurazione. Al ricevimento di una richiesta da un client, il server DHCP determina la rete a cui il client DHCP è connesso e assegna un indirizzo IP o un prefisso appropriato al client, oltre a inviare le informazioni di configurazione specifiche di tale client.

Il server e il client DHCP devono essere connessi allo stesso collegamento di rete. Nelle reti più estese, ogni collegamento di rete contiene uno o più agenti di relay DHCP. Questi ultimi ricevono messaggi dai client DHCP e li inoltrano ai server DHCP. I server DHCP inviano le risposte all'agente di relay, che a sua volta le invia al client DHCP sul collegamento di rete locale.

Generalmente, i server DHCP assegnano ai client indirizzi IP per un intervallo di tempo limitato denominato *lease*. I client DHCP sono responsabili del rinnovo dell'indirizzo IP prima della scadenza dell'intervallo. Se alla scadenza del lease, i client non sono in grado di rinnovarlo, devono interrompere l'utilizzo dell'indirizzo.

Il protocollo DHCP è utilizzato per il traffico IPv4 e IPv6. Entrambe le versioni assolvono lo stesso scopo, ma i dettagli del protocollo per IPv4 e IPv6 sono diversi al punto da doverli considerare come due protocolli separati.

Configurazione di DHCP

La finestra Configurazione DHCP consente di importare il protocollo DHCP per IPv4 o IPv6. Consente, inoltre, ad alcuni dispositivi di scaricare la loro configurazione da un server TFTP. Se un dispositivo non dispone di un indirizzo IP e di un indirizzo IP del server TFTP pre-configurati quando viene avviato, invia una richiesta con Option 66, 67 e 150 al server DHCP per ottenere tali informazioni.

Il parametro Option 150 di DHCP è proprietario di Cisco. Lo standard IEEE simile a tale requisito è Option 66. Come Option 150, il parametro Option 66 è utilizzato per specificare il nome del server TFTP. Il parametro Option 67 fornisce il nome del file di avvio.

Il parametro Option 82 (opzione per le informazioni dell'agente di relay DHCP) consente a un agente di relay DHCP di includere informazioni su di sé quando inoltra pacchetti DHCP originati dal client a un server DHCP. Il server DHCP può utilizzare tali informazioni per implementare l'indirizzamento IP o altri criteri di assegnazione dei parametri.

Per accedere alla configurazione DHCP, selezionare **DHCP > Configurazione DHCP**.

Per configurare la versione IPv4 di DHCP, fare clic sulla scheda **IPv4**. Per configurare la versione IPv6 di DHCP, fare clic sulla scheda **IPv6**.

Configurazione di DHCP per IPv4

Per configurare il protocollo DHCP per IPv4, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **VLAN** oppure **Option 82**.

PASSAGGIO 2 Se si seleziona **Option 82**, aggiungere gli ID di circuito; a tal fine, selezionare DHCP > **Option 82**. Gli ID di circuito sono elencati nel menu a discesa **ID circuito**.

Se si seleziona **VLAN**, selezionare la VLAN dal menu **ID VLAN** e specificare i parametri seguenti:

- **Indirizzo IP dispositivo**: l'indirizzo IP di gestione.
- **Subnet mask**: la subnet mask dell'IP di gestione.

PASSAGGIO 3 Selezionare un'opzione per **Modalità DHCP**:

- **Disattiva**: disattiva DHCP sul dispositivo. Non è necessario impostare ulteriori parametri.

- **Server DHCP**: comunica le richieste DHCP del client al server DHCP del dispositivo.
- **Relay DHCP**: trasmette le richieste DHCP e risponde da un altro server DHCP attraverso il dispositivo. Se si seleziona questa opzione, immettere l'indirizzo IP del server DHCP remoto nell'apposito campo.
- **Periodo di validità client**: l'intervallo, in minuti, durante il quale un utente di rete può connettersi al router con l'indirizzo IP corrente. I valori validi sono compresi tra 5 e 43200 minuti. L'impostazione predefinita è 1440 minuti (pari a 24 ore).
- **Inizio intervallo** e **Fine intervallo**: l'indirizzo IP iniziale e quello finale che creano un intervallo di indirizzi IP che è possibile assegnare in maniera dinamica. L'intervallo può estendersi fino al numero massimo di indirizzi IP che il server può assegnare senza sovrapporre le funzionalità, come PPTP e VPN SSL. Non includere l'indirizzo IP LAN del dispositivo in questo intervallo IP dinamico. Ad esempio, se il router utilizza l'indirizzo IP LAN predefinito, **192.168.1.1**, il valore iniziale deve essere 192.168.1.2 o superiore.
- **Server DNS**: il tipo di servizio DNS, dove viene acquisito l'indirizzo IP del server DNS.
- **DNS statico 1** e **DNS statico 2**: l'indirizzo IP statico di un server DNS. (Facoltativo) Se si immette un secondo server DNS, il dispositivo utilizza il primo server DNS per rispondere a una richiesta.
- **WINS**: l'indirizzo IP facoltativo di un server WINS (Windows Internet Naming Service) che converte i nomi NetBIOS in indirizzi IP. Se non si conosce l'indirizzo IP del server WINS, utilizzare l'impostazione predefinita 0.0.0.0.

PASSAGGIO 4 Immettere i parametri del server TFTP:

- **Nome host server TFTP**: il nome host del server TFTP.
- **IP server TFTP**: l'indirizzo IP del server TFTP.
- **Nome file di configurazione**: il nome del file di configurazione utilizzato per aggiornare un dispositivo.

Configurazione di DHCP per IPv6

Per configurare il protocollo DHCP per IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Immettere un indirizzo nel campo **Indirizzo IPv6**.

PASSAGGIO 2 Immettere un valore nel campo **Lunghezza prefisso**.

PASSAGGIO 3 Selezionare un'opzione per **Modalità DHCP**:

- **Disattiva**: disattiva DHCP sul dispositivo. Non è necessario impostare ulteriori parametri.
- **Server DHCP**: comunica le richieste DHCP del client al server DHCP del dispositivo.
- **Relay DHCP**: trasmette le richieste DHCP e risponde da un altro server DHCP attraverso il dispositivo.
- **Periodo di validità client**: l'intervallo durante il quale un utente di rete può connettersi al router con l'indirizzo IP corrente. L'intervallo è espresso in minuti. I valori validi sono compresi tra 5 e 43200 minuti. L'impostazione predefinita è 1440 minuti (pari a 24 ore).
- **Server DNS 1** e **Server DNS 2**: (facoltativo) l'indirizzo IP di un server DNS. Se si immette un secondo server DNS, il dispositivo utilizza il primo server DNS per rispondere. Se si specifica un server DNS è possibile accedere più rapidamente rispetto all'utilizzo di un server DNS assegnato dinamicamente. L'impostazione predefinita 0.0.0.0 consente di utilizzare un server DNS con assegnazione dinamica.

PASSAGGIO 4 Immettere il pool di indirizzi IPv6:

- **Indirizzo iniziale**: l'indirizzo iniziale del pool di indirizzi IPv6.
- **Indirizzo finale**: l'indirizzo finale del pool di indirizzi IPv6.
- **Lunghezza prefisso**: lunghezza del prefisso dell'indirizzo IP IPv6.

Visualizzazione dello stato DHCP

Nella pagina Stato DHCP viene visualizzato lo stato del server DHCP e dei relativi client.

Per accedere a questa pagina, selezionare **DHCP** > **Stato DHCP** nel riquadro di spostamento.

La scheda IPv6 è disponibile soltanto se nella pagina **Configurazione della rete** è stato attivato l'IP dual stack.

Per visualizzare lo stato e i client DHCP, fare clic sulla scheda **IPv4** o sulla scheda **IPv6**. Per IPv4, selezionare **VLAN** oppure **Option 82**. Per IPv6, selezionare **Prefisso**.

Per il server DHCP, vengono mostrate le seguenti informazioni:

- **Server DHCP**: l'indirizzo IP del server DHCP.
- **IP dinamici utilizzati**: il numero di indirizzi IP dinamici utilizzati.
- **IP statici utilizzati (solo IPv4)**: il numero di indirizzi IP statici utilizzati.
- **DHCP disponibile**: il numero di indirizzi IP dinamici disponibili.
- **Totale**: il numero totale di indirizzi IP dinamici gestiti dal server DHCP.

Nella tabella dei client vengono mostrate le informazioni relative ai client DHCP:

- **Nome host client**: il nome assegnato a un host client.
- **Indirizzo IP**: l'indirizzo IP dinamico assegnato a un client.
- **Indirizzo MAC (solo IPv4)**: l'indirizzo MAC di un client.
- **Periodo di validità client**: l'intervallo durante il quale un utente di rete può restare connesso al router con un indirizzo IP dinamico.

Per rilasciare un indirizzo IP client IPv4, selezionare **Nome host client** e fare clic su **Elimina**.

Fare clic su **Aggiorna** per aggiornare i dati.

Option 82

Il parametro Option 82 (opzione per le informazioni dell'agente di relay DHCP) consente a un agente di relay DHCP di includere informazioni su di sé quando inoltra pacchetti DHCP originati dal client a un server DHCP. Il server DHCP può utilizzare tali informazioni per implementare l'indirizzamento IP o altri criteri di assegnazione dei parametri.

L'ID di circuito configurabile Option 82 di DHCP ottimizza la sicurezza della convalida consentendo all'utente di determinare le informazioni fornite nella descrizione dell'ID di circuito Option 82.

Per accedere a questa pagina, selezionare **DHCP> Option 82** nel riquadro di spostamento.

Per aggiungere un **ID circuito**, fare clic su **Aggiungi**. Viene aggiunta una nuova riga alla tabella e gli ID di circuito sono elencati nel relativo menu a discesa nella finestra **Configurazione di DHCP**.

Per modificare un **ID circuito**, selezionare la riga e fare clic su **Modifica**. La riga viene aperta per la modifica.

Binding di indirizzi IP e MAC

Se il dispositivo è configurato come server DHCP o per il relay DHCP, è possibile eseguire il binding di indirizzi IP statici per un massimo di 80 dispositivi di rete, ad esempio un server Web o un server FTP.

Generalmente, l'indirizzo MAC di un dispositivo è stampato su un'etichetta apposta sul pannello inferiore o posteriore di un dispositivo.

Per accedere alla funzione di binding, selezionare **DHCP > Binding degli indirizzi IP e MAC** nel riquadro di spostamento.

Eseguire il binding di indirizzi IP tramite rilevamento

Per eseguire il binding di indirizzi IP noti a indirizzi MAC e assegnare un nome al binding, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Mostra indirizzi MAC sconosciuti**. Viene visualizzata la tabella di binding degli indirizzi IP e MAC. Se nel browser Web viene visualizzato un messaggio relativo alle finestre a comparsa, consentire il contenuto bloccato.

I dispositivi sono elencati per indirizzo IP e indirizzo MAC. Se necessario, fare clic su **Aggiorna** per aggiornare i dati.

PASSAGGIO 2 Immettere un **Nome** descrittivo.

PASSAGGIO 3 Selezionare la casella **Attiva**. In alternativa, fare clic sulla casella di controllo nella parte superiore della colonna Attiva per selezionare tutti i dispositivi dell'elenco.

PASSAGGIO 4 Fare clic su **Salva** per aggiungere i dispositivi all'elenco di indirizzi IP statici oppure fare clic su **Chiudi** per chiudere la finestra a comparsa senza aggiungere i dispositivi selezionati.

Eseguire il binding manuale di indirizzi IP

Per aggiungere un nuovo binding all'elenco, fare clic su **Aggiungi** e immettere le seguenti informazioni:

- **Indirizzo IPv4 statico:** inserire l'indirizzo IP da assegnare al dispositivo.
- **Indirizzo MAC: indirizzo MAC** Dispositivo .
- **Nome**: il nome descrittivo del dispositivo.
- **Attiva**: selezionare questa casella per eseguire il binding dell'indirizzo IP statico a questo dispositivo.

Modifica o eliminazione di voci di binding

Per **modificare** le impostazioni, selezionare una voce dall'elenco e fare clic su **Modifica**. Nei campi di testo vengono visualizzate le informazioni disponibili. Effettuare le modifiche, quindi fare clic su **Salva**.

Per **eliminare** una voce dall'elenco, selezionare la voce desiderata e fare clic su **Elimina**. Per selezionare un gruppo di voci, fare clic sulla prima voce, quindi tenere premuto **MAIUSC** e fare clic sull'ultima voce del gruppo. Per selezionare singole voci, tenere premuto **CTRL** e fare clic su ogni voce da includere nella selezione. Per deselezionare una voce, tenere premuto **CTRL** e fare clic sulla voce desiderata.

Utilizzo dell'elenco di indirizzi IP statici per bloccare i dispositivi

È possibile utilizzare l'elenco di indirizzi IP statici per controllare l'accesso alla rete.

Per bloccare l'accesso da parte di dispositivi che non sono presenti nell'elenco o non dispongono dell'indirizzo IP corretto, attenersi alla seguente procedura:

- **Blocco indirizzo MAC nell'elenco con indirizzo IP errato**: selezionare questa casella per impedire a un dispositivo di accedere alla rete se il suo indirizzo IP è stato modificato. Ad esempio, se è stato assegnato l'indirizzo IP statico 192.168.1.100 e qualcuno configura il dispositivo per utilizzare l'indirizzo 192.168.149, il dispositivo non potrà collegarsi alla rete. In questo modo gli utenti non hanno motivo di modificare gli indirizzi IP del dispositivo senza autorizzazione. Deselezionare questa casella per consentire l'accesso a prescindere dall'indirizzo IP attuale.

- **Blocco indirizzo MAC non presente nell'elenco**: selezionare questa casella per bloccare l'accesso tramite dispositivi non inclusi nell'elenco degli indirizzi IP statici. Ciò impedisce a dispositivi sconosciuti di accedere alla rete. Deselezionare la casella per consentire l'accesso a tutti i dispositivi configurati con un indirizzo IP nell'intervallo corretto.

Database locale DNS

DNS (Domain Name Service) abbina un nome di dominio al suo indirizzo IP indirizzabile. È possibile configurare un database locale DNS che consenta al dispositivo di agire come server DNS locale per i nomi di dominio di uso comune. L'utilizzo di un database locale può essere più rapido rispetto all'uso di un server DNS esterno. Se un nome di dominio richiesto non è presente nel database locale, la richiesta viene inoltrata al server DNS specificato nella pagina **Configurazione della rete** > Impostazioni WAN.

Se si attiva questa funzionalità, è necessario configurare anche i dispositivi client in modo che utilizzino il dispositivo come server DNS. Per impostazione predefinita, i computer Windows sono configurati per ottenere l'indirizzo di un server DNS automaticamente dal gateway predefinito.

Per modificare le impostazioni di connessione TCP/IP, ad esempio, su un PC Windows, accedere alla finestra *Proprietà connessione alla rete locale (LAN) > Protocollo Internet > Proprietà TCP/IP*. Selezionare **Utilizza l'indirizzo server DNS seguente** e immettere l'indirizzo IP LAN del router come server DNS preferito. Per ulteriori informazioni, fare riferimento alla documentazione del client che si sta configurando.

Come aggiungere, modificare o eliminare voci DNS locali

Per aggiungere una nuova voce, fare clic su **Aggiungi** e immettere le seguenti informazioni:

- **Nome host**: immettere il nome di dominio, ad esempio *esempio.com* oppure *esempio.org*. Se non si include il livello finale del nome di dominio, Microsoft Windows® aggiungerà automaticamente *.com* alla voce.
- **Indirizzo IP**: immettere l'indirizzo IP della risorsa.

Per modificare le impostazioni, selezionare una voce dall'elenco. Nei campi di testo vengono visualizzate le informazioni disponibili. Effettuare le modifiche, quindi fare clic su **Salva**.

Per eliminare una voce dall'elenco, selezionare la voce desiderata e fare clic su **Elimina**. Per selezionare un gruppo di voci, fare clic sulla prima voce, quindi tenere premuto **MAIUSC** e fare clic sull'ultima voce del gruppo. Per selezionare singole voci, tenere premuto **CTRL** e fare clic su ogni voce da includere nella selezione. Per deselezionare una voce, tenere premuto **CTRL** e fare clic sulla voce desiderata.

Annuncio router (IPv6)

Il daemon RADVD (Router Advertisement Daemon) viene utilizzato per la configurazione automatica e il routing IPv6. Se attivato, i messaggi vengono inviati periodicamente dal router e su richiesta. Un host utilizza queste informazioni per ottenere i prefissi e i parametri per la rete locale. Se si disattiva questa funzione, viene disattivata anche la configurazione automatica ed è necessario configurare manualmente l'indirizzo IPv6, il prefisso della sottorete e il gateway predefinito su ogni dispositivo.

Questa pagina è disponibile se nella pagina **Configurazione della rete** è stato attivato l'IP dual stack. In caso contrario, se si tenta di aprire questa pagina, viene visualizzato un messaggio.

Per aprire questa pagina, selezionare **DHCP** > **Annuncio router** nel riquadro di spostamento.

Per attivare questa funzionalità, selezionare la casella **Attiva annuncio router** e completare gli altri campi:

- **Modalità annuncio**: scegliere una delle opzioni seguenti:
  - **Multicast non richiesto**: invia annunci router a tutte le interfacce che appartengono al gruppo multicast. Questa è l'impostazione predefinita. Immettere anche un valore nel campo **Intervallo annuncio**; questo valore indica l'intervallo in base al quale vengono inviati i messaggi. Immettere un valore compreso tra 10 e 1800 secondi. L'impostazione predefinita è 30 secondi.
  - **Solo unicast**: invia messaggi con annunci router solo a indirizzi IPv6 noti.

- **Flag RA**: determina se gli host possono utilizzare o meno DHCPv6 per ottenere indirizzi IP e informazioni correlate. Sono disponibili le seguenti opzioni:
  - **Gestito**: gli host utilizzano un protocollo di configurazione stateful/gestito (DHCPv6) per ricevere gli indirizzi stateful e altre informazioni tramite DHCPv6.
  - **Altro**: utilizza un protocollo di configurazione stateful/gestito (DHCPv6) per ricevere informazioni diverse dagli indirizzi, come gli indirizzi di server DNS.
- **Preferenza router**: la metrica di preferenza Alta, Media o Bassa utilizzata in una topologia di rete in cui host multihomed hanno accesso a più router. Questa metrica consente all'host di scegliere il router appropriato. Se è possibile raggiungere due router, verrà selezionato quello con la preferenza maggiore. Questi valori sono ignorati dagli host che non implementano la preferenza router. L'impostazione predefinita è Alta.
- **MTU**: la dimensione del pacchetto più grande che può essere inviato sulla rete. Il valore MTU (Maximum Transmission Unit) viene utilizzato nei messaggi di annunci router per garantire che tutti i nodi della rete utilizzino lo stesso MTU quando il valore MTU della LAN non è noto. L'impostazione predefinita è 1500 byte, che corrisponde al valore standard per le reti Ethernet. Per le connessioni PPPoE questo valore è di 1492 byte. Non modificare questa impostazione, salvo diversa indicazione da parte dell'ISP.
- **Durata del router**: il tempo, in secondi, di durata dei messaggi di annunci router sul percorso. L'impostazione predefinita è 3600 secondi.

Per aggiungere una nuova sottorete, fare clic su **Aggiungi** e completare i campi **Indirizzo IPv6**, **Lunghezza prefisso** e **Durata**.

6

Gestione sistema

La finestra Gestione sistema consente di configurare impostazioni avanzate, come gli strumenti diagnostici, e di eseguire attività, come gli aggiornamenti del firmware, i backup e i riavvii del dispositivo.

Connessioni dual WAN

Utilizzare questa funzionalità per configurare le impostazioni per le connessioni Internet se si utilizzano più interfacce WAN.

Per configurare le porte WAN, selezionare **Gestione sistema** > **Dual WAN** nel riquadro di spostamento.

Per configurare il bilanciamento del carico, selezionare una delle seguenti modalità per gestire le connessioni WAN:

- **Backup Smart Link**: garantisce la continua connettività. Se la connessione WAN primaria non è disponibile, si utilizza la connessione WAN di backup. Selezionare l'interfaccia WAN primaria dal menu a discesa.
- **Bilanciamento del carico**: utilizzare simultaneamente entrambe le connessioni WAN per aumentare la larghezza di banda disponibile. Il router bilancia il traffico tra le due interfacce in modalità WRR (Weighted Round-Robin).

NOTA Le query DNS non sono soggette al bilanciamento del carico.

Per configurare le impostazioni dell'interfaccia, selezionare l'interfaccia WAN desiderata e fare clic su **Modifica**. Viene visualizzata la finestra delle impostazioni per l'interfaccia. Immettere i parametri seguenti.

Larghezza di banda massima fornita dall'ISP

Immettere le impostazioni della larghezza di banda massima specificate dall'ISP. Se la larghezza di banda supera il numero specificato, il router utilizza un'altra interfaccia WAN per la connessione successiva.

- **Upstream**: larghezza di banda upstream massima fornita dall'ISP. L'impostazione predefinita è 10000 kbs. Il valore massimo consentito è 1000000 kbs.
- **Downstream**: larghezza di banda downstream massima fornita dall'ISP. L'impostazione predefinita è 10000 kbs.

Rilevamento servizi di rete

È possibile selezionare questa casella per consentire al dispositivo di rilevare la connettività di rete eseguendo il ping di dispositivi specifici e immettere le impostazioni come descritto di seguito:

- **Conteggio tentativi**: numero di ping da eseguire su un dispositivo. L'intervallo è compreso tra 1 e 99999; il valore predefinito è 3.
- **Timeout tentativi**: numero di secondi di attesa tra un ping e l'altro. L'intervallo è compreso tra 1 e 9999999; il valore predefinito è 10 secondi.
- **Se non riesce**: azione eseguita in caso di test di ping non riuscito:
  - **Genera condizione di errore nel log di sistema**: registra il guasto nel log di sistema. Non si esegue il failover sull'altra interfaccia.
  - **Mantieni log di sistema e Rimuovi connessione**: si esegue il failover e si utilizza l'interfaccia di backup. Al ripristino della connettività della porta WAN, viene ripristinato anche il relativo traffico.
- **Gateway predefinito, Host ISP, Host remoto** e **Host ricerca DNS**: selezionare il dispositivo di cui si desidera eseguire il ping per determinare la connettività di rete. Per un host ISP o un host remoto, immettere l'indirizzo IP. Per un host di ricerca DNS, immettere un nome host o un nome di dominio. Deselezionare la casella se non si desidera eseguire il ping di questo dispositivo per il rilevamento del servizio di rete.

del protocollo

Il del protocollo richiede l'utilizzo dell'interfaccia per protocolli e indirizzi di origine e destinazione specifici. Consente a un amministratore di eseguire il di un determinato tipo traffico in un'uscita a un'interfaccia WAN. Questa opzione viene utilizzata, in genere, quando le due interfacce WAN hanno caratteristiche diverse o laddove parte del traffico da LAN a WAN debba passare attraverso la stessa interfaccia WAN.

Per aggiungere o modificare voci della tabella, fare clic su **Aggiungi** o **Modifica** e immettere le seguenti informazioni:

- **Servizio**: il servizio (o tutto il traffico) per il quale eseguire il a questa interfaccia WAN. Se un servizio non compare nell'elenco, fare clic su **Gestione servizio** per aggiungerlo. Per ulteriori informazioni, vedere la sezione **Aggiunta o modifica di un servizio**.
- **IP origine** e **IP destinazione**: l'origine interna e la destinazione esterna per il traffico che attraversa questa porta WAN. Se si desidera specificare un intervallo di indirizzi IP, immettere il primo indirizzo nel primo campo e l'indirizzo finale nel campo *A*. Se si desidera specificare un intervallo IP, immettere lo stesso indirizzo in entrambi i campi.

Per attivare il del protocollo, selezionare la casella oppure deselezionarla per disattivarlo.

Per **modificare** le impostazioni, selezionare una voce dall'elenco. Nei campi di testo vengono visualizzate le informazioni disponibili. Effettuare le modifiche, quindi fare clic su **Salva**.

Per **eliminare** una voce dall'elenco, selezionare la voce desiderata e fare clic su **Elimina**. Per selezionare un gruppo di voci, fare clic sulla prima voce, quindi tenere premuto **MAIUSC** e fare clic sull'ultima voce del gruppo. Per selezionare singole voci, tenere premuto **CTRL** e fare clic su ogni voce da includere nella selezione. Per deselezionare una voce, tenere premuto **CTRL** e fare clic sulla voce desiderata.

Aggiunta o modifica di un servizio

Per aggiungere una nuova voce all'elenco dei servizi o per modificare una voce esistente, fare clic su **Gestione servizio**. Nell'elenco è possibile inserire fino a 30 servizi. Se nel browser Web viene visualizzato un messaggio relativo alle finestre a comparsa, consentire il contenuto bloccato.

Per aggiungere un servizio all'elenco, fare clic su **Aggiungi** e immettere le seguenti informazioni:

- **Nome servizio**: una breve descrizione.
- **Protocollo**: il protocollo richiesto. Fare riferimento alla documentazione del servizio per il quale si sta effettuando l'hosting.
- **Intervallo porte**: intervallo di porte richiesto.

Per **modificare** le impostazioni, selezionare una voce dall'elenco e fare clic su **Modifica**. Nei campi di testo vengono visualizzate le informazioni disponibili. Effettuare le modifiche, quindi fare clic su **Salva**.

Per **eliminare** una voce dall'elenco, selezionare la voce desiderata e fare clic su **Elimina**. Per selezionare un gruppo di voci, fare clic sulla prima voce, quindi tenere premuto **MAIUSC** e fare clic sull'ultima voce del gruppo. Per selezionare singole voci, tenere premuto **CTRL** e fare clic su ogni voce da includere nella selezione. Per deselezionare una voce, tenere premuto **CTRL** e fare clic sulla voce desiderata.

Gestione larghezza di banda

La finestra Gestione larghezza di banda consente di regolare le impostazioni della larghezza di banda per il traffico upstream e downstream e di configurare i parametri QoS (Quality of Service) per vari tipi di traffico, ad esempio i servizi voce.

NOTA Se non vengono aggiunte regole di QoS, la larghezza di banda WAN totale non è limitata al valore massimo della larghezza di banda configurato. (P59)

Per accedere alla gestione della larghezza di banda, selezionare **Gestione sistema** > **Gestione larghezza di banda** nel riquadro di spostamento.

Larghezza di banda massima fornita dall'ISP

Immettere le impostazioni della larghezza di banda massima specificate dall'ISP:

- **Upstream**: larghezza di banda upstream massima fornita dall'ISP.

- **Downstream**: larghezza di banda downstream massima fornita dall'ISP.

Tipo di gestione larghezza di banda

Scegliere una delle opzioni di gestione seguenti:

- **Controllo intervallo**: larghezza di banda minima (garantita) e massima (limitata) per ciascun servizio o indirizzo IP. È possibile immettere fino a un massimo di 100 servizi.
- **Priorità**: consente di gestire la larghezza di banda tramite l'identificazione di servizi ad alta e a bassa priorità.

Controllo intervallo

Per aggiungere un'interfaccia soggetta alla gestione della larghezza di banda, fare clic su **Aggiungi** e immettere le impostazioni seguenti:

- **Interfaccia**: l'interfaccia che supporta il servizio.
- **Servizio**: il servizio da gestire. Se un servizio non compare nell'elenco, fare clic su **Gestione servizio** per aggiungerlo.
- **IP**: l'indirizzo IP o l'intervallo da controllare.
- **Direzione**: selezionare **Upstream** per il traffico in uscita. Selezionare **Downstream** per il traffico in ingresso.
- **Velocità minima**: velocità minima in kbs per la larghezza di banda garantita.
- **Velocità massima**: velocità massima in kbs per la larghezza di banda garantita.

Selezionare la casella per attivare il servizio.

Configurazione della priorità

Per aggiungere un'interfaccia soggetta alla gestione della larghezza di banda, fare clic su **Aggiungi** e immettere le impostazioni seguenti:

- **Interfaccia**: l'interfaccia che supporta il servizio.
- **Servizio**: il servizio da gestire. Se un servizio non compare nell'elenco, fare clic su **Gestione servizio** per aggiungerlo.
- **Direzione**: selezionare **Upstream** per il traffico in uscita. Selezionare **Downstream** per il traffico in ingresso.

- **Priorità**: selezionare la priorità per questo servizio: **Alta** o **Bassa**. Il livello di priorità predefinito è Media; questa opzione è implicita e non viene visualizzata nell'interfaccia Web.

Selezionare la casella per attivare il servizio.

Per **modificare** le impostazioni, selezionare una voce dall'elenco e fare clic su **Modifica**. Nei campi di testo vengono visualizzate le informazioni disponibili. Effettuare le modifiche, quindi fare clic su **Salva**.

Per **eliminare** una voce dall'elenco, selezionare la voce desiderata e fare clic su **Elimina**. Per selezionare un gruppo di voci, fare clic sulla prima voce, quindi tenere premuto **MAIUSC** e fare clic sull'ultima voce del gruppo. Per selezionare singole voci, tenere premuto **CTRL** e fare clic su ogni voce da includere nella selezione. Per deselezionare una voce, tenere premuto **CTRL** e fare clic sulla voce desiderata.

SNMP

Il protocollo SNMP (Simple Network Management Protocol) consente agli amministratori di rete di gestire, monitorare e ricevere notifiche di eventi critici man mano che si verificano sulla rete. Il dispositivo supporta SNMP v1/v2c e SNMP v3. Il dispositivo supporta MIB (Management Information Base) standard, come MIBII, oltre a MIB private.

Il dispositivo agisce da agente SNMP che risponde ai comandi SNMP da sistemi di gestione di rete SNMP. Sono supportati i comandi SNMP standard get/next/set. Vengono generati anche messaggi trap per inviare al gestore SNMP un notifica quando si verificano condizioni di allarme, ad esempio riavvii, cicli di accensione ed eventi di collegamento WAN.

Per accedere a questa pagina, selezionare **Gestione sistema > SNMP** nel riquadro di spostamento.

Configurazione di SNMP

- **Nome sistema**: nome host per il dispositivo.
- **Contatto del sistema**: nome dell'amministratore di rete che può essere contattato per aggiornamenti sul dispositivo.

- **Percorso di sistema**: informazioni sui recapiti dell'amministratore di rete**:** indirizzo e-mail, numero di telefono o numero di cercapersone.
- **Nome della comunità trap**: password inviata con ciascun trap al gestore SNMP. La stringa può essere composta da un massimo di 64 caratteri alfanumerici. L'impostazione predefinita è **public**.
- **Attiva SNMPv1/v2c**: attiva SNMP v1/v2c.
  - **Ottieni nome comunità**: stringa della comunità per l'autenticazione dei comandi GET SNMP. È possibile immettere massimo 64 caratteri alfanumerici. L'impostazione predefinita è *public*.
  - **Imposta nome comunità**: stringa della comunità per l'autenticazione dei comandi SET SNMP. È possibile immettere massimo 64 caratteri alfanumerici. L'impostazione predefinita è *private*.
  - **Indirizzo IP ricevitore trap SNMPv1/v2c**: l'indirizzo IP o il nome di dominio del server su cui è in esecuzione il software di gestione SNMP.
- **Attiva SNMPv3**: attiva SNMPv3. Selezionare la casella e fare clic su **Salva** prima di creare gruppi e utenti SNMP. Seguire le istruzioni della sezione **Configurazione di SNMPv3**.
  - **Indirizzo IP ricevitore trap SNMPv3**: l'indirizzo IP o il nome di dominio del server su cui è in esecuzione il software di gestione SNMP.
  - **Utente ricevitore trap SNMPv3**: il nome utente per il server su cui è in esecuzione il software di gestione SNMP.

Configurazione di SNMPv3

È possibile creare gruppi SNMPv3 per gestire l'accesso MIB SNMP e identificare gli utenti che hanno accesso a ciascun gruppo.

Per aggiungere o modificare un gruppo, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Aggiungi** oppure selezionare un gruppo e fare clic su **Modifica** nella tabella dei gruppi.

PASSAGGIO 2 Immettere il nome del gruppo nell'apposito campo.

PASSAGGIO 3 Selezionare il livello di sicurezza dal rispettivo menu a discesa. Se si seleziona **Autenticazione** o **Privacy** gli utenti devono immettere una password per autenticarsi. Se si seleziona **Nessuna autenticazione**, **Nessuna privacy**, gli utenti del gruppo non dovranno impostare una password di autenticazione o per la privacy. L'impostazione predefinita è **Nessuna autenticazione, Nessuna privacy**.

Le password per l'autenticazione e la privacy devono essere composte da almeno 8 caratteri.

PASSAGGIO 4 Selezionare le **MIB** a cui i membri del gruppo possono accedere.

PASSAGGIO 5 Fare clic su **Salva**.

Per aggiungere o modificare un utente, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Aggiungi** oppure selezionare un utente e fare clic su **Modifica** nella tabella degli utenti.

PASSAGGIO 2 Immettere il nome utente nel rispettivo campo.

PASSAGGIO 3 Selezionare un'opzione dal menu a discesa **Gruppo**.

PASSAGGIO 4 Selezionare un'opzione per **Metodo di autenticazione** e immettere una password nel campo **Password di autenticazione**.

PASSAGGIO 5 Selezionare un'opzione per **Metodo privacy** e immettere una password nel campo **Password privacy**.

PASSAGGIO 6 Fare clic su **Salva**.

SMTP

Il protocollo SMPT (Simple Mail Transfer Protocol) è uno standard Internet per la trasmissione della posta elettronica (e-mail). Per configurare il protocollo SMTP, fornire le impostazioni SMTP che verranno utilizzate per inviare il Log o il file di configurazione OpenVPN.

Per configurare il protocollo SMTP, selezionare Gestione di sistema > SMTP, inserire le seguenti impostazioni e fare clic su Salva.

- Mittente: l'indirizzo e-mail del mittente.
- Server di posta: il nome o l'indirizzo IP del server di posta.
- Autenticazione: il tipo di autenticazione per l'accesso al server di posta.
  - Nessuna: nessun tipo di autenticazione.
  - Accesso in chiaro: autenticazione in formato testo normale.

- TLS: protocollo di autenticazione per connessioni sicure; ad esempio Gmail utilizza il tipo di autenticazione TLS sulla porta 587.
- SSS: protocollo di autenticazione per connessioni sicure; ad esempio Gmail utilizza il tipo di autenticazione SSL sulla porta 465.

▪ Porta SMTP: il numero di porta del protocollo SMTP (Simple Mail Transfer Protocol).

- Nome utente: il nome utente associato all'indirizzo e-mail. Ad esempio:
  - Server di posta: smtp.gmail.com Autenticazione: SSL
  - PORTA SMTP: 465
  - Nome utente: xxxxx@gmail.com
  - Password: yyyyyy
- Password: la password associata all'indirizzo e-mail.

Rilevamento - Bonjour

Bonjour è un protocollo per il rilevamento del servizio che individua i dispositivi di rete, come computer e server, sulla LAN. Se questa funzione è attivata, il dispositivo invia periodicamente tramite multicast i dati del servizio Bonjour alla LAN per dichiararne l'esistenza.

NOTA Per il rilevamento di prodotti Cisco, Cisco fornisce l'utilità FindIt, che appare come barra degli strumenti nel browser Web. Questa utilità rileva i dispositivi Cisco nella rete e visualizza le informazioni di base, ad esempio i numeri di serie e gli indirizzi IP. Per ulteriori informazioni e per scaricare l'utilità, visitare il sito www.cisco.com/go/findit.

Per accedere a questa pagina, selezionare **Gestione sistema > Rilevamento - Bonjour** nel riquadro di spostamento.

Per attivare Bonjour a livello globale, selezionare la casella **Attivazione rilevamento**. Questa funzione è selezionata per impostazione predefinita.

Per attivare Bonjour per una VLAN, selezionare la casella nella colonna **Attiva Bonjour**. Questa funzione è selezionata per impostazione predefinita.

Proprietà LLDP

LLDP (Link Layer Discovery Protocol) è un protocollo universale della suite di protocolli Internet utilizzato dai dispositivi di rete per dichiarare la propria identità, le proprie funzionalità e i router adiacenti su una LAN IEEE 802, principalmente di tipo Ethernet cablato. I dispositivi inviano le informazioni LLDP da ciascuna delle loro interfacce a intervalli fissi sotto forma di frame Ethernet. Ciascun frame contiene una LLDPDU (LLDP Data Unit). Ogni LLDPDU è una sequenza di strutture TLV (tipo-lunghezza-valore).

Per accedere a questa pagina, selezionare **Gestione sistema > Proprietà LLDP** nel riquadro di spostamento.

Per attivare le proprietà LLDP, selezionare la casella **Attiva**. Questa funzione è selezionata per impostazione predefinita.

Per attivare le proprietà LLDP su un'interfaccia, selezionare la casella **Attiva**, **WAN1** o **.WAN2** Queste caselle sono selezionate per impostazione predefinita.

Nella Tabella Router LLDP adiacenti vengono visualizzate le seguenti informazioni:

- **Porta locale**: l'identificatore della porta.
- **Sottotipo ID chassis**: il tipo di ID chassis, ad esempio indirizzo MAC.
- **ID chassis**: l'identificatore del chassis. Se il sottotipo ID chassis è un indirizzo MAC, viene visualizzato l'indirizzo MAC del dispositivo.
- **Sottotipo ID porta**: il tipo di identificatore della porta.
- **ID porta**: l'identificatore della porta.
- **Nome del sistema**: il nome del dispositivo.
- **Durata**: la velocità, in secondi, con cui vengono inviati gli aggiornamenti degli annunci LLDP.

Diagnostica

La pagina Diagnostica consente di accedere a due strumenti integrati: Ricerca nome DNS e Ping. Se si sospetta che ci siano problemi legati alla connettività, è possibile utilizzare questi strumenti per cercare di individuare le cause.

Per accedere a questa pagina, selezionare **Gestione del sistema > Diagnostica**.

Per utilizzare DNS per apprendere un indirizzo IP, selezionare **Ricerca DNS**, immettere un nome di dominio nel campo **Ricerca nome di dominio**, ad esempio www.cisco.com, e fare clic su **Vai**. Viene visualizzato l'indirizzo IP.

Per testare la connettività a un host specifico, selezionare **Ping**, immettere un indirizzo IP o un nome host e fare clic su **Vai**. Se non si conosce l'indirizzo IP, utilizzare lo strumento di ricerca DNS per apprenderlo. L'esecuzione del ping mostra se il dispositivo è in grado di inviare un pacchetto a un host remoto e di ricevere una risposta.

Se il test ha esito positivo, vengono visualizzate le seguenti informazioni:

- **Stato**: lo stato del test: Test in corso, Test riuscito, Test non riuscito.
- **Pacchetti**: il numero di pacchetti trasmessi, il numero di pacchetti ricevuti e la percentuale di pacchetti persi nel test Ping.
- **Tempo di andata e ritorno**: il tempi minimo, massimo e medio di andata e ritorno-per il test Ping.

Impostazioni predefinite

Per accedere a questa pagina, selezionare **Gestione del sistema > Impostazioni predefinite**.

Per riavviare il dispositivo e ripristinare tutti i parametri di fabbrica, fare clic su **Impostazioni predefinite**.

Per ripristinare sul dispositivo le impostazioni predefinite, inclusi i certificati predefiniti, fare clic su **Impostazioni predefinite di fabbrica inclusi i certificati**.

Aggiornamento firmware

Questa funzionalità scarica il firmware per il dispositivo da un PC o da un'unità flash USB e lo installa. Nella finestra viene visualizzata la **versione del firmware** attualmente in esecuzione sul dispositivo.

NOTA Se si seleziona una versione precedente del firmware, potrebbero essere ripristinati i valori predefiniti di fabbrica del dispositivo. Si raccomanda di utilizzare la procedura **Backup e ripristino** per eseguire il backup della configurazione prima di aggiornare il firmware.

L'aggiornamento del firmware potrebbe durare diversi minuti.

Durante questo processo, non scollegare l'alimentazione, non premere il pulsante di reimpostazione dell'hardware, non chiudere la finestra del browser e non effettuare la disconnessione.

Per accedere a questa pagina, selezionare **Gestione del sistema > Aggiornamento firmware**.

Per caricare il firmware da un PC, selezionare **Aggiornamento firmware da PC**, quindi selezionare il file.

Per caricare il firmware da un'unità flash USB, selezionare **Aggiornamento firmware da USB**, quindi selezionare il file.

Selezione lingua o Configurazione della lingua

Nella pagina Selezione lingua o Configurazione della lingua è possibile modificare la lingua associata all'interfaccia utente e alla Guida del dispositivo.

Per le versioni del firmware successive alla 1.0.2.03, la scelta della lingua avviene nella pagina Selezione lingua.

PASSAGGIO 1 Selezionare **Gestione sistema** > **Selezione lingua**.

PASSAGGIO 2 Scegliere una lingua dall'elenco a discesa **Seleziona lingua**.

PASSAGGIO 3 Fare clic su **Salva**.

In alternativa, è possibile scegliere la lingua nei seguenti modi:

- Nella pagina Accesso scegliere una lingua dall'elenco a discesa **Lingua**.
- In qualsiasi pagina di configurazione scegliere una lingua dall'elenco a discesa in alto a destra.

Per le versioni del firmware 1.0.2.03 o precedenti, scegliere una nuova lingua nella pagina Configurazione della lingua caricando un pacchetto lingua nel dispositivo.

Per accedere a questa pagina, selezionare **Gestione del sistema > Configurazione lingua**.

Per aggiungere un pacchetto lingua e scegliere una lingua:

PASSAGGIO 1 Selezionare **Gestione sistema** > **Configurazione della lingua**.

PASSAGGIO 2 Scegliere **Aggiungi** dall'elenco a discesa **Modalità**.

PASSAGGIO 3 Immettere un nome nel campo **Nuovo nome lingua**.

PASSAGGIO 4 Per caricare il file della nuova lingua, individuarlo da **Nome file della lingua**.

PASSAGGIO 5 Fare clic su **Salva**.

PASSAGGIO 6 Una volta caricato il pacchetto lingua, scegliere una lingua dall'elenco a discesa in alto a destra della pagina Configurazione della lingua o di qualsiasi pagina di configurazione.

Riavvio

Se si riavvia il dispositivo dalla pagina Riavvia, il router invia il file di log (se la registrazione è attivata) prima di reimpostare il dispositivo. I parametri del dispositivo vengono conservati.

Per accedere a questa pagina, selezionare **Gestione sistema > Riavvia** nel riquadro di spostamento.

Per riavviare il dispositivo, fare clic su **Riavvia router**.

Backup e ripristino

È possibile importare, esportare e copiare i file di configurazione. Il router dispone di due file di configurazione gestiti: un file di avvio e un file mirror. All'avvio, il dispositivo carica il file di avvio dalla memoria nella configurazione di esecuzione e lo copia nel file mirror. Quindi, il file mirror contiene l'ultima configurazione valida nota.

Se il file di configurazione di avvio è danneggiato o presenta qualsiasi tipo di errore, viene utilizzato il file di configurazione mirror. Il router copia automaticamente la configurazione di avvio nella configurazione mirror dopo 24 ore di esecuzione in condizioni stabili, ovvero nessun riavvio e nessuna modifica della configurazione nell'arco di 24 ore.

Ripristino delle impostazioni da un file di configurazione

Per ripristinare la configurazione di avvio da un file salvato in precedenza su un PC o un'unità flash USB, attenersi alla seguente procedura:

PASSAGGIO 1 Nella sezione Ripristina file di configurazione avvio, selezionare **Ripristina file di configurazione avvio da PC** e fare clic su **Sfoglia**. In alternativa, selezionare **Ripristina file di configurazione avvio da USB** e fare clic su **Aggiorna**.

PASSAGGIO 2 Selezionare un file di configurazione (.config).

PASSAGGIO 3 Fare clic su **Ripristina**. La procedura potrebbe richiedere fino a un minuto. Se il file di configurazione contiene una password diversa rispetto a quella corrente del dispositivo, verrà chiesto di immettere la password prima di procedere al ripristino del file di configurazione.

PASSAGGIO 4 Fare clic su **Gestione sistema > Riavvia** nel riquadro di spostamento.

Le impostazioni importate verranno applicate solo dopo il riavvio del dispositivo tramite **Gestione sistema > Riavvia**.

In alternativa, premere il pulsante **Reset** sul dispositivo per un secondo, quindi rilasciarlo per riavviare il router.

Backup dei file di configurazione e dei file mirror

Per salvare i file di configurazione di avvio e mirror sul computer o su un'unità flash USB, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **File di configurazione backup su PC** oppure **File di configurazione backup su USB.**

PASSAGGIO 2 Fare clic su **Backup configurazione avvio** o **Backup configurazione mirror.** Viene visualizzata la finestra Download file.

PASSAGGIO 3 Fare clic su **Salva** e scegliere il percorso del file. In alternativa, immettere il nome di un file e fare clic su **Salva**.

SUGGERIMENTO I nomi file predefiniti sono *Startup.config* e *Mirror.config*. L'estensione *.config* è obbligatoria. Per una più semplice identificazione, può essere utile immettere un nome file che includa la data e l'ora attuali.

Copia del file mirror nel file di avvio

È possibile copiare manualmente il file di configurazione di avvio del dispositivo nel file di configurazione mirror.

È possibile utilizzare questa procedura per eseguire il backup di una configurazione valida prima di apportare modifiche alla configurazione di avvio:

- Il file di configurazione di avvio viene copiato automaticamente nel file di configurazione mirror ogni 24 ore.
- Quando si salvano le modifiche ai parametri del dispositivo, il contatore viene reimpostato e la successiva copia automatica avviene 24 ore dopo, a meno che il file di avvio non venga salvato manualmente come file mirror.

Per copiare il file di avvio nel file mirror, fare clic su **Copia mirror su avvio**. L'operazione di copia viene effettuata immediatamente e non è possibile annullarla. Al termine dell'operazione la pagina viene aggiornata.

Disinfezione della configurazione

Se si esegue la disinfezione della configurazione, il file mirror e il file per la configurazione di avvio vengono eliminati.

Per eliminare il file mirror e il file per la configurazione di avvio, fare clic su **Disinfetta configurazione**.

ATTENZIONE La configurazione mirror viene eliminata immediatamente e non è possibile annullare l'operazione. Sul dispositivo vengono ripristinate le impostazioni predefinite e viene eseguito il riavvio.

Backup del firmware su un'unità flash USB

Per eseguire il backup del firmware su un'unità flash sulla porta USB, selezionare la porta dal menu a discesa e fare clic su **Backup**. L'immagine firmware viene salvata dal dispositivo come **`image.bin`**.

7

Gestione porte

Uilizzare Gestione porte per consentire il mirroring delle porte, configurare le impostazioni della porta e visualizzare lo stato e le statistiche di traffico della porta. Inoltre, è possibile configurare la VLAN, 802.1x, associare la pagina DSCP a una coda e associare le impostazioni a DSCP.

Configurazione delle porte

È possibile attivare o disattivare il mirroring delle porte, gestire le impostazioni della porta LAN/WLAN, inclusa la disattivazione amministrativa della porta e attivare o disattivare la modalità EEE, priorità porta e negoziazione della porta.

Il mirroring delle porte è un metodo di monitoraggio del traffico di rete. Quando è attivato il mirroring delle porte, il router invia una copia di tutti i pacchetti di rete, che sono visibili su una o più porte, a un'altra porta dedicata, dove i pacchetti possono essere analizzati.

Per attivare il mirroring delle porte, selezionare **Gestione porte > Configurazione porte** e selezionare **Mirror All WAN e LAN Traffic alla porta 1**. I pacchetti in arrivo e in uscita sulle porte WAN e LAN vengono copiati sulla LAN1.

NOTA Quando la copia dell'indirizzo MAC è attiva, il mirroring delle porte non acquisirà il traffico WAN.

Per ogni porta vengono visualizzate le seguenti informazioni di sola lettura:

- **ID porta**: il numero o il nome della porta, come indicato sul dispositivo.
- **Interfaccia**: il tipo di interfaccia: LAN, WAN o DMZ.

Configurare le seguenti impostazioni:

- **Disattiva**: selezionare questa casella per disattivare una porta. Tutte le porte sono attive per impostazione predefinita.
- **EEE**: selezionare questa casella di controllo per abilitare la modalità Energy Efficient Ethernet che riduce il consumo energetico nei periodi con attvità dati ridotta.
- **Priorità**: selezionare il livello di priorità appropriato per ogni porta: **Alta** o **Normale**. In questo modo è possibile dare priorità al traffico dei dispositivi su determinate porte, garantendo così la qualità del servizio (QoS, Quality of Service). Ad esempio, è possibile assegnare una priorità alta a una porta utilizzata per giochi o videoconferenze. L'impostazione predefinita è Normale.
- **Modalità**: velocità della porta e modalità duplex. Se è attiva la **negoziazione automatica**, il dispositivo esegue automaticamente la negoziazione delle velocità di connessione e della modalità duplex con il dispositivo connesso.

Stato delle porte

Nella pagina Stato delle porte viene visualizzato un riepilogo dello stato delle porte. Fare clic su **Aggiorna** per aggiornare i dati.

Per accedere alla pagina Stato delle porte, fare clic su **Gestione porte > Stato delle porte** nel riquadro di spostamento.

Nella tabella Ethernet vengono visualizzate le informazioni seguenti:

- **ID porta**: la posizione della porta.
- **Tipo**: il tipo di porta.
- **Stato collegamento**: lo stato della connessione.
- **Attività porta**: lo stato della porta.
- **Priorità**: la priorità della porta impostata nella finestra Impostazione porte.
- **Stato velocità**: la velocità della porta: 10 Mbps, 100 Mbps o 1000 Mbps.

- **Stato duplex**: la modalità duplex: *Half* o *Full*.
- **Negoziazione automatica**: lo stato della modalità duplex.

Statistiche traffico

Per accedere alle statistiche relative al traffico, fare clic su **Gestione porte > Statistiche traffico** nel riquadro di spostamento.

Nella tabella delle statistiche vengono visualizzate le informazioni seguenti per la porta selezionata:

- **ID porta**: la posizione della porta.
- **Stato collegamento**: lo stato della connessione.
- **Pacchetti Rx**: il numero di pacchetti ricevuti sulla porta.
- **Pacchetti Rx**: il numero di pacchetti ricevuti, misurato in byte.
- **Pacchetti Tx**: il numero di pacchetti inviati sulla porta.
- **Pacchetti Tx**: il numero di pacchetti inviati, misurato in byte.
- **Pacchetti con errori**: il numero di pacchetti con errori.

Appartenenza VLAN

Tutte le porte LAN si trovano sulla VLAN1 per impostazione predefinita.

Per accedere alla pagina Appartenenza VLAN, fare clic su **Gestione porte > Appartenenza VLAN** nel riquadro di spostamento.

Per attivare le VLAN, selezionare **Attiva VLAN**.

Per aggiungere o modificare una VLAN, attenersi alla seguente procedura:

- **ID VLAN**: l'identificatore della VLAN.
- **Descrizione**: la descrizione della VLAN.

- **Routing inter-VLAN**: consente la trasmissione di pacchetti fra le VLAN. Una VLAN con routing inter-VLAN disattivato è isolata dalle altre VLAN. È possibile configurare regole di accesso al firewall per regolare ulteriormente (consentire o negare) il traffico inter-VLAN.
- **Per RV320**, da **LAN 1** a **LAN 4**: è possibile taggare o annullare il tag di una porta oppure escludere una porta dalla VLAN.
- **Per RV325**, da **LAN 1** a **LAN 14**: è possibile taggare o annullare il tag di una porta oppure escludere una porta dalla VLAN.

Impostazioni QoS: CoS/DSCP

Questa opzione consente di raggruppare il traffico per classi di servizio (CoS, Class of Service), garantendo la larghezza di banda necessaria e una priorità più alta per i dispositivi specificati. Tutto il traffico non incluso nel gruppo IP utilizza la modalità Intelligent Balancer.

Per accedere a questa pagina, fare clic su **Gestione porte > QoS: impostazione di CoS/DSCP** nel riquadro di spostamento.

Per configurare la coda dei servizi, selezionare la priorità **Coda** (4 è la priorità più alta e 1 è la priorità più bassa) dall'elenco a discesa.

Per impostare DSCP (Differential Services Code Point), selezionare **Coda** dagli elenchi a discesa.

Contrassegno DSCP

Differential Services Code Point o DiffServ specifica un metodo scalabile e semplice per la classificazione e la gestione del traffico di rete e garantisce la qualità del servizio (QoS). È possibile utilizzare DiffServ per fornire bassa latenza a traffico di rete importante, ad esempio dati voce o streaming multimediale, fornendo allo stesso tempo un servizio best-effort a servizi meno importanti, ad esempio traffico Web o trasferimenti di file.

Per accedere a questa pagina, fare clic su **Gestione porte > Contrassegno DSCP** nel riquadro di spostamento.

Per configurare la coda dei servizi, fare clic su **Aggiungi** o e impostare i valori Cos/802.1p, l'azione e la priorità.

Configurazione 802.1x

Il controllo dell'accesso di rete basato sulle porte utilizza le caratteristiche dell'accesso fisico delle infrastrutture LAN IEEE 802 per offrire un metodo di autenticazione e autorizzazione dei dispositivi collegati a una porta LAN con caratteristiche di connessione point-to-point e impedire l'accesso a tale porta in caso di autenticazione e autorizzazione fallite. In questo contesto, una porta rappresenta un singolo punto di collegamento all'infrastruttura LAN.

Per visualizzare questa pagina, selezionare **Gestione porte > Configurazione 802.1X.** Per configurare l'autenticazione basata sulle porte, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare **Autenticazione basata su porte** per attivare la funzione.

PASSAGGIO 2 Immettere l'indirizzo IP del server RADIUS.

PASSAGGIO 3 Immettere un numero nel campo **Porta UDP RADIUS**.

PASSAGGIO 4 Compilare il campo **Segreto RADIUS**.

PASSAGGIO 5 Selezionare uno stato dall'elenco a discesa **Stato amministrazione** della tabella delle porte:

- **Imposizione autorizzata:** è lo stato predefinito della porta LAN. Autorizza l'interfaccia senza autorizzazione.
- **Imposizione non autorizzata:** nega l'accesso all'interfaccia modificando l'interfaccia nello stato non autorizzato. Il dispositivo non fornisce i servizi di autenticazione al client attraverso l'interfaccia.

  NOTA L'accesso alla rete comprensivo della utility di gestione del router verrà bloccato dalla LAN quando tutte le porte LAN saranno configurate con Imposizione non autorizzata. Verrà richiesta la reimpostazione a predefinito se l'accesso remoto non è attivato.
- **Auto**: imposta l'autenticazione basata sulle porte. L'interfaccia passa dallo stato autorizzato allo stato non autorizzato (e viceversa) in base allo scambio di autenticazione tra il dispositivo e il client.

PASSAGGIO 6 Fare clic su **Salva**.

8

Firewall

L'obiettivo principale di un firewall è di controllare il traffico di rete in entrata e in uscita e stabilire se i pacchetti di dati, analizzati in base a un determinato set di regole, possono essere trasmessi o meno. Un firewall di rete funge da ponte fra una rete interna, ritenuta sicura e attendibile, e un'altra rete, in genere una rete esterna come Internet, ritenuta non sicura e non attendibile.

Impostazioni generali

I controlli generali del firewall consentono di gestire le funzionalità tipiche utilizzate dalle applicazioni e dai browser Internet.

Per accedere alle impostazioni generali, selezionare **Firewall > Generale** nel riquadro di spostamento.

Abilitazione delle funzionalità del firewall

Per attivare la funzione **Firewall**, selezionare la casella **Attiva**. È possibile attivare o disattivare le seguenti funzionalità del firewall, come necessario:

- **SPI (Stateful Packet Inspection)**: monitora lo stato delle connessioni di rete, come flussi TCP e comunicazioni UDP. Il firewall riconosce pacchetti accettabili per diversi tipi di connessioni. Vengono accettati soltanto i pacchetti che corrispondono a una connessione attiva nota; gli altri vengono rifiutati.
- **DoS (Denial-of-service)**: rileva tentativi che causano un sovraccarico del server. In termini generali, un attacco DoS causa il reset dei computer colpiti oppure consuma le risorse di tali computer impedendo l'erogazione dei servizi o bloccando i supporti di comunicazione fra gli utenti autorizzati e la vittima, danneggiando così lo scambio di dati.
- **Blocco richiesta WAN**: elimina le richieste TCP e i pacchetti ICMP.

- **Gestione remota**: consente la gestione remota del dispositivo, se abilitata. La porta predefinita è 443, ma è possibile selezionarne una diversa. La stringa è nel formato seguente: https://<ip-wan>:<porta-gestione-remota>.
- **Multicast Pass Through**: consente la trasmissione di messaggi multicast attraverso il dispositivo.
- **HTTPS**: Hypertext Transfer Protocol Secure è un protocollo utilizzato per garantire comunicazioni sicure su una rete di computer; questo protocollo viene implementato, in particolare, su Internet.
- **SIP ALG**: gateway del livello applicativo utilizzato come complemento di un firewall o NAT. Consente di associare filtri trasversali NAT personalizzati al gateway per supportare la conversione di indirizzi e porte per i protocolli di *controllo/dati* SIP.
- **UPnP**: Universal Plug and Play è un insieme di protocolli di rete che consentono a dispositivi di rete, come computer, stampanti, gateway Internet, access point Wi-Fi e dispositivi mobili, di rilevare senza problemi la presenza di altri dispositivi sulla rete e stabilire servizi di rete funzionali per la condivisione dei dati e le comunicazioni.
- SSH: SSH (Secure Shell) è un protocollo di rete che fornisce agli amministratori un modo sicuro per accedere a un computer remoto. SSH è ampiamente utilizzato dagli amministratori di rete per la gestione remota di sistemi e applicazioni, consentendo loro di accedere a un altro computer su una rete, eseguire comandi e spostare file da un computer all'altro.
- SSH remoto: Secure Shell remoto è un metodo per eseguire l'accesso remoto sicuro da un computer a un altro. Fornisce diverse opzioni alternative per l'autenticazione a due fattori e consente di proteggere la sicurezza e l'integrità delle comunicazioni con crittografia forte.

Impostazione di limiti per le funzionalità Web

Per applicare restrizioni a funzionalità Web, come **Java**, **cookie**, **ActiveX** o l'**accesso a server proxy HTTP**, selezionare la casella appropriata.

Per consentire *solo* le funzionalità selezionate (Java, cookie, ActiveX o l'accesso a server proxy HTTP) e applicare restrizioni a tutte le altre, selezionare **Eccezione**.

Configurazione di nomi di dominio attendibili

Per aggiungere un dominio attendibile, fare clic su **Aggiungi**, quindi immettere un nome nel campo **Nome dominio**.

Per modificare un dominio attendibile, fare clic su **Modifica**, quindi cambiare il nome nel campo **Nome dominio**.

Regole di accesso

Le regole di accesso consentono o impediscono a determinati servizi o dispositivi identificati mediante il loro indirizzo IP di accedere alla sottorete.

Per accedere alle regole di accesso, selezionare **Firewall > Regole di accesso** nel riquadro di spostamento.

Per aggiungere o modificare un servizio, fare clic su **Gestione servizio**. Per la descrizione di questa funzionalità, vedere la sezione **Aggiunta o modifica del nome di un servizio**.

Aggiunta di una regola di accesso alla tabella delle regole IPv4

Per aggiungere o modificare una regola di accesso IPv4, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic sulla scheda IPv4.

PASSAGGIO 2 Fare clic su Aggiungi (o selezionare la riga e fare clic su Modifica).

PASSAGGIO 3 Selezionare l'azione, Consenti o Nega, per questa regola dal menu a discesa.

PASSAGGIO 4 Selezionare un Servizio dal menu a discesa.

PASSAGGIO 5 Selezionare Registra pacchetti che corrispondono alla regola o Non registrare.

PASSAGGIO 6 Selezionare un'interfaccia di origine dal menu a discesa.

PASSAGGIO 7 Selezionare l'indirizzo IP di origine dal menu a discesa. Se si seleziona l'opzione Indirizzo singolo, immettere l'indirizzo IP di origine. Se si seleziona l'opzione Intervallo di indirizzi, immettere l'intervallo di indirizzi IP di origine.

PASSAGGIO 8 Selezionare un'opzione dall'elenco a discesa **IP di destinazione**. Se si seleziona l'opzione **Indirizzo singolo**, immettere l'indirizzo IP di destinazione. Se si seleziona l'opzione **Intervallo di indirizzi**, immettere l'intervallo di indirizzi IP di destinazione.

PASSAGGIO 9 Selezionare un orario per configurare la programmazione della regola di accesso. Selezionare **Sempre** per lasciare la regola sempre attiva. Selezionare **Intervallo** per impostare un orario, quindi immettere l'orario (ora e minuti) in cui la regola è attiva nei campi **Da** e **A**. Ad esempio, immettere dalle *07:00* alle *20:00*. La regola di accesso non consente di impostare due intervalli temporali.

PASSAGGIO 10 Selezionare i giorni della settimana desiderati nella casella **Attiva**.

PASSAGGIO 11 Fare clic su **Salva**.

Aggiunta di una regola di accesso alla tabella delle regole IPv6

Per aggiungere o modificare una regola di accesso IPv6, attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare la scheda **IPv6**.

PASSAGGIO 2 Fare clic su **Aggiungi** oppure selezionare la riga desiderata e fare clic su **Modifica**.

PASSAGGIO 3 Dall'elenco a discesa, selezionare l'azione da associare alla regola: **Consenti** o **Nega**.

PASSAGGIO 4 Selezionare un'opzione dall'elenco a discesa **Servizio**.

PASSAGGIO 5 Selezionare un'opzione dall'elenco a discesa **Log**.

PASSAGGIO 6 Selezionare un'opzione dall'elenco a discesa **Interfaccia di origine**.

PASSAGGIO 7 Selezionare un'opzione dall'elenco a discesa **Lunghezza prefisso IP di origine**. Se si seleziona l'opzione **Singolo**, immettere il prefisso IP di origine. Se si seleziona l'opzione **Intervallo**, immettere il prefisso IP iniziale e la lunghezza del prefisso.

PASSAGGIO 8 Selezionare un'opzione dall'elenco a discesa **Lunghezza prefisso di destinazione**. Se si seleziona l'opzione **Singolo**, immettere il prefisso IP di destinazione. Se si seleziona l'opzione **Intervallo**, immettere il prefisso IP iniziale e la lunghezza del prefisso.

PASSAGGIO 9 Fare clic su **Salva**.

Filtro dei contenuti

Il Filtro contenuti consente di limitare l'accesso a determinati siti Web non desiderati. L'accesso ai siti Web può essere bloccato in base ai nomi dominio e alle parole chiave. È anche possibile pianificare quando il filtro contenuti è attivo. Per configurare e attivare il Filtro contenuti, seguire questi passaggi.

PASSAGGIO 1 Fare clic su Firewall > Filtro contenuti.

PASSAGGIO 2 Selezionare Block Forbidden Domains (Blocca domini vietati) per bloccare determinate pagine Web o selezionare Accept Allowed Domains (Accetta domini consentiti) per accettare determinate pagine Web.

PASSAGGIO 3 Nella sezione Domini vietati, selezionare Attiva per attivare i domini vietati.

PASSAGGIO 4 Nella Tabella domini vietati, fare clic su Aggiungi per aggiungere il nome dominio e inserire il nome del dominio. Fare clic su Modifica o Elimina per modificare un dominio esistente nella Tabella domini vietati.

PASSAGGIO 5 Nella sezione Blocco sito Web mediante parole chiave, selezionare Attiva per attivare il blocco del sito Web.

PASSAGGIO 6 Nella tabella Blocco del sito Web mediante parole chiave, fare clic su Aggiungi e inserire le parole chiave da bloccare.

PASSAGGIO 7 Per specificare quando le regole di filtro contenuti sono attive, configurare la pianificazione selezionando l'ora dall'elenco a discesa. È possibile personalizzare i campi Da e A nonché selezionare il giorno il cui il filtro contenuti diventa effettivo.

PASSAGGIO 8 Fare clic su Salva per salvare le impostazioni.

9

VPN

Una rete VPN è una connessione tra due endpoint di reti diverse che consente di trasmettere in modo sicuro dati riservati tramite una rete pubblica o condivisa, ad esempio Internet. Questo tunnel stabilisce una rete privata che può inviare dati in modo sicuro utilizzando tecniche di crittografia e autenticazione standard del settore per proteggere i dati inviati.

Riepilogo

In questa pagina vengono visualizzate informazioni generali sulle impostazioni del tunnel VPN. Il dispositivo supporta fino a 100 tunnel. L'intervallo di indirizzi IP virtuali è riservato agli utenti di EasyVPN o ai client VPN che si connettono al dispositivo con l'opzione Configurazione modalità, descritta nella sezione **Impostazioni avanzate per IKE**, attivata.

Per accedere a questa pagina, selezionare **VPN > Riepilogo** nel riquadro di spostamento.

Per impostare un intervallo di indirizzi IP da utilizzare per i tunnel VPN, fare clic su **Modifica** e immettere i seguenti parametri:

- **Inizio intervallo** e **Fine intervallo**: l'indirizzo IP iniziale e quello finale utilizzati per i tunnel VPN.
- **Server DNS 1** e **Server DNS 2**: indirizzo IP facoltativo di un server DNS. Se si immette un secondo server DNS, il dispositivo utilizza il primo server DNS per rispondere. Se si specifica un server DNS è possibile accedere più rapidamente rispetto all'utilizzo di un server DNS assegnato dinamicamente. L'impostazione predefinita 0.0.0.0 consente di utilizzare un server DNS con assegnazione dinamica.
- **Server WINS 1** e **Server WINS 2**: indirizzo IP facoltativo di un server WINS. Windows Internet Naming Service traduce i nomi NetBIOS in indirizzi IP. Se non si conosce l'indirizzo IP del server WINS, utilizzare l'impostazione predefinita 0.0.0.0.

- Da **Nome dominio 1** a **4**: se il router ha un indirizzo IP statico e un nome di dominio registrato, ad esempio*MioServer.MioDominio.com*, immettere il **nome di dominio** da utilizzare per l'autenticazione. Un nome di dominio può essere utilizzato per una sola connessione tunnel.

In **Stato del tunnel VPN** viene mostrato il numero di **tunnel utilizzati**, **tunnel disponibili**, **tunnel attivati** e **tunnel definiti**.

Tabella delle connessioni

Nella tabella di connessione vengono mostrate le voci create in **VPN** > **Da gateway a gateway** e **VPN** > **Da client a gateway**:

- (Tunnel) **N.**: numero ID del tunnel generato automaticamente.
- (Tunnel) **Nome**: il nome del tunnel VPN, ad esempio Ufficio Los Angeles, Filiale Chicago o Divisione New York. Questa descrizione viene utilizzata come riferimento e non deve necessariamente corrispondere al nome utilizzato all'altra estremità del tunnel.
- **Stato**: lo stato del tunnel VPN: *Connesso* o *In attesa della connessione*.
- **Cri/Aut/Grp Fase2**: tipo di crittografia fase 2 (NULL/DES/3DES/AES-128/AES-192/AES-256), metodo di autenticazione (NULL/MD5/SHA1) e numero gruppo DH (1/2/5).
- **Gruppo locale**: l'indirizzo IP e la subnet mask del gruppo locale.
- **Gruppo remoto**: l'indirizzo IP e la subnet mask del gruppo remoto.
- **Gateway remoto**: l'indirizzo IP del gateway remoto.
- **Test tunnel**: stato del tunnel VPN.

Stato tunnel FlexVPN

Nella Tabella di connessione vengono mostrate le voci create in VPN >FlexVPN (Spoke). Per aggiungere un nuovo tunnel, fare clic su Aggiungi.

- Tunnel Name (Nome tunnel): nome del tunnel FlexVPN. Questa descrizione viene utilizzata come riferimento e non deve necessariamente corrispondere al nome utilizzato all'altra estremità del tunnel.
- Stato: lo stato del FlexVPN, che può essere Connesso o In attesa di connessione.
- Rete Spoke: la sottorete di Spoke.
- Indirizzo IP virtuale Spoke: l'indirizzo IP virtuale di Spoke.

- Indirizzo IP hub: l'indirizzo IP di Hub.
- Azione: Connetti o Disconnetti il tunnel

Tabella di connessione relativa allo stato VPN del gruppo

Nella tabella di connessione vengono mostrate le voci create in **VPN** > **Da client a gateway**:

- **Nome gruppo**: il nome del tunnel VPN. Questa descrizione viene utilizzata come riferimento e non deve necessariamente corrispondere al nome utilizzato all'altra estremità del tunnel.
- **Tunnel**: il numero di utenti che hanno effettuato l'accesso alla VPN di gruppo.
- **Cri/Aut/Grp Fase2**: tipo di crittografia fase 2 (NULL/DES/3DES/AES-128/AES-192/AES-256), metodo di autenticazione (NULL/MD5/SHA1) e numero gruppo DH (1/2/5).
- **Gruppo locale**: l'indirizzo IP e la subnet mask del gruppo locale.
- **Client remoto**: l'indirizzo IP e la subnet mask del client remoto.
- **Dettagli**: l'indirizzo IP del gateway remoto.
- **Test tunnel**: stato del tunnel VPN.

Da gateway a gateway

In una VPN da sito a sito o da gateway a gateway, il router locale di un ufficio si connette a un router remoto attraverso un tunnel VPN. I dispositivi client possono accedere alle risorse di rete come se si trovassero tutte presso la stessa sede. Questo modello può essere utilizzato per più utenti presso un ufficio remoto.

Per accedere a questa pagina, selezionare **VPN > Da gateway a gateway** nel riquadro di spostamento.

Per una corretta connessione, è necessario che almeno uno dei router sia identificato da un indirizzo IP statico o da un nome host DNS dinamico. In alternativa, se un router dispone soltanto di un indirizzo IP dinamico, è possibile utilizzare qualsiasi indirizzo e-mail come autenticazione per stabilire la connessione.

Le due estremità del tunnel non possono essere sulla stessa sottorete. Ad esempio, se la LAN del Sito A utilizza la sottorete 192.168.1.x/24, il Sito B può utilizzare 192.168.2.x/24.

Per configurare un tunnel, immettere le impostazioni corrispondenti nella configurazione dei due router, invertendo *locale* e *remoto*. Supponendo che questo router sia identificato come Router A, immettere le relative impostazioni nella sezione *Configurazione gruppo locale*; immettere, invece, le impostazioni dell'altro router (Router B) nella sezione *Configurazione gruppo remoto*. Quando si configura l'altro router (Router B), immettere le relative impostazioni nella sezione *Configurazione gruppo locale* e le impostazioni del Router A nella sezione *Configurazione gruppo remoto*.

Aggiunta di un nuovo tunnel

Immettere le impostazioni relative a un tunnel:

- **Tunnel n.**: il numero ID del tunnel.
- **Nome tunnel**: il nome del tunnel VPN, ad esempio Ufficio Los Angeles, Filiale Chicago o Divisione New York. Questa descrizione viene utilizzata come riferimento. Non deve necessariamente corrispondere al nome utilizzato all'altra estremità del tunnel.
- **Interfaccia**: la porta WAN da utilizzare per il tunnel.
- **Modalità chiavi**: identifica la sicurezza del tunnel: Manuale, IKE con chiave precondivisa, IKE con certificato.
- **Attiva**: selezionare questa casella per attivare il tunnel VPN o deselezionarla per disattivare il tunnel. Il tunnel è attivato per impostazione predefinita.

Configurazione gruppo locale

Immettere le impostazioni relative alla configurazione del gruppo locale per il router. Riportare le stesse impostazioni quando si configura il tunnel VPN sull'altro router.

NOTA Tutte le opzioni sono documentate, ma vengono visualizzate soltanto quelle relative al parametro selezionato.

Modalità chiavi = Manuale o IKE con chiave precondivisa

- **Tipo gateway di sicurezza locale**: metodo per identificare il router per stabilire il tunnel VPN. Il gateway di sicurezza locale è su questo router; il gateway di sicurezza remota è sull'altro router. Per effettuare la connessione è necessario che almeno uno dei router abbia un indirizzo IP statico o un nome host DNS.
  - **Indirizzo IP**: il router ha un indirizzo IP WAN statico. L'indirizzo IP WAN viene visualizzato automaticamente.
  - **IP + Certificato**: il router ha un indirizzo IP WAN statico che viene visualizzato automaticamente. Questa opzione è disponibile soltanto se si seleziona l'opzione IKE con certificato.
  - **IP + Autenticazione nome di dominio (FQDN)**: il dispositivo ha un indirizzo IP statico e un nome di dominio registrato, ad esempio *MioServer.MioDominio.com*. Immettere anche il **nome di dominio** da utilizzare per l'autenticazione. Il nome di dominio può essere utilizzato per una sola connessione tunnel.
  - **IP + Autenticazione indirizzo e-mail (FQDN UTENTE)**: il dispositivo ha un indirizzo IP statico e utilizza un indirizzo e-mail per l'autenticazione. L'indirizzo IP WAN viene visualizzato automaticamente. Immettere l'**indirizzo e-mail** da utilizzare per l'autenticazione.
  - **IP dinamico + Autenticazione nome di dominio (FQDN)**: il router ha un indirizzo IP dinamico e un nome host DNS dinamico registrato (disponibile presso dei provider, come ad esempio DynDNS.com). Immettere un **nome di dominio** da utilizzare per l'autenticazione. Il nome di dominio può essere utilizzato per una sola connessione tunnel.
  - **IP dinamico + Autenticazione indirizzo e-mail (FQDN UTENTE)**: il router ha un indirizzo IP dinamico e non dispone di nome host DNS dinamico. Immettere un **indirizzo e-mail** da utilizzare per l'autenticazione.

    Se entrambi i router hanno indirizzi IP dinamici (come con le connessioni PPPoE), non selezionare **IP dinamico + Indirizzo e-mail** per entrambi i gateway. Per il gateway remoto, selezionare **Indirizzo IP** e **Indirizzo IP per DNS risolto**.
- **Tipo gruppo di sicurezza locale**: consente di selezionare un singolo indirizzo **IP**, una **sottorete** o un **intervallo** (di indirizzi) **IP** in una sottorete.
  - **Indirizzo IP**: specificare un dispositivo che può utilizzare questo tunnel. Immettere l'indirizzo IP del dispositivo nel rispettivo campo.

- **Sottorete**: consente a tutti i dispositivi di una sottorete di utilizzare il tunnel VPN. Immettere l'indirizzo IP e la subnet mask della sottorete nei rispettivi campi.

Configurazione gruppo remoto

Immettere le impostazioni per la configurazione del gruppo remoto per il router:

- **Tipo gateway di sicurezza remoto**: metodo per l'identificazione del router per stabilire il tunnel VPN. Il gateway di sicurezza remoto è l'altro router. Per effettuare la connessione è necessario che almeno uno dei router abbia un indirizzo IP statico o un nome host DNS dinamico.
  - **Solo IP**: l'indirizzo IP WAN statico. Se si conosce l'indirizzo IP del router VPN remoto, selezionare **Indirizzo IP** e immettere l'indirizzo. Se non si conosce l'indirizzo IP del router VPN remoto, selezionare **IP per DNS risolto** e immettere il nome di dominio del router. Un router Cisco può ottenere l'indirizzo IP di un dispositivo VPN remoto per DNS risolto.
  - **IP + Autenticazione nome di dominio (FQDN)**: il router ha un indirizzo IP statico e un nome di dominio registrato, ad esempio *MioServer.MioDominio.com*. Se si conosce l'indirizzo IP del router VPN remoto, selezionare **Indirizzo IP** e immettere l'indirizzo. Se non si conosce l'indirizzo IP del router VPN remoto, selezionare **IP per DNS risolto** e immettere il nome di dominio del router. I router Cisco possono ottenere l'indirizzo IP di un dispositivo VPN remoto per DNS risolto.
  - **IP + Autenticazione indirizzo e-mail (FQDN UTENTE)**: il router ha un indirizzo IP statico e si desidera utilizzare un indirizzo e-mail per l'autenticazione. Se si conosce l'indirizzo IP del router VPN remoto, selezionare **Indirizzo IP** e immettere l'indirizzo IP. Se non si conosce l'indirizzo IP del router VPN remoto, selezionare **IP per DNS risolto** e immettere il nome di dominio reale del router. I router Cisco possono ottenere l'indirizzo IP di un dispositivo VPN remoto per DNS risolto.
  - **IP dinamico + Autenticazione nome di dominio (FQDN)**: il router ha un indirizzo IP dinamico e un nome host DNS dinamico registrato (disponibile presso dei provider, come ad esempio DynDNS.com). Immettere un **nome di dominio** da utilizzare per l'autenticazione. Il nome di dominio può essere utilizzato per una sola connessione tunnel.
  - **IP dinamico + Autenticazione indirizzo e-mail (FQDN UTENTE)**: il router ha un indirizzo IP dinamico e non dispone di nome host DNS dinamico. Immettere un **indirizzo e-mail** da utilizzare per l'autenticazione.
    Se entrambi i router hanno indirizzi IP dinamici (come con le connessioni

PPPoE), *non* selezionare **IP dinamico + Indirizzo e-mail** per entrambi i gateway. Per il gateway remoto, selezionare **Indirizzo IP** o **Indirizzo IP per DNS risolto**.

- **Tipo gruppo di sicurezza locale**: risorse LAN che possono utilizzare questo tunnel. Il gruppo di sicurezza locale è per le risorse LAN del router; il gruppo di sicurezza remoto è per le risorse LAN dell'altro router.
  - **Indirizzo IP**: specificare un dispositivo che può utilizzare questo tunnel. Immettere l'indirizzo IP del dispositivo nel rispettivo campo.
  - **Sottorete**: consente a tutti i dispositivi di una sottorete di utilizzare il tunnel VPN. Immettere l'indirizzo IP e la subnet mask della sottorete nei rispettivi campi.

Configurazione IPSec

Per una corretta crittografia, le due estremità di un tunnel VPN devono utilizzare gli stessi metodi di crittografia, decrittografia e autenticazione. Immettere esattamente le stesse impostazioni su entrambi i router.

Immettere le impostazioni per Fase 1 e Fase 2. La Fase 1 stabilisce le chiavi precondivise per creare un canale di comunicazione autenticato protetto. Nella Fase 2, i peer IKE utilizzano il canale sicuro per negoziare associazioni di sicurezza per conto di altri servizi, ad esempio IPsec. Accertarsi di immettere le stesse impostazioni quando si configura l'altro router per questo tunnel.

- **Gruppo DH fase 1/fase 2**: DH (Diffie-Hellman) è un protocollo di scambio delle chiavi. Sono disponibili tre gruppi di diverse lunghezze della chiave primaria: Gruppo 1 - 768 bit, Gruppo 2 - 1.024 bit e Gruppo 5 - 1.536 bit. Per una maggiore velocità e una minore sicurezza, selezionare **Gruppo 1**. Per una minore velocità e una maggiore sicurezza, selezionare **Gruppo 5**. Il Gruppo 1 è selezionato per impostazione predefinita.
- **Crittografia fase 1/fase 2**: il metodo di crittografia per questa fase: DES, 3DES, AES-128, AES-192 o AES-256. Il metodo di crittografia determina la lunghezza della chiave utilizzata per crittografare o decodificare i pacchetti ESP. AES-256 è l'opzione consigliata perché è più sicura.
- **Autenticazione fase 1/fase 2**: il metodo di autenticazione per questa fase: MD5 o SHA1. Il metodo di autenticazione determina la modalità di convalida dei pacchetti con intestazione ESP (Encapsulating Security Payload Protocol). MD5 è un algoritmo di hashing unidirezionale che produce digest a 128 bit. SHA1 è un algoritmo di hashing unidirezionale che produce digest a 160 bit. SHA1 è l'opzione consigliata perché è più sicura. Accertarsi che entrambe le estremità del tunnel VPN utilizzino lo stesso metodo di autenticazione.

- **Durata SA fase 1/fase 2**: periodo di attività di un tunnel VPN in questa fase. Il valore predefinito per la fase 1 è 28800 secondi. Il valore predefinito per la fase 2 è 3.600 secondi.
- **Perfect Forward Secrecy**: se l'opzione Perfect Forward Secrecy (PFS) è attivata, la negoziazione di fase 2 IKE genera nuovo materiale delle chiavi per la crittografia e l'autenticazione del traffico IP, quindi i pirati informatici che utilizzano la forza bruta per intercettare le chiavi di crittografia non potranno ottenere le chiavi IPsec future. Selezionare questa casella per attivare la funzionalità oppure deselezionarla per disattivarla. Si consiglia di attivare questa funzionalità.
- **Chiave precondivisa**: la chiave precondivisa da utilizzare per l'autenticazione del peer IKE remoto. È possibile immettere fino a 30 caratteri della tastiera o valori esadecimali, ad esempio Mio_@123 o 4d795f40313233 (i caratteri ' ' " \ non sono supportati). Entrambe le estremità del tunnel VPN devono utilizzare la stessa chiave precondivisa. Si raccomanda vivamente di cambiare periodicamente la chiave precondivisa per massimizzare la sicurezza VPN.
- **Complessità chiave precondivisa minima**: selezionare la casella **Attiva** per attivare il misuratore della complessità della chiave precondivisa.
- **Misuratore complessità chiave precondivisa**: se si attiva l'opzione Complessità chiave precondivisa minima, il valore di questo campo indica la complessità della chiave precondivisa. Durante la digitazione di una chiave precondivisa, vengono visualizzate delle barre colorate. Le opzioni sono rosso (debole), giallo (accettabile) e verde (complessa).

SUGGERIMENTO Immettere una chiave precondivisa complessa che includa più di otto caratteri, lettere maiuscole e minuscole, numeri e simboli, come -*^+=.

Impostazioni avanzate per IKE con chiave precondivisa e IKE con certificato

Per la maggior parte degli utenti saranno sufficienti le impostazioni di base; gli utenti avanzati possono fare clic su **Impostazioni avanzate** per visualizzare le impostazioni avanzate. Eventuali modifiche alle impostazioni avanzate su un router, devono essere riportate anche sull'altro router.

- **Modalità aggressiva**: sono possibili due modalità di negoziazione SA IKE: Modalità principale e Modalità aggressiva. Se si preferisce la sicurezza di rete, si consiglia la Modalità principale. Se, invece, si preferisce la velocità di rete, si consiglia la Modalità aggressiva. Selezionare questa casella per attivare la Modalità aggressiva oppure deselezionarla per utilizzare la Modalità principale.

  Se il tipo di gateway di sicurezza remoto è uno dei tipi *IP dinamico*, è necessario selezionare la Modalità aggressiva. In questo caso, la casella è selezionata automaticamente e non è possibile modificare l'impostazione.

- **Compressione (supporto Protocollo di compressione Payload IP (IPComp))**: un protocollo che riduce le dimensioni dei datagrammi IP. Selezionare questa casella per attivare il router in modo da proporre la compressione quando viene avviata la connessione. Se il responder rifiuta la proposta, il router non implementa la compressione. Se il router agisce da responder, accetta la compressione anche se questa non è attivata. Se si attiva questa funzionalità per questo router, è necessario attivarla anche sul router all'altra estremità del tunnel.

- **Mantieni connessione attiva**: tenta di ristabilire la connessione VPN in caso di interruzione.

- **Algoritmo hash AH**: il protocollo AH (Authentication Header) descrive il formato del pacchetto e gli standard predefiniti per la struttura del pacchetto. Se AH è il protocollo di sicurezza, la protezione è estesa fino all'intestazione IP per verificare l'integrità dell'intero pacchetto. Selezionare questa casella per utilizzare la funzionalità, quindi scegliere un metodo di autenticazione: MD5 o SHA1. MD5 produce digest a 128 bit per autenticare i dati del pacchetto. SHA1 produce digest a 160 bit per autenticare i dati del pacchetto. Entrambe le estremità del tunnel devono utilizzare lo stesso algoritmo.

- **Trasmissione NetBIOS**: messaggi broadcast utilizzati per la risoluzione dei nomi nel networking Windows per identificare risorse come computer, stampanti e file server. Questi messaggi sono utilizzati da alcune applicazioni software e funzionalità Windows come Risorse di rete. Il traffico broadcast dalle LAN non viene generalmente inoltrato su un tunnel VPN. Tuttavia, è possibile selezionare questa casella per far sì che le trasmissioni NetBIOS da un'estremità del tunnel vengano ritrasmesse all'altra estremità.
- **NAT Traversal**: NAT (Network Address Translation) consente agli utenti con indirizzi LAN privati di accedere alle risorse Internet utilizzando un indirizzo IP indirizzabile pubblicamente come indirizzo di origine. Tuttavia, per il traffico in entrata, il gateway NAT non ha un metodo automatico per tradurre l'indirizzo IP pubblico in una destinazione particolare sulla LAN privata. Questo problema impedisce scambi IPsec corretti. Se il router VPN è dietro un gateway NAT, selezionare questa casella per attivare NAT Traversal. È necessario utilizzare la stessa impostazione su entrambe le estremità del tunnel.
- **DPD (Dead Peer Detection)**: invia messaggi HELLO/ACK periodici per controllare lo stato del tunnel VPN. È necessario attivare questa funzionalità su entrambe le estremità del tunnel VPN. Specificare l'intervallo tra i messaggi HELLO/ACK nel campo **Intervallo**.
- **Autenticazione estesa**: utilizza un nome utente e una password host IPsec per l'autenticazione dei client VPN o utilizza il database utente trovato nella Gestione utenti. Sia l'host IPSec che il dispositivo periferico devono attivare l'autenticazione estesa. Per utilizzare l'host IPsec, fare clic sul pulsante di scelta **Host IPsec** e immettere il **nome utente** e la **password** nei rispettivi campi. Per utilizzare il dispositivo periferico, fare clic sul pulsante di scelta **Dispositivo periferico** e selezionare il database dal menu a discesa. Per aggiungere o modificare il database, fare clic su **Aggiungi/Modifica** per visualizzare la finestra Gestione utenti.
- **Backup tunnel**: se DPD determina che il peer remoto non è disponibile, questa funzionalità attiva il router per ristabilire il tunnel VPN utilizzando un indirizzo IP alternativo per il peer remoto o un'interfaccia WAN locale alternativa. Selezionare questa casella per attivare la funzionalità e immettere le seguenti impostazioni. Questa funzionalità è disponibile solo se è attivato il metodo Dead Peer Detection.
  - **Indirizzo IP backup remoto**: l'indirizzo IP alternativo per il peer remoto oppure immettere di nuovo l'indirizzo IP WAN già impostato per il gateway remoto.

- **Interfaccia locale**: interfaccia WAN da utilizzare per ristabilire la connessione.
- **Tempo di inattività del backup tunnel VPN**: se all'avvio del router il tunnel primario non è connesso entro il periodo specificato, si utilizza il tunnel di backup. Il tempo di inattività predefinito è 30 secondi.

- **Dividi DNS**: invia alcune delle richieste DNS a un server DNS e altre richieste DNS a un altro server DNS in base ai nomi di dominio specificati. Quando il router riceve una richiesta di risoluzione dell'indirizzo dal client, verifica il nome di dominio. Se corrisponde a uno dei nomi di dominio nelle impostazioni Dividi DNS, trasmette la richiesta al server DNS specificato. In caso contrario, la richiesta viene trasmessa al server DNS specificato nelle impostazioni dell'interfaccia WAN.

  Server DNS 1 e **Server DNS 2**: l'indirizzo IP del server DNS da utilizzare per i domini specificati. Se si desidera, specificare un server DNS secondario nel campo **Server DNS 2**.

  Nome di dominio 1 a **Nome di dominio 4**: specificare i nomi di dominio per i server DNS. Le richieste inviate a questi domini sono trasmesse ai server DNS specificati.

Da client a gateway

Questa funzionalità crea un nuovo tunnel VPN per consentire ai telelavoratori e a chi viaggia per lavoro di accedere alla rete utilizzando software client VPN di terzi, come TheGreenBow.

Per accedere a questa pagina, selezionare **VPN > Da client a gateway** nel riquadro di spostamento.

Configurare un tunnel VPN per un utente remoto, una VPN di gruppo per più utenti remoti o EasyVPN:

- **Tunnel**: crea un tunnel per un singolo utente remoto. Il numero del tunnel viene generato automaticamente.

- **VPN Gruppo**: crea un tunnel per un gruppo di utenti; in questo modo non è necessario configurare le impostazioni per i singoli utenti. Tutti gli utenti remoti possono utilizzare la stessa chiave precondivisa per connettersi al dispositivo fino al raggiungimento del numero massimo di tunnel supportati. Il router supporta fino a due gruppi VPN. Il numero del gruppo viene generato automaticamente.
- **EasyVPN**: consente agli utenti remoti di connettersi al dispositivo utilizzando l'utilità Cisco VPN Client, nota anche come *Cisco EasyVPN Client* (disponibile sul CD del prodotto):
  - La versione 5.0.07 supporta Windows 7 (32 bit e 64 bit), Windows Vista (32 bit e 64 bit) e Windows XP (32 bit).
  - La versione 4.9 supporta Mac OS X 10.4 e 10.5.
  - La versione 4.8 supporta Linux basato su Intel.

  Per configurare EasyVPN, impostare una password di gruppo in questa pagina, quindi aggiungere un nome utente e una password per ciascun utente Cisco VPN Client nella tabella Gestione utenti della sezione **Gestione degli utenti**. Quando si aggiunge un utente, selezionare il gruppo Non assegnato. Gli altri gruppi sono utilizzati per VPN SSL.

Configurazione di una VPN Tunnel o Gruppo

Immettere le seguenti informazioni:

- **Nome tunnel**: il nome che descrive il tunnel. Per un singolo utente, è possibile immettere il nome utente o l'ubicazione. Per una VPN di gruppo, è possibile identificare il ruolo aziendale o l'ubicazione del gruppo. Questa descrizione viene utilizzata come riferimento e non deve necessariamente corrispondere al nome utilizzato all'altra estremità del tunnel.
- **Interfaccia**: la porta WAN.
- **Modalità chiavi**: selezionare il metodo di gestione delle chiavi:
  - **Manuale**: consente di generare la chiave manualmente, ma non consente la negoziazione delle chiavi. Questa opzione viene utilizzata in ambienti statici di piccole dimensioni o per la risoluzione dei problemi. Immettere le impostazioni richieste.
  - **IKE** (Internet Key Exchange) **con chiave precondivisa:** utilizzare il protocollo IKE per configurare una SA (Security Association, associazione di sicurezza) per il tunnel. Impostazione consigliata. Se è stata selezionata l'opzione **VPN Gruppo**, questa è l'unica opzione disponibile.

- **IKE con certificato:** utilizzare un certificato per autenticare un peer IKE remoto.

- **Attiva**: selezionare questa casella per attivare la VPN.

Configurazione gruppo locale

Immettere le seguenti informazioni:

- **Tipo gateway di sicurezza locale**: metodo per identificare il router per stabilire il tunnel VPN. Il gateway di sicurezza remoto è l'altro router. Per effettuare la connessione è necessario che almeno uno dei router abbia un indirizzo IP statico o un nome host DNS dinamico.

  - **Solo IP**: l'indirizzo IP WAN statico. Se si conosce l'indirizzo IP del router VPN remoto, selezionare **Indirizzo IP** e immettere l'indirizzo. Se non si conosce l'indirizzo IP del router VPN remoto, selezionare **IP per DNS risolto** e immettere il nome di dominio del router. Un router Cisco può ottenere l'indirizzo IP di un dispositivo VPN remoto per DNS risolto.

  - **IP + Autenticazione nome di dominio (FQDN)**: il dispositivo ha un indirizzo IP statico e un nome di dominio registrato, ad esempio *MioServer.MioDominio.com*. Se si conosce l'indirizzo IP del router VPN remoto, selezionare **Indirizzo IP** e immettere l'indirizzo. Se non si conosce l'indirizzo IP del router VPN remoto, selezionare **IP per DNS risolto** e immettere il nome di dominio del router. I router Cisco possono ottenere l'indirizzo IP di un dispositivo VPN remoto per DNS risolto.

  - **IP + Autenticazione indirizzo e-mail (FQDN UTENTE)**: il dispositivo ha un indirizzo IP statico e utilizza un indirizzo e-mail per l'autenticazione. Se si conosce l'indirizzo IP del router VPN remoto, selezionare **Indirizzo IP** e immettere l'indirizzo IP. Se non si conosce l'indirizzo IP del router VPN remoto, selezionare **IP per DNS risolto** e immettere il nome di dominio reale del router. I router Cisco possono ottenere l'indirizzo IP di un dispositivo VPN remoto per DNS risolto.

  - **IP dinamico + Autenticazione nome di dominio (FQDN)**: il router ha un indirizzo IP dinamico e un nome host DNS dinamico registrato (disponibile presso dei provider, come ad esempio DynDNS.com). Immettere un **nome di dominio** da utilizzare per l'autenticazione. Il nome di dominio può essere utilizzato per una sola connessione tunnel.

  - **IP dinamico + Autenticazione indirizzo e-mail (FQDN UTENTE)**: il router ha un indirizzo IP dinamico e non dispone di nome host DNS dinamico. Immettere un **indirizzo e-mail** da utilizzare per l'autenticazione.

Se entrambi i router hanno indirizzi IP dinamici (come con le connessioni PPPoE), non selezionare IP dinamico + Indirizzo e-mail per entrambi i gateway. Per il gateway remoto, selezionare **Indirizzo IP** e **Indirizzo IP per DNS risolto**.

- **Tipo gruppo di sicurezza locale**: specificare le risorse LAN che possono accedere a questo tunnel.
  - **Indirizzo IP**: scegliere questa opzione per consentire a un solo dispositivo LAN di accedere al tunnel VPN. Quindi, immettere l'indirizzo IP del computer. Soltanto questo dispositivo può utilizzare il tunnel VPN.
  - **Sottorete**: opzione predefinita. Selezionare questa opzione per consentire a tutti i dispositivi su una sottorete di accedere al tunnel VPN. Quindi immettere l'indirizzo IP della sottorete e la maschera.

Configurazione del client remoto per singolo utente

Specificare il metodo di identificazione del client per stabilire il tunnel VPN. Le seguenti opzioni sono disponibili per una VPN Singolo utente o *Tunnel*:

- **Solo IP**: il client VPN remoto ha un indirizzo IP WAN statico. Se si conosce l'indirizzo IP del client, selezionare **Indirizzo IP** e immettere l'indirizzo. Se non si conosce l'indirizzo IP del client, selezionare **IP per DNS risolto** e immettere il nome di dominio del client su Internet. Il router ottiene l'indirizzo IP del client VPN remoto utilizzando DNS risolto; l'indirizzo IP del client VPN remoto viene visualizzato nella sezione Stato VPN della pagina Riepilogo.
- **IP + Autenticazione nome di dominio (FQDN)**: il client ha un indirizzo IP statico e un nome di dominio registrato. Immettere anche un **nome di dominio** da utilizzare per l'autenticazione. Il nome di dominio può essere utilizzato per una sola connessione tunnel.

  Se si conosce l'indirizzo IP del client VPN remoto, selezionare **Indirizzo IP** e immettere l'indirizzo. Se non si conosce l'indirizzo IP del client VPN remoto, selezionare **IP per DNS risolto** e immettere il nome di dominio reale del client su Internet. Il router otterrà l'indirizzo IP del client VPN remoto per DNS risolto; l'indirizzo IP del client VPN remoto verrà visualizzato nella sezione Stato VPN della pagina Riepilogo.
- **IP + Autenticazione indirizzo e-mail (FQDN UTENTE)**: il client ha un indirizzo IP statico e si desidera utilizzare un indirizzo e-mail per l'autenticazione. L'indirizzo IP WAN corrente viene visualizzato automaticamente. Immettere un **indirizzo e-mail** da utilizzare per l'autenticazione.

Se si conosce l'indirizzo IP del client VPN remoto, selezionare **Indirizzo IP** e immettere l'indirizzo. Se non si conosce l'indirizzo IP del client VPN remoto, selezionare **IP per DNS risolto** e immettere il nome di dominio reale del client su Internet. Il dispositivo ottiene l'indirizzo IP del client VPN remoto per DNS risolto; l'indirizzo IP del dispositivo VPN remoto viene visualizzato nella sezione Stato VPN della pagina Riepilogo.

- **IP dinamico + Autenticazione nome di dominio (FQDN)**: il client ha un indirizzo IP dinamico e un nome host DNS dinamico registrato (disponibile presso il provider come DynDNS.com). Immettere il **nome di dominio** da utilizzare per l'autenticazione. Il nome di dominio può essere utilizzato per una sola connessione tunnel.
- **IP dinamico + Autenticazione indirizzo e-mail (FQDN UTENTE)**: il client ha un indirizzo IP dinamico e non dispone di nome host DNS dinamico. Immettere un **indirizzo e-mail** da utilizzare per l'autenticazione.

Configurazione del client remoto per un gruppo

Specificare il metodo di identificazione dei client per stabilire il tunnel VPN. Per una VPN di gruppo, sono disponibili le seguenti opzioni:

- **Autenticazione nome di dominio (FQDN)**: identifica il client tramite un nome di dominio registrato. Immettere un **nome di dominio** da utilizzare per l'autenticazione. Il nome di dominio può essere utilizzato per una sola connessione tunnel.
- **Autenticazione indirizzo e-mail (FQDN UTENTE)**: identifica il client con un indirizzo e-mail per l'autenticazione. Immettere l'indirizzo nei campi forniti.
- **Client VPN Microsoft XP/2000**: il software client è il client VPN integrato in Microsoft XP/2000.

Configurazione di IPSec

Per una corretta crittografia, le due estremità di un tunnel VPN devono utilizzare gli stessi metodi di crittografia, decrittografia e autenticazione. Immettere esattamente le stesse impostazioni su entrambi i router.

Immettere le impostazioni per Fase 1 e Fase 2. La Fase 1 stabilisce le chiavi precondivise per creare un canale di comunicazione autenticato protetto. Nella Fase 2, i peer IKE utilizzano il canale sicuro per negoziare associazioni di sicurezza per conto di altri servizi, ad esempio IPsec. Accertarsi di immettere le stesse impostazioni quando si configurano gli altri router per questo tunnel.

- **Gruppo DH fase 1/fase 2**: DH (Diffie-Hellman) è un protocollo di scambio delle chiavi. Sono disponibili tre gruppi di diverse lunghezze della chiave primaria: Gruppo 1 - 768 bit, Gruppo 2 - 1.024 bit e Gruppo 5 - 1.536 bit. Per una maggiore velocità e una minore sicurezza, selezionare **Gruppo 1**. Per una minore velocità e una maggiore sicurezza, selezionare **Gruppo 5**. Il Gruppo 1 è selezionato per impostazione predefinita.
- **Crittografia fase 1/fase 2**: il metodo di crittografia per questa fase: DES, 3DES, AES-128, AES-192 o AES-256. Il metodo di crittografia determina la lunghezza della chiave utilizzata per crittografare o decodificare i pacchetti ESP. AES-256 è l'opzione consigliata perché è più sicura.
- **Autenticazione fase 1/fase 2**: il metodo di autenticazione per questa fase: MD5 o SHA1. Il metodo di autenticazione determina la modalità di convalida dei pacchetti con intestazione ESP (Encapsulating Security Payload Protocol). MD5 è un algoritmo di hashing unidirezionale che produce digest a 128 bit. SHA1 è un algoritmo di hashing unidirezionale che produce digest a 160 bit. SHA1 è l'opzione consigliata perché è più sicura. Accertarsi che entrambe le estremità del tunnel VPN utilizzino lo stesso metodo di autenticazione.
- **Durata SA fase 1/fase 2**: periodo di attività di un tunnel VPN in questa fase. Il valore predefinito per la fase 1 è 28800 secondi. Il valore predefinito per la fase 2 è 3.600 secondi.
- **Perfect Forward Secrecy**: se l'opzione Perfect Forward Secrecy (PFS) è attivata, la negoziazione di fase 2 IKE genera nuovo materiale delle chiavi per la crittografia e l'autenticazione del traffico IP, quindi i pirati informatici che utilizzano la forza bruta per intercettare le chiavi di crittografia non potranno ottenere le chiavi IPsec future. Selezionare questa casella per attivare la funzionalità oppure deselezionarla per disattivarla. Si consiglia di attivare questa funzionalità.
- **Complessità chiave precondivisa minima**: selezionare la casella **Attiva** per attivare il misuratore della complessità della chiave precondivisa.
- **Chiave precondivisa**: la chiave precondivisa da utilizzare per l'autenticazione del peer IKE remoto. È possibile immettere fino a 30 caratteri della tastiera o valori esadecimali, ad esempio Mio_@123 o 4d795f40313233. Entrambe le estremità del tunnel VPN devono utilizzare la stessa chiave precondivisa. Si raccomanda di cambiare periodicamente la chiave precondivisa per massimizzare la sicurezza VPN.

- **Misuratore complessità chiave precondivisa**: se si attiva l'opzione Complessità chiave precondivisa minima, il valore di questo campo indica la complessità della chiave precondivisa. Durante la digitazione di una chiave precondivisa, vengono visualizzate delle barre colorate. Le opzioni sono rosso (debole), giallo (accettabile) e verde (complessa).

SUGGERIMENTO Immettere una chiave precondivisa complessa che includa più di otto caratteri, lettere maiuscole e minuscole, numeri e simboli, come -*^+= (i caratteri ' ' " \ non sono supportati).

Impostazioni avanzate per IKE

Per la maggior parte degli utenti saranno sufficienti le impostazioni di base; gli utenti avanzati possono fare clic su **Impostazioni avanzate** per visualizzare le impostazioni avanzate. Eventuali modifiche alle impostazioni avanzate su un router, devono essere riportate anche sull'altro router.

- **Modalità aggressiva**: sono possibili due modalità di negoziazione SA IKE: Modalità principale e Modalità aggressiva. Se si preferisce la sicurezza di rete, si consiglia la Modalità principale. Se, invece, si preferisce la velocità di rete, si consiglia la Modalità aggressiva. Selezionare questa casella per attivare la Modalità aggressiva oppure deselezionarla per utilizzare la Modalità principale.
  Se **Tipo gateway di sicurezza remoto** è impostato su uno dei tipi *IP dinamico*, è necessario selezionare la Modalità aggressiva. In questo caso, la casella è selezionata automaticamente e non è possibile modificare l'impostazione.
- **Compressione (supporto Protocollo di compressione Payload IP (IPComp))**: un protocollo che riduce le dimensioni dei datagrammi IP. Selezionare questa casella per attivare il router in modo da proporre la compressione quando viene avviata la connessione. Se il responder rifiuta la proposta, il router non implementa la compressione. Se il router agisce da responder, accetta la compressione anche se questa non è attivata. Se si attiva questa funzionalità per questo router, è necessario attivarla anche sul router all'altra estremità del tunnel.
- **Mantieni connessione attiva**: tenta di ristabilire la connessione VPN in caso di interruzione.

- **Algoritmo hash AH**: il protocollo AH (Authentication Header) descrive il formato del pacchetto e gli standard predefiniti per la struttura del pacchetto. Se AH è il protocollo di sicurezza, la protezione è estesa fino all'intestazione IP per verificare l'integrità dell'intero pacchetto. Selezionare questa casella per utilizzare la funzionalità, quindi scegliere un metodo di autenticazione: MD5 o SHA1. MD5 produce digest a 128 bit per autenticare i dati del pacchetto. SHA1 produce digest a 160 bit per autenticare i dati del pacchetto. Entrambe le estremità del tunnel devono utilizzare lo stesso algoritmo.
- **Trasmissione NetBIOS**: messaggi broadcast utilizzati per la risoluzione dei nomi nel networking Windows per identificare risorse come computer, stampanti e file server. Questi messaggi sono utilizzati da alcune applicazioni software e funzionalità Windows come Risorse di rete. Il traffico broadcast dalle LAN non viene generalmente inoltrato su un tunnel VPN. Tuttavia, è possibile selezionare questa casella per far sì che le trasmissioni NetBIOS da un'estremità del tunnel vengano ritrasmesse all'altra estremità.
- **NAT Traversal**: NAT (Network Address Translation) consente agli utenti con indirizzi LAN privati di accedere alle risorse Internet utilizzando un indirizzo IP indirizzabile pubblicamente come indirizzo di origine. Tuttavia, per il traffico in entrata, il gateway NAT non ha un metodo automatico per tradurre l'indirizzo IP pubblico in una destinazione particolare sulla LAN privata. Questo problema impedisce scambi IPsec corretti. Se il router VPN è dietro un gateway NAT, selezionare questa casella per attivare NAT Traversal. È necessario utilizzare la stessa impostazione su entrambe le estremità del tunnel.
- Intervallo DPD (Dead Peer Detection): è un metodo di rilevamento di un peer IKE (Internet Key Exchange) dead. In questo metodo vengono utilizzati modelli di traffico IPsec per ridurre al minimo il numero di messaggi. L'intervallo di controllo minimo in VPN Dead Peer Detection è 10 secondi.
- **Autenticazione estesa**: consente di specificare un nome utente e una password per autenticare le richieste tunnel IPSec in arrivo oltre a una chiave precondivisa o un certificato.
  - **Host IPsec**: indica l'uso di un **host IPsec** per l'autenticazione estesa.
    Nome utente: nome utente per l'autenticazione.
    Password: password per l'autenticazione.
  - **Dispositivo periferico**: fornisce un indirizzo IP al richiedente del tunnel in ingresso (dopo l'autenticazione) dall'intervallo IP virtuale configurato nella finestra **Riepilogo**. Selezionare il dispositivo dal menu a discesa. Per aggiungere o modificare il dominio del dispositivo, fare clic su

Aggiungi/Modifica per visualizzare la finestra **Gestione degli utenti**.

- **Configurazione modalità**: fornisce un indirizzo IP al richiedente del tunnel in ingresso (dopo l'autenticazione) dall'intervallo IP virtuale configurato nella finestra VPN > **Riepilogo**.

FlexVPN (Spoke)

FlexVPN utilizza IKEv2 basati su standard aperti come tecnologia di protezione e fornisce livelli di protezione elevati. FlexVPN è stato creato per semplificare la distribuzione di VPN e risolvere la complessità delle soluzioni multiple. Come ecosistema unificato, è in grado di coprire tutti i tipi di servizi VPN, accesso remoto, teleworker, site to site, mobilità, protezione gestita e altri.

Aggiunta di un nuovo tunnel FlexVPN

Per aggiungere un nuovo tunnel, configurare quanto segue:

- Tunnel Name (Nome tunnel): inserire un nome per il tunnel FlexVPN.
- Interfaccia: selezionare la porta WAN dall'elenco a discesa per utilizzare questo tunnel.
- Attiva: selezionare per attivare o deselezionare per disattivare il tunnel. Il tunnel FlexVPN è attivato per impostazione predefinita.

Configurazione spoke

Immettere le impostazioni per la configurazione Spoke per il router:

- Tipo gateway di sicurezza Spoke: selezionare un'opzione dall'elenco a discesa per identificare il router per stabilire il tunnel FlexVPN.
  - Solo IP: il router ha un indirizzo IP WAN statico. L'indirizzo IP WAN viene visualizzato automaticamente.
  - IP + Autenticazione nome di dominio (FQDN): il dispositivo ha un indirizzo IP statico e un nome di dominio registrato, ad esempio
  - MioServer.MioDominio.com. Immettere anche il nome di dominio da utilizzare per l'autenticazione. Il nome di dominio può essere utilizzato per una sola connessione tunnel.
  - IP + Autenticazione indirizzo e-mail (FQDN UTENTE): il dispositivo ha un indirizzo IP statico e utilizza un indirizzo e-mail per l'autenticazione.

L'indirizzo IP WAN viene visualizzato automaticamente. Immettere l'indirizzo e-mail da utilizzare per l'autenticazione.

- IP dinamico + Autenticazione nome di dominio (FQDN): il router ha un indirizzo IP dinamico e un nome host DNS dinamico registrato (disponibile presso dei provider, come ad esempio DynDNS.com). Immettere un nome di dominio da utilizzare per l'autenticazione. Il nome di dominio può essere utilizzato per una sola connessione tunnel.
- IP dinamico + Autenticazione indirizzo e-mail (FQDN UTENTE): il router ha un indirizzo IP dinamico e non dispone di nome host DNS dinamico. Immettere un indirizzo e-mail da utilizzare per l'autenticazione.
- Nome dominio: inserire un nome di dominio.
- Indirizzo IP GRE: l'indirizzo IP dell'interfaccia virtuale (GRE).
- Ottieni da Hub: l'indirizzo IP GRE assegnato da Hub.
- Configura staticamente: configurazione manuale dell'indirizzo IP GRE.
- Complessità chiave precondivisa minima: selezionare la casella Attiva per attivare il misuratore della complessità della chiave precondivisa.
- Chiave precondivisa: la chiave precondivisa da utilizzare per l'autenticazione dell'IKE Spoke. È possibile immettere fino a 30 caratteri della tastiera o valori esadecimali, ad esempio Mio_@123 o 4d795f40313233 (i caratteri ' ' " \ non sono supportati). Entrambe le estremità del tunnel FlexVPN devono utilizzare la stessa chiave precondivisa. Si raccomanda vivamente di cambiare periodicamente la chiave precondivisa per massimizzare la sicurezza del FlexVPN.
- Misuratore complessità chiave precondivisa: se si attiva l'opzione Complessità chiave precondivisa minima, il valore di questo campo indica la complessità della chiave precondivisa. Durante la digitazione di una chiave precondivisa, vengono visualizzate delle barre colorate. Le opzioni sono rosso (debole), giallo (accettabile) e verde (complessa).

Rete spoke

La Rete Spoke consente a tutti i dispositivi sulla rete Spoke di utilizzare il tunnel FlexVPN. Per aggiungere una nuova rete spoke, fare clic su Aggiungi e inserire Indirizzo IP e Subnet Mask della sottorete.

Configurazione hub

Immettere le impostazioni per la configurazione Hub per il router:

- Tipo gateway di sicurezza Hub: metodo per identificare il router per stabilire il FlexVPN. Selezionare una delle seguenti opzioni:
  - Solo IP: l'indirizzo IP WAN statico. Se si conosce l'indirizzo IP dell'Hub, selezionare Indirizzo IP e immettere l'indirizzo. Se non si conosce l'indirizzo IP dell'Hub, selezionare IP per DNS risolto e immettere il nome di dominio del router. Un router Cisco può ottenere l'indirizzo IP dell'Hub per DNS risolto.
  - IP + Autenticazione nome di dominio (FQDN): il router ha un indirizzo IP statico e un nome di dominio registrato, ad esempio MioServer. MioDominio.com. Se si conosce l'indirizzo IP dell'Hub, selezionare Indirizzo IP e immettere l'indirizzo. Se non si conosce l'indirizzo IP dell'Hub, selezionare IP per DNS risolto e immettere il nome di dominio del router. I router Cisco possono ottenere l'indirizzo IP dell'Hub per DNS risolto.
  - IP + Autenticazione indirizzo e-mail (FQDN UTENTE): il router ha un indirizzo IP statico e si desidera utilizzare un indirizzo e-mail per l'autenticazione. Se si conosce l'indirizzo IP dell'Hub, selezionare Indirizzo IP e immettere l'indirizzo IP. Se non si conosce l'indirizzo IP dell'Hub, selezionare IP per DNS risolto e immettere il vero nome di dominio del router. I router Cisco possono ottenere l'indirizzo IP dell'Hub per DNS risolto.
  - Complessità chiave precondivisa minima: selezionare Attiva per attivare il misuratore della complessità della chiave precondivisa.
- Chiave precondivisa: la chiave precondivisa da utilizzare per l'autenticazione dell'IKE Hub. È possibile immettere fino a 30 caratteri della tastiera o valori esadecimali, ad esempio Mio_@123 o 4d795f40313233 (i caratteri ' ' " \ non sono supportati). Entrambe le estremità del tunnel FlexVPN devono utilizzare la stessa chiave precondivisa. Si raccomanda di cambiare periodicamente la chiave precondivisa per massimizzare la sicurezza FlexVPN.
- Misuratore complessità chiave precondivisa: se l'opzione Complessità chiave precondivisa minima è attivata, il valore di questo campo indica la complessità della chiave precondivisa. Durante la digitazione di una chiave precondivisa, vengono visualizzate delle barre colorate. Le opzioni sono rosso (debole), giallo (accettabile) e verde (complessa).

Configurazione IPSec

Per una corretta crittografia, le due estremità di un tunnel FlexVPN devono utilizzare gli stessi metodi di crittografia, decrittografia e autenticazione. Immettere esattamente le stesse impostazioni su entrambi i router.

Immettere le impostazioni per Fase 1 e Fase 2. Fase 1 consente di stabilire le chiavi precondivise per creare un canale di comunicazione autenticato sicuro. Nella Fase 2, i peer IKE utilizzano il canale sicuro per negoziare associazioni di sicurezza per conto di altri servizi, ad esempio IPSec. Accertarsi di immettere le stesse impostazioni quando si configura l'altro router per questo tunnel.

- Gruppo DH fase 1/fase 2: DH (Diffie-Hellman) è un protocollo di scambio delle chiavi. Sono disponibili tre gruppi di diverse lunghezze della chiave primaria: Gruppo 1 - 768 bit, Gruppo 2 - 1.024 bit e Gruppo 5 - 1.536 bit. Per una maggiore velocità e una minore sicurezza, selezionare Gruppo 1. Per una minore velocità e una maggiore sicurezza, selezionare Gruppo 5. Il Gruppo 2 è selezionato per impostazione predefinita.
- Crittografia fase 1/fase 2: il metodo di crittografia per questa fase: DES, 3DES, AES-128, AES-192 o AES-256. Questo metodo determina la lunghezza della chiave utilizzata per crittografare o decrittografare i pacchetti ESP. AES-256 è l'opzione consigliata perché è più sicura.
- Autenticazione fase 1/fase 2: il metodo di autenticazione per questa fase: MD5 o SHA1. Il metodo di autenticazione determina la modalità di convalida dei pacchetti con intestazione ESP (Encapsulating Security Payload Protocol). MD5 è un algoritmo di hashing unidirezionale che produce digest a 128 bit. SHA1 è un algoritmo di hashing unidirezionale che produce digest a 160 bit. SHA1 è l'opzione consigliata perché è più sicura. Accertarsi che entrambe le estremità del tunnel VPN utilizzino lo stesso metodo di autenticazione.
- Durata SA fase 1/fase 2: periodo di attività di un tunnel VPN in questa fase. Il valore predefinito per la fase 1 è 28.800 secondi. Il valore predefinito per la fase 2 è 3.600 secondi.

Configurazione avanzata

Per la maggior parte degli utenti, le impostazioni di base sono più che sufficienti. Eventuali modifiche alle impostazioni avanzate su un router, devono essere riportate anche sull'altro router.

- Mantieni connessione attiva: tenta di ristabilire la connessione VPN in caso di interruzione.

- DPD (Dead Peer Detection): invia messaggi HELLO/ACK periodici per controllare lo stato del tunnel FlexVPN. Specificare l'intervallo tra i messaggi HELLO/ACK nel campo Intervallo.
- Backup tunnel: se DPD determina che il peer remoto non è disponibile, questa funzionalità attiva il router per ristabilire il tunnel FlexVPN utilizzando un indirizzo IP alternativo per il peer remoto o un'interfaccia WAN locale alternativa. Selezionare questa casella per attivare la funzionalità e immettere le seguenti impostazioni. Questa funzionalità è disponibile solo se è attivato il metodo Dead Peer Detection.
  - Indirizzo IP Hub: l'indirizzo IP alternativo per il peer remoto oppure immettere di nuovo l'indirizzo IP WAN già impostato per il gateway remoto.
  - Interfaccia Spoke: l'interfaccia WAN da utilizzare per ristabilire la connessione.
  - Tempo di inattività del backup tunnel VPN: se all'avvio del router il tunnel primario non è connesso entro il periodo specificato, si utilizza il tunnel di backup. Il tempo di inattività predefinito è 30 secondi.

Passthrough VPN

Il Passthrough VPN consente ai client VPN di attraversare il router e connettersi a un endpoint VPN ed è attivato per impostazione predefinita.

Per accedere a questa pagina, selezionare **VPN > Passthrough VPN** nel riquadro di spostamento.

Per attivare il Passthrough VPN, selezionare **Attiva** per i protocolli consentiti:

- **Passthrough IPSec**: IPsec (Internet Protocol Security) è una suite di protocolli utilizzati per implementare lo scambio sicuro di pacchetti a livello IP.
- **Passthrough PPTP**: il protocollo PPTP (Point-to-Point Tunneling Protocol) consente il tunnel del protocollo PPP (Point-to-Point Protocol) all'interno di una rete IP.
- **Passthrough L2TP**: il protocollo L2TP (Layer 2 Tunneling Protocol) consente l'esecuzione di sessioni point-to-point tramite Internet a livello 2.

Server PPTP

È possibile attivare fino a 10 tunnel VPN PPTP (Point-to-Point Tunneling Protocol) per gli utenti con software client PPTP. Ad esempio, in Windows XP o 2000, un utente apre il pannello Connessioni di rete e crea una nuova connessione. Nella procedura guidata, l'utente seleziona l'opzione per creare una connessione al luogo di lavoro utilizzando una VPN. L'utente deve conoscere l'indirizzo IP WAN del dispositivo. Per ulteriori informazioni, fare riferimento alla documentazione o ai file della guida del sistema operativo.

Per accedere a questa pagina, selezionare **VPN > Server PPTP** nel riquadro di spostamento.

Per attivare il server PPTP e consentire tunnel VPN PPTP, selezionare la casella **Attiva** e inserire l'intervallo:

Inizio intervallo e **Fine intervallo**: intervallo di indirizzi LAN da assegnare ai client VPN PPTP. L'intervallo di indirizzi IP LAN per client VPN PPTP deve essere al di fuori del normale intervallo DHCP del router.

L'opzione PPTP Tunnel Status (Stato tunnel PPTP) mostra il numero di tunnel utilizzati e il numero di tunnel disponibili.

Nella **tabella di connessione** vengono mostrati i tunnel in uso.

10

OpenVPN

OpenVPN è una tecnica di rete privata virtuale (VPN) per creare connessioni sicure point-to-point o site-to-site all'interno delle configurazioni bridge o di percorso e delle infrastrutture di accesso remoto mediante un protocollo di sicurezza personalizzato che utilizza SSL/TLS per lo scambio delle chiavi.

OpenVPN consente ai peer di autenticarsi a vicenda tramite nome utente/password o certificati. Se utilizzata in una configurazione server multiclient, consente al server dirilasciare un certificato di autenticazione per ogni client, utilizzando firma e autorità di certificazione.

Riepilogo

In questa pagina vengono visualizzate le informazioni generali sulle impostazioni del tunnel OpenVPN. Il dispositivo supporta fino a 50 account OpenVPN.

In OpenVPN Tunnel Number (Numero del tunnel OpenVPN) viene mostrato il numero di tunnel utilizzati, tunnel disponibili, tunnel abilitati e tunnel definiti.

Tabella delle impostazioni server

Nella tabella delle impostazioni server vengono mostrate le voci create in OpenVPN > OpenVPN Server.

- Attiva: selezionare questa casella per attivare il server OpenVPN o deselezionarla per disattivare il server.
- Autenticazione: la sola password oppure la combinazione di password e certificato.
- Protocollo: il protocollo richiesto e il numero della porta.
- Crittografia: il metodo di crittografia per questa fase: NULL, DES, 3DES, AES128, AES-192 o AES-256. Questo metodo determina la lunghezza della chiave utilizzata per crittografare o decrittografare i pacchetti.
- Pool di indirizzi client: fornisce l'indirizzo IP del client da questo pool.

Server OpenVPN

Stato ID account OpenVPN

Nella tabella relativa all'impostazione dell'ID account vengono mostrate le voci create in OpenVPN > Account OpenVPN. Fare clic su Aggiungi per aggiungere un account OpenVPN.

- Attiva: selezionare questa casella per attivare un account OpenVPN esistente o deselezionarla per disattivare l'account.

Indica i responsabili che possono aggiungere o modificare le impostazioni del server OpenVPN.

Per aggiungere un server OpenVPN, configurare le seguenti impostazioni e fare clic su Salva.

Configurazione di base

- Attiva: selezionare questa casella per attivare il server OpenVPN o deselezionarla per disattivare il server.

Account OpenVPN

Indica i responsabili che possono aggiungere o modificare gli utenti del client OpenVPN.

Per aggiungere un account OpenVPN, configurare le seguenti impostazioni e fare clic su Salva.

- Attiva: selezionare questa casella per attivare l'account OpenVPN o deselezionarla per disattivare l'account.
- Autenticazione: password.
- Server OpenVPN: il nome o l'indirizzo IP del server OpenVPN.
- Nome utente: il nome utente del client OpenVPN.
- Password: la password del client OpenVPN.

11

Gestione dei certificati

Un certificato digitale dimostra che il soggetto indicato al suo interno è proprietario di una chiave pubblica. Questo consente agli altri (relying party) di considerare attendibili le firme o le dichiarazioni della chiave privata associata alla chiave pubblica certificata. In questo modello di relazioni di fiducia, un'autorità di certificazione (CA) è una terza parte considerata attendibile sia dal soggetto (proprietario) del certificato che dalla relying party. Le CA sono alla base di molti schemi di infrastruttura a chiave pubblica (PKI, Public Key Infrastructure).

Utilizzare la funzione di gestione dei certificati per generare e installare certificati SSL.

Certificato personale

È possibile aggiungere fino a 50 certificati con firma automatica oppure con autorizzazione di una terza parte. È anche possibile utilizzare lo **Strumento di generazione dei certificati** per creare certificati o importarli da un PC o un dispositivo USB.

I certificati SSL con firma automatica non vengono considerati automaticamente attendibili dai browser e, anche se è possibile utilizzarli per la crittografia, nei browser vengono visualizzati messaggi di avviso per informare che il certificato non è stato rilasciato da un ente ritenuto affidabile dall'utente.

La connessione è possibile anche senza aver installato un certificato sul PC. In questo caso, quando si effettua la connessione al tunnel VPN, viene visualizzato un messaggio di sicurezza, ma è possibile procedere senza questa protezione aggiuntiva.

Per accedere alla gestione dei certificati, fare clic su **Gestione certificati > Certificato personale** nel riquadro di spostamento.

Per impostare il certificato primario, fare clic sul pulsante di scelta accanto al certificato desiderato, quindi fare clic su **Seleziona come certificato primario**.

Per visualizzare le informazioni relative al certificato, fare clic su **Dettagli**.

Esportazione o visualizzazione di un certificato o di una chiave privata

Il certificato del client consente la connessione di un client alla VPN. Per esportare o visualizzare un certificato o una chiave privata, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic sull'icona appropriata: **Esporta certificato per client**, **Esporta certificato per amministratore** oppure **Esporta chiave privata**. Viene visualizzata la finestra Download file.

Esporta certificato per client: il certificato del client consente la connessione di un client alla VPN.

Esporta certificato per amministratore: il certificato per l'amministratore contiene la chiave privata ed è possibile esportarne una copia da utilizzare come backup. Ad esempio, è possibile esportare il certificato prima di ripristinare le impostazioni predefinite di fabbrica sul dispositivo. Dopo il riavvio del dispositivo, importare il file esportato per ripristinare il certificato.

Esporta chiave privata: alcuni software client per VPN richiedono credenziali con chiave privata, certificato CA e certificato separati.

PASSAGGIO 2 Fare clic su **Apri** per visualizzare la chiave. Fare clic su **Salva** per salvarla.

Importazione di un certificato di terze parti o con firma automatica

Non è possibile autorizzare o firmare una richiesta di firma del certificato (CSR, Certificate Signing Request) generata esternamente; per aggiungere una CSR esterna è necessario utilizzare la finestra **Autorizzazione CSR**.

Per importare un certificato, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Aggiungi**.

PASSAGGIO 2 Selezionare **Autorizzato da terzi** o **Con firma automatica**.

PASSAGGIO 3 Selezionare **Importa da PC** o **Importa da dispositivo USB**.

PASSAGGIO 4 Selezionare un file nella casella **Certificato CA** (solo terza parte).

PASSAGGIO 5 Selezionare un file nella casella **Certificato e chiave privata** (terza parte o con firma automatica).

PASSAGGIO 6 Fare clic su **Salva**.

Certificato IPsec attendibile

La tecnologia IPsec viene utilizzata nello scambio dei dati di generazione e autenticazione delle chiavi, nel protocollo di definizione delle chiavi, nell'algoritmo di crittografia o nei meccanismi di autenticazione e convalida sicure di transazioni online con i certificati SSL.

Per accedere alla gestione dei certificati IPsec, fare clic su **Gestione certificati > Certificato IPsec attendibile** nel riquadro di spostamento.

Per visualizzare le informazioni relative al certificato, fare clic su **Dettagli**.

Per esportare o visualizzare un certificato, fare clic su **Esporta certificato**. Viene visualizzata una finestra a comparsa in cui è possibile fare clic su **Apri** per esaminare il certificato oppure fare clic su **Salva** per salvare il certificato su un PC.

Per importare un certificato di terze parti, fare clic su **Aggiungi** e attenersi alla seguente procedura:

PASSAGGIO 1 Selezionare un file nella casella **Certificato CA**.

PASSAGGIO 2 Selezionare **Importa da PC** o **Importa da dispositivo USB**.

PASSAGGIO 3 Selezionare un file nella casella **Certificato** (di terze parti o con firma automatica).

PASSAGGIO 4 Fare clic su **Salva**.

Certificato OpenVPN

Supporta i metodi di autenticazione OpenVPN basati sui certificati.

Per accedere a questa pagina, selezionare Gestione certificati > Certificato OpenVPN nella struttura di navigazione.

Per visualizzare le informazioni relative al certificato, fare clic su Dettagli.

Per creare il nuovo certificato per il server o il client OpenVPN, fare clic su Aggiungi e passare alla pagina Gestione certificati > Strumento di generazione dei certificati.

Strumento di generazione dei certificati

Lo strumento di generazione delle richieste di certificato raccoglie le informazioni, quindi genera un file con la chiave privata e una richiesta di certificato. È possibile scegliere di generare un certificato con firma automatica o una CSR che dovrà essere firmata da un'autorità di certificazione esterna. Se si salva la configurazione, la CSR o il certificato con firma automatica generati vengono visualizzati nella pagina **Certificato personale**.

Per accedere allo strumento di gestione dei certificati, fare clic su **Gestione certificati > Generazione certificati** nel riquadro di spostamento.

Per generare un certificato, attenersi alla seguente procedura:

PASSAGGIO 1 Immettere i parametri seguenti.

- **Tipo**: il tipo di richiesta di certificato.
- **Nome Paese**: il Paese di origine.
- **Stato o provincia**: il nome dello stato o della provincia (facoltativo).
- **Località**: il nome della località (facoltativo).
- **Nome organizzazione**: il nome dell'organizzazione (facoltativo).
- **Nome unità organizzativa**: il nome della filiale dell'organizzazione.
- **Nome comune**: il nome comune dell'organizzazione.
- **Indirizzo e-mail**: l'indirizzo e-mail di contatto (facoltativo).
- **Lunghezza crittografia chiave**: la lunghezza della chiave.
- **Durata validità**: la durata del certificato, espressa in numero di giorni.

PASSAGGIO 2 Fare clic su **Salva**. Viene visualizzata la finestra **Certificato personale**.

Autorizzazione CSR

La CSR (Certificate Signing Request) è un certificato di identità digitale creato da uno strumento di generazione di certificati. Questo certificato è completo solo dopo essere stato firmato da un'autorità di certificazione (CA). La finestra Gestione certificati > Autorizzazione CSR consente di utilizzare questo dispositivo come CA per firmare o autorizzare una CSR generata esternamente. Dopo aver ottenuto la firma da parte del dispositivo, la CSR generata esternamente diventa un certificato attendibile e viene spostata nella finestra **Certificato IPsec attendibile**. Per ripristinare i valori predefiniti di fabbrica per la configurazione del dispositivo, inclusi i certificati predefiniti, utilizzare la finestra **Impostazioni predefinite**.)

Per firmare un certificato, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Sfoglia** per selezionare la CSR desiderata.

PASSAGGIO 2 Per selezionare la chiave privata corrispondente per autorizzare e firmare la CSR, fare clic sul certificato da associare alla richiesta nell'elenco a discesa **Certificato personale**.

PASSAGGIO 3 Fare clic su **Salva**.

12

Log

I log documentano lo stato del sistema mediante trap o su base periodica.

Log di sistema

Configurare i log e gli avvisi tramite SMS (Short Message Service)

Per accedere a questa pagina, selezionare **Log** > **Log di sistema** nel riquadro di spostamento.

Configurazione dell'invio di SMS relativi al log di sistema

Per configurare il collegamento al log, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Attiva**.

PASSAGGIO 2 Selezionare **USB1** o **USB2** per inviare il log tramite le porte USB.

PASSAGGIO 3 Selezionare **Componi numero 1** e/o **Componi numero 2**, quindi immettere il numero di telefono da chiamare.

PASSAGGIO 4 Fare clic su **Prova** per provare il collegamento.

PASSAGGIO 5 Indicare quando viene inviato il log:

- All'attivazione di un collegamento.
- Alla disattivazione di un collegamento.
- Se l'autenticazione fallisce.
- All'avvio del sistema.

PASSAGGIO 6 Fare clic su **Salva**.

Configurazione dei server del log di sistema

Per attivare un server, fare clic su **Attiva** e immettere il nome del server nel campo **Server log di sistema**.

Configurazione delle notifiche tramite e-mail

Per configurare la funzione Notifica e-mail, selezionare la relativa casella **Attiva** e impostare i parametri seguenti:

- **Server di posta**: il nome o l'indirizzo IP del server di posta.
- **Autenticazione**: il tipo di autenticazione per l'accesso al server di posta.
  - **Nessuna**: nessun tipo di autenticazione.
  - **Accesso in chiaro**: autenticazione in formato testo normale.
  - **TLS**: protocollo di autenticazione per connessioni sicure; ad esempio Gmail utilizza il tipo di autenticazione TLS sulla porta 587.
  - **SSS**: protocollo di autenticazione per connessioni sicure; ad esempio Gmail utilizza il tipo di autenticazione SSL sulla porta 465.
- **Porta SMTP**: il numero di porta del protocollo SMTP (Simple Mail Transfer Protocol).
- **Nome utente**: il nome utente associato all'indirizzo e-mail. Esempio:
  Server di posta: smtp.gmail.com
  Autenticazione: SSL
  Porta SMTP: 465
  Nome utente: xxxxx@gmail.com
  Password: yyyyyy
- **Password**: la password associata all'indirizzo e-mail.
- **Indirizzo destinatario 1** e (facoltativamente) **2**: l'indirizzo e-mail. Esempio:
  Indirizzo destinatario: `zzz@azienda.com`.
- **Lunghezza coda log**: il numero di voci di log da creare prima di inviare una notifica. Ad esempio, *10* voci.
- **Soglia periodo di log**: intervallo tra le notifiche del log. Ad esempio, *10* minuti.
- **Avviso in tempo reale**: evento che avvia una notifica immediata.
- **Avviso quando si accede a contenuti bloccati/filtrati**: messaggio e-mail di avviso inviato quando un dispositivo bloccato o escluso mediante filtro tenta di effettuare l'accesso.

- **Avviso e-mail per attacchi hacker**: messaggio e-mail di avviso inviato quando un hacker cerca di effettuare l'accesso e di lanciare un attacco DOS (denial-of-service).

Per inviare il log immediatamente tramite e-mail, fare clic su **Invia log ora**.

Configurazione dei log

Per attivare la registrazione di voci, selezionare gli eventi seguenti:

- **Flooding Syn**: le richieste di connessioni TCP sono ricevute a una velocità superiore a quella di elaborazione del dispositivo.
- **Spoofing IP**: pacchetti IP con indirizzi IP di origine apparentemente falsificati inviati con l'intento di nascondere l'identità del mittente o di simulare un altro sistema di elaborazione.
- **Tentativo di accesso non autorizzato**: tentativo di accesso alla rete rifiutato.
- **Ping of Death**: viene rilevato un ping in formato non corretto o dannoso inviato a un computer. Le dimensioni normali di un ping sono di 32 byte (o 84 se si considera l'intestazione IP o Internet Protocol); in genere, molti computer non sono in grado di gestire pacchetti ping di dimensioni superiori alla dimensione massima dei pacchetti IPv4 di 65.535 byte. L'invio di ping superiori alla dimensione massima può bloccare il computer di destinazione.
- **Win Nuke**: un attacco remoto di tipo DoS (denial-of-service) lanciato ai sistemi operativi Microsoft Windows 95, Microsoft Windows NT e Microsoft Windows 3.1x.
- **Criteri di rifiuto**: l'accesso è stato negato in base a criteri configurati.
- **Accesso autorizzato**: un utente autorizzato ha effettuato l'accesso alla rete.
- **Messaggi di errore del sistema**: vengono registrati i messaggi di errore del sistema.
- **Criteri di autorizzazione**: un utente autorizzato ha effettuato l'accesso alla rete mediante criteri configurati.
- **Kernel**: tutti i messaggi del kernel di sistema.
- **Modifiche configurazione**: istanze in cui è stata modificata la configurazione del dispositivo.
- **VPN PPTP e IPsec**: stato di negoziazione del tunnel VPN, connessione e disconnessione.

- **VPN SSL**: stato di negoziazione del tunnel SSL, connessione e disconnessione del tunnel SSL.
- **Rete**: indica se l'interfaccia WAN/DMZ è connessa o disconnessa.

Informazioni aggiuntive (pulsanti del log)

Se nel browser Web viene visualizzato un messaggio relativo alle finestre a comparsa, consentire il contenuto bloccato. Fare clic su **Aggiorna** per aggiornare i dati.

Fare clic sui pulsanti seguenti per visualizzare informazioni aggiuntive:

- **Visualizza log di sistema**: mostra il **log di sistema**. Per specificare un determinato log, selezionare un filtro dall'elenco a discesa.

  Le voci di log includono la data e l'ora dell'evento, il tipo di evento e un messaggio. Nel messaggio viene specificato il tipo di criterio, ad esempio Regola di accesso, l'indirizzo IP LAN di origine (SRC) e l'indirizzo MAC.
- **Tabella log in uscita**: informazioni sui pacchetti in uscita.
- **Tabella log in arrivo**: informazioni sui pacchetti in arrivo.
- **Cancella log**: fare clic su questo pulsante per cancellare il log e non inviarlo tramite e-mail; eseguire questa operazione solo se non si desidera visualizzare le informazioni in futuro.

Statistiche del sistema

Per accedere alle statistiche del sistema, selezionare **Log** > **Statistiche del sistema** nel riquadro di spostamento.

Vengono visualizzate informazioni dettagliate sulle porte e sui dispositivi collegati.

Processi

Per accedere alla pagina Processi, selezionare **Log** > **Processi** nel riquadro di spostamento.

Vengono visualizzate informazioni dettagliate sui processi in corso.

13

Gestione degli utenti

La gestione degli utenti consente di controllare il dominio e l'accesso da parte degli utenti; questa funzione viene utilizzata principalmente per PPTP e client VPN di Cisco (noto come EasyVPN).

Per accedere alla gestione degli utenti, selezionare **Gestione utenti** nel riquadro di spostamento.

Per aggiungere o modificare un dominio, attenersi alla seguente procedura:

PASSAGGIO 1 Fare clic su **Aggiungi** oppure selezionare la voce desiderata e fare clic su **Modifica**.

PASSAGGIO 2 Scegliere un'opzione dall'elenco **Tipo di autenticazione** e immettere le informazioni necessarie:

- **Database locale**: esegue l'autenticazione a fronte di un database locale.
  - **Dominio**: Nome del dominio selezionato dagli utenti per effettuare l'accesso.
- **Radius (PAP, CHAP, MSCHAP, MSCHAPv2)**: esegue l'autenticazione a un server RADIUS mediante i protocolli PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP (Microsoft Challenge Handshake Authentication Protocol) e MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2).
  - **Dominio**: Nome del dominio selezionato dagli utenti per effettuare l'accesso.
  - **Server RADIUS**: l'indirizzo IP del server RADIUS.
  - **Password Radius**: il *segreto* di autenticazione.

- Active Directory: autenticazione Active Directory di Windows. Con l'autenticazione Active Directory è molto facile commettere errori. Se non è possibile autenticarsi tramite Active Directory, leggere la procedura per la risoluzione dei problemi alla fine di questa sezione.
  - **Dominio**: Nome del dominio selezionato dagli utenti per effettuare l'accesso.
  - **Indirizzo server AD**: indirizzo IPv4 del server Active Directory.
  - **Nome dominio AD**: il nome di dominio del server Active Directory.
- **LDAP**: Lightweight Directory Access Protocol.
  - **Dominio**: Nome del dominio selezionato dagli utenti per effettuare l'accesso.
  - **Indirizzo server LDAP**: l'indirizzo IPv4 del server LDAP.
  - **DN base LDAP**: la base di ricerca per le query LDAP. Esempio di stringa della base di ricerca: `CN=Users,DC=dominio,DC=com`.

PASSAGGIO 3 Fare clic su **OK**.

Per aggiungere o modificare un utente, fare clic su **Aggiungi** oppure selezionare la voce desiderata e fare clic su **Modifica**, quindi immettere le seguenti informazioni:

- **Nome utente**: il nome inserito dall'utente per accedere al portale VPN SSL.
- **Password**: la password utilizzata per l'autenticazione.
- **Gruppo**: Il gruppo Non assegnato include gli utenti VPN PPTP ed EasyVPN. Il gruppo Amministratore contiene un solo utente; il nome utente predefinito del gruppo Amministratore è **cisco**.
- **Dominio**: il nome del dominio indicato nella tabella Gestione domini.

14

Filtri Web

I filtri Web possono proteggere dall'accesso ai siti Web inappropriati, in base al meccanismo di funzionamento indicato di seguito.

PASSAGGIO 1 Se l'URL in arrivo è presente nell'**Elenco di esclusione** e il relativo valore dell'indice di **Reputazione Web** non è inferiore a 40, l'URL è sicuro e consentito e viceversa.

PASSAGGIO 2 Se l'URL in arrivo non è incluso nell'**Elenco di esclusione**, verificare se è contenuto nella **Black list**. In tal caso, l'URL viene bloccato. Se non è presente nella **Black list**, verificarne la presenza nella **White list**.

PASSAGGIO 3 Se è presente nella **White list**, l'URL in arrivo è consentito. In caso contrario, verificare la categoria Web.

PASSAGGIO 4 Se l'URL appartiene agli elementi selezionati della categoria, è bloccato. In caso contrario, verificare la **Reputazione Web**.

PASSAGGIO 5 Se il valore dell'indice di reputazione è superiore a 40, è consentito e viceversa.

Filtri Web: per applicare sempre i filtri Web, fare clic su **Sempre attivi**. Per applicare i filtri Web secondo le pianificazioni, fare clic su **Pianificati**. Per disabilitare tale funzione, fare clic su **Sempre disattivati** e su **Salva**.

Reputazione Web: selezionare **Reputazione Web** per abilitare l'analisi della reputazione Web.

Categorie: fare clic su **Categorie** e si aprirà la pagina delle categorie dei filtri Web. Selezionare **Alta**, **Media**, **Bassa** o **Personalizzata** per definire rapidamente l'ampiezza del filtro. Inoltre, è possibile scegliere gli elementi dalle categorie **Contenuti per adulti/per soli adulti**, **Business/Investimenti**, **Svago**, **Illegale/opinabile**, **Risorse IT**, **Stile di vita/cultura**, **Altro** e **Sicurezza**. Gli URL in arrivo appartenenti agli elementi selezionati sono bloccati. Fare clic su **Salva** e su **Torna** alla pagina dei filtri Web.

Eccezioni: fare clic su **Eccezioni** e si aprirà la pagina della **White list**, della **Black list** e dell'**Elenco di esclusione**. In ogni campo dell'elenco, selezionare il **Tipo** di meccanismo di filtro dal menu a discesa e immettere il **valore** per aggiungere/modificare un elemento. Fare clic su **Salva** e su **Torna** alla pagina dei filtri Web.

Elenco di pianificazione: per aggiungere e visualizzare le pianificazioni relative all'applicazione di filtri Web.

- Fare clic su **Aggiungi** e immettere il valore dei campi.
  - **Nome:** il nome della pianificazione.
  - **Descrizione:** la descrizione della pianificazione.
  - Verificare le date di implementazione della pianificazione.
  - **Inizio:** l'ora di inizio della pianificazione.
  - **Fine:** l'ora di fine della pianificazione.
  - **Attiva:** selezionare questa opzione per attivare la pianificazione.
  - Fare clic su **Salva** per salvare la configurazione.

15

Risorse aggiuntive

Supporto	
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 relativo ai prodotti Cisco. Dati di accesso non richiesti.
Richiesta 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 e firewall Cisco	www.cisco.com/go/smallbizrouters

Per i risultati dei test relativi a EU Lot 26, visitare il sito www.cisco.com/go/eu-lot26-results

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Copyright © 2018

15