ADMINISTRATOR-HANDBUCH

Cisco RV130 Multifunktions-VPN-Router

Cisco RV130W Wireless-Multifunktions-VPN-Router

Inhalt

1

Erste Schritte

Auf der Seite **Erste Schritte** werden die am häufigsten anfallenden Konfigurationsaufgaben für das Gerät angezeigt. Klicken Sie auf der Webseite auf die Links, um die entsprechende Konfigurationsseite aufzurufen.

Diese Seite wird bei jedem Start des Gerätemanagers angezeigt. Wenn Sie dies ändern möchten, aktivieren Sie **Nicht beim Start anzeigen**.

Anfangseinstellungen

Vorgegebenes Administratorkennwort ändern	Zeigt die Seite **Benutzer** an. Hier können Sie das Administratorkennwort ändern und ein Gastkonto einrichten. Weitere Informationen hierzu finden Sie unter **Konfigurieren von Benutzerkonten**.
Einrichtungsassistent starten	Startet den Setup-Assistenten. Befolgen Sie die Anweisungen auf dem Bildschirm.
WAN-Einstellungen konfigurieren	Die Seite **WAN-Konfiguration** wird geöffnet, auf der Sie Parameter ändern können. Beispiel: Hostname des Geräts. Weitere Informationen hierzu finden Sie unter **Konfigurieren von drahtgebundenen WAN-Verbindungen**.
LAN-Einstellungen konfigurieren	Die Seite **LAN-Konfiguration** wird geöffnet, auf der Sie LAN-Parameter ändern können. Beispiel: IP-Verwaltungsadresse. Weitere Informationen hierzu finden Sie unter **Konfigurieren der LAN-Einstellungen**.
WLAN-Einstellungen konfigurieren	Öffnet die Seite **Basiseinstellungen**, auf der Sie die Funkverbindung (Wi-Fi) verwalten können. Weitere Informationen hierzu finden Sie unter **Konfigurieren von WLANs**.

Schnellzugriff

Firmware des Routers aktualisieren	Die Seite **Firmware-/Sprach-Upgrade** wird geöffnet, auf der Sie die Firmware und das Sprachpaket für das Gerät aktualisieren können. Weitere Informationen hierzu finden Sie unter **Aktualisieren der Firmware oder Ändern der Sprache**.
VPN-Clients hinzufügen	Die Seite **PPTP-Server** wird geöffnet, auf der Sie VPN-Tunnel einrichten und verwalten können. Weitere Informationen hierzu finden Sie unter **Konfigurieren von PPTP**.
Remoteverwaltungszugriff konfigurieren	Die Seite **Basiseinstellungen** wird geöffnet, auf der Sie die Basisfunktionen des Geräts aktivieren können. Weitere Informationen hierzu finden Sie unter **Konfigurieren der grundlegenden Firewalleinstellungen**.

Gerätestatus

Systemübersicht	Die Seite **Systemübersicht** wird angezeigt, auf der Sie den Status der Firmware, der IPv4- und IPv6-Konfiguration, der WLAN-Verbindung und der Firewall auf dem Gerät ermitteln können. Weitere Informationen hierzu finden Sie unter **Anzeigen der Systemzusammenfassung**.
WLAN-Status	Zeigt die **WLAN-Statistik** an, auf der der Funkstatus aufgeführt wird. Weitere Informationen hierzu finden Sie unter **Anzeigen von WLAN-Statistiken**.
VPN-Status	Die Seite **IPSec-VPN-Server** wird angezeigt, auf der Sie das von diesem Gerät verwaltete VPN ermitteln können. Weitere Informationen hierzu finden Sie unter **Anzeigen des Status von Site-to-Site-IPSec-VPN-Verbindungen**.

Andere Ressourcen

Support	Klicken Sie auf diese Option, um die Supportseite von Cisco zu öffnen.
Foren	Klicken Sie auf diese Option, um die Online-Supportforen von Cisco zu besuchen.

Verbinden von Geräten mit dem WLAN

Um ein Clientgerät (beispielsweise einen Computer) mit dem WLAN zu verbinden, müssen Sie die WLAN-Verbindung auf dem Clientgerät mit den Informationen zur WLAN-Sicherheit konfigurieren, die Sie mithilfe des Setup-Assistenten für den Router konfiguriert haben.

Die folgenden Schritte sollen als Beispiel dienen. Möglicherweise müssen Sie Ihr Gerät anders konfigurieren. Nähere Anweisungen finden Sie in der Dokumentation zum Clientgerät.

SCHRITT 1 Öffnen Sie für Ihr Gerät das Fenster oder das Programm mit den Einstellungen für die WLAN-Verbindung.

Möglicherweise ist auf Ihrem Computer eine spezielle Software zur Verwaltung von WLAN-Verbindungen installiert, oder Sie finden Angaben zu WLAN-Verbindungen in der Systemsteuerung unter **Netzwerkverbindungen** oder **Netzwerk und Internet**. (Wie Sie auf diese Einstellungen zugreifen, hängt vom jeweiligen Betriebssystem ab.)

SCHRITT 2 Geben Sie den Netzwerknamen (SSID) ein, den Sie im Setup-Assistenten für das Netzwerk ausgewählt haben.

SCHRITT 3 Wählen Sie den Verschlüsselungstyp aus und geben Sie den Sicherheitsschlüssel ein, den Sie im Setup-Assistenten angegeben haben.

Wenn Sie die Sicherheit nicht aktiviert haben (nicht empfohlen), lassen Sie die Felder für die Verschlüsselung der WLAN-Verbindung, die mit dem Sicherheitstyp und dem Kennwort konfiguriert wurden, leer.

SCHRITT 4 Überprüfen Sie Ihre WLAN-Verbindung und speichern Sie Ihre Einstellungen.

2

Anzeigen des Gerätestatus

Damit Daten und Statistiken auf den Seiten unter „Status“ häufig aktualisiert werden, wählen Sie in der Dropdown-Liste **Aktualisierungsrate** eine entsprechende Rate aus.

Anzeigen des Dashboards

Wählen Sie **Status** > **Dashboard** aus, um eine Momentaufnahme der Gerätekonfiguration anzuzeigen. Auf der Seite „Dashboard“ werden Informationen zur Firmwareversion, zur CPU- und Speicherauslastung sowie zu den Einstellungen für Fehlerprotokolle, LAN, WAN, WLAN, Site-to-Site-IPSec-VPN und PPTP-VPN-Server des Geräts angezeigt.

Um die angezeigten Informationen zu ändern, klicken Sie auf den Link **Details**, um die Konfigurationsseite für den entsprechenden Abschnitt aufzurufen. Weitere Informationen zum Verwalten der auf der Seite **Dashboard** angezeigten Einstellungen finden Sie in den folgenden Abschnitten:

- **Konfigurieren von Protokolleinstellungen**
- **Konfigurieren grundlegender Einstellungen für ein Site-to-Site-IPSec-VPN**
- **Konfigurieren der LAN-Einstellungen**
- **Konfigurieren von drahtgebundenen WAN-Verbindungen**
- **Konfigurieren der Basis-WLAN-Einstellungen**

Wählen Sie in der Dropdown-Liste **Aktualisierungsrate** die Rate aus, mit der die aktuellen Statistiken und Parameterwerte auf dem Dashboard aktualisiert werden sollen.

Auf der Seite „Dashboard“ wird außerdem eine interaktive Ansicht der Geräterückseite angezeigt, wenn Sie auf **Panelansicht anzeigen** klicken. Bewegen Sie den Mauszeiger über einen Anschluss, um die Verbindungsinformationen für den Anschluss anzuzeigen.

Anzeigen der Systemzusammenfassung

Wählen Sie **Status** > **Systemübersicht** aus, um Details zu den Geräteeigenschaften, den Netzwerkeinstellungen für alle IP-Adressmodi sowie den Firewall-, WLAN- und VPN-Einstellungen anzuzeigen. Klicken Sie auf **Aktualisieren**, um die aktuellen Informationen anzuzeigen.

Klicken Sie auf den unterstrichenen Link, um das entsprechende Konfigurationsfenster aufzurufen. Wenn Sie z. B. die LAN-IP-Adresse ändern möchten, klicken Sie auf **LAN-IP**. Das Fenster „LAN-Konfiguration“ wird angezeigt.

Auf der Seite **Systemübersicht** werden Informationen in den folgenden Abschnitten angezeigt:

Systeminformationen

- **Firmwareversion**: Die zurzeit auf dem Gerät ausgeführte Softwareversion.
- **Firmware-MD5-Prüfsumme**: Der MD5-Algorithmus, der zum Überprüfen der Integrität von Dateien verwendet wird.
- **Gebietsschema**: Die im Router installierte Sprache.
- **Sprachversion**: Die Version des installierten Sprachpakets. Die Sprachpaketversion sollte mit der zurzeit installierten Firmware kompatibel sein. In manchen Fällen kann ein älteres Sprachpaket mit einem neueren Firmware-Image verwendet werden. Der Router überprüft, ob die Sprachpaketversion mit der aktuellen Firmwareversion kompatibel ist.
- **Sprach-MD5-Prüfsumme**: MD5-Prüfsumme des Sprachpakets.
- **CPU-Modell**: Der zurzeit verwendete CPU-Chipsatz.
- **Seriennummer**: Die Seriennummer des Geräts.
- **Systembetriebszeit**: Betriebsdauer des Systems.
- **Aktuelle Zeit**: Die Tageszeit.
- **PID VID**: Die Produkt-ID und Versions-ID des Geräts.

IPv4-Konfiguration

- **LAN-IP**: LAN-IP-Adresse des Geräts.
- **WAN-IP**: WAN-IP-Adresse des Geräts. Um die aktuelle IP-Adresse freizugeben und eine neue zu beziehen, klicken Sie auf **Freigeben** oder **Erneuern**.
- **Gateway**: IP-Adresse des Gateways, mit dem das Gerät verbunden ist (beispielsweise das Kabelmodem).
- **Modus**: Zeigt **Gateway** an, wenn NAT aktiviert ist, oder **Router**.
- **DNS 1**: Die IP-Adresse des primären DNS-Servers des WAN-Anschlusses.
- **DNS 2**: Die IP-Adresse des sekundären DNS-Servers des WAN-Anschlusses.
- **DDNS**: Gibt an, ob Dynamic DNS aktiviert oder deaktiviert ist.

IPv6-Konfiguration

- **LAN-IP**: LAN-IP-Adresse des Geräts.
- **WAN-IP**: WAN-IP-Adresse des Geräts.
- **Gateway**: IP-Adresse des Gateways, mit dem das Gerät verbunden ist (beispielsweise das Kabelmodem).
- **NTP**: Network Time Protocol-Server (Hostname oder IPv6-Adresse).
- **Präfix-Delegation**: Präfix, das vom Gerät des ISPs zurückgegeben und an IPv6-Adressen auf dem Gerät vergeben wird.
- **DNS 1**: IP-Adresse des primären DNS-Servers.
- **DNS 2**: IP-Adresse des sekundären DNS-Servers.

WLAN-Übersicht

Öffentlicher Name und Sicherheitseinstellungen für die WLANs, die auf der Seite **WLAN > Basiseinstellungen** konfiguriert sind. Weitere Informationen finden Sie unter **Konfigurieren der Basis-WLAN-Einstellungen**.

Firewall-Einstellungsstatus

Einstellungen zu DoS, WAN-Anfragen und Remoteverwaltung, die auf der Seite **Firewall > Basiseinstellungen** konfiguriert sind. Weitere Informationen finden Sie unter **Konfigurieren der grundlegenden Firewalleinstellungen**.

VPN-Einstellungsstatus

Verfügbare IPSec- und PPTP-VPN-Verbindungen sowie die verbundenen Benutzer für jeden VPN-Typ.

- **IPSec-VPN-Verbindungen verfügbar**: Anzahl der verfügbaren IPSec-VPN-Verbindungen.
- **PPTP-VPN-Verbindungen verfügbar**: Anzahl der verfügbaren PPTP-VPN-Verbindungen.
- **Verbundene IPSec-VPN-Benutzer**: Anzahl der verbundenen IPSec-VPN-Benutzer.
- **Verbundene PPTP-VPN-Benutzer**: Anzahl der verbundenen PPTP-VPN-Benutzer.

Weitere Informationen zum Konfigurieren von VPN-Serververbindungen und -Benutzerkonten finden Sie unter **Konfigurieren grundlegender Einstellungen für ein Site-to-Site-IPSec-VPN** und **Konfigurieren von PPTP**.

Anzeigen aktiver TCP/IP-Services

Wählen Sie **Status > Aktive TCP/IP-Services** aus, um aktive IPv4- und IPv6-TCP/IP-Verbindungen auf dem Gerät anzuzeigen. In der **Liste der aktiven Services** für IPv4 und IPv6 werden die aktiven Protokolle und Services auf dem Gerät angezeigt.

Anzeigen von WLAN-Statistiken

Wählen Sie **Status > WLAN-Statistik** aus, um statistische Daten für den WLAN-Sender des Geräts anzuzeigen. Wählen Sie im Feld **Aktualisierungsrate** die Rate aus, mit der die aktuellen Statistiken angezeigt werden sollen.

Um die Bytes in Kilobyte (KB) und die numerischen Daten als gerundete Werte anzuzeigen, aktivieren Sie das Kontrollkästchen **Vereinfachte Statistik anzeigen**, und klicken Sie auf **Speichern**. Standardmäßig werden Byte-Daten in Bytes und andere numerische Daten im Langformat angezeigt.

Zum Zurücksetzen der Zähler der WLAN-Statistik klicken Sie auf **Zähler löschen**. Die Zähler werden zurückgesetzt, wenn das Gerät neu gestartet wird.

Anzeigen des Captive Portal-Status

Wählen Sie **Status > Captive Portal-Status** aus, um Informationen zu den verbundenen Captive Portal-Benutzern anzuzeigen. Weitere Informationen zum Konfigurieren von Captive Portals auf dem Gerät finden Sie unter **Konfigurieren eines Captive Portal**.

Anzeigen des Status von Site-to-Site-IPSec-VPN-Verbindungen

Wählen Sie **Status > Site-to-Site-IPSec-VPN** aus, um den Verbindungsstatus aktiver Site-to-Site-IPSec-VPN-Richtlinien auf dem Gerät anzuzeigen. Informationen zum Konfigurieren von VPN-Richtlinien finden Sie unter **Konfigurieren grundlegender Einstellungen für ein Site-to-Site-IPSec-VPN**.

Um die Rate zu ändern, mit der der aktuelle Verbindungsstatus in Echtzeit angezeigt wird, wählen Sie in der Dropdown-Liste **Aktualisierungsrate** eine Rate aus.

Standardmäßig werden Byte-Daten in Bytes und andere numerische Daten im Langformat angezeigt. Um die Bytes in Kilobyte (KB) und die numerischen Daten im gerundeten Format anzuzeigen, aktivieren Sie das Kontrollkästchen **Vereinfachte Statistik anzeigen**, und klicken Sie auf **Speichern**.

Zum Beenden einer aktiven VPN-Verbindung klicken Sie auf **Trennen**.

Anzeigen des IPSec-VPN-Serverstatus

Wählen Sie **Status > IPSec-VPN-Server** aus, um eine Liste der IPSec-VPN-Verbindungen und ihrer jeweiligen Dauer anzuzeigen. Weitere Informationen zum Konfigurieren von IPSec-VPN-Verbindungen finden Sie unter **Konfigurieren des IPSec-VPN-Servers**.

Anzeigen des PPTP-Serverstatus

Wählen Sie **Status > PPTP-Server**, um eine Liste der PPTP-VPN-Verbindungen, ihrer jeweiligen Dauer und den jeweils möglichen Aktionen anzuzeigen. Weitere Informationen zum Konfigurieren von PPTP-VPN-Verbindungen finden Sie unter **Konfigurieren von PPTP**.

Anzeigen von Protokollen

Wählen Sie **Status > Protokolle anzeigen** aus. Klicken Sie auf **Protokolle aktualisieren**, um die neuesten Protokolleinträge anzuzeigen.

Zum Filtern der Protokolle oder zum Angeben des Schweregrads der anzuzeigenden Protokolle aktivieren Sie die Kontrollkästchen neben dem Protokolltyp und klicken auf **Los**. Beachten Sie, dass alle Protokolltypen über einem ausgewählten Protokolltyp automatisch enthalten sind und dass Sie diese Auswahl nicht aufheben können. Beispiel: Mit dem Kontrollkästchen **Fehler** werden neben Protokollen des Typs „Fehler“ automatisch auch Protokolle der Typen „Notfall“, „Alarm“ und „Kritisch“ ausgewählt.

Es stehen die folgenden Schweregrade für Ereignisse zur Verfügung, aufgelistet von der höchsten bis zur niedrigsten Gewichtung:

- **Notfall**: Das System kann nicht verwendet werden.
- **Alarm**: Es ist eine Aktion erforderlich.
- **Kritisch**: Das System befindet sich in einem kritischen Zustand.
- **Fehler**: Das System befindet sich im Fehlerzustand.
- **Warnung**: Es ist eine Systemwarnung aufgetreten.
- **Benachrichtigung**: Das System funktioniert ordnungsgemäß, es ist jedoch ein Systemhinweis aufgetreten.
- **Informationen**: Geräteinformationen.
- **Fehlerbehebung**: Bietet detaillierte Informationen zu einem Ereignis.

Wenn Sie alle Einträge im Protokollfenster löschen möchten, klicken Sie auf **Protokolle löschen**.

Um alle Protokollmeldungen des Geräts auf der lokalen Festplatte zu speichern, klicken Sie auf **Protokolle speichern**.

Wenn Sie die Anzahl der Einträge angeben möchten, die pro Seite angezeigt werden sollen, wählen Sie im Dropdown-Menü eine Anzahl aus.

Über die Schaltflächen für die Seitennavigation können Sie zwischen den Protokollseiten wechseln.

Anzeigen von verbundenen Geräten

Auf der Seite **Verbundene Geräte** werden Informationen zu den mit dem Router verbundenen aktiven Clientgeräten angezeigt. Zum Anzeigen von verbundenen Geräten wählen Sie die Optionen **Status** > **Verbundene Geräte** aus.

Um die Typen der anzuzeigenden Schnittstellen anzugeben, wählen Sie im Dropdown-Menü **Filter** einen Wert aus.

- **Alle**: Alle mit dem Router verbundenen Geräte.
- **WLAN**: Alle Geräte, die über die drahtlose Schnittstelle verbunden sind.
- **Kabel**: Alle über die Ethernet-Anschlüsse am Router verbundenen Geräte.
- **WDS**: Alle mit dem Router verbundenen WDS-Geräte (Wireless Distribution System).

IPv4-ARP-Tabelle: Informationen anderer Router, die auf die ARP-Anfrage (Address Resolution Protocol) des Geräts geantwortet haben. Wenn ein Gerät auf die Anforderung nicht antwortet, wird es aus der Liste entfernt.

IPv6-NDP-Tabelle: Alle IPv6-NDP-Geräte (Neighbor Discovery Protocol), die lokal mit dem Gerät verbunden sind.

Anzeigen von Anschlussstatistiken

Auf der Seite **Anschlussstatistik** werden detaillierte Anschlussaktivitäten angezeigt.

Zum Anzeigen der Anschlussstatistiken wählen Sie die Optionen **Status > Anschlussstatistik** aus.

Damit die Seite regelmäßig aktualisiert wird, wählen Sie in der Dropdown-Liste **Aktualisierungsrate** eine entsprechende Rate aus.

Um die Bytes in Kilobyte (KB) und die numerischen Daten im gerundeten Format anzuzeigen, aktivieren Sie das Kontrollkästchen **Vereinfachte Statistik anzeigen**, und klicken Sie auf **Speichern**. Standardmäßig werden Byte-Daten in Bytes und andere numerische Daten im Langformat angezeigt.

Zum Zurücksetzen der Zähler der Anschlussstatistik klicken Sie auf **Zähler löschen**.

Auf der Seite **Anschlussstatistik** werden folgende Informationen angezeigt:

Schnittstelle	Name der Netzwerkschnittstelle.
Paket	Anzahl der empfangenen und gesendeten Pakete.
Byte	Anzahl der pro Sekunde empfangenen und gesendeten Datenbytes.
Fehler	Anzahl der empfangenen und gesendeten Paketfehler.
Gelöscht	Anzahl der empfangenen und gesendeten Pakete, die gelöscht wurden.
Multicast	Anzahl der über diesen Sender gesendeten Multicast-Pakete.
Kollisionen	Anzahl der an diesem Anschluss aufgetretenen Signalkollisionen. Eine Kollision tritt auf, wenn der Anschluss zum gleichen Zeitpunkt wie ein Anschluss an einem anderen Router oder Computer, der mit diesem Anschluss verbunden ist, Daten zu senden versucht.

Anzeigen des Status des mobilen Netzwerks

Die Statistiken zum mobilen 3G/4G-Netzwerk und zum auf dem Gerät konfigurierten Kommunikationsgerät (Dongle).

Zum Anzeigen des Status des mobilen Netzwerks wählen Sie **Status > Mobiles Netzwerk** aus. Die folgenden Informationen werden angezeigt:

- **Verbindung**: Das mit dem Gastnetzwerk verbundene Gerät.
- **WAN-IP-Adresse**: Die dem USB-Gerät zugewiesene IP-Adresse.
- **Subnetzmaske**: Subnetzmaske des USB-Geräts.
- **Standardgateway**: IP-Adresse des Standardgateways.
- **Aktive Verbindungszeit**: Dauer der aktiven Verbindung.
- **Aktuelle Sitzungsverwendung**: Datenvolumen, das von der mobilen Verbindung empfangen (Rx) und dorthin übertragen (Tx) wurde.
- **Monatliche Nutzung**: Monatliche Statistiken zu Datendownloads und Bandbreitennutzung.

- **Hersteller**: Name des Herstellers der Karte.
- **Kartenmodell**: Nummer des Kartenmodells.
- **Karten-Firmware**: Version der Karten-Firmware.
- **SIM-Status**: SIM-Status (Subscriber Identification Module).
- **IMSI**: Die eindeutige Identifizierung, die den Benutzern von Mobiltelefonen im GSM-, UMTS- oder LTE-Netzwerk zugeordnet ist.
- **Anbieter**: Anbieter des mobilen Netzwerks.
- **Diensttyp**: Art des Dienstes, auf den zugegriffen wird.
- **Signalstärke**: Stärke des Signals des drahtlosen mobilen Netzwerks.
- **Kartenstatus**: Status der Datenkarte.

3

Konfigurieren der Netzwerkfunktionen

Konfigurieren von drahtgebundenen WAN-Verbindungen

Auf welche Weise Sie die WAN-Eigenschaften für ein IPv4-Netzwerk konfigurieren, hängt vom Typ der Internetverbindung ab.

Konfigurieren von DHCP (Automatische Konfiguration)

Wenn Ihr Internet Service Provider (ISP) Ihnen über DHCP (Dynamic Host Control Protocol) eine IP-Adresse zuweist, erhalten Sie eine IP-Adresse, die bei jeder Anmeldung dynamisch generiert wird.

So konfigurieren Sie die DHCP-WAN-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie in der Dropdown-Liste **Internetverbindungstyp** die Option **Automatische Konfiguration (DHCP)** aus.

SCHRITT 3 Wählen Sie in der Dropdown-Liste **DNS-Serverquelle** eine der folgenden Methoden zum Festlegen der DNS-Serveradresse aus:

- Wenn Sie bereits DNS-Serveradressen von Ihrem ISP erhalten haben, wählen Sie **Diese DNS-Server verwenden** aus, und geben Sie die Adressen des primären und des sekundären DNS-Servers ein.
- Wenn Sie noch keine DNS-Serveradressen von Ihrem ISP erhalten haben, wählen Sie **Dynamisch vom Internetdienstanbieter abrufen** aus.
- Um Webadressen über die von OpenDNS bereitgestellten DNS-Server (208.67.222.222, 208.67.220.220) aufzulösen, wählen Sie **OpenDNS verwenden** aus.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von statischen IP-Adressen

Wenn Ihnen der ISP eine permanente IP-Adresse zugewiesen hat, führen Sie die folgenden Schritte aus, um die WAN-Einstellungen zu konfigurieren:

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Internetverbindungstyp** die Option **Statische IP-Adresse** aus.

SCHRITT 3 Geben Sie folgende Informationen ein:

WAN-IP-Adresse	IP-Adresse des WAN-Anschlusses.
Subnetzmaske	Subnetzmaske des WAN-Anschlusses.
DNS-Serverquelle	Die Adresse des DNS-Servers. Wenn Sie bereits DNS-Serveradressen von Ihrem ISP erhalten haben, wählen Sie **Diese DNS-Server verwenden** aus, und geben Sie die Adressen des primären und des sekundären DNS-Servers in die Felder **Statischer DNS 1** und **Statischer DNS 2** ein. Um Webadressen über die von OpenDNS bereitgestellten DNS-Server (208.67.222.222, 208.67.220.220) aufzulösen, wählen Sie **OpenDNS verwenden** aus.
Standardgateway	IP-Adresse des Standardgateways.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von PPPoE

So konfigurieren Sie die PPPoE-Einstellungen (Point-to-Point Protocol over Ethernet):

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Internetverbindungstyp** die Option **PPPoE** aus.

SCHRITT 3 Wählen Sie ein PPPoE-Profil aus, oder klicken Sie auf **Profil konfigurieren**, um ein neues Profil zu erstellen.

SCHRITT 4 Geben Sie auf der Seite „PPPoE-Profile“ die folgenden Informationen ein (möglicherweise müssen Sie die PPPoE-Anmeldeinformationen bei Ihrem ISP erfragen):

Profilname	Ein eindeutiger Name für das PPPoE-Profil.
Benutzername	Der vom ISP zugewiesene Benutzername.
Kennwort	Das vom ISP zugewiesene Kennwort.
DNS-Serverquelle	Die Adresse des DNS-Servers. Wenn Sie bereits DNS-Serveradressen von Ihrem ISP erhalten haben, wählen Sie **Diese DNS-Server verwenden** aus, und geben Sie die Adressen des primären und des sekundären DNS-Servers ein. Wählen Sie anderenfalls **Dynamisch vom Internetdienstanbieter abrufen** aus. Um Webadressen über die von OpenDNS bereitgestellten DNS-Server (208.67.222.222, 208.67.220.220) aufzulösen, wählen Sie **OpenDNS verwenden** aus.
Verbindung bei Bedarf herstellen	Wählen Sie diese Option aus, wenn Ihnen der ISP die Dauer der Verbindung in Rechnung stellt. Wenn Sie diese Option auswählen, ist die Internetverbindung nur aktiv, wenn Daten übertragen werden. Wenn sich die Verbindung im Leerlauf befindet (das heißt, wenn kein Verkehr fließt), wird die Verbindung getrennt. Wenn Sie auf **Verbindung bei Bedarf** klicken, geben Sie in das Feld **Max. Leerlaufzeit** ein, nach wie vielen Minuten, die Verbindung getrennt wird.
Keep-Alive	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld „Wahlwiederholung nach X Sekunden“ die Wartezeit in Sekunden ein, nach der das Gerät versuchen soll, eine getrennte Verbindung wiederherzustellen.

Authentifizierungstyp	**Automatisch aushandeln**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Das Gerät sendet die Anmeldeinformationen mit dem vom Server gesendeten Sicherheitstyp zurück. **PAP**: Das Password Authentication Protocol (PAP) wird von PPP (Point-to-Point Protocol) verwendet, um eine Verbindung zum ISP herzustellen. **CHAP**: Das Challenge Handshake Authentication Protocol (CHAP) erfordert, dass sowohl der Client als auch der Server den geheimen Schlüssel zur Verwendung der Dienste des ISPs kennen. **MS-CHAP oder MS-CHAPv2**: Die Microsoft-Version von CHAP, die für den Zugriff auf die Dienste des ISPs verwendet wird.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von PPTP

So konfigurieren Sie die PPTP-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Internetverbindungstyp** die Option **PPTP** aus.

SCHRITT 3 Geben Sie folgende Informationen ein:

WAN-IP-Adresse	IP-Adresse des WAN-Anschlusses.
Subnetzmaske	Subnetzmaske des WAN-Anschlusses.
Standardgateway	IP-Adresse des Standardgateways.
PPTP-Server	IP-Adresse des PPTP-Servers (Point-to-Point Tunneling Protocol).
Benutzername	Der Ihnen vom ISP zugewiesene Benutzername.
Kennwort	Das Ihnen vom ISP zugewiesene Kennwort.

Verbindung bei Bedarf herstellen	Wählen Sie diese Option aus, wenn Ihnen der ISP die Dauer der Verbindung in Rechnung stellt. Wenn Sie diese Option auswählen, ist die Internetverbindung nur aktiv, wenn Daten übertragen werden. Wenn sich die Verbindung im Leerlauf befindet (das heißt, wenn kein Verkehr fließt), wird die Verbindung getrennt. Wenn Sie auf **Verbindung bei Bedarf herstellen** klicken, geben Sie in das Feld **Max. Leerlaufzeit** ein, nach wie vielen Minuten, die Verbindung getrennt wird.
Keep-Alive	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld **Wahlwiederholung nach X Sekunden** die Wartezeit in Sekunden ein, nach der das Gerät versuchen soll, eine getrennte Verbindung wiederherzustellen.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus: **Automatisch aushandeln**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Das Gerät sendet daraufhin Anmeldeinformationen mit dem vorher vom Server gesendeten Sicherheitstyp zurück. **PAP**: Das Gerät verwendet PAP (Password Authentication Protocol) zum Herstellen der Verbindung mit dem ISP. **CHAP**: Das Gerät verwendet CHAP (Challenge Handshake Authentication Protocol) zum Herstellen der Verbindung mit dem ISP. **MS-CHAP oder MS-CHAPv2**: Das Gerät verwendet das Microsoft Challenge Handshake Authentication-Protokoll zum Herstellen der Verbindung mit dem ISP.
Dienstname	Geben Sie einen Namen für den neuen PPTP-Dienst ein.

MPPE-Verschlüsselung	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um Microsoft Point-to-Point Encryption für die PPTP-Verbindung zu aktivieren.
DNS-Serverquelle	Die Adresse des DNS-Servers. Wenn Sie bereits DNS-Serveradressen von Ihrem ISP erhalten haben, wählen Sie **Diese DNS-Server verwenden** aus, und geben Sie die Adressen des primären und des sekundären DNS-Servers in die Felder **Primärer DNS-Server** und **Sekundärer DNS-Server** ein. Um die DNS-Serveradressen von Ihrem ISP zu beziehen, wählen Sie **Dynamisch vom Internetdienstanbieter abrufen** aus. Um Webadressen über die von OpenDNS bereitgestellten DNS-Server (208.67.222.222, 208.67.220.220) aufzulösen, wählen Sie **OpenDNS verwenden** aus.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von L2TP

So konfigurieren Sie die L2TP-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Internetverbindungstyp** die Option **L2TP** aus.

SCHRITT 3 Geben Sie folgende Informationen ein:

WAN-IP-Adresse	Die IP-Adresse des WAN-Anschlusses.
Subnetzmaske	Die Subnetzmaske des WAN-Anschlusses.
Standardgateway	Die IP-Adresse des Standardgateways.
L2TP-Server	Die IP-Adresse des L2TP-Servers.

Version	Die L2TP-Version, die verwendet werden soll. Wenn Sie Version 3 auswählen, geben Sie die Anbieter-ID und die virtuelle Verbindungs-ID ein.
Cookie-Länge	Die Größe des Cookies im Datenpaket von L2TP-Version 3, das die L2TP-Sitzung angibt.
Anbieter-ID	Die im Codierungsformat des Attribut-Wert-Paars für L2TP enthaltene Anbieter-ID. Um die Attributwerte der IETF in dem Attribut-Wert-Paar zu verwenden, wählen Sie „Standard“ aus. Um die L2TP-Erweiterungen und privaten Attributwerte von Cisco zu verwenden, wählen Sie „Cisco“ aus.
Virtuelle Verbindungs-ID	Die ID für die Schicht 2-Verbindung, über die L2TP-Datenpakete übertragen werden. Diese Angabe ist obligatorisch, wenn Sie „Cisco“ als **Anbieter-ID** für L2TP-Version 3 ausgewählt haben.
Benutzername	Geben Sie den Benutzernamen ein, der Ihnen vom ISP zugewiesen wurde.
Kennwort	Geben Sie das Kennwort ein, das Ihnen vom ISP zugewiesen wurde.
Verbindung bei Bedarf herstellen	Wählen Sie diese Option aus, wenn Ihnen der ISP die Dauer der Verbindung in Rechnung stellt. Wenn Sie diese Option auswählen, ist die Internetverbindung nur aktiv, wenn Daten übertragen werden. Wenn sich die Verbindung im Leerlauf befindet (das heißt, wenn kein Verkehr fließt), wird die Verbindung getrennt. Wenn Sie auf **Verbindung bei Bedarf** klicken, geben Sie in das Feld **Max. Leerlaufzeit** ein, nach wie vielen Minuten, die Verbindung getrennt wird.
Keep-Alive	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld „Wahlwiederholung nach X Sekunden“ die Wartezeit in Sekunden ein, nach der das Gerät versuchen soll, eine getrennte Verbindung wiederherzustellen.

Authentifizierungstyp	**Automatisch aushandeln**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Das Gerät sendet die Anmeldeinformationen mit dem vom Server gesendeten Sicherheitstyp zurück. **PAP**: Password Authentication Protocol (PAP), wird verwendet, um eine Verbindung zum ISP herzustellen. **CHAP**: CHAP (Challenge Handshake Authentication Protocol) wird verwendet, um eine Verbindung zum ISP herzustellen. **MS-CHAP oder MS-CHAPv2**: Das Microsoft Challenge Handshake Authentication-Protokoll wird verwendet, um eine Verbindung mit dem ISP herzustellen.
Dienstname	Geben Sie einen Namen für den neuen L2TP-Dienst ein.
MPPE-Verschlüsselung	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um Microsoft Point-to-Point Encryption für die L2TP-Verbindung zu aktivieren.
DNS-Serverquelle	Die Adresse des DNS-Servers. Wenn Sie bereits DNS-Serveradressen von Ihrem ISP erhalten haben, wählen Sie **Diese DNS-Server verwenden** aus, und geben Sie die Adressen des primären und des sekundären DNS-Servers in die Felder **Primärer DNS-Server** und **Sekundärer DNS-Server** ein. Um die DNS-Serveradressen von Ihrem ISP zu beziehen, wählen Sie **Dynamisch vom Internetdienstanbieter abrufen** aus. Um Webadressen über die von OpenDNS bereitgestellten DNS-Server (208.67.222.222, 208.67.220.220) aufzulösen, wählen Sie **OpenDNS verwenden** aus.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren der optionalen Netzwerkeinstellungen

So konfigurieren Sie die optionalen Einstellungen:

SCHRITT 1 Konfigurieren Sie im Abschnitt **Optionale Einstellungen** die folgenden Einstellungen:

MTU	Bei der MTU (Maximum Transmission Unit) handelt es sich um die Größe des größten Pakets, das über das Netzwerk gesendet werden kann. Wenn vom ISP nichts anderes verlangt wird, sollten Sie **Automatisch** auswählen. Die MTU-Standardgröße beträgt 1.500 Byte. Wenn der ISP eine benutzerdefinierte MTU-Einstellung verwendet, wählen Sie **Manuell** aus und geben Sie die MTU-Größe ein.
Größe	Die Größe der benutzerdefinierten MTU. Der MTU-Standardwert für Ethernet-Netzwerke beträgt in der Regel 1.500 Byte. Bei PPPoE-Verbindungen beträgt der Wert 1.492 Byte.
VLAN ohne Tag	Aktivieren Sie das Kontrollkästchen, um das VLAN-Tagging zu aktivieren. Wenn die Option aktiviert ist (Standardeinstellung), wird der gesamte Verkehr mit einer VLAN-ID versehen. Standardmäßig wird für den gesamten Verkehr des Geräts VLAN 1 verwendet, das Standard-VLAN ohne Tag. Für den gesamten Verkehr werden so lange keine Tags verwendet, bis Sie das VLAN ohne Tag deaktivieren, die VLAN-ID für den Verkehr ohne Tag oder die VLAN-ID ändern.

VLAN-ID ohne Tag	Eine Zahl zwischen 1 und 4094 für die VLAN-ID ohne Tag. Der Standardwert lautet 1. Der Verkehr in dem in diesem Feld angegebenen VLAN wird bei der Weiterleitung an das Netzwerk nicht mit einer VLAN-ID versehen. VLAN 1 ist das Standard-VLAN ohne Tag.
VLAN für die Zugriffspunktverwaltung	Das VLAN, das der IP-Adresse zugewiesen ist, über die der Zugriff auf das Gerät erfolgt, wenn es als Zugriffspunkt konfiguriert ist. Wenn Sie zusätzliche VLANs erstellen, wählen Sie aus Sicherheitsgründen einen Wert aus, der dem VLAN entspricht, das in anderen Switches im Netzwerk konfiguriert ist. Möglicherweise müssen Sie das Verwaltungs-VLAN ändern, um den Zugriff auf den Geratemanager einzuschränken.

SCHRITT 2 Klicken Sie auf **Speichern**.

Konfigurieren eines mobilen Netzwerkes

Wählen Sie **Netzwerk > WAN > Mobiles Netzwerk**, um das Gerät für die Verbindung mit einem mobilen USB-Breitbandmodem zu konfigurieren, das an die USB-Schnittstelle angeschlossen ist.

Konfigurieren der globalen Einstellungen eines mobilen Netzwerks

So konfigurieren Sie die globalen Einstellungen für unterstützte USB-Geräte:

SCHRITT 1 Schließen Sie das USB-Modem an. Wenn das Modem unterstützt wird, wird es automatisch erkannt und auf der Seite „Mobiles Netzwerk“ angezeigt.

SCHRITT 2 Wählen Sie den Verbindungsmodus **Automatisch** oder **Manuell**. Die Ethernet-Wiederherstellung funktioniert nur, wenn der Verbindungsmodus auf „Automatisch“ gesetzt ist.

- Wählen Sie den Modus **Automatisch**, um das Modem für den automatischen Aufbau einer Verbindung zu aktivieren. Wenn Sie „Automatisch“ auswählen, legen Sie eine Zeit für **Verbindung bei Bedarf herstellen**, oder wählen Sie **Keep-Alive** aus. Wenn „Verbindung bei Bedarf herstellen“ ausgewählt ist, wird die Internetverbindung getrennt, wenn sie die im Feld **Max. Leerlaufzeit** angegebene Zeit lang inaktiv ist.

  Wenn die Internetverbindung aufgrund von Inaktivität getrennt wird, stellt das Modem automatisch eine Verbindung wieder her, sobald ein Benutzer versucht, auf das Internet zuzugreifen. Geben Sie in das Feld **Max. Leerlaufzeit** die Anzahl der Minuten für die Leerlaufzeit an, die vor dem Trennen der Internetverbindung vergehen soll. Wählen Sie **Keep-Alive** aus, wenn die Verbindung immer bestehen bleiben soll.

- Wenn Sie die Modemverbindung manuell herstellen oder trennen möchten, wählen Sie den Modus **Manuell** aus.

Das Gerät zeigt den aktuellen Modemverbindungsstatus an: „Initialisierung“, „Wird verbunden“, „Wird getrennt“ oder „Getrennt“.

SCHRITT 3 Prüfen Sie, ob im Feld **Kartenstatus** angezeigt wird, dass Ihre mobile Datenkarte **Verbunden** ist.

Manuelles Konfigurieren der Einstellungen eines mobilen Netzwerks

Um die Parameter des mobilen Netzwerks im Bereich **Setup für mobiles Netzwerk** zu ändern, klicken Sie auf die Optionsschaltfläche **Manuell**. Das Gerät erkennt automatisch unterstützte Modems und führt die entsprechenden Konfigurationsparameter auf. Um die globalen Parameter außer Kraft zu setzen, wählen Sie **Manuell** aus.

SCHRITT 1 Geben Sie in die folgenden Felder Informationen ein:

Feld	Beschreibung
Name des Zugriffpunkts (APN)	Internetnetzwerk, mit dem das mobile Geräte eine Verbindung herstellt. Geben Sie den Namen des Zugriffspunktes ein, den Sie von Ihrem Dienstanbieter für mobiles Netzwerk erhalten haben. Wenn Sie den Namen des Zugriffspunktes nicht kennen, wenden Sie sich an den Dienstanbieter.

Feld	Beschreibung
Einwählnummer	Die Einwählnummer, die Sie von Ihrem Dienstanbieter für mobiles Netzwerk für die Internetverbindung erhalten haben.
Benutzername Kennwort	Benutzername und Kennwort, die Sie von Ihrem Dienstanbieter für mobiles Netzwerk erhalten haben.
SIM-Prüfung	Prüfung der SIM-Karte aktivieren oder deaktivieren.
SIM-PIN	PIN-Code für die SIM-Karte. Dieses Feld wird nur für GSM-SIM-Karten angezeigt. Sie können die SIM-PIN im Modus „Automatisch“ und im Modus „Manuell“ ändern.
Servername	Name des Servers für die Internetverbindung (falls vom Dienstanbieter erhalten).
Authentifizierung	Authentifizierung, die vom Dienstanbieter verwendet wird. Der Wert kann durch Auswählen des Typs „Automatisch“ aus der Dropdown-Liste geändert werden. Der Standardwert lautet „Automatisch“. Wenn Sie nicht wissen, welcher Authentifizierungstyp verwendet werden soll, wählen Sie „Automatisch“ aus.
Diensttyp	Der am häufigsten verwendete Typ einer mobilen Datendienstverbindung, ermittelt auf der Grundlage des lokalen Dienstsignals in Ihrem Bereichs. Wenn an Ihrem Standort nur ein mobiler Datendienst unterstützt wird, können Sie Ihre bevorzugte Option einschränken, indem Sie die Häufigkeit der Verbindungseinrichtungen reduzieren. Die erste Auswahl sucht immer nach dem HSPDA/3G/UMTS-Dienst und schaltet automatisch auf GPRS um, wenn dieser Dienst verfügbar ist.
LTE-Dienst	Einstellung für den LTE-Dienst (Long-term Evolution Service). Wählen Sie **Automatisch** aus, um ein auf dem lokalen Dienstsignal in Ihrem Bereich basierendes Signal zu verwenden. Wählen Sie **Nur 4G** aus, um nur 4G-Signale zu verwenden. Wählen Sie **Nur 3G** aus, um nur 3G-Signale zu verwenden.

SCHRITT 2 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Bandbreitenobergrenze

Das Gerät überwacht die Datenaktivität in der mobile Netzwerkverbindung und sendet eine Benachrichtigung, sobald es einen angegebenen Schwellenwert erreicht hat.

So aktivieren bzw. deaktivieren Sie die Option „Nachverfolgung Bandbreitenobergrenze“ und legen Grenzwerte fest:

SCHRITT 1 Klicken Sie auf **Aktivieren** oder **Deaktivieren**.

SCHRITT 2 Wählen Sie in der Dropdown-Liste den Eintrag „Datum für monatliche Verlängerung“, um anzugeben, an welchem Tag des Monats die Bandbreitenobergrenze zurückgesetzt werden soll.

SCHRITT 3 Geben Sie im Feld **Datum für monatliche Verlängerung** den Höchstbetrag an Daten in Megabyte ein, der übertragen werden darf, bevor das Gerät eine Aktion (z. B. Senden einer E-Mail an den Administrator) ausführt.

E-Mail-Einstellung

Wenn die Bandbreitengrenze erreicht ist, kann eine E-Mail-Benachrichtigung an den Administrator gesendet werden. Informationen zum Einrichten der E-Mail-Adresse des Empfängers finden Sie unter **Konfigurieren des E-Mail-Versands für Protokolle**.

Wenn die Option aktiviert ist, wird unter folgenden Bedingungen eine E-Mail versendet:

- Die Nutzung des mobilen Netzwerk hat einen angegebenen Prozentwert überschritten.
- Das Gerät wechselt in den Sicherungspfad (Failover-Modus) bzw. die Standardverbindung wird wiederhergestellt.
- In jedem während einer aktiven mobilen Netzwerkverbindung angegebenen Intervall.

Einrichten von Failover und Wiederherstellung

Obwohl sowohl Ethernet- als auch mobile Netzwerkverbindungen möglich sind, kann immer nur eine Verbindung zum Aufbau einer WAN-Verbindung verwendet werden. Wenn eine WAN-Verbindung getrennt wird, versucht das Gerät, eine Verbindung über eine andere Schnittstelle herzustellen. Diese Funktion wird Failover genannt. Wenn die primäre WAN-Verbindung wiederhergestellt ist, wird wieder diese verwendet, und die Sicherungsverbindung wird getrennt. Diese Funktion wird Wiederherstellung genannt.

SCHRITT 1 Wählen Sie **Netzwerk > WAN > Failover und Wiederherstellung**, um den Bildschirm „Failover und Wiederherstellung“ anzuzeigen.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Failover zu 3G-WAN**, um die mobile Netzwerkverbindung zu aktivieren und als Failover von der Ethernet-Verbindung festzulegen. Wenn die Ethernet-WAN-Verbindung nicht aktiv ist, versucht das Gerät, die mobile Netzwerkverbindung über die USB-Schnittstelle herzustellen. (Wenn kein Failover aktiviert ist, ist die mobile Netzwerkverbindung immer deaktiviert.)

SCHRITT 3 Aktivieren Sie die Option **Wiederherstellung zu Ethernet-WAN**, damit, falls möglich, wieder die Ethernet-Verbindung verwendet und die mobile Netzwerkverbindung getrennt wird. Der Verbindungsmodus unter **WAN > Mobiles Netzwerk** muss auf „Automatisch“ gesetzt werden, damit die Wiederherstellung der Ethernet-WAN-Verbindung verwendet werden kann.

SCHRITT 4 Geben Sie in das Feld **Failover-Prüfintervall** das Intervall (in Sekunden) ein, nachdem das Gerät jeweils versuchen soll, die physische Verbindung oder Verkehr über die mobile Netzwerkverbindung zu ermitteln. Wenn die Verbindung im Leerlauf ist, versucht das Gerät in diesem Intervall einen Ping an ein Ziel zu senden. Wenn keine Antwort auf das Ping-Paket erhalten wird, geht das Gerät davon aus, dass die Verbindung getrennt ist, und versucht erneut, die Ethernet-WAN-Schnittstelle zu aktivieren.

SCHRITT 5 Geben Sie in das Feld **Wiederherstellungs-Prüfintervall** das Intervall (in Sekunden) ein, in dem das Gerät versuchen soll, die physische Verbindung oder Verkehr über die Ethernet-WAN-Verbindung zu ermitteln. Wenn die Verbindung im Leerlauf ist, versucht das Gerät, in diesem Intervall einen Ping an ein Ziel zu senden. Wenn auf das Ping-Paket eine Antwort eingeht, geht das Gerät davon aus, dass die Verbindung hergestellt ist, und versucht, die mobile Netzwerkverbindung zu deaktivieren und die Ethernet-WAN-Verbindung zu aktivieren.

SCHRITT 6 Klicken Sie auf **Wenn Ethernet verfügbar ist, sofort zu Ethernet umschalten** oder auf **Innerhalb eines bestimmten Zeitrahmens zu Ethernet umschalten**, und geben Sie Start- und Endzeit für den Zeitrahmen ein.

SCHRITT 7 Wählen Sie im Feld **Site für Verbindungsvalidierung** die Site aus, über die die Failover-Validierung erfolgen soll. Verwenden Sie das Gateway für den nächsten Hop (standardmäßig sendet das Gerät einen Ping an das Standardgateway) oder eine benutzerdefinierte Site, und geben Sie die IPv4- oder IPv6-Adresse der Site ein.

SCHRITT 8 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

In der Tabelle „WAN-Schnittstelle“ wird der Status der Ethernet-WAN- und der mobilen Netzwerkverbindung mit dem Internet angezeigt. Klicken Sie auf den Hyperlink **Status**, um die Anschlussdetails anzuzeigen.

Konfigurieren der LAN-Einstellungen

Die Standardeinstellungen für DHCP und TCP/IP sind für die meisten Anwendungen geeignet. Wenn Sie einen anderen PC im Netzwerk als DHCP-Server verwenden oder die Netzwerkeinstellungen aller Geräte manuell konfigurieren möchten, deaktivieren Sie DHCP.

Außerdem können Sie anstelle eines DNS-Servers, der Internetdomänennamen (beispielsweise www.cisco.com) IP-Adressen zuordnet, einen WINS-Server (Windows Internet Naming Service) verwenden. Ein WINS-Server ist das Äquivalent eines DNS-Servers, verwendet jedoch zum Auflösen von Hostnamen das NetBIOS-Protokoll. Das Gerät nimmt die IP-Adresse des WINS-Servers in die DHCP-Konfiguration auf, die es an DHCP-Clients sendet.

Wenn das Gerät mit einem Modem oder einem anderen Gerät verbunden ist, für das ein Netzwerk im selben Subnetz (192.168.1.x) konfiguriert ist, ändert es automatisch das LAN-Subnetz in ein zufällig ausgewähltes Subnetz nach dem Schema 10.x.x.x, sodass kein Konflikt mit dem Subnetz auf der WAN-Seite des Routers entsteht.

Ändern der IP-Adresse für die Geräteverwaltung

Die IP-Adresse für die Verwaltung lokaler Geräte des Geräts ist statisch und lautet standardmäßig 192.168.1.1.

So ändern Sie die IP-Adresse für die Verwaltung lokaler Geräte:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **LAN-Konfiguration** aus.

SCHRITT 2 Geben Sie im Bereich **IPv4** diese Informationen ein:

VLAN	Die VLAN-Nummer.
Lokale IP-Adresse	Die IP-Adresse des Geräts im LAN. Stellen Sie sicher, dass diese IP-Adresse nicht von einem anderen Gerät verwendet wird.
Subnetzmaske	Subnetzmaske für die lokale IP-Adresse. Die Standardsubnetzmaske lautet 255.255.255.0.

SCHRITT 3 Klicken Sie auf **Speichern**.

Wenn Sie die IP-Adresse des Geräts geändert haben, kann der PC den Gerätemanager nicht mehr anzeigen.

Gehen Sie wie folgt vor, um den Gerätemanager anzuzeigen:

- Wenn DHCP auf dem Gerät konfiguriert ist, geben Sie die IP-Adresse des PCs frei und erneuern Sie sie.
- Weisen Sie dem PC manuell eine IP-Adresse zu. Die Adresse muss sich im selben Subnetz wie das Gerät befinden. Wenn Sie beispielsweise die IP-Adresse des Geräts in 10.0.0.1 ändern, weisen Sie dem PC eine IP-Adresse im Bereich von 10.0.0.2 bis 10.0.0.255 zu.

Öffnen Sie ein neues Browserfenster und geben Sie die neue IP-Adresse des Geräts ein, um die Verbindung wiederherzustellen.

Konfigurieren eines DHCP-Servers

Standardmäßig fungiert das Gerät für die Hosts im WLAN (Funknetz) und im LAN (Kabelnetz) als DHCP-Server. Der DHCP-Server weist IP-Adressen zu und stellt DNS-Serveradressen bereit.

Bei aktiviertem DHCP weist das Gerät anderen Netzwerkgeräten im LAN IP-Adressen aus einem Pool von IPv4-Adressen zu. Das Gerät testet jede Adresse vor der Zuweisung, um doppelte Adressen im LAN zu vermeiden.

Der Standard-IP-Adresspool lautet 192.168.1.100 bis 192.168.1.149. Wenn Sie eine statische IP-Adresse auf einem Netzwerkgerät festlegen möchten, verwenden Sie eine IP-Adresse außerhalb des Pools. Beispiel: Wenn für den DHCP-Pool die Standardparameter festgelegt sind, können im IP-Adresspool statische IP-Adressen von 192.168.1.2 bis 192.168.1.99 verwendet werden, um Konflikte mit dem DHCP-IP-Adresspool zu vermeiden.

So konfigurieren Sie die DHCP-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **LAN-Konfiguration** aus.

SCHRITT 2 (Optional) Wählen Sie in der Dropdown-Liste ein zu bearbeitendes VLAN aus.

SCHRITT 3 Wählen Sie im Feld **DHCP-Server** eine der folgenden Optionen aus:

Aktivieren	Das Gerät kann als DHCP-Server im Netzwerk agieren.
Deaktivieren	DHCP wird auf dem Gerät deaktiviert. Dies ist beispielsweise sinnvoll, wenn Sie die IP-Adressen aller Netzwerkgeräte manuell konfigurieren möchten.
DHCP-Relais	Die IP-Adressen, die den Netzwerkgeräten von einem anderen DHCP-Server zugewiesen wurden, werden weitergeleitet.

Wenn Sie den DHCP-Server des Geräts aktiviert haben, geben Sie folgende Informationen ein:

IP-Startadresse	Die erste Adresse aus dem IP-Adressenpool. Jedem DHCP-Client, der dem LAN beitritt, wird eine IP-Adresse in diesem Bereich zugewiesen.
Maximale Anzahl an DHCP-Benutzern	Die maximale Anzahl der DHCP-Clients.
IP-Adressbereich	(Schreibgeschützt) Der Bereich der IP-Adressen, die für die DHCP-Clients zur Verfügung stehen.
Leasedauer	Dauer (in Stunden), für die IP-Adressen an Clients vergeben werden.
Statischer DNS-Server 1	IP-Adresse des primären DNS-Servers.

Statischer DNS-Server 2	IP-Adresse des sekundären DNS-Servers.
Statischer DNS-Server 3	IP-Adresse des tertiären DNS-Servers.
WINS	IP-Adresse des primären WINS-Servers.

SCHRITT 4 Wenn Sie **DHCP-Relais** ausgewählt haben, geben Sie die Adresse des Relais-Gateways in das Feld **Remote-DHCP-Server** ein. Das Relais-Gateway überträgt DHCP-Nachrichten an Netzwerkgeräte, auch an solche anderer Subnetzwerke.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von VLANs

Bei einem virtuellen LAN (VLAN) handelt es sich um eine Gruppe von Endpunkten in einem Netzwerk, die einander aufgrund ihrer Funktion oder anderer gemeinsamer Merkmale zugeordnet werden. Im Gegensatz zu LANs, die normalerweise auf dem geografischen Standort basieren, können in VLANs Endpunkte ungeachtet des physischen Standorts der Geräte oder Benutzer gruppiert werden.

Das Gerät hat ein Standard-VLAN (VLAN 1), das nicht gelöscht werden kann. Sie können auf dem Gerät bis zu vier weitere VLANs erstellen.

So erstellen Sie ein VLAN:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **VLAN-Mitgliedschaft** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie folgende Informationen ein:

VLAN-ID	Numerische VLAN-ID, die Endpunkten in der VLAN-Mitgliedschaft zugewiesen werden soll. Sie müssen eine Zahl zwischen 3 und 4094 eingeben. VLAN-ID 1 ist für das Standard-VLAN reserviert, das für an der Schnittstelle empfangene Frames ohne Tag verwendet wird.

Beschreibung	Eine Beschreibung des VLAN.
Anschluss 1 **Anschluss 2** **Anschluss 3** **Anschluss 4**	Sie können VLANs den LAN-Anschlüssen am Gerät zuordnen. Standardmäßig gehören alle Anschlüsse zu VLAN 1. Sie können diese Anschlüsse bearbeiten, um sie anderen VLANS zuzuordnen. Wählen Sie für jeden Anschluss den Typ der ausgehenden Frames aus: **Ohne Tag**: Die Schnittstelle gehört dem VLAN als Mitglied ohne Tag an. Frames des VLANs werden ohne Tag an das Anschluss-VLAN gesendet. **Mit Tag**: Der Anschluss gehört dem VLAN als Mitglied mit Tag an. Frames des VLANs werden mit Tag an das Anschluss-VLAN gesendet. **Ausgeschlossen**: Der Anschluss ist zurzeit kein Mitglied des VLANs. Dies ist bei der anfänglichen Erstellung des VLANs die Standardeinstellung für alle Anschlüsse.

SCHRITT 4 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen eines VLANs wählen Sie das VLAN aus und klicken auf **Bearbeiten**. Zum Löschen eines ausgewählten VLANs klicken Sie auf **Löschen**. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Konfigurieren von statischem DHCP

Sie können den Router so konfigurieren, dass einem Clientgerät mit einer bestimmten MAC-Adresse eine bestimmte IP-Adresse zugewiesen wird.

So konfigurieren Sie statisches DHCP:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **Statisches DHCP** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **VLAN** eine VLAN-Nummer aus.

SCHRITT 3 Klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie folgende Informationen ein:

Beschreibung	Beschreibung des Clients.
IP-Adresse	IP-Adresse, die dem Clientgerät zugewiesen werden soll. Die zugewiesene IP-Adresse sollte nicht zum Pool der DHCP-Adressen gehören. Bei der statischen DHCP-Zuweisung weist der DHCP-Server einer definierten MAC-Adresse bei jeder Verbindung des Clientgeräts mit dem Netzwerk dieselbe IP-Adresse zu. Der DHCP-Server weist die reservierte IP-Adresse zu, wenn das Clientgerät mit der entsprechenden MAC-Adresse eine IP-Adresse anfordert.
MAC-Adresse	MAC-Adresse des Clientgeräts. Das Format einer MAC-Adresse lautet XX:XX:XX:XX:XX:XX. Dabei ist „X“ eine Zahl zwischen 0 und 9 (einschließlich) oder ein Buchstabe zwischen A und F (einschließlich).

Zum Bearbeiten der Einstellungen eines statischen DHCP-Clients wählen Sie den Client aus und klicken auf **Bearbeiten**. Zum Löschen eines ausgewählten DHCP-Clients klicken Sie auf **Löschen**. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Anzeigen von DHCP-Lease-Clients

Sie können eine Liste der Endpunkte im Netzwerk aufrufen (identifiziert durch Hostname, IP-Adresse oder MAC-Adresse) und die IP-Adressen anzeigen, die den Endpunkten vom DHCP-Server zugewiesen wurden. Das VLAN der Endpunkte wird ebenfalls angezeigt.

Um die DHCP-Clients anzuzeigen, wählen Sie **Netzwerk** > **LAN** > **DHCP-Clients** aus.

Für jedes auf dem Gerät definierte VLAN wird in einer Tabelle eine Liste der jeweils zugeordneten Clients angezeigt.

So weisen Sie einem der verbundenen Geräte eine statische IP-Adresse zu:

SCHRITT 1 Aktivieren Sie in der Zeile des verbundenen Geräts das Kontrollkästchen **Zu statischem DHCP hinzufügen**.

SCHRITT 2 Klicken Sie auf **Speichern**.

Der DHCP-Server auf dem Gerät weist dann immer die angezeigte IP-Adresse zu, wenn das Gerät eine IP-Adresse anfordert.

Konfigurieren eines DMZ-Hosts

Das Gerät unterstützt demilitarisierte Zonen (DMZs). Bei einer DMZ handelt es sich um ein Subnetzwerk, das öffentlich verfügbar ist, sich aber hinter der Firewall befindet. Mithilfe einer DMZ können Sie an die IP-Adresse des WAN-Anschlusses gerichtete Pakete an eine bestimmte IP-Adresse im LAN umleiten.

Wir empfehlen, Hosts, die für das WAN verfügbar gemacht werden müssen (beispielsweise Webserver oder Mailserver) im DMZ-Netzwerk zu platzieren. Sie können Firewallregeln konfigurieren, um den Zugriff auf bestimmte Services und Ports in der DMZ über das LAN oder das WAN zuzulassen. Im Fall eines Angriffs auf einen der DMZ-Knoten ist das LAN nicht zwangsläufig ebenfalls verwundbar.

Sie müssen eine feste (statische) IP-Adresse für den Endpunkt konfigurieren, den Sie als DMZ-Host festlegen. Sie müssen dem DMZ-Host eine IP-Adresse zuweisen, die sich im selben Subnetz befindet wie die LAN-IP-Adresse des Geräts. Die IP-Adresse darf jedoch nicht mit der IP-Adresse identisch sein, die für die LAN-Schnittstelle dieses Gateways vergeben wird.

So konfigurieren Sie die DMZ:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **DMZ-Host** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die DMZ im Netzwerk zu aktivieren.

SCHRITT 3 Wählen Sie im Dropdown-Menü **VLAN** die ID des VLANs aus, in dem die DMZ aktiviert ist.

SCHRITT 4 Geben Sie in das Feld **Host-IP-Adresse** die IP-Adresse des DMZ-Hosts ein. Der DMZ-Host ist der Endpunkt, der die umgeleiteten Pakete empfängt.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von RSTP

RSTP (Rapid Spanning Tree Protocol) ist ein Netzwerkprotokoll, das Schleifen im Netzwerk verhindert und dynamisch neu konfiguriert, welche physischen Verbindungen Frames weiterleiten sollen. So konfigurieren Sie RTSP:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **RSTP** aus.

SCHRITT 2 Geben Sie folgende Informationen ein:

Systempriorität	Wählen Sie im Dropdown-Menü die Systempriorität aus: Sie können eine Systempriorität von 0 bis 61440 in Schritten von 4096 auswählen. Gültige Werte: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 und 61440. Je niedriger die Systempriorität, umso größer ist die Wahrscheinlichkeit, dass das Gerät zum Stamm des Spanning Tree wird. Der Standardwert lautet **327688**.
Hello-Zeit	Die Hello-Zeit ist der Zeitraum, in dem der Stamm des Spanning Tree wartet, bis Hello-Nachrichten gesendet werden. Geben Sie eine Zahl von 1 bis 10 ein. Der Standardwert lautet **2**.
Maximales Alter	Das maximale Alter ist der Zeitraum, während dessen der Router auf den Empfang einer Hello-Nachricht wartet. Wenn das maximale Alter erreicht ist, versucht der Router, den Spanning Tree zu ändern. Geben Sie eine Zahl von 6 bis 40 ein. Der Standardwert lautet **20**.
Weiterleitungsverzögerung	Die Weiterleitungsverzögerung ist das Intervall, nach dem eine Schnittstelle vom Status „Blockieren“ zum Status „Weiterleiten“ wechselt. Geben Sie eine Zahl von 4 bis 30 ein. Der Standardwert lautet **15**.

Version erzwingen	Wählen Sie die Protokollversion aus, die standardmäßig verwendet werden soll. Wählen Sie **Normal** (RSTP verwenden) oder **Kompatibel** (kompatibel mit dem alten STP) aus. Der Standardwert lautet **Normal**.

SCHRITT 3 Konfigurieren Sie in der **Einstellungstabelle** die folgenden Einstellungen:

Protokoll aktiviert	Aktivieren Sie dieses Kontrollkästchen, um RSTP für den zugeordneten Anschluss zu aktivieren. RSTP ist standardmäßig deaktiviert.
Edge	Aktivieren Sie dieses Kontrollkästchen, um anzugeben, dass der zugeordnete Anschluss ein Edge-Anschluss ist (Endpunkt). Deaktivieren Sie das Kontrollkästchen, um anzugeben, dass der zugeordnete Anschluss eine Verbindung (Bridge) zu einem anderen STP-Gerät ist. Der Edge-Anschluss ist standardmäßig aktiviert.
Pfadkosten	Geben Sie die RSTP-Pfadkosten für die festgelegten Anschlüsse ein. Verwenden Sie „0“ als Standardwert (das Gerät bestimmt den Pfadwert automatisch). Sie können auch eine Zahl von 2 bis 200.000.000 eingeben.

SCHRITT 4 Klicken Sie auf **Speichern**.

Anschlussverwaltung

Sie können die Einstellungen für die Geschwindigkeit und die Flusssteuerung der vier LAN-Anschlüsse des Geräts konfigurieren.

So konfigurieren Sie die Anschlussgeschwindigkeit und die Flusssteuerung::

SCHRITT 1 Wählen Sie **Netzwerk** > **Anschlussverwaltung** aus.

SCHRITT 2 Konfigurieren Sie diese Informationen:

Anschluss	Die Anschlussnummer.
Leitung	Die Leitungsgeschwindigkeit. Wenn kein Gerät mit dem Anschluss verbunden ist, wird in diesem Feld **Nicht genutzt** angezeigt.
Modus	Wählen Sie im Dropdown-Menü eine der folgenden Anschlussgeschwindigkeiten aus: • **Automatisch aushandeln**: Das Gerät und das verbundene Gerät wählen eine gemeinsame Geschwindigkeit aus. • **10 MBit/s Halbduplex**: 10 MBit/s in beide Richtungen, aber nur jeweils eine Richtung. • **10 MBit/s Vollduplex**: 10 MBit/s in beide Richtungen gleichzeitig. • **100 MBit/s Halbduplex**: 100 MBit/s in beide Richtungen, aber nur jeweils eine Richtung. • **100 MBit/s Vollduplex**: 100 MBit/s in beide Richtungen gleichzeitig.
Jumbo-Frame	Aktivieren Sie diese Option, um Jumbo-Frames auf dem Gerät zu aktivieren und innerhalb des LANs Frames mit einer Datenmenge von jeweils bis zu 9.000 Byte zu senden. Ein Standard-Ethernet-Frame enthält 1.500 Byte Daten.

Flusskontrolle	Aktivieren Sie dieses Kontrollkästchen, um die Flusskontrolle für diesen Anschluss zu aktivieren. Die Flusskontrolle ist ein Vorgang, bei dem die Datenübertragungsrate zwischen zwei Knoten verwaltet wird, um zu verhindern, dass ein Sender mit höherer Geschwindigkeit einen Empfänger mit niedrigerer Geschwindigkeit „überholt“. Es wird ein Mechanismus bereitgestellt, mit dem der Empfänger die Übertragungsgeschwindigkeit steuern kann, damit der empfangende Knoten nicht mit Daten vom sendenden Knoten überflutet wird.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren der Link-Aggregation

Auf der Seite „Link-Aggregation“ können Sie mehrere Ethernet-Verbindungen zu einem logischen Kanal zusammenfassen. Durch Link-Aggregation lassen sich Kosten einsparen, da die kumulative Bandbreite ohne Hardwareupgrades erhöht wird. Gleichzeitig wird die Umleitung im Fall eines Anschluss- oder Kabelausfalls erleichtert.

So weisen Sie Anschlüsse einer Link-Aggregationsgruppe zu:

SCHRITT 1 Wählen Sie **Netzwerk > LAN > Link-Aggregation**. Unter **Anschlussstatus** werden Modus und der Status für die Anschlüsse des Geräts angezeigt.

SCHRITT 2 Aktivieren Sie unter **Link-Aggregations-Einstellungen** die Kontrollkästchen für alle Anschlüsse, die in die Gruppe aufgenommen werden sollen.

SCHRITT 3 Klicken Sie auf **Speichern**.

Klonen der MAC-Adresse

Manchmal müssen Sie möglicherweise für den WAN-Anschluss des Geräts eine MAC-Adresse festlegen, die mit der MAC-Adresse des PCs oder einer anderen MAC-Adresse identisch ist. Dies wird als Klonen der MAC-Adresse bezeichnet.

Einige ISPs registrieren beispielsweise bei der Erstinstallation des Service die MAC-Adresse der Netzwerkkarte des Computers. Wenn Sie einen Router hinter dem Kabel- oder DSL-Modem anschließen, wird die MAC-Adresse des WAN-Anschlusses des Geräts vom ISP nicht erkannt.

In diesem Fall können Sie das Gerät so konfigurieren, dass es vom ISP erkannt wird, indem Sie die MAC-Adresse des WAN-Anschlusses klonen, sodass sie mit der MAC-Adresse des Computers identisch ist.

So konfigurieren Sie eine geklonte MAC-Adresse:

SCHRITT 1 Wählen Sie **Netzwerk** > **MAC-Adressklon** aus.

SCHRITT 2 Aktivieren Sie im Feld **MAC-Adressklon** das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Führen Sie einen der folgenden Schritte aus, um die MAC-Adresse des WAN-Anschlusses für das Gerät festzulegen:

- Wenn Sie die MAC-Adresse des WAN-Anschlusses auf die MAC-Adresse des PCs festlegen möchten, klicken Sie auf **MAC-Adresse meines PCs klonen**.
- Wenn Sie eine andere MAC-Adresse angeben möchten, geben Sie diese in das Feld **MAC-Adresse** ein.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren des Routing

Auf der Seite „Routing“ können Sie den Betriebsmodus und weitere Routingoptionen für das Gerät konfigurieren.

Konfigurieren des Betriebsmodus

So konfigurieren Sie den Betriebsmodus:

SCHRITT 1 Wählen Sie **Netzwerk** > **Routing** aus.

SCHRITT 2 Wählen Sie im Feld **Betriebsmodus** eine der folgenden Optionen aus:

Gateway	Konfiguriert das Gerät als Gateway. (Empfohlen) Behalten Sie diese Standardeinstellung bei, wenn das Gerät zum Hosten der Verbindung zwischen Netzwerk und Internet verwendet wird und Routing-Funktionen ausführt.
Router	Konfiguriert das Gerät als Router. (Nur für fortgeschrittene Benutzer) Wählen Sie diese Option aus, wenn sich das Gerät in einem Netzwerk mit anderen Routern befindet. Durch das Aktivieren des Routermodus wird NAT (Network Address Translation) auf dem Gerät deaktiviert.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von dynamischem Routing

Das RIP-Protokoll (Routing Information Protocol) ist ein IGP-Protokoll (Interior Gateway Protocol), das häufig in internen Netzwerken verwendet wird. Es ermöglicht dem Router den automatischen Austausch von Routing-Informationen mit anderen Routern sowie die dynamische Anpassung der Routingtabellen und die Anpassung an Änderungen im Netzwerk.

Mithilfe von dynamischem Routing (RIP) kann sich das Gerät automatisch an physische Änderungen im Layout des Netzwerks anpassen und Routingtabellen mit den anderen Routern austauschen.

Der Router bestimmt die Route der Netzwerkpakete basierend auf der kleinsten Anzahl von Hops zwischen Quelle und Ziel.

HINWEIS RIP ist auf dem Gerät standardmäßig deaktiviert.

So konfigurieren Sie dynamisches Routing:

SCHRITT 1 Wählen Sie **Netzwerk** > **Routing** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Einstellungen:

RIP	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um RIP zu aktivieren. Damit ermöglichen Sie dem Gerät die Weiterleitung von Verkehr mithilfe von RIP.
Version der RIP Send-Pakete	Wählen Sie die Version für RIP Send-Pakete (**RIPv1** oder **RIPv2**) aus. Die zum Senden von Routing-Aktualisierungen an andere Router im Netzwerk verwendete RIP-Version hängt von den Konfigurationseinstellungen der anderen Router ab. RIPv2 ist abwärtskompatibel mit RIPv1.
Version der RIP Recv-Pakete	Wählen Sie die Version für RIP Recv-Pakete aus.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von Inter-VLAN-Routing

Wenn ein Endpunkt in einem VLAN mit einem Endpunkt in einem anderen VLAN kommunizieren können soll, aktivieren Sie das Kontrollkästchen **Inter-VLAN-Routing**.

Konfigurieren von statischem Routing

Sie können statische Routen konfigurieren, um Pakete an das Zielnetzwerk zu leiten. Eine statische Route ist ein zuvor festgelegter Pfad, den ein Paket zurücklegen muss, um einen bestimmten Host oder ein bestimmtes Netzwerk zu erreichen.

Manche ISPs erfordern für die Erstellung der Routingtabelle statische Routen anstelle dynamischer Routing-Protokolle. Bei statischen Routen werden keine CPU-Ressourcen benötigt, um Routing-Informationen mit einem Peer-Router auszutauschen.

Sie können statische Routen auch verwenden, um Peer-Router zu erreichen, die keine dynamischen Routing-Protokolle unterstützen. Statische Routen können zusammen mit dynamischen Routen verwendet werden. Das Gerät unterstützt bis zu 30 statische Routen.

Achten Sie darauf, dass im Netzwerk keine Routing-Schleifen entstehen.

So konfigurieren Sie statisches Routing:

SCHRITT 1 Wählen Sie **Netzwerk** > **Routing** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Einträge der Routingtabelle** einen Routeneintrag aus.

Zum Löschen des Routeneintrags klicken Sie auf **Diesen Eintrag löschen**.

SCHRITT 3 Konfigurieren Sie die folgenden Einstellungen für den ausgewählten Routeneintrag:

Routenname	Geben Sie den Namen der Route ein.
Ziel-LAN-IP	Geben Sie die IP-Adresse des Ziel-LANs ein.
Subnetzmaske	Geben Sie die Subnetzmaske des Zielnetzwerks ein.
Gateway	Geben Sie die IP-Adresse des für diese Route verwendeten Gateways ein.
Schnittstelle	Wählen Sie die Schnittstelle aus, an die Pakete für diese Route gesendet werden: • **LAN und WLAN**: Wählen Sie diese Option, um Pakete an das LAN und das WLAN zu leiten. • **WAN**: Wählen Sie diese Option, um Pakete an das WAN (Internet) zu leiten.

SCHRITT 4 Klicken Sie auf **Speichern**.

Anzeigen der Routingtabelle

Die Routingtabelle enthält Informationen zur Topologie des sie unmittelbar umgebenden Netzwerks.

Zum Anzeigen der Routing-Informationen im Netzwerk klicken Sie auf **Netzwerk** > **Routingtabelle**, und wählen Sie eine der folgenden Optionen aus:

- **IPv4-Routingtabelle anzeigen**: Die Routingtabelle wird mit den auf den Seiten **Netzwerk** > **Routing** konfigurierten Feldern angezeigt.
- **IPv6-Routingtabelle anzeigen**: Die Routingtabelle wird mit den auf der Seite **Netzwerk** > **IPv6** konfigurierten Feldern angezeigt.

Konfigurieren von dynamischem DNS

Dynamic DNS (DDNS) ist ein Internetdienst, der das Auffinden von Routern mit variierenden öffentlichen IP-Adressen anhand von Internetdomänennamen ermöglicht. Um DDNS zu verwenden, müssen Sie ein Konto bei einem DDNS-Anbieter einrichten (beispielsweise DynDNS.com, TZO.com, 3322.org oder noip.com).

Der Router benachrichtigt Dynamic DNS-Server über Änderungen an der WAN-IP-Adresse, sodass der Zugriff auf öffentliche Services in Ihrem Netzwerk anhand des Domänennamens möglich ist.

So konfigurieren Sie DDNS:

SCHRITT 1 Wählen Sie **Netzwerk** > **Dynamic DNS** aus.

SCHRITT 2 Wählen Sie in der Drop-down-Liste **Update-Intervall** aus.

SCHRITT 3 Unter **DDNS-Dienste** werden die DDNS-Dienste aufgeführt, die Sie auf dem Gerät aktivieren können.

SCHRITT 4 Aktivieren Sie das Kontrollkästchen für den zu aktivierenden Dienst, und klicken Sie auf **Bearbeiten**.

SCHRITT 5 Aktivieren Sie das Kontrollkästchen **Aktivieren** für den Dienst.

SCHRITT 6 Konfigurieren Sie diese Informationen:

Benutzername/E-Mail-Adresse	Der Benutzername des DDNS-Kontos oder die E-Mail-Adresse, mit der Sie das DDNS-Konto erstellt haben.
Kennwort	Das Kennwort für das DDNS-Konto.
Host-/Domänenname	Hostname des DDNS-Servers oder Name der Domäne für den Netzwerkzugriff.
WAN-IP-Adresse	(Schreibgeschützt) Die Internet-IP-Adresse des Geräts.
Status	(Schreibgeschützt) Zeigt an, dass die DDNS-Aktualisierung erfolgreich abgeschlossen wurde oder dass beim Senden der Kontoaktualisierungsinformationen an den DDNS-Server ein Fehler aufgetreten ist.

SCHRITT 7 Klicken Sie auf **Konfiguration testen**, um die DDNS-Konfiguration zu testen.

SCHRITT 8 Klicken Sie auf **Speichern**.

Konfigurieren des IP-Modus

Die Eigenschaften der WAN-Konfiguration können für IPv4-Netzwerke und für IPv6-Netzwerke konfiguriert werden. Sie können auf diesen Seiten Informationen zum Internetverbindungstyp und andere Parameter eingeben.

So wählen Sie einen IP-Modus aus:

SCHRITT 1 Wählen Sie **Netzwerk** > **IP-Modus** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **IP-Modus** eine der folgenden Optionen aus:

LAN: IPv4, WAN: IPv4	Verwendet IPv4 für die LAN- und WAN-Anschlüsse.
LAN: IPv6, WAN: IPv4	Verwendet IPv6 für die LAN-Anschlüsse und IPv4 für die WAN-Anschlüsse.

LAN: IPv6, WAN: IPv6	Verwendet IPv6 für die LAN- und WAN-Anschlüsse.
LAN: IPv4 + IPv6, WAN: IPv4	Verwendet IPv4 und IPv6 für die LAN-Anschlüsse und IPv4 für die WAN-Anschlüsse.
LAN: IPv4 + IPv6, WAN: IPv4 + IPv6	Verwendet IPv4 und IPv6 für die LAN- und WAN-Anschlüsse.
LAN: IPv4, WAN: IPv6	Verwendet IPv4 für die LAN-Anschlüsse und IPv6 für die WAN-Anschlüsse.

SCHRITT 3 (Optional) Wenn Sie 6to4-Tunneling verwenden, das die Übertragung von IPv6-Paketen über ein IPv4-Netzwerk ermöglicht, führen Sie die folgenden Schritte aus:

a. Klicken Sie auf **Statischen 6to4-DNS-Eintrag anzeigen**.

b. Geben Sie in die Felder **Domäne** und **IP-Adresse** bis zu fünf Zuordnungen zwischen Domäne und IP-Adresse ein.

Die Funktion für 6to4-Tunneling wird normalerweise verwendet, wenn eine Site oder ein Endbenutzer über das vorhandene IPv4-Netzwerk eine Verbindung mit dem IPv6-Internet herstellen möchte.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von IPv6

Das Internetprotokoll Version 6 (IPv6) ist als Nachfolger von Internetprotokoll Version 4 (IPv4) vorgesehen. Die Konfiguration der WAN-Eigenschaften für ein IPv6-Netzwerk richtet sich nach dem Typ Ihrer Internetverbindung.

Konfigurieren von IPv6-WAN-Verbindungen

Sie können das Gerät als DHCPv6-Client des ISPs für dieses WAN konfigurieren oder eine vom ISP bereitgestellte statische IPv6-Adresse verwenden.

Zum Konfigurieren der IPv6-WAN-Einstellungen auf dem Gerät müssen Sie zuerst den IP-Modus auf einen der folgenden Modi festlegen:

- LAN: IPv6, WAN: IPv6

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

Eine Anleitung zum Festlegen des IP-Modus finden Sie unter **Konfigurieren des IP-Modus**.

Konfigurieren von SLAAC

Um eine Adresse anhand des IPv6-Präfix automatisch zuzuweisen, konfigurieren Sie das Gerät für die Verwendung von Stateless Address Auto-Configuration (SLAAC) zum Zuweisen von IPv6-Clientadressen.

So verwenden Sie SLAAC:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-WAN-Konfiguration** aus.

SCHRITT 2 Wählen Sie im Feld **WAN-Verbindungstyp** die Option „SLAAC“ aus. Bei statuslosem DHCP ist es nicht notwendig, dass beim Internetdienstanbieter ein DHCPv6-Server zur Verfügung steht. Stattdessen wird vom Gerät eine ICMPv6-Erkennungsnachricht gesendet, die für die automatische Konfiguration verwendet wird.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von DHCPv6

Wenn Ihnen der ISP eine dynamisch zugewiesene Adresse bereitstellt, konfigurieren Sie das Gerät als DHCPv6-Client.

So konfigurieren Sie das Gerät als DHCPv6-Client:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-WAN-Konfiguration** aus.

SCHRITT 2 Wählen Sie im Feld **WAN-Verbindungstyp** die Option **Automatische Konfiguration (DHCPv6)** aus. Das Gateway stellt eine Verbindung mit dem DHCPv6-Server des ISPs her, um eine Lease-Adresse zu beziehen.

SCHRITT 3 Um die Zuweisung von Präfixen zum Gerät (DHCP-Client) zu automatisieren, aktivieren Sie die Optionsschaltfläche **Präfix-Delegation**.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren einer statischen IPv6-WAN-Adresse

Wenn Ihnen der ISP eine feste Adresse für den Zugriff auf das WAN zuweist, konfigurieren Sie das Gerät für die Verwendung einer statischen IPv6-Adresse.

So konfigurieren Sie eine statische IPv6-WAN-Adresse:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-WAN-Konfiguration** aus.

SCHRITT 2 Wählen Sie im Feld **WAN-Verbindungstyp** die Option **Statisches IPv6** aus.

SCHRITT 3 Geben Sie folgende Informationen ein:

IPv6-Adresse	IPv6-Adresse des WAN-Anschlusses.
IPv6-Präfixlänge	Geben Sie die normalerweise vom ISP definierte IPv6-Präfixlänge ein. Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Alle Hosts im Subnetzwerk haben dasselbe Präfix. So lautet beispielsweise in der IPv6-Adresse `2001:0DB8:AC10:FE01::` das Präfix `2001`.
Standard-IPv6-Gateway	IPv6-Adresse des Standardgateways. Dies ist normalerweise die IP-Adresse des Servers beim ISP.
Statischer DNS-Server 1	IP-Adresse des primären IPv6-DNS-Servers.
Statischer DNS-Server 2	IP-Adresse des sekundären IPv6-DNS-Servers.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren der PPPoE-Einstellungen unter IPv6

Sie können PPPoE-IPv4, PPPoE-IPv6 oder beide gleichzeitig ausführen. Wenn Sie sich für beide entscheiden, müssen die PPPoE-IPv6-WAN-Einstellungen mit den PPPoE-IPv4-WAN-Einstellungen übereinstimmen. Wenn Sie nicht übereinstimmen, wird eine Nachricht mit der Frage angezeigt, ob Sie das IPv6-Protokoll so einstellen möchten, dass es mit dem IPv4-Protokoll übereinstimmt. Weitere Informationen hierzu finden Sie unter **Konfigurieren von PPPoE**.

So konfigurieren Sie die PPPoE-IPv6-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-WAN-Konfiguration** aus.

SCHRITT 2 Wählen Sie im Feld **WAN-Verbindungstyp** die Option **PPPoE-IPv6** aus.

SCHRITT 3 Geben Sie die folgenden Informationen ein (möglicherweise müssen Sie den ISP nach den PPPoE-Anmeldeinformationen fragen):

Benutzername	Der Ihnen vom ISP zugewiesene Benutzername.
Kennwort	Das Ihnen vom ISP zugewiesene Kennwort.
Verbindung bei Bedarf	Wenn beim ISP Kosten auf der Grundlage der Verbindungszeit entstehen, aktivieren Sie das Optionsfeld. Wenn diese Option aktiviert ist, ist die Internetverbindung nur aktiv, wenn Verkehr vorhanden ist. Wenn sich die Verbindung im Leerlauf befindet (das heißt, wenn kein Verkehr fließt), wird die Verbindung getrennt. Geben Sie im Feld **Maximale Leerlaufzeit** an, wie lange (in Minuten) kein Verkehr auf der Verbindung erkannt worden sein muss, damit die Verbindung getrennt wird.
Keep-Alive	Hält die WAN-Verbindung aufrecht, indem eine „Aufrechterhalten“-Nachricht über den Anschluss gesendet wird. Geben Sie in das Feld „Zeit bis Neueinwahl“ die Wartezeit in Sekunden ein, nach der das Gerät versuchen soll, eine getrennte Verbindung wiederherzustellen.

Authentifizierungstyp	Authentifizierungstypen: **Automatisch aushandeln**: Ein Server sendet eine Konfigurationsanforderung, in der der auf dem Server festgelegte Sicherheitsalgorithmus angegeben ist. Das Gerät antwortet mit den Anmeldeinformationen einschließlich dem vom Server gesendeten Sicherheitstyp. **PAP**: PAP (Password Authentication Protocol) Zum Herstellen der Verbindung mit dem ISP verwenden. **CHAP**: Zum Herstellen der Verbindung mit dem ISP CHAP (Challenge Handshake Authentication Protocol) verwenden. **MS-CHAP oder MS-CHAPv2**: Das Microsoft Challenge Handshake Authentication-Protokoll wird verwendet, um eine Verbindung mit dem ISP herzustellen.
Dienstname	Name, den der ISP für eine Anmeldung auf dem PPPoE-Server anfordern kann.
MTU	Bei der MTU (Maximum Transmission Unit) handelt es sich um die Größe des größten Pakets, das über das Netzwerk gesendet werden kann. Wenn vom ISP nichts anderes verlangt wird, sollten Sie **Automatisch** auswählen. Der MTU-Standardwert für Ethernet-Netzwerke beträgt 1.500 Byte. Bei PPPoE-Verbindungen beträgt der Wert 1.492 Byte. Wenn der ISP eine benutzerdefinierte MTU-Einstellung verwendet, wählen Sie **Manuell** aus.
Größe	MTU-Größe. Wenn der ISP eine benutzerdefinierte MTU-Einstellung verwendet, geben Sie die MTU-Größe ein.
Adressmodus	Modus für dynamische Adresse oder Modus für statische Adressen. Wenn Sie „Statisch“ auswählen, geben Sie im nachfolgenden Feld die IPv6-Adresse ein.
IPv6-Präfixlänge	IPv6-Präfixlänge.
Standard-IPv6-Gateway	IP-Adresse des Standard-IPv6-Gateways.

Statischer DNS-Server 1	IP-Adresse des primären DNS-Servers.
Statischer DNS-Server 2	IP-Adresse des sekundären DNS-Servers.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von IPv6-LAN-Verbindungen

Im IPv6-Modus ist der LAN-DHCP-Server standardmäßig aktiviert (ähnlich wie im IPv4-Modus). Der DHCPv6-Server weist IPv6-Adressen aus konfigurierten Adressenpools zu, die die dem LAN zugewiesene IPv6-Präfixlänge verwenden.

Zum Konfigurieren der IPv6-LAN-Einstellungen auf dem Gerät müssen Sie zuerst den IP-Modus auf einen der folgenden Modi festlegen:

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

Weitere Informationen zum Festlegen des IP-Modus finden Sie unter **Konfigurieren des IP-Modus**.

So konfigurieren Sie IPv6-LAN-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-LAN-Konfiguration** aus.

SCHRITT 2 Geben Sie die folgenden Informationen ein, um die IPv6-LAN-Adresse zu konfigurieren:

IPv6-Adresse	Geben Sie die IPv6-Adresse des Geräts ein. Die Standard-IPv6-Adresse für das Gateway lautet „fec0::1“ (oder „FEC0:0000:0000:0000:0000:0000:0000:0001“). Sie können diese 128-Bit-IPv6-Adresse je nach Netzwerkanforderungen ändern.

IPv6-Präfixlänge	Geben Sie die IPv6-Präfixlänge ein. Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Standardmäßig hat das Präfix eine Länge von 64 Bits. Die Anfangs-Bits der IPv6-Adressen aller Hosts im Netzwerk sind identisch. In diesem Feld legen Sie die Anzahl der gemeinsamen Anfangs-Bits in den Netzwerkadressen fest.

SCHRITT 3 Klicken Sie auf **Speichern**, oder fahren Sie mit der Konfiguration der IPv6-DHCP-LAN-Einstellungen fort.

SCHRITT 4 Geben Sie die folgenden Informationen ein, um die DHCPv6-Einstellungen zu konfigurieren:

DHCP-Status	Aktivieren Sie dieses Kontrollkästchen, um den DHCPv6-Server zu aktivieren. Wenn diese Funktion aktiviert ist, weist das Gerät jedem LAN-Endpunkt, der über DHCP bereitgestellte Adressen anfordert, eine IP-Adresse innerhalb des angegebenen Bereichs zu und stellt zusätzliche Informationen bereit.
Domänenname	(Optional) Domänenname des DHCPv6-Servers.
Serverpriorität	Die Serverprioritätsstufe dieses DHCP-Servers. DHCP-Ankündigungsnachrichten mit dem höchsten Servervoreinstellungswert an einen LAN-Host werden gegenüber anderen DHCP-Serverankündigungsnachrichten bevorzugt. Der Standardwert lautet „255“.
Statischer DNS-Server 1	IPv6-Adresse des primären DNS-Servers im IPv6-Netzwerk des ISPs.
Statischer DNS-Server 2	IPv6-Adresse des sekundären DNS-Servers im IPv6-Netzwerk des ISPs.

Client-Lease-Dauer	Dauer der Client-Lease-Zeit (in Stunden), während der IPv6-Adressen an Endpunkte im LAN vergeben werden.

SCHRITT 5 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-LAN-Konfiguration** aus.

SCHRITT 6 Klicken Sie in der **Tabelle für IPv6-Adressenpools** auf **Hinzufügen**.

SCHRITT 7 Geben Sie folgende Informationen ein:

Startadresse	Start-IPv6-Adresse im Pool.
Endadresse	End-IPv6-Adresse im Pool.
IPv6-Präfixlänge	Präfixlänge, die die Anzahl der gemeinsamen Anfangs-Bits in den Netzwerkadressen bestimmt.

SCHRITT 8 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen eines Pools wählen Sie den Pool aus und klicken Sie auf **Bearbeiten**. Zum Löschen eines ausgewählten Pools klicken Sie auf **Löschen**. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Konfigurieren von statischem IPv6-Routing

Sie können statische Routen konfigurieren, um Pakete an das Zielnetzwerk zu leiten. Eine statische Route ist ein zuvor festgelegter Pfad, den ein Paket zurücklegen muss, um einen bestimmten Host oder ein bestimmtes Netzwerk zu erreichen.

Manche ISP verwenden für die Erstellung einer Routingtabelle statische Routen anstelle dynamischer Routing-Protokolle. Bei statischen Routen werden keine CPU-Ressourcen benötigt, um Routing-Informationen mit einem Peer-Router auszutauschen.

Sie können statische Routen auch verwenden, um Peer-Router zu erreichen, die keine dynamischen Routing-Protokolle unterstützen. Statische Routen können zusammen mit dynamischen Routen verwendet werden. Achten Sie darauf, dass im Netzwerk keine Routing-Schleifen entstehen.

So erstellen Sie eine statische Route:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Statisches IPv6-Routing** aus.

SCHRITT 2 Klicken Sie in der Liste der statischen Routen auf **Hinzufügen**.

SCHRITT 3 Geben Sie folgende Informationen ein:

Name	Routenname.
Ziel	IPv6-Adresse des Zielhosts oder -netzwerks für diese Route.
Präfixlänge	Anzahl der Präfix-Bits in der IPv6-Adresse, die das Zielsubnetz definieren.
Gateway	IPv6-Adresse des Gateways, über das der Zielhost bzw. das Zielnetzwerk erreicht werden kann.
Schnittstelle	Schnittstelle für die Route: **LAN**, **WAN** oder **6to4**.
Metrik	Priorität der Route. Wählen Sie einen Wert zwischen 2 und 15 aus. Wenn mehrere Routen mit demselben Ziel vorhanden sind, wird die Route mit der niedrigsten Metrik verwendet.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Route zu aktivieren. Wenn Sie eine inaktive Route hinzufügen, wird diese in der Routingtabelle aufgelistet, aber nicht vom Gerät verwendet. Sie können beispielsweise eine inaktive Route eingeben, wenn Sie eine Route hinzufügen möchten, die Route aber nicht verfügbar ist. Sie können dann die Route aktivieren, sobald das Netzwerk verfügbar ist.

SCHRITT 4 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen einer Route wählen Sie die Route aus und klicken Sie auf **Bearbeiten**. Zum Löschen einer ausgewählten Route klicken Sie auf **Löschen**. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Konfigurieren von Routing (RIPng)

RIP Next Generation (RIPng) ist ein Routing-Protokoll, das auf dem Distanzvektoralgorithmus (D-V) basiert. RIPng verwendet UDP-Pakete, um über Port 521 Routing-Informationen auszutauschen.

RIPng verwendet zum Messen der Distanz zu einem Ziel die Hop-Anzahl. Die Hop-Anzahl wird als Metrik bzw. Kosten bezeichnet. Die Hop-Anzahl von einem Router zu einem direkt verbundenen Netzwerk beträgt 0. Die Hop-Anzahl zwischen zwei direkt verbundenen Routern beträgt 1. Wenn die Hop-Anzahl größer oder gleich 16 ist, ist das Zielnetzwerk bzw. der Zielhost nicht erreichbar.

Standardmäßig wird die Routing-Aktualisierung alle 30 Sekunden gesendet. Wenn der Router nach 180 Sekunden keine Routing-Aktualisierungen von einem Nachbarn empfangen hat, werden die vom Nachbarn gelernten Routen als nicht erreichbar betrachtet. Wenn nach weiteren 240 Sekunden keine Routing-Aktualisierung empfangen wurde, entfernt der Router diese Routen aus der Routingtabelle.

Auf dem Gerät ist RIPng standardmäßig deaktiviert.

So konfigurieren Sie RIPng:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Routing (RIPng)** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von Tunneling

IPv6-to-IPv4-Tunneling (6to4-Tunneling) ermöglicht die Übertragung von IPv6-Paketen über ein IPv4-Netzwerk. IPv4-to-IPv6-Tunneling (4to6-Tunneling) ermöglicht die Übertragung von IPv4-Paketen über ein IPv6-Netzwerk.

6to4-Tunneling

6to4-Tunneling wird normalerweise verwendet, wenn eine Site oder ein Endbenutzer über das vorhandene IPv4-Netzwerk eine Verbindung mit dem IPv6-Internet herstellen möchte.

So konfigurieren Sie 6to4-Tunneling:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Tunneling** aus.

SCHRITT 2 Aktivieren Sie im Feld **6to4-Tunneling** das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Wählen Sie den Tunneling-Typ:

- **6to4**
- **6RD** (Rapid Deployment)
- **ISATAP** (Intra-Site Automatic Tunnel Addressing Protocol): Wählen Sie **Automatisch** oder **Manuell** aus.

SCHRITT 4 Wählen Sie bei 6RD-Tunneling **Automatisch** oder **Manuell** aus. Wenn Sie **Manuell** auswählen, geben Sie folgende Informationen ein:

- **IPv6-Präfix**
- **IPv6-Präfixlänge**
- **Border-Relais**
- **IPv4-Maskenlänge**

SCHRITT 5 Wählen Sie bei ISATAP-Tunneling **Automatisch** oder **Manuell** aus. Wenn Sie **Manuell** auswählen, geben Sie folgende Informationen ein:

- **IPv6-Präfix**
- **IPv6-Präfixlänge**

SCHRITT 6 Klicken Sie auf **Speichern**.

4to6-Tunneling

So konfigurieren Sie 4to6-Tunneling:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Tunneling** aus.

SCHRITT 2 Aktivieren Sie im Feld **4to6-Tunneling** das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Geben Sie die lokale WAN-IPv6-Adresse auf dem Gerät ein.

SCHRITT 4 Geben Sie die Remote IPv6-Adresse oder die IP-Adresse des Remoteendpunkts ein.

SCHRITT 5 Klicken Sie auf **Speichern**.

Anzeigen des IPv6-Tunnelstatus

So zeigen Sie den IPv6-Tunnelstatus an:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-Tunnelstatus** aus.

SCHRITT 2 Klicken Sie auf **Aktualisieren**, um die aktuellen Informationen anzuzeigen.

Auf dieser Seite werden Informationen zum automatischen Tunnel angezeigt, der über die dedizierte WAN-Schnittstelle eingerichtet wurde. Sie sehen in der Tabelle den Namen des Tunnels und die im Gerät erstellte IPv6-Adresse.

Konfigurieren der Routeranzeige

Der Router Advertisement Daemon (RADVD) auf dem Gerät hört Routeranfragen im IPv6-LAN mit und antwortet nach Bedarf mit Routeranzeigen. Dabei handelt es sich um eine statuslose automatische IPv6-Konfiguration. Das Gerät verteilt IPv6-Präfixe an alle Knoten im Netzwerk.

So konfigurieren Sie RADVD:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Routeranzeige** aus.

SCHRITT 2 Geben Sie folgende Informationen ein:

RADVD-Status	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um RADVD zu aktivieren.
Anzeigemodus	Wählen Sie einen der folgenden Modi aus: **Unaufgefordertes Multicast**: Routeranzeigen (RAs) an alle Schnittstellen senden, die zur Multicast-Gruppe gehören. **Nur Unicast**: Beschränkt Anzeigen auf allgemein bekannte IPv6-Adressen (RAs werden nur an die Schnittstelle gesendet, die zur bekannten Adresse gehört).

Anzeigeintervall	Anzeigeintervall (4–1800) für **Unaufgefordertes Multicast**. Der Standardwert lautet 30. Das Anzeigeintervall ist ein zufälliger Wert zwischen dem Mindestintervall für die Routeranzeige (Minimum Router Advertisement Interval, MinRtrAdvInterval) und dem Maximalintervall für die Routeranzeige (Maximum Router Advertisement Interval, MaxRtrAdvInterval). MinRtrAdvInterval = 0.33 * MaxRtrAdvInterval
RA-Kennzeichen	Aktivieren Sie **Verwaltet**, um das verwaltete/ statusbehaftete Protokoll für die automatische Adressenkonfiguration zu verwenden. Aktivieren Sie **Andere**, um das verwaltete/ statusbehaftete Protokoll für die automatische Konfiguration anderer Informationen, bei denen es sich nicht um Adressen handelt, zu verwenden.
Routerpriorität	Wählen Sie im Dropdown-Menü **Niedrig**, **Mittel** oder **Hoch** aus. Der Standardwert lautet „Mittel“. Die Router-Voreinstellung stellt eine Voreinstellungsmetrik für Standardrouter bereit. Die Werte „Niedrig“, „Mittel“ und „Hoch“ werden in nicht verwendeten Bits in RA-Nachrichten signalisiert. Diese Erweiterung ist sowohl für Router (Festlegen des Router-Voreinstellungswerts) als auch für Hosts (Interpretieren des Router-Voreinstellungswerts) abwärtskompatibel. Diese Werte werden von Hosts ignoriert, die keine Routerpriorität implementieren. Die Funktion ist hilfreich, wenn im LAN andere RADVD-fähige Geräte vorhanden sind.

MTU	MTU-Größe (0 oder 1.280 bis 1.500). Der Standardwert beträgt 1.500 Bytes. Bei der MTU (Maximum Transmission Unit) handelt es sich um die Größe des größten Pakets, das über das Netzwerk gesendet werden kann. Die MTU-Größe wird in RAs verwendet, um sicherzustellen, dass alle Knoten im Netzwerk den gleichen MTU-Wert verwenden, wenn die LAN-MTU-Größe nicht allgemein bekannt ist.
Router-Lebensdauer	Router-Lebensdauerwert oder die Zeit in Sekunden, während der die Anzeigenachrichten in der Route vorhanden sind. Der Standardwert beträgt 3.600 Sekunden.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von Anzeigepräfixen

So konfigurieren Sie die verfügbaren RADVD-Präfixe:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Anzeigepräfixe** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie folgende Informationen ein:

IPv6-Präfixtyp	Wählen Sie eine der folgenden Typen aus: **6to4**: Ermöglicht die Übertragung von IPv6-Paketen über ein IPv4-Netzwerk. Es wird verwendet, wenn ein Endbenutzer über eine vorhandene IPv4-Verbindung eine Verbindung zum IPv6-Internet herstellen möchte. **Global/Lokal**: Eine lokal eindeutige IPv6-Adresse, die Sie in privaten IPv6-Netzwerken verwenden können, oder eine global eindeutige IPv6-Internetadresse.

SLA-ID	Wenn Sie **6to4** als IPv6-Präfixtyp auswählen, geben Sie die SLA-ID (Site-Level Aggregation Identifier) ein. Die SLA-ID im 6to4-Adresspräfix ist auf die Schnittstellen-ID der Schnittstelle festgelegt, über die die Anzeigen gesendet werden.
IPv6-Präfix	Wenn Sie **Global/Lokal** als IPv6-Präfixtyp auswählen, geben Sie das IPv6-Präfix ein. Das IPv6-Präfix gibt die IPv6-Netzwerkadresse an.
IPv6-Präfixlänge	Wenn Sie **Global/Lokal** als IPv6-Präfixtyp auswählen, geben Sie die Präfixlänge ein. Die Präfixlänge ist ein Dezimalwert, der die Anzahl der zusammenhängenden höherwertigen Bits der Adresse angibt, die den Netzwerkteil der Adresse bilden.
Präfixgültigkeitsdauer	Präfixgültigkeitsdauer oder der Zeitraum, in dem der anfordernde Router das Präfix verwenden darf.

SCHRITT 4 Klicken Sie auf **Speichern**.

4

Konfigurieren von WLANs

Sicherheitsfunktionen bei der WLAN-Datenübermittlung

WLANs sind praktisch und einfach zu installieren. Da in WLANs Informationen über Funkwellen gesendet werden, sind diese Netzwerke anfälliger für Eindringlinge als herkömmliche Kabelnetzwerke.

Sie können nicht physisch verhindern, dass jemand eine Verbindung mit Ihrem WLAN herstellt, aber Sie können das Netzwerk mit den folgenden Schritten schützen:

- Ändern Sie den Standardnamen des WLANs (die SSID).

  WLAN-Geräte haben im WLAN einen Standardnamen bzw. eine Standard-SSID. Dies ist der Name des WLANs, der aus maximal 32 Zeichen bestehen kann.

  Ändern Sie zum Schutz des Netzwerks den Standardnamen für das WLAN in einen eindeutigen Namen, um das WLAN von anderen WLANs in der Umgebung zu unterscheiden.

  Verwenden Sie bei der Auswahl des Namens keine persönlichen Informationen, da diese für jeden sichtbar sind, der nach WLANs sucht.

- Ändern Sie das Standardkennwort.

  Bei WLAN-Produkten wie Zugriffspunkten, Routern und Gateways werden Sie nach einem Kennwort gefragt, wenn Sie die Einstellungen ändern möchten. Diese Geräte haben ein Standardkennwort. Das Standardkennwort lautet oft **cisco**.

  Hacker kennen diese Standardwerte und versuchen möglicherweise, mit diesen Standardwerten auf Ihr WLAN-Gerät zuzugreifen und die Netzwerkeinstellungen zu ändern. Verhindern Sie nicht autorisierte Zugriffe, indem Sie für das Gerät ein schwer zu erratendes Kennwort wählen.

- Aktivieren Sie die MAC-Adressenfilterung.

Bei Routern und Gateways von Cisco haben Sie die Möglichkeit, die MAC-Adressenfilterung zu aktivieren. Die MAC-Adresse ist eine eindeutige Folge von Ziffern und Buchstaben, die jedem Netzwerkgerät zugewiesen wird.

Wenn die MAC-Adressenfilterung aktiviert ist, können nur WLAN-Geräte mit bestimmten MAC-Adressen auf das WLAN zugreifen. Sie können beispielsweise die MAC-Adressen der einzelnen Computer im Netzwerk angeben, sodass nur diese Computer auf das WLAN zugreifen können.

- Aktivieren Sie die Verschlüsselung.

  Verschlüsselung schützt Daten, die über ein WLAN übertragen werden. WPA/WPA2 (Wi-Fi Protected Access) und WEP (Wired Equivalent Privacy) bieten unterschiedliche Sicherheitsstufen für WLAN-Kommunikation. Zurzeit müssen Wi-Fi-zertifizierte Geräte WPA2 unterstützen, WEP jedoch nicht.

  Ein mit WPA/WPA2 verschlüsseltes Netzwerk ist sicherer als ein mit WEP verschlüsseltes Netzwerk, da bei WPA/WPA2 eine Verschlüsselung mit dynamischen Schlüsseln verwendet wird.

  Aktivieren Sie zum Schutz der Informationen bei der Funkübertragung die höchste Verschlüsselungsstufe, die von den Netzwerkgeräten unterstützt wird.

  WEP ist ein älterer Verschlüsselungsstandard und ist möglicherweise bei einigen älteren Geräten ohne WPA-Unterstützung die einzige verfügbare Option.

- Stellen Sie WLAN-Router, Zugriffspunkte oder Gateways nicht in der Nähe von Außenwänden und Fenstern auf.
- Schalten Sie WLAN-Router, Zugriffspunkte oder Gateways aus, wenn sie nicht verwendet werden (beispielsweise nachts oder wenn Sie im Urlaub sind).
- Verwenden Sie sichere Kennwörter bzw. Schlüssel mit mindestens acht Zeichen. Kombinieren Sie Buchstaben und Ziffern, um die Verwendung von Standardwörtern zu vermeiden, die in einem Wörterbuch gefunden werden können.

Allgemeine Richtlinien für die Netzwerksicherheit

Die Sicherheit in einem WLAN ist wirkungslos, wenn das zugrunde liegende Netzwerk nicht sicher ist. Es wird empfohlen, die folgenden Vorsichtsmaßnahmen zu treffen:

- Schützen Sie alle Computer im Netzwerk mit einem Kennwort, und schützen Sie vertrauliche Dateien individuell mit Kennwörtern.

- Ändern Sie die Kennwörter regelmäßig.
- Installieren Sie Antivirensoftware und Personal Firewall-Software.
- Deaktivieren Sie Dateifreigaben (Peer-to-Peer), um zu verhindern, dass Anwendungen ohne Ihre Einwilligung Dateifreigaben verwenden.

WLANs auf dem Gerät

Auf dem Gerät werden vier virtuelle WLANs bzw. vier SSIDs (Service Set Identifiers) bereitgestellt: ciscosb1“, ciscosb2“, ciscosb3“ und ciscosb4“. Dabei handelt es sich um die Standardnamen oder SSIDs dieser Netzwerke, die Sie jedoch in aussagekräftigere Namen ändern können. In dieser Tabelle werden die Standardeinstellungen für die Netzwerke beschrieben.

SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Aktiviert	Ja	Nein	Nein	Nein
SSID-Übertragung	Aktiviert	Deaktiviert	Deaktiviert	Deaktiviert
Sicherheits-modus	Deaktiviert[1]	Deaktiviert	Deaktiviert	Deaktiviert
MAC-Filter	Deaktiviert	Deaktiviert	Deaktiviert	Deaktiviert
VLAN	1	1	1	1
WLAN-Isolation mit SSID	Deaktiviert	Deaktiviert	Deaktiviert	Deaktiviert
WMM	Aktiviert	Aktiviert	Aktiviert	Aktiviert
WPS-Hardwaretaste	Aktiviert	Deaktiviert	Deaktiviert	Deaktiviert

1. Wählen Sie beim Verwenden des Setup-Assistenten die Option „Höchste Sicherheit“ oder „Höhere Sicherheit“ aus, um das Gerät vor nicht autorisierten Zugriffen zu schützen.

Konfigurieren der Basis-WLAN-Einstellungen

Wählen Sie **WLAN** > **Basiseinstellungen** aus, um die grundlegenden WLAN-Einstellungen zu konfigurieren.

So konfigurieren Sie grundlegende WLAN-Einstellungen:

SCHRITT 1 Wählen Sie **WLAN** > **Basiseinstellungen** aus.

SCHRITT 2 Aktivieren Sie im Feld **Funk** das Kontrollkästchen **Aktivieren**, um den WLAN-Sender zu aktivieren. Standardmäßig ist nur ein WLAN aktiviert (**ciscosb1**).

SCHRITT 3 Wählen Sie im Feld **WLAN-Modus** im Dropdown-Menü eine dieser Optionen aus:

B/G/N gemischt	Wählen Sie diese Option aus, wenn im Netzwerk Wireless-N-, Wireless-B- und Wireless-G-Geräte vorhanden sind. Dies ist die Standardeinstellung (empfohlen).
Nur B	Wählen Sie diese Option aus, wenn im Netzwerk nur Wireless-B-Geräte vorhanden sind.
Nur G	Wählen Sie diese Option aus, wenn im Netzwerk nur Wireless-G-Geräte vorhanden sind.
Nur N	Wählen Sie diese Option aus, wenn im Netzwerk nur Wireless-N-Geräte vorhanden sind.
B/G gemischt	Wählen Sie diese Option aus, wenn im Netzwerk Wireless-B- und Wireless-G-Geräte vorhanden sind.
G/N gemischt	Wählen Sie diese Option aus, wenn im Netzwerk Wireless-G- und Wireless-N-Geräte vorhanden sind.

SCHRITT 4 Wenn Sie **B/G/N gemischt**, **Nur N** oder **G/N gemischt** ausgewählt haben, wählen Sie im Feld **Frequenzband** die WLAN-Bandbreite des Netzwerks aus (**20MHz** oder **20/40MHz**). Wenn Sie „Nur N“ auswählen, müssen Sie im Netzwerk WPA2-Sicherheit verwenden. Weitere Informationen hierzu finden Sie unter **Konfigurieren des Sicherheitsmodus**.

SCHRITT 5 Wählen Sie im Feld **Kanal** im Dropdown-Menü den Kanal aus.

SCHRITT 6 Wählen Sie im Feld **VLAN für die Zugriffspunktverwaltung** die Option **VLAN 1** aus, wenn Sie die Standardeinstellungen verwenden.

Wenn Sie zusätzliche VLANs erstellen, wählen Sie einen Wert aus, der dem VLAN entspricht, das in anderen Switches im Netzwerk konfiguriert ist. Dies dient zu Sicherheitszwecken. Möglicherweise müssen Sie das Verwaltungs-VLAN ändern, um den Zugriff auf den Gerätemanager einzuschränken.

SCHRITT 7 (Optional) Aktivieren Sie im Feld **U-APSD (WMM-Energieeinsparung)** das Kontrollkästchen **Aktivieren**, um die U-APSD-Funktion (Unscheduled Automatic Power Save Delivery) zu aktivieren, die auch als WMM Power Save (WMM-Energieeinsparung) bezeichnet wird und Energieeinsparungen am Sender ermöglicht.

U-APSD ist eine Energiesparfunktion, die für Echtzeitanwendungen wie beispielsweise VoIP optimiert wurde, bei denen Vollduplexdaten über ein WLAN übertragen werden. Durch die Klassifizierung des ausgehenden IP-Verkehrs als Sprachdaten ermöglichen diese Anwendungsarten eine Verlängerung der Akkulaufzeit um ca. 25 % und minimieren Übertragungsverzögerungen.

SCHRITT 8 (Optional) Konfigurieren Sie die Einstellungen der vier WLANs (siehe **Bearbeiten der WLAN-Einstellungen**).

SCHRITT 9 Klicken Sie auf **Speichern**.

Bearbeiten der WLAN-Einstellungen

In der Tabelle **WLANs** auf der Seite **Basiseinstellungen** werden die Einstellungen der vier auf dem Gerät unterstützten WLANs aufgeführt.

So konfigurieren Sie die Einstellungen für WLANs:

SCHRITT 1 Aktivieren Sie die Kontrollkästchen der Netzwerke, die Sie konfigurieren möchten.

SCHRITT 2 Klicken Sie auf **Bearbeiten**.

SCHRITT 3 Konfigurieren Sie die folgenden Einstellungen:

SSID aktivieren	Klicken Sie auf **Ein**, um das Netzwerk zu aktivieren.
SSID	Geben Sie den Namen des Netzwerks ein.

SSID-Übertragung	Aktivieren Sie dieses Kontrollkästchen, um die Übertragung der SSID zu aktivieren. Wenn die SSID-Übertragung aktiviert ist, kündigt der WLAN-Router WLAN-fähigen Geräten in seiner Reichweite seine Verfügbarkeit an.
Sicherheitsmodus	Weitere Informationen hierzu finden Sie unter **Konfigurieren des Sicherheitsmodus**.
MAC-Filter	Weitere Informationen hierzu finden Sie unter **Konfigurieren der MAC-Filterung**.
VLAN	Wählen Sie das dem Netzwerk zugeordnete VLAN aus.
WLAN-Isolation mit SSID	Aktivieren Sie dieses Kontrollkästchen, um die WLAN-Isolation innerhalb der SSID zu aktivieren.
WMM (Wi-Fi Multimedia)	Aktivieren Sie dieses Kontrollkästchen, um WMM zu aktivieren.
Max. zugeordnete Clients	Die maximale Anzahl von Clients, die eine Verbindung mit dem ausgewählten WLAN herstellen können. Geben Sie einen Wert zwischen 1 und 64 ein.
WPS	Aktivieren Sie dieses Kontrollkästchen, um die WPS-Taste an der Vorderseite des Geräts diesem Netzwerk zuzuordnen.
Portalprofil	Weitere Informationen hierzu finden Sie unter **Konfigurieren eines Captive Portal**.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren des Sicherheitsmodus

Sie können einen der folgenden Sicherheitsmodi für WLANs konfigurieren:

Konfigurieren von WEP

Der WEP-Sicherheitsmodus bietet ein niedriges Sicherheitsniveau mit einer einfachen Verschlüsselungsmethode, die nicht so sicher ist wie WPA. Möglicherweise müssen Sie WEP verwenden, wenn die Netzwerkgeräte nicht für WPA geeignet sind.

HINWEIS Wenn Sie WEP nicht verwenden müssen, empfehlen wir die Verwendung von WPA2. Wenn Sie den WLAN-Modus „Nur N“ verwenden, müssen Sie WPA2 verwenden.

So konfigurieren Sie den WEP-Sicherheitsmodus:

SCHRITT 1 Wählen Sie **WLAN** > **Basiseinstellungen** aus. Aktivieren Sie in der Tabelle **WLANs** das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **Sicherheitsmodus bearbeiten**. Die Seite **Sicherheitseinstellungen** wird angezeigt.

SCHRITT 3 Wählen Sie im Feld **SSID auswählen** die SSID aus, für die Sie die Sicherheitseinstellungen konfigurieren möchten.

SCHRITT 4 Wählen Sie im Menü **Sicherheitsmodus** die Option **WEP** aus.

SCHRITT 5 Wählen Sie im Feld **Authentifizierungstyp** eine der folgenden Optionen aus:

- **Offenes System**: Dies ist die Standardoption.
- **Gemeinsamer Schlüssel**: Wählen Sie diese Option aus, wenn der Netzwerkadministrator diese Einstellung empfiehlt. Wenn Sie nicht sicher sind, wählen Sie die Standardoption aus.

In beiden Fällen muss der WLAN-Client den richtigen gemeinsamen Schlüssel (Kennwort) angeben, um Zugriff auf das WLAN zu erhalten.

SCHRITT 6 Wählen Sie im Feld **Verschlüsselung** den Verschlüsselungstyp aus:

- **10/64-Bit (10 HEX-Zeichen):** Stellt einen 40-Bit-Schlüssel bereit.
- **26/128-Bit (26 HEX-Zeichen)**: Stellt einen 104-Bit-Schlüssel bereit, der stärkere Verschlüsselung bietet und daher schwerer zu entschlüsseln ist. Wir empfehlen 128-Bit-Verschlüsselung.

SCHRITT 7 (Optional) Geben Sie in das Feld **Kennsatz** einen alphanumerischen Begriff ein (optimale Sicherheit erreichen Sie mit mehr als acht Zeichen), und klicken Sie auf

Schlüssel generieren, um in den Feldern **WEP** vier eindeutige WEP-Schlüssel zu generieren.

Wenn Sie einen eigenen Schlüssel angeben möchten, geben Sie diesen direkt in das Feld **Schlüssel 1** ein (empfohlen). Die Länge des Schlüssels sollte 5 ASCII-Zeichen (oder 10 Hexadezimalzeichen) für 64-Bit-WEP und 13 ASCII-Zeichen (oder 26 Hexadezimalzeichen) für 128-Bit WEP betragen. Gültige Hexadezimalzeichen sind 0 bis 9 und A bis F.

SCHRITT 8 Wählen Sie im Feld **TX-Schlüssel** aus, welcher Schlüssel als Pre-Shared Key verwendet werden soll, den Geräte verwenden müssen, um auf das WLAN zuzugreifen.

SCHRITT 9 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

SCHRITT 10 Klicken Sie auf **Zurück**, um zur Seite **Basiseinstellungen** zurückzukehren.

Konfigurieren von WPA-Personal, WPA2-Personal und WPA2-Personal Mixed

Die Sicherheitsmodi WPA-Personal, WPA2-Personal und WPA2-Personal Mixed können als Ersatz für WEP genutzt werden und bieten hohe Sicherheit.

- **WPA-Personal**: WPA ist ein Bestandteil des Wireless-Sicherheitsstandards (802.11i) der Wi-Fi Alliance und sollte als Übergangslösung WEP ersetzen, während der 802.11i-Standard erarbeitet wurde. WPA-Personal unterstützt TKIP (Temporal Key Integrity Protocol) und AES-Verschlüsselung (Advanced Encryption Standard).
- **WPA2-Personal**: (Empfohlen) WPA2 ist die Implementierung des im endgültigen 802.11i-Standard vorgegebenen Sicherheitsstandards. WPA2 unterstützt AES-Verschlüsselung und Authentifizierung über PSK (Pre-Shared Key).
- **WPA2-Personal Mixed**: Ermöglicht WPA- sowie WPA2-Clients gleichzeitige Verbindungen mit PSK-Authentifizierung.

Bei der persönlichen Authentifizierung wird der PSK verwendet, bei dem es sich um eine alphanumerische Passphrase handelt, die mit dem WLAN-Peer ausgetauscht wird.

So konfigurieren Sie den Sicherheitsmodus WPA-Personal:

SCHRITT 1 Aktivieren Sie in der **WLAN-Tabelle** (**WLAN** > **Basiseinstellungen**) das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **Sicherheitsmodus bearbeiten**. Die Seite **Sicherheitseinstellungen** wird angezeigt.

SCHRITT 3 Wählen Sie im Feld **SSID auswählen** die SSID aus, für die Sie die Sicherheitseinstellungen konfigurieren möchten.

SCHRITT 4 Wählen Sie im Menü **Sicherheitsmodus** eine der drei Optionen für WPA-Personal aus.

SCHRITT 5 (Nur WPA-Personal) Wählen Sie im Feld **Verschlüsselung** eine der folgenden Optionen aus:

- **TKIP/AES**: Wählen Sie **TKIP/AES** aus, um die Kompatibilität mit älteren WLAN-Geräten sicherzustellen, die AES möglicherweise nicht unterstützen.
- **AES**: Dies ist die sicherere Option.

SCHRITT 6 Geben Sie in das Feld **Sicherheitsschlüssel** eine alphanumerische Zeichenfolge (8 – 63 ASCII-Zeichen oder 64 hexadezimale Ziffern) ein. Die Kennwortsicherheitsmessung zeigt die Sicherheit des Schlüssels an: „Unter Minimum“, „Schwach“, „Stark“, „Sehr stark“ oder „Sicher“. Wir empfehlen, einen Sicherheitsschlüssel zu verwenden, der in der Sicherheitsmessung als „Sicher“ eingestuft wird.

SCHRITT 7 Zum Anzeigen des Sicherheitsschlüssels bei der Eingabe aktivieren Sie das Kontrollkästchen **Kennwortmaskierung aufheben**.

SCHRITT 8 Geben Sie in das Feld **Schlüsselerneuerung** die Zeit (600-7.200 Sekunden) ein, die zwischen Schlüsselerneuerungen verstreichen soll. Der Standardwert lautet „3.600“.

SCHRITT 9 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern. Klicken Sie auf **Zurück**, um zur Seite **Basiseinstellungen** zurückzukehren.

Konfigurieren von WPA-Enterprise, WPA2-Enterprise und WPA2-Enterprise Mixed

Die Sicherheitsmodi WPA-Enterprise, WPA2-Enterprise und WPA2-Enterprise Mixed ermöglichen die Verwendung von RADIUS-Serverauthentifizierung.

- **WPA-Enterprise**: Ermöglicht die Verwendung von WPA mit RADIUS-Serverauthentifizierung.
- **WPA2-Enterprise**: Ermöglicht die Verwendung von WPA2 mit RADIUS-Serverauthentifizierung.
- **WPA2-Enterprise Mixed**: Ermöglicht WPA- sowie WPA2-Clients gleichzeitige Verbindungen mit RADIUS-Authentifizierung.

So konfigurieren Sie den Sicherheitsmodus WPA-Enterprise:

SCHRITT 1 Aktivieren Sie in der **WLAN-Tabelle** (**WLAN** > **Basiseinstellungen**) das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **Sicherheitsmodus bearbeiten**.

SCHRITT 3 Wählen Sie im Feld **SSID auswählen** die SSID aus, für die Sie die Sicherheitseinstellungen konfigurieren möchten.

SCHRITT 4 Wählen Sie im Menü **Sicherheitsmodus** eine der drei Optionen für WPA-Enterprise aus.

SCHRITT 5 (Nur WPA-Enterprise) Wählen Sie im Feld **Verschlüsselung** eine der folgenden Optionen aus:

- **TKIP/AES**: Wählen Sie **TKIP/AES** aus, um die Kompatibilität mit älteren WLAN-Geräten sicherzustellen, die AES möglicherweise nicht unterstützen.
- **AES**: Dies ist die sicherere Option.

SCHRITT 6 Geben Sie in das Feld **RADIUS-Server** die IP-Adresse des RADIUS-Servers ein.

SCHRITT 7 Geben Sie in das Feld **RADIUS-Port** den Port ein, der für den Zugriff auf den RADIUS-Server verwendet wird.

SCHRITT 8 Geben Sie eine alphanumerische Zeichenfolge in das Feld **Gemeinsamer Schlüssel** ein.

SCHRITT 9 Geben Sie in das Feld **Schlüsselerneuerung** die Zeit (600-7.200 Sekunden) ein, die zwischen Schlüsselerneuerungen verstreichen soll. Der Standardwert lautet „3.600“.

SCHRITT 10 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

SCHRITT 11 Klicken Sie auf **Zurück**, um zur Seite **Basiseinstellungen** zurückzukehren.

Konfigurieren der MAC-Filterung

Sie können die MAC-Filterung verwenden, um den Zugriff auf das WLAN basierend auf der MAC-Adresse (Hardwareadresse) des anfordernden Geräts zuzulassen oder zu verweigern. Sie können beispielsweise die MAC-Adressen einer Gruppe von Computern eingeben und nur für diese Computer den Zugriff auf das Netzwerk zulassen. Sie können die MAC-Filterung für jedes Netzwerk bzw. jede SSID konfigurieren.

So konfigurieren Sie die MAC-Filterung:

SCHRITT 1 Aktivieren Sie in der **WLAN-Tabelle** (**WLAN** > **Basiseinstellungen**) das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **MAC-Filter bearbeiten**. Die Seite **WLAN-MAC-Filter** wird angezeigt.

SCHRITT 3 Aktivieren Sie im Feld **MAC-Filter bearbeiten** das Kontrollkästchen **Aktivieren**, um die MAC-Filterung für diese SSID zu aktivieren.

SCHRITT 4 Wählen Sie im Feld **Verbindungssteuerung** die Art des Zugriffs auf das WLAN aus:

- **Verhindern**: Wählen Sie diese Option aus, um zu verhindern, dass Geräte mit den in der **MAC-Adresstabelle** aufgelisteten Adressen auf das WLAN zugreifen. Diese Option ist standardmäßig ausgewählt.
- **Zulassen**: Wählen Sie diese Option aus, um zuzulassen, dass Geräte mit den in der **MAC-Adresstabelle** aufgelisteten Adressen auf das WLAN zugreifen.

SCHRITT 5 Zum Anzeigen der Computer und anderen Geräte im WLAN klicken Sie auf **Clientliste anzeigen**.

SCHRITT 6 Aktivieren Sie im Feld **In MAC-Adressfilterliste speichern** das Kontrollkästchen, um das Gerät der Liste der Geräte hinzuzufügen, die der **MAC-Adresstabelle** hinzugefügt werden sollen.

SCHRITT 7 Klicken Sie auf **Zu MAC hinzufügen**, um die in der **Client-Liste** ausgewählten Geräte der Tabelle **MAC-Adressen** hinzuzufügen.

SCHRITT 8 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

SCHRITT 9 Klicken Sie auf **Zurück**, um zur Seite **Basiseinstellungen** zurückzukehren.

Konfigurieren des Tageszeitzugriffs

Sie können das Netzwerk weiter schützen, indem Sie den Zugriff auf bestimmte Zeiten beschränken, zu denen die Benutzer auf das Netzwerk zugreifen können.

So konfigurieren Sie den Tageszeitzugriff:

SCHRITT 1 Aktivieren Sie in der **WLAN-Tabelle** (**WLAN** > **Basiseinstellungen**) das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **Tageszeitzugriff**. Die Seite **Tageszeitzugriff** wird angezeigt.

SCHRITT 3 Aktivieren Sie im Feld **Aktive Zeit** das Kontrollkästchen **Aktivieren**, um den Tageszeitzugriff zu aktivieren.

SCHRITT 4 Geben Sie in den Feldern **Startzeit** und **Stoppzeit** den Tageszeitraum an, in dem der Zugriff auf das Netzwerk zulässig ist.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren der erweiterten WLAN-Einstellungen

Die erweiterten WLAN-Einstellungen sollten nur von einem erfahrenen Administrator angepasst werden; falsche Einstellungen können die WLAN-Leistung beeinträchtigen.

So konfigurieren Sie die erweiterten WLAN-Einstellungen:

SCHRITT 1 Wählen Sie **WLAN** > **Erweiterte Einstellungen** aus. Die Seite „Erweiterte Einstellungen“ wird angezeigt.

SCHRITT 2 Konfigurieren Sie diese Einstellungen:

Frame Burst	Aktivieren Sie diese Option, um die Leistung der WLANs abhängig vom Hersteller der WLAN-Produkte zu verbessern. Wenn Sie nicht sicher sind, wie diese Option verwendet wird, behalten Sie die Standardeinstellung bei (aktiviert).
Keine WMM-Bestätigung	Durch Aktivieren der Option „Keine WMM-Bestätigung“ können Sie einen effizienteren Durchsatz erzielen. In einer Funkumgebung mit starkem Rauschen kann dies jedoch zu höheren Fehlerraten führen. Standardmäßig ist diese Einstellung deaktiviert.

Basisrate	Die Einstellung „Basisrate“ bezieht sich nicht auf die Übertragungsrate, sondern auf eine Reihe von Raten, mit der die Services Ready-Plattform Daten übertragen kann. Das Gerät kündigt seine Basisrate den anderen WLAN-Geräten im Netzwerk an, sodass diesen die verwendeten Raten bekannt sind. Die Services Ready-Plattform kündigt außerdem an, dass automatisch die beste Rate für die Übertragung ausgewählt wird. Die Standardeinstellung ist „Standard“, wenn das Gerät alle Standardfunkraten unterstützt (1 MBit/s, 2 MBit/s, 5,5 MBit/s, 11 MBit/s, 18 MBit/s, 24 MBit/s, 36 MBit/s, 48 MBit/s und 54 MBit/s). Neben den B- und G-Geschwindigkeiten unterstützt das Gerät auch N-Geschwindigkeiten. Als weitere Optionen stehen 1-2 MBit/s für die Verwendung mit älteren WLAN-Technologien sowie „Alle“ zur Verfügung, wenn das Gerät die Übertragung mit allen WLAN-Raten unterstützt. Die Basisrate entspricht nicht der Rate, mit der Daten tatsächlich übertragen werden. Wenn Sie die Datenübertragungsrate des Geräts angeben möchten, konfigurieren Sie die Einstellung „Übertragungsrate“.
Übertragungsrate	Die Datenübertragungsrate sollte abhängig von der Geschwindigkeit des WLANs festgelegt werden. Neben verschiedenen Übertragungsgeschwindigkeiten steht zudem die Option **Automatisch** zur Verfügung, mit der das Gerät automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert. Beim automatischen Fallback wird die höchstmögliche Verbindungsgeschwindigkeit zwischen dem Gerät und einem WLAN-Client ausgehandelt. Der Standardwert lautet „Automatisch“.

N-Übertragungsrate	Die Datenübertragungsrate sollte abhängig von der Geschwindigkeit des Wireless-N-Netzwerks festgelegt werden. Neben verschiedenen Übertragungsgeschwindigkeiten steht zudem die Option **Automatisch** zur Verfügung, mit der das Gerät automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert. Beim automatischen Fallback wird die höchstmögliche Verbindungsgeschwindigkeit zwischen dem Gerät und einem WLAN-Client ausgehandelt. Der Standardwert lautet „Automatisch“.
CTS-Schutzmodus	Das Gerät verwendet automatisch den CTS-Schutz (Clear To Send), wenn bei den Wireless-N- und Wireless-G-Geräten schwerwiegende Probleme auftreten und die Geräte in einer Umgebung mit hohem 802.11b-Verkehrsaufkommen keine Daten an das Gerät übertragen können. Diese Funktion optimiert Wireless-N- und Wireless-G-Übertragungen über das Gerät, führt jedoch zu einer spürbaren Beeinträchtigung der Leistung. Der Standardwert lautet „Automatisch“.
Beacon-Intervall	Der Wert für das Beacon-Intervall gibt das Häufigkeitsintervall des Beacons an. Ein Beacon ist ein vom Gerät zur Synchronisierung des WLANs gesendetes Paket. Geben Sie einen Wert zwischen 40 und 3.500 Millisekunden ein. Der Standardwert lautet „100“.
DTIM-Intervall	Dieser Wert (zwischen 1 und 255) gibt das Intervall für DTIM (Delivery Traffic Indication Message) an. Ein DTIM-Feld ist ein Countdownfeld, das Clients über das nächste Fenster zum Mithören von Broadcast- und Multicast-Nachrichten informiert. Wenn das Gerät Broadcast- oder Multicast-Nachrichten für zugeordnete Clients zwischengespeichert hat, sendet es die nächste DTIM mit einem DTIM-Intervallwert. Die Clients empfangen die Beacons und werden aktiviert, sodass sie die Broadcast- und Multicast-Nachrichten empfangen. Der Standardwert lautet „1“.

Fragmentation Threshold	Dieser Wert gibt die maximal mögliche Paketgröße an, bevor Daten in mehrere Pakete aufgeteilt werden. Wenn Sie eine hohe Paketfehlerrate beobachten, können Sie den Fragmentierungsschwellenwert etwas erhöhen. Wenn Sie einen zu niedrigen Fragmentierungsschwellenwert festlegen, kann dies die Netzwerkleistung beeinträchtigen. Es wird empfohlen, den Wert nur geringfügig zu verringern. In den meisten Fällen sollten Sie den Standardwert „2.346“ beibehalten.
RTS Threshold	Wenn Sie einen uneinheitlichen Datenfluss beobachten, geben Sie nur einen geringfügig niedrigeren Wert ein. Empfohlen wird der Standardwert „2.347“. Wenn die Größe eines Netzwerkpakets den vorgegebenen RTS-Schwellenwert (Request to Send) unterschreitet, wird der RTS/CTS-Mechanismus (Clear to Send) nicht aktiviert. Die Services Ready-Plattform sendet RTS-Frames an eine bestimmte Empfängerstation und handelt das Senden eines Daten-Frames aus. Nach Empfang eines RTS antwortet die Funkstation mit einem CTS-Frame, um zu bestätigen, dass die Übertragung beginnen kann.

SCHRITT 3 Klicken Sie auf **Speichern**.

Erkennen unberechtigter Zugriffspunkte

Ein unberechtigter Zugriffspunkt ist ein Zugriffspunkt, der ohne explizite Autorisierung eines Systemadministrators in einem sicheren Netzwerk installiert wurde. Unberechtigte Zugriffspunkte stellen ein Sicherheitsrisiko dar, da beliebige Personen mit Zugang zum Standort einen WLAN-Zugriffspunkt installieren können, der nicht autorisierten Personen den Zugriff auf das Netzwerk ermöglicht.

Auf der Seite „Erkennung unberechtigter Zugriffspunkte“ können Sie das Gerät so konfigurieren, dass Informationen zu allen vom Gerät in der Nähe des Netzwerks erkannten Zugriffspunkten angezeigt werden. Wenn ein als unberechtigt aufgeführter Zugriffspunkt tatsächlich berechtigt ist, können Sie ihn in die Tabelle **Autorisierte Zugriffspunkte** aufnehmen. Wählen Sie eine Aktualisierungsrate aus, damit auf der Seite „Erkennung unberechtigter Zugriffspunkte“ immer aktuelle Informationen angezeigt werden.

So aktivieren Sie die Erkennung unberechtigter Zugriffspunkte:

SCHRITT 1 Wählen Sie **WLAN > Unberechtigter Zugriffspunkt** aus.

SCHRITT 2 Klicken Sie unter **Erkennung unberechtigter Zugriffspunkte** auf die Optionsschaltfläche „Ein“.

SCHRITT 3 Klicken Sie auf **Speichern**.

So autorisieren Sie erkannte Zugriffspunkte:

SCHRITT 1 Aktivieren Sie in der Tabelle **Erkannte unberechtigte Zugriffspunkte** das Kontrollkästchen für den Zugriffspunkt, den Sie autorisieren möchten.

SCHRITT 2 Klicken Sie auf **Autorisieren**.

So nehmen Sie einen Zugriffspunkt in die Tabelle „Autorisierte Zugriffspunkte“ auf:

SCHRITT 1 Klicken Sie auf **Hinzufügen**.

SCHRITT 2 Geben Sie die MAC-Adresse des Zugriffspunkts ein, den Sie autorisieren möchten.

SCHRITT 3 Geben Sie die SSID oder den Namen des WLANs ein.

SCHRITT 4 Wählen Sie den Sicherheitsmodus für den Zugriffspunkt aus.

SCHRITT 5 Wählen Sie „TKIP“ (Temporal Key Integrity Protocol) oder „CCMP“ (Counter Cipher Mode Protocol) als Verschlüsselungsalgorithmus für den Zugriffspunkt aus.

SCHRITT 6 Wählen Sie „RADIUS-Server“ oder „PSK“ (Pre-Shared Key) für die Authentifizierung des Zugriffspunkts aus.

SCHRITT 7 Wählen Sie den WLAN-Modus des Zugriffspunkts aus.

SCHRITT 8 Wählen Sie die Sendefrequenz des Zugriffspunkts aus.

SCHRITT 9 Klicken Sie auf **Speichern**.

Importieren von Listen mit autorisierten Zugriffspunkten

Sie können eine Liste mit autorisierten Zugriffspunkten in Form einer CSV-Datei importieren. Verwenden Sie beim Erstellen der CSV-Datei die folgenden Werte als Referenz.

Feld	Werte
Sicherheit	• 0 : Offen • 1 : WEP • 2 : WPA-Personal • 3 : WPA-Enterprise • 4 : WPA2-Personal • 5 : WPA2-Enterprise
Netzwerkmodus	• 0 : Nur B • 1 : Nur G • 2 : Nur N • 3 : B/G gemischt • 4 : G/N gemischt • 5 : B/G/N gemischt

Feld	Werte
Kanal	• 0 : Automatisch • 1 — 2,412 • 2 — 2,417 • 3 — 2,422 • 4 — 2,427 • 5 — 2,432 • 6 — 2,437 • 7 — 2,442 • 8 — 2,447 • 9 — 2,452 • 10 — 2,457 • 11 — 2,462
Verschlüsselung	• 2 : TKIP • 4 : CCMP
Authentifizierung	• 2 : PSK • 1 : RADIUS

Die Daten in der CSV-Datei müssen wie im folgenden Beispiel dargestellt angeordnet sein:

BSSID	Sicherheit	Verschlüsse-lung	Authentifizie-rung	Wireless-Netzwerk	Kanal	SSID
00:1C:10:CE:44:48	4	2	2	3	1	Auth_Guest

So importieren Sie eine Liste mit autorisierten Zugriffspunkten:

SCHRITT 1 Klicken Sie auf **Zusammenführen**, um die Liste mit den zu importierenden Zugriffspunkten den in der Tabelle **Autorisierte Zugriffspunkte** angezeigten Zugriffspunkten hinzuzufügen. Klicken Sie auf **Ersetzen**, um die Zugriffspunkte in der Tabelle durch die Zugriffspunkte in der zu importierenden Liste zu ersetzen.

SCHRITT 2 Klicken Sie auf **Durchsuchen**, um die zu importierende Datei auszuwählen.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von WDS

Ein Wireless Distribution System (WDS) ist ein System, das WLAN-Verbindungen zwischen Zugriffspunkten in einem Netzwerk ermöglicht. So kann ein WLAN mit mehreren Zugriffspunkten erweitert werden, ohne dass diese über einen drahtgebundenen Backbone verbunden sein müssen.

Zum Einrichten einer WDS-Verbindung müssen Sie das Gerät und sonstige WDS-Remote-Peers mit denselben Einstellungen für WLAN-Modus, Kanal, Frequenzbandauswahl und Verschlüsselungstypen („Keine“ oder „WEP“) konfigurieren.

Sie können WDS im Bridge-Modus, in dem ein Zugriffspunkt als gemeinsame Verbindung zwischen mehreren Zugriffspunkten fungiert, oder im Repeater-Modus konfigurieren, in dem ein Zugriffspunkt ohne drahtgebundene LAN-Verbindung mit zwei Zugriffspunkten verbunden wird, indem die Signale über die WLAN-Verbindung übertragen werden.

WDS wird nur für eine SSID unterstützt.

So konfigurieren Sie WDS im Bridge-Modus:

SCHRITT 1 Wählen Sie **WLAN** > **WDS** aus.

SCHRITT 2 Wählen Sie in der Drop-down-Liste **Update-Intervall** aus.

SCHRITT 3 Aktivieren Sie die Optionsschaltfläche **WDS-Bridge**.

SCHRITT 4 Geben Sie unter **MAC-Adresse der Remote-WLAN-Bridge** in die Felder **MAC 1**, **MAC 2**, **MAC 3** und **MAC 4** die MAC-Adressen von bis zu vier Zugriffspunkten ein, die als Bridges verwendet werden sollen.

SCHRITT 5 Klicken Sie auf **Speichern**.

So konfigurieren Sie WDS im Repeater-Modus:

SCHRITT 1 Wählen Sie **WLAN** > **WDS** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **WDS**.

SCHRITT 3 Wählen Sie den Repeater-Modus aus. Wenn Sie **Wi-Fi-Signal darf durch einen Repeater wiederholt werden** ausgewählt haben, geben Sie in die Felder **MAC 1**, **MAC 2** und **MAC 3** die MAC-Adressen von maximal drei Zugriffspunkten ein, die als Repeater verwendet werden sollen.

SCHRITT 4 Wenn Sie **Wi-Fi-Signal darf durch einen Repeater wiederholt werden** ausgewählt haben, führen Sie folgende Schritte aus:

- Geben Sie in das Feld **MAC** die MAC-Adresse eines WLAN-Zugriffspunkts ein.
- Klicken Sie zum Anzeigen der Tabelle **Verfügbare Netzwerke** auf **Verfügbare Netzwerke einblenden.** Klicken Sie auf **Verbinden**, um die MAC-Adresse des ausgewählten Zugriffspunkts in das Feld **MAC** einzufügen.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von WPS

Konfigurieren Sie WPS, damit WPS-fähige Geräte einfach und sicher mit dem WLAN verbunden werden können. Weitere Anweisungen zum Einrichten von WPS auf Ihrem Clientgerät finden Sie in der Dokumentation zum jeweiligen Clientgerät.

So konfigurieren Sie WPS:

SCHRITT 1 Wählen Sie **WLAN** > **WPS** aus. Die Seite „WPS“ wird angezeigt.

SCHRITT 2 Wählen Sie im Drop-down-Menü die Option "SSID" aus.

SCHRITT 3 Konfigurieren Sie WPS für Clientgeräte mit einer der drei folgenden Methoden:

a. Klicken Sie auf den WPS-Knopf am Clientgerät (oder drücken Sie darauf), und klicken Sie dann auf das WPS-Symbol auf dieser Seite.

b. Geben Sie die WPS-PIN-Nummer des Client ein, und klicken Sie auf **Registrieren**.

c. Wenn ein Clientgerät die PIN-Nummer dieses Routers anfordert, geben Sie die angezeigte PIN-Nummer ein.

Geräte-PIN-Status: PIN-Status des WPA-Geräts.

Geräte-PIN: Gibt die PIN des Gerätes an, das versucht eine Verbindung herzustellen.

PIN-Gültigkeitsdauer: Die Gültigkeitsdauer des Schlüssels. Wenn die Gültigkeit abläuft, wird ein neuer Schlüssel ausgehandelt.

Wenn Sie WPS konfiguriert haben, werden unten auf der Seite **WPS** die folgenden Informationen angezeigt: Wi-Fi Protected Setup-Status, Netzwerkname (SSID) und Sicherheit.

Konfigurieren eines Captive Portal

Mit der Funktion „Captive Portal“ können Sie kontrollierten, authentifizierten Zugriff auf das Internet und auf Netzwerkressourcen gewähren, ohne die Sicherheit zu beeinträchtigen. In einem Captive Portal wird eine spezielle Webseite zur Authentifizierung von Clients angezeigt, bevor diese Internetzugriff erhalten. Sie können die Captive Portal-Überprüfung konfigurieren, um den Zugriff für Gastbenutzer und authentifizierte Benutzer des Netzwerks zuzulassen.

Konfigurieren Sie Captive Portal-Instanzen für alle virtuellen WLANs auf dem Gerät, indem Sie sie jeweils mit einem Portalprofil verknüpfen.

Erstellen von Captive Portal-Profilen

So erstellen Sie ein Captive Portal-Profil:

SCHRITT 1 Wählen Sie **WLAN > Captive Portal > Portalprofil.** Klicken Sie in der Tabelle **Portalprofile** auf **Hinzufügen**. Um das auf dem Gerät bereitgestellte Portalprofil zu ändern, aktivieren Sie das Kontrollkästchen **Default_Portal_Profile**, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Geben Sie einen Namen für das Captive Portal-Profil ein.

SCHRITT 3 Geben Sie an, ob Gastbenutzer oder Benutzer im Netzwerk anhand des Profils authentifiziert werden sollen.

SCHRITT 4 Um Benutzer nach der Authentifizierung an eine URL umzuleiten, aktivieren Sie das Kontrollkästchen **URL für automatische Umleitung**, und geben Sie in das Feld

URL für Umleitung einen voll qualifizierten Domänennamen oder eine IP-Adresse ein. Geben Sie beispielsweise die URL einschließlich „http://“ ein.

SCHRITT 5 Geben Sie im Feld **Sitzungs-Timeout** die Dauer in Minuten an, während der eine Authentifizierungssitzung mit dem zugeordneten WLAN-Client im Gerät geöffnet bleibt. Der Standard-Timeout beträgt 60 Minuten.

SCHRITT 6 Wählen Sie eine Schriftfarbe für den Text, der auf der Seite angezeigt wird.

SCHRITT 7 Geben Sie den Text an, der angezeigt werden soll, beispielsweise der Name des Unternehmens oder der Text für die Felder für Benutzername und Kennwort und für die Anmeldeschaltfläche.

SCHRITT 8 Geben Sie den Copyright-Standardtext des Unternehmens ein.

SCHRITT 9 Geben Sie in die Felder **Fehler 1** und **Fehler 2** die Fehlermeldungen ein, die für Clients angezeigt werden sollen, wenn die Anmeldung fehlschlägt und wenn die maximale Anzahl von Verbindungen überschritten wird.

SCHRITT 10 Um ein Kontrollkästchen zu anzuzeigen, über das Benutzer vor dem Fortfahren die Nutzungsbedingungen akzeptieren können, aktivieren Sie das Kontrollkästchen **Vereinbarung**. Der Text im Feld **Text der Vereinbarung** wird als Beschriftung für das Kontrollkästchen angezeigt.

SCHRITT 11 Geben Sie in das Feld **Nutzungsrichtlinie akzeptieren** die Nutzungsbedingungen ein, die Benutzern angezeigt werden sollen.

SCHRITT 12 Wählen Sie unter **Dateien hochladen** entsprechende Dateien aus, um beispielsweise das Unternehmenslogo und Hintergrundbilder gemäß Markenrichtlinie des Unternehmens hochzuladen. Speichern Sie das Profil.

Um eine Vorschau des Profils anzuzeigen, wählen Sie **Captive Portal > Portalvorschau** aus, und wählen Sie in der Dropdown-Liste **Portalprofil** das Profil aus.

Konfigurieren von Captive Portal-Instanzen

So konfigurieren Sie eine Captive Portal-Instanz für das Gerät:

SCHRITT 1 Wählen Sie **WLAN > Basiseinstellungen** aus.

SCHRITT 2 Aktivieren Sie in der Tabelle **WLANs** das Kontrollkästchen **Aktivieren** für die SSID, für die Sie ein Captive Portal konfigurieren möchten. Klicken Sie auf **Bearbeiten**.

SCHRITT 3 Wählen Sie ein Portalprofil für die SSID aus.

Sie können mit der SSID für das Gerät bis zu vier Captive Portals erstellen. Um ein neues Portalprofil zu erstellen, wählen Sie in der Dropdown-Liste die Option **Neues Portalprofil erstellen** aus. Wählen Sie „Default_Portal_Profile“ aus, um das auf dem Gerät bereitgestellte Portalprofil zu verwenden.

SCHRITT 4 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um das Captive Portal für die SSID zu aktivieren.

SCHRITT 5 Speichern Sie die Captive Portal-Instanzen.

Erstellen von Captive Portal-Benutzerkonten

So erstellen Sie ein Captive Portal-Benutzerkonto:

SCHRITT 1 Wählen Sie **WLAN > Captive Portal > Benutzerkonten**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie einen Benutzernamen und ein Kennwort ein. Geben Sie das Kennwort zur Bestätigung erneut ein.

Kennwörter sollten keine Wörter aus einem Wörterbuch irgendeiner Sprache enthalten. Außerdem sollten sie sowohl Buchstaben (Groß- und Kleinbuchstaben) als auch Ziffern und Symbole enthalten. Das Kennwort darf maximal 64 Zeichen enthalten.

SCHRITT 4 Geben Sie im Feld **Zugriffszeit (Minuten)** die Dauer an, nach der ein Timeout der Authentifizierungssitzung auftritt.

SCHRITT 5 Um Benutzernamen und Kennwörter aus einer CSV-Datei zu importieren, klicken Sie auf **Importieren**. Die Seite **Administration > Benutzer** wird angezeigt. Klicken Sie unter **Benutzername und Kennwort importieren** auf **Durchsuchen**, wählen Sie die Datei aus, und klicken Sie auf **Importieren**. Weitere Informationen finden Sie unter **Importieren von Benutzerkonten**.

SCHRITT 6 Speichern Sie die Benutzerkonten.

Konfigurieren des Gerätemodus

Sie können das Gerät für den Betrieb in den folgenden Modi konfigurieren:

- **Router**: Betrieb als WLAN-Router.

- **Zugriffspunkt**: Bereitstellung von WLAN-Verbindungen für Clients und Erweiterung eines Kabelnetzwerks um die WLAN-Funktion. Alle LAN-Anschlüsse werden deaktiviert, wenn das Gerät als Zugriffspunkt betrieben wird.

  Stellen Sie sicher, dass Sie auf der Seite **Netzwerk > WAN > WAN-Konfiguration** die Einstellungen unter „VLAN für die Zugriffspunktverwaltung“ konfigurieren. Weitere Informationen finden Sie unter **Konfigurieren der optionalen Einstellungen**.

So konfigurieren Sie den Gerätemodus:

SCHRITT 1 Wählen Sie **WLAN > Gerätemodus** aus, und wählen Sie den Modus aus, in dem das Gerät betrieben werden soll.

SCHRITT 2 Klicken Sie auf **Speichern**.

5

Konfigurieren der Firewall

Firewallfunktionen

Sie können das Netzwerk schützen, indem Sie Regeln erstellen und anwenden, anhand derer das Gerät ein- und ausgehenden Internetverkehr selektiv blockiert bzw. zulässt. Dann geben Sie an, auf welche Weise und für welche Geräte die Regeln angewendet werden sollen. Hierzu müssen Sie Folgendes definieren:

- Services oder Verkehrstypen, die der Router zulassen oder blockieren soll. Beispiel: Webbrowsing, VoIP, andere Standardservices sowie benutzerdefinierte Services.
- Die Verkehrsrichtung, indem Sie Quelle und Ziel des Verkehrs angeben; hierzu geben Sie die „Von“-Zone (LAN/WAN/DMZ) und die „An“-Zone (LAN/WAN/DMZ) an.
- Zeitpläne, nach denen der Router Regeln anwenden soll.
- Schlüsselwörter (in einem Domänennamen oder in der URL einer Webseite), die der Router zulassen oder blockieren soll.
- Regeln für das Blockieren des ein- und ausgehenden Internetverkehrs für bestimmte Services nach vorgegebenen Zeitplänen.
- MAC-Adressen von Geräten, bei denen der Router den eingehenden Zugriff auf das Netzwerk blockieren soll.
- Portauslöser, die dem Router signalisieren, dass der Zugriff auf bestimmte durch die Portnummer definierte Services zugelassen oder blockiert werden soll.
- Berichte und Warnungen, die der Router an Sie senden soll.

Sie können beispielsweise Regeln für eingeschränkten Zugriff festlegen, die auf der Tageszeit, auf Webadressen und auf Schlüsselwörtern in Webadressen basieren. Sie können den Internetzugriff durch Anwendungen und Services im LAN blockieren, beispielsweise für Chaträume oder Spiele. Sie können den Zugriff auf bestimmte PC-Gruppen im Netzwerk durch das WAN oder das öffentliche DMZ-Netzwerk blockieren.

Eingangsregeln (von WAN zu LAN/DMZ) schränken den Zugriff für im Netzwerk eingehenden Verkehr ein, sodass nur bestimmte Benutzer von außen auf bestimmte lokale Ressourcen zugreifen können. Standardmäßig wird der gesamte Zugriff von der nicht sicheren WAN-Seite auf das sichere LAN blockiert, sofern es sich nicht um Antworten auf Anforderungen aus dem LAN oder der DMZ handelt. Wenn Sie externen Geräten den Zugriff auf Services im sicheren LAN ermöglichen möchten, müssen Sie für jeden Service eine Firewallregel erstellen.

Wenn Sie eingehenden Verkehr zulassen möchten, müssen Sie die IP-Adresse des WAN-Anschlusses des Routers öffentlich bekannt machen. Dies wird als „Exponierung des Hosts“ bezeichnet, der nun bekannt und von außen zugänglich, aber auch angreifbar ist. Wie Sie die Adresse bekannt geben, hängt von der Konfiguration der WAN-Anschlüsse ab; für das Gerät können Sie die IP-Adresse verwenden, wenn dem WAN-Anschluss eine statische Adresse zugewiesen ist. Bei einer dynamischen WAN-Adresse kann ein DDNS-Name (Dynamic DNS) verwendet werden.

Ausgangsregeln (von LAN/DMZ zu WAN) schränken den Zugriff für Verkehr ein, der das Netzwerk verlässt. Dabei können nur bestimmte lokale Benutzer auf bestimmte externe Ressourcen zugreifen. Die Standardausgangsregel lässt den Zugriff aus der sicheren Zone (LAN) auf die öffentliche DMZ oder das nicht sichere WAN zu. Um den Zugriff von Hosts im sicheren LAN auf Services im externen (nicht sicheren) WAN zu blockieren, müssen Sie für jeden Service eine Firewallregel erstellen.

Konfigurieren der grundlegenden Firewalleinstellungen

So konfigurieren Sie grundlegende Firewalleinstellungen:

SCHRITT 1 Wählen Sie **Firewall** > **Basiseinstellungen** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Firewalleinstellungen:

IP-Spoofing-Schutz	Um das Netzwerk vor IP-Spoofing zu schützen, aktivieren Sie das Kontrollkästchen **Aktivieren**.
DoS-Schutz	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um den Denial of Service-Schutz zu aktivieren.
WAN-Anfrage sperren	Blockiert über das WAN gesendete Ping-Anforderungen an das Gerät.
LAN-/VPN-Webzugriff	Wählen Sie den Typ des Webzugriffs aus, der für Verbindungen mit der Firewall verwendet werden kann: HTTP oder HTTPS (sicheres HTTP).
Remoteverwaltung **Remote-Zugriff** **Remote-Upgrade** **Zulässige Remote-IP-Adresse** **Remoteverwaltungsport**	Weitere Informationen hierzu finden Sie unter **Konfigurieren der Remoteverwaltung**.
IPv4-Multicast-Passthrough (IGMP-Proxy)	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um Multicast-Passthrough für IPv4 zu aktivieren.
IPv6-Multicast-Passthrough (IGMP-Proxy)	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um Multicast-Passthrough für IPv6 zu aktivieren.
SIP-ALG	Um SIP-Verkehr (Session Initiation Protocol) durch die Firewall zuzulassen, aktivieren Sie das Kontrollkästchen **SIP-ALG**. Das Gerät unterstützt maximal 256 Sitzungen.
UPnP **Konfiguration durch Benutzer zulassen** **Deaktivierung des Internetzugriffs durch Benutzer zulassen**	Weitere Informationen hierzu finden Sie unter **Konfigurieren von Universal Plug and Play**.

Java blockieren	Aktivieren Sie dieses Kontrollkästchen, um Java-Applets zu blockieren. Java-Applets sind kleine Programme, die in Webseiten eingebettet sind und dynamische Funktionen auf der Seite aktivieren. Ein bösartiges Applet kann verwendet werden, um Computer zu gefährden oder zu infizieren. Durch Aktivieren dieser Einstellung blockieren Sie das Herunterladen von Java-Applets. Klicken Sie auf **Automatisch**, um Java automatisch zu blockieren, oder klicken Sie auf **Manuell** und geben Sie einen bestimmten Port ein, für den Java blockiert werden soll.
Cookies blockieren	Aktivieren Sie dieses Kontrollkästchen, um Cookies zu blockieren. Cookies werden verwendet, um Sitzungsinformationen von Websites zu speichern, für die in der Regel eine Anmeldung erforderlich ist. Verschiedene Websites verwenden Cookies jedoch zum Speichern von Nachverfolgungsinformationen und Informationen zum Surfverhalten. Wenn Sie diese Option aktivieren, wird die Erstellung von Cookies durch Websites verhindert. Bei vielen Websites müssen Cookies akzeptiert werden, damit der ordnungsgemäße Zugriff auf die Website möglich ist. Das Blockieren von Cookies kann bei vielen Websites dazu führen, dass bestimmte Funktionen nicht zur Verfügung stehen. Klicken Sie auf **Automatisch**, um Cookies automatisch zu blockieren, oder klicken Sie auf **Manuell** und geben Sie einen bestimmten Port ein, für den Cookies blockiert werden sollen.

ActiveX blockieren	Aktivieren Sie dieses Kontrollkästchen, um ActiveX-Inhalte zu blockieren. ActiveX-Steuerelemente werden ähnlich wie Java-Applets beim Ausführen von Internet Explorer auf einem Computer unter Windows installiert. Ein bösartiges ActiveX-Steuerelement kann verwendet werden, um Computer zu gefährden oder zu infizieren. Durch Aktivieren dieser Einstellung blockieren Sie das Herunterladen von ActiveX-Steuerelementen. Klicken Sie auf **Automatisch**, um ActiveX automatisch zu blockieren, oder klicken Sie auf **Manuell** und geben Sie einen bestimmten Port ein, für den ActiveX blockiert werden soll.
Proxy blockieren	Aktivieren Sie dieses Kontrollkästchen, um Proxyserver zu blockieren. Ein Proxyserver (oder Proxy) ermöglicht Computern das Weiterleiten von Verbindungen an andere Computer durch den Proxy, sodass bestimmte Firewallregeln umgangen werden. Wenn beispielsweise Verbindungen mit einer bestimmten IP-Adresse durch eine Firewallregel blockiert werden, können die Anforderungen durch einen Proxy geleitet werden, der nicht durch die Regel blockiert wird. Dadurch wird die Einschränkung unwirksam. Wenn Sie diese Funktion aktivieren, werden Proxyserver blockiert. Klicken Sie auf **Automatisch**, um Proxyserver automatisch zu blockieren, oder klicken Sie auf **Manuell** und geben Sie einen bestimmten Port ein, für den Proxyserver blockiert werden sollen.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren der Remoteverwaltung

Sie können das Remote-Management aktivieren, damit Sie über ein Remote-WAN auf das Gerät zugreifen können.

Zum Konfigurieren der Remoteverwaltung konfigurieren Sie auf der Seite **Basiseinstellungen** diese Einstellungen:

Remoteverwaltung	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Remoteverwaltung zu aktivieren.
Remotezugriff	Wählen Sie den Typ des Webzugriffs aus, der für Verbindungen mit der Firewall verwendet werden kann: HTTP oder HTTPS (sicheres HTTP).
Remote-Upgrade	Wenn Sie Remote-Upgrades des Geräts zulassen möchten, aktivieren Sie das Kontrollkästchen **Aktivieren**.
Zulässige Remote-IP-Adresse	Klicken Sie auf die Schaltfläche **Beliebige IP-Adresse**, um die Remoteverwaltung über beliebige IP-Adressen zuzulassen, oder geben Sie eine bestimmte IP-Adresse in das Adressfeld ein.
Remoteverwaltungsport	Geben Sie den Port ein, über den der Remotezugriff zulässig ist. Standardmäßig wird der Port 443 verwendet. Wenn Sie remote auf den Router zugreifen, müssen Sie den Remoteverwaltungsport als Teil der IP-Adresse eingeben. Beispiel: **https://<Remote-IP>:<Remoteport>** oder **https://168.10.1.11:443**

VORSICHT Wenn die Remoteverwaltung aktiviert ist, kann jeder, der die IP-Adresse kennt, auf den Router zugreifen. Da ein böswilliger WAN-Benutzer das Gerät umkonfigurieren und missbrauchen könnte, wird dringend empfohlen, das Administratorkennwort und alle Gastkennwörter zu ändern, bevor Sie fortfahren.

Konfigurieren von Universal Plug and Play

Universal Plug and Play (UPnP) ermöglicht die automatische Erkennung von Geräten, die mit dem Gerät kommunizieren können.

Zum Konfigurieren von UPnP konfigurieren Sie auf der Seite **Basiseinstellungen** diese Einstellungen:

UPnP	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um UPnP zu aktivieren.
Konfigurieren durch Benutzer zulassen	Aktivieren Sie dieses Kontrollkästchen, um zuzulassen, dass Benutzer, auf deren Computern oder anderen UPnP-fähigen Geräten die UPnP-Unterstützung aktiviert ist, UPnP-Portzuordnungsregeln festlegen. Wenn das Kontrollkästchen deaktiviert ist, lässt das Gerät nicht zu, dass die Weiterleitungsregel von Anwendungen hinzugefügt wird.
Deaktivierung des Internetzugriffs durch Benutzer zulassen	Aktivieren Sie dieses Kontrollkästchen, um zuzulassen, dass Benutzer den Internetzugriff deaktivieren.

Verwalten von Firewallzeitplänen

Sie können Firewallzeitpläne erstellen, um Firewallregeln an bestimmten Tagen oder zu bestimmten Tageszeiten anzuwenden.

Hinzufügen oder Bearbeiten eines Firewallzeitplans

So erstellen oder bearbeiten Sie einen Zeitplan:

SCHRITT 1 Wählen Sie **Firewall** > **Zeitplanverwaltung** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie in das Feld **Name** einen eindeutigen Namen zum Identifizieren des Zeitplans ein. Dieser Name steht auf der Seite „Firewallregelkonfiguration“ in der Liste **Zeitplan auswählen** zur Verfügung. (Weitere Informationen hierzu finden Sie unter **Konfigurieren von Zugriffsregeln**.)

SCHRITT 4 Wählen Sie unter **Geplante Tage** aus, ob der Zeitplan an allen Tagen oder an bestimmten Tagen angewendet werden soll. Wenn Sie **Bestimmte Tage**

auswählen, aktivieren Sie das Kontrollkästchen neben den Tagen, die Sie in den Zeitplan aufnehmen möchten.

SCHRITT 5 Wählen Sie unter **Geplante Tageszeit** die Tageszeit aus, zu der der Zeitplan angewendet werden soll. Wenn Sie **Bestimmte Zeit** auswählen, geben Sie die Start- und Endzeit ein.

SCHRITT 6 Klicken Sie auf **Speichern**.

Konfigurieren der Serviceverwaltung

Wenn Sie eine Firewallregel erstellen, können Sie einen Service angeben, der durch die Regel gesteuert wird. Es stehen allgemeine Servicetypen zur Auswahl und Sie können auch eigene benutzerdefinierte Services erstellen.

Auf der Seite **Serviceverwaltung** können Sie benutzerdefinierte Services erstellen, für die Firewallregeln definiert werden können. Wenn Sie die Regeln definiert haben, wird der neue Service in der Tabelle **Verfügbare benutzerdefinierte Services** angezeigt.

So erstellen Sie einen benutzerdefinierten Service:

SCHRITT 1 Wählen Sie **Firewall** > **Serviceverwaltung** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie in das Feld **Dienstname** zu Identifizierungs- und Verwaltungszwecken den Dienstnamen ein.

SCHRITT 4 Wählen Sie im Dropdown-Menü im Feld **Protokoll** das vom Service verwendete Schicht-4-Protokoll aus:

- **TCP**
- **UDP**
- **TCP & UDP**
- **ICMP**

SCHRITT 5 Geben Sie in das Feld **Startport** den ersten TCP- oder UDP-Port des vom Service verwendeten Bereichs ein.

SCHRITT 6 Geben Sie in das Feld **Endport** den letzten TCP- oder UDP-Port des vom Service verwendeten Bereichs ein.

SCHRITT 7 Klicken Sie auf **Speichern**.

Zum Bearbeiten eines Eintrags wählen Sie den Eintrag aus und klicken auf **Bearbeiten**. Nehmen Sie die Änderungen vor, und klicken Sie dann auf **Speichern**.

Konfigurieren von Zugriffsregeln

Konfigurieren der Standardausgangsrichtlinie

Auf der Seite **Zugriffsregeln** können Sie die Standardausgangsrichtlinie für den Verkehr konfigurieren, der vom sicheren Netzwerk (LAN) zum nicht sicheren Netzwerk (dediziertes WAN/optional) geleitet wird.

Die Standardeingangsrichtlinie für Verkehr, der aus der nicht sicheren Zone in die sichere Zone fließt, blockiert den Verkehr immer und kann nicht geändert werden.

HINWEIS Zugriffsregeln werden durch Internetzugriffsregeln außer Kraft gesetzt, sofern beide Regeltypen auf dem Gerät konfiguriert sind.

So konfigurieren Sie die Standardausgangsrichtlinie:

SCHRITT 1 Wählen Sie **Firewall** > **Zugriffsregeln** aus.

SCHRITT 2 Wählen Sie **Zulassen** oder **Verweigern** aus.

Hinweis: Stellen Sie sicher, dass die IPv6-Unterstützung im Gerät konfiguriert ist, wenn Sie eine IPv6-Firewall konfigurieren möchten. Weitere Informationen hierzu finden Sie unter **Konfigurieren von IPv6**.

SCHRITT 3 Klicken Sie auf **Speichern**.

Ändern der Reihenfolge der Zugriffsregeln

Die Reihenfolge, in der die Zugriffsregeln in der Zugriffsregeltabelle angezeigt werden, entspricht der Reihenfolge, in der die Regeln angewendet werden. Wenn die Regeln in einer bestimmten Reihenfolge angewendet werden sollen, müssen Sie ggf. die Reihenfolge in der Tabelle ändern. So können Sie beispielsweise festlegen, dass eine Regel zum Zulassen bestimmter Verkehrstypen vor der Blockierung anderer Verkehrstypen angewendet wird.

So ändern Sie die Reihenfolge der Zugriffsregeln:

SCHRITT 1 Wählen Sie **Firewall** > **Zugriffsregeln** aus.

SCHRITT 2 Klicken Sie auf **Neu ordnen**.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen in der Zeile mit der zu verschiebenden Regel, und klicken Sie auf die Pfeile, um die Regel um eine Zeile nach oben oder unten zu verschieben. Sie können auch die gewünschte Position der Regel aus der Dropdown-Liste auswählen und dann auf **Verschieben nach** klicken.

SCHRITT 4 Klicken Sie auf **Speichern**.

Hinzufügen von Zugriffsregeln

Alle im Gerät konfigurierten Firewallregeln werden in der **Zugriffsregeltabelle** angezeigt. Aus dieser Liste geht außerdem hervor, ob die Regel aktiviert (aktiv) ist. Des Weiteren sehen Sie eine Zusammenfassung der „Von“-/„An“-Zone sowie der von der Regel betroffenen Services und Benutzer.

So erstellen Sie eine Zugriffsregel:

SCHRITT 1 Wählen Sie **Firewall** > **Zugriffsregeln** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Wählen Sie im Feld **Verbindungstyp** die Quelle des Verkehrs aus:

- **Ausgehend (LAN > WAN)**: Wählen Sie diese Option aus, um eine Ausgangsregel zu erstellen.
- **Eingehend (WAN > LAN)**: Wählen Sie diese Option aus, um eine Eingangsregel zu erstellen.
- **Eingehend (WAN > DMZ)**: Wählen Sie diese Option aus, um eine Eingangsregel zu erstellen.

SCHRITT 4 Wählen Sie im Dropdown-Menü **Aktion** die Aktion aus:

- **Immer blockieren**: Der ausgewählte Verkehrstyp wird immer blockiert.
- **Immer zulassen**: Der ausgewählte Verkehrstyp wird nie blockiert.
- **Gemäß Zeitplan blockieren**: Der ausgewählte Verkehrstyp wird nach einem Zeitplan blockiert.

- **Gemäß Zeitplan zulassen**: Der ausgewählte Verkehrstyp wird nach einem Zeitplan zugelassen.

SCHRITT 5 Wählen Sie im Dropdown-Menü **Services** den Service aus, der für diese Regel zugelassen oder blockiert werden soll. Wählen Sie **Gesamter Datenverkehr** aus, um zuzulassen, dass die Regel auf alle Anwendungen und Services angewendet wird, oder wählen Sie eine einzelne Anwendung aus, die blockiert werden soll:

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

SCHRITT 6 Wählen Sie im Feld **Quell-IP** die Benutzer aus, auf die die Firewallregel angewendet werden soll:

- **Beliebig**: Die Regel gilt für Verkehr, der von einem beliebigen Host im lokalen Netzwerk ausgeht.
- **Einzelne Adresse**: Die Regel gilt für Verkehr, der von einer einzelnen IP-Adresse im lokalen Netzwerk ausgeht. Geben Sie die Adresse in das Feld **Start** ein.

- **Adressbereich**: Die Regel gilt für Verkehr, der von einer IP-Adresse in einem Adressbereich ausgeht. Geben Sie in das Feld **Start** die IP-Startadresse und in das Feld **Ende** die IP-Endadresse ein.

SCHRITT 7 Geben Sie im Feld **Protokollieren** an, ob die Pakete für diese Regel protokolliert werden sollen.

Wenn Sie Details für alle dieser Regel entsprechenden Pakete protokollieren möchten, wählen Sie im Dropdown-Menü **Immer** aus. Wenn beispielsweise für einen Zeitplan die Ausgangsregel **Immer blockieren** ausgewählt ist, wird für jedes Paket, das eine ausgehende Verbindung für diesen Service herzustellen versucht, im Protokoll eine Meldung mit der Quell- und Zieladresse des Pakets (und weiteren Informationen) aufgezeichnet.

Das Aktivieren der Protokollierung kann zu einer großen Menge von Protokollmeldungen führen und wird nur zu Fehlerbehebungszwecken empfohlen.

Wählen Sie **Nie** aus, um die Protokollierung zu deaktivieren.

Hinweis: Wenn Verkehr vom LAN oder von der DMZ zum WAN fließt, setzt das System voraus, dass die Quell- oder Ziel-IP-Adresse eingehender IP-Pakete beim Passieren der Firewall neu geschrieben wird.

SCHRITT 8 Aktivieren Sie unter **Regelstatus** das Kontrollkästchen „Aktivieren“, um die neue Zugriffsregel zu aktivieren.

SCHRITT 9 Klicken Sie auf **Speichern**.

Erstellen einer Internetzugriffsrichtlinie

Das Gerät unterstützt verschiedene Optionen zum Blockieren des Internetzugriffs. Sie können den gesamten Internetverkehr blockieren, den Internetverkehr zu bestimmten PCs oder Endpunkten blockieren oder den Zugriff auf Internetsites blockieren, indem Sie Schlüsselwörter angeben, die blockiert werden sollen. Wenn diese Schlüsselwörter im Namen der Website gefunden werden (beispielsweise in einer Website-URL oder in einem Newsgroupnamen), wird die Website blockiert.

Hinzufügen oder Bearbeiten einer Internetzugriffsrichtlinie

So erstellen Sie eine Internetzugriffsrichtlinie:

SCHRITT 1 Wählen Sie **Firewall** > **Internetzugriffsrichtlinie** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Aktivieren Sie unter **Status** das Kontrollkästchen **Aktivieren**.

SCHRITT 4 Geben Sie zu Identifizierungs- und Verwaltungszwecken einen Richtliniennamen ein.

SCHRITT 5 Wählen Sie im Dropdown-Menü **Aktion** den Typ der gewünschten Zugriffseinschränkung aus:

- **Immer blockieren**: Internetverkehr wird immer blockiert. Damit blockieren Sie den Internetverkehr zu und von allen Endpunkten. Wenn Sie den gesamten Verkehr blockieren möchten, aber bestimmten Endpunkten den Empfang von Internetverkehr ermöglichen möchten, finden Sie weitere Informationen in Schritt 7.
- **Immer zulassen**: Internetverkehr ist immer zulässig. Sie können diese Einstellung optimieren, um Internetverkehr für bestimmte Endpunkte zu blockieren (siehe Schritt 7). Sie können auch sämtlichen Internetverkehr mit Ausnahme bestimmter Websites zulassen (siehe Schritt 8).
- **Gemäß Zeitplan blockieren**: Blockiert Internetverkehr gemäß einem Zeitplan (beispielsweise wenn Sie Internetverkehr an Wochentagen während der Geschäftszeiten blockieren, außerhalb der Geschäftszeiten und an Wochenenden jedoch zulassen möchten).
- **Gemäß Zeitplan zulassen**: Internetverkehr wird nach einem Zeitplan zugelassen.

Wenn Sie **Gemäß Zeitplan blockieren** oder **Gemäß Zeitplan zulassen** ausgewählt haben, klicken Sie auf **Zeitpläne konfigurieren**, um einen Zeitplan zu erstellen. Weitere Informationen hierzu finden Sie unter **Verwalten von Firewallzeitplänen**.

SCHRITT 6 Wählen Sie im Dropdown-Menü einen Zeitplan aus.

SCHRITT 7 (Optional) Wenden Sie die Zugriffsrichtlinie auf bestimmte PCs an, um Verkehr von bestimmten Geräten zuzulassen oder zu blockieren:

a. Klicken Sie in der Tabelle **Zugriffsrichtlinie auf die folgenden PCs anwenden** auf **Hinzufügen**.

b. Wählen Sie im Dropdown-Menü **Typ** aus, wie der PC identifiziert werden soll (anhand der MAC-Adresse, anhand der IP-Adresse oder anhand eines IP-Adressbereichs).

c. Geben Sie in das Feld **Wert** abhängig von Ihrer Auswahl im vorherigen Schritt einen der folgenden Werte ein:

- Die MAC-Adresse (xx:xx:xx:xx:xx:xx) des PCs, für den die Richtlinie gilt.
- Die IP-Adresse des PCs, für den die Richtlinie gilt.
- Die erste und letzte IP-Adresse des zu blockierenden Adressbereichs (beispielsweise 192.168.1.2 – 192.168.1.253).

SCHRITT 8 So blockieren Sie Verkehr von bestimmten Websites:

a. Klicken Sie in der Tabelle **Website-Domänenname und Schlüsselwort** auf **Hinzufügen**.

b. Wählen Sie im Dropdown-Menü **Typ** aus, wie eine Website blockiert werden soll (durch Angeben des Domänennamens oder eines in der URL enthaltenen Schlüsselworts).

c. Geben Sie in das Feld **Wert** die URL oder das Schlüsselwort ein, die bzw. das zum Blockieren der Website verwendet werden soll.

Wenn Sie beispielsweise die URL Beispiel.com blockieren möchten, wählen Sie im Dropdown-Menü die Option **URL-Adresse** aus und geben **Beispiel.com** in das Feld **Wert** ein. Wenn Sie eine URL blockieren möchten, die das Schlüsselwort „Beispiel“ enthält, wählen Sie im Dropdown-Menü die Option **Schlüsselwort** aus, und geben Sie in das Feld **Wert** den Begriff **Beispiel** ein.

SCHRITT 9 Klicken Sie auf **Speichern**.

Konfigurieren von One-to-One-NAT (Network Address Translation)

Auf der Seite „One-to-One-NAT“ können Sie lokale IP-Adressen hinter der Firewall globalen IP-Adressen zuordnen. Mit One-to-One-NAT können Sie mit privaten IP-Adressen konfigurierte Systeme hinter einer Firewall den Eindruck erwecken, dass es sich um öffentliche IP-Adressen handelt.

So fügen Sie eine One-to-One-NAT-Regel hinzu:

SCHRITT 1 Wählen Sie **Firewall > One-to-One-NAT** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie in das Feld **Anfang privater Bereich** die IP-Startadresse in der privaten IP-Adresse (LAN) ein.

SCHRITT 4 Geben Sie in das Feld **Anfang öffentlicher Bereich** die IP-Startadresse in der öffentlichen IP-Adresse (WAN) ein.

SCHRITT 5 Geben Sie in das Feld **Bereichslänge** die Anzahl der öffentlichen IP-Adressen ein, die privaten Adressen zugeordnet werden sollen.

SCHRITT 6 Wählen Sie im Feld **Service** den Service aus, für den die Regel gelten soll. Sie können Services für One-to-One-NAT so konfigurieren, dass diese von der privaten IP-Adresse (LAN) akzeptiert werden, wenn Verkehr an die entsprechende öffentliche IP-Adresse gesendet wird. Konfigurierte Services an privaten IP-Adressen im Bereich werden akzeptiert, wenn an der entsprechenden öffentlichen IP-Adresse Verkehr verfügbar ist.

SCHRITT 7 Klicken Sie auf **Speichern**.

Konfigurieren der Portweiterleitung

Die Portweiterleitung wird verwendet, um Verkehr aus dem Internet von einem Port im WAN an einen anderen Port im LAN umzuleiten. Häufig verwendete Services sind bereits vordefiniert. Alternativ können Sie einen benutzerdefinierten Service und zugeordnete Ports für die Weiterleitung definieren.

Auf den Seiten **Regeln für die Einzelportweiterleitung** und **Regeln für die Portbereichsweiterleitung** werden alle verfügbaren Portweiterleitungsregeln für das Gerät aufgeführt und Sie können Portweiterleitungsregeln konfigurieren.

HINWEIS Für Server im LAN ist die Portweiterleitung nicht geeignet, da die eingehenden Ports erst geöffnet werden, wenn das LAN-Gerät eine ausgehende Verbindung hergestellt hat.

Manche Anwendungen funktionieren beim Herstellen einer Verbindung durch externe Geräte nur dann ordnungsgemäß, wenn sie Daten über einen bestimmten Port oder Portbereich empfangen. Der Router darf alle eingehenden Daten für diese Anwendung nur über den erforderlichen Port oder Portbereich senden.

Das Gateway verfügt über eine Liste gängiger Anwendungen und Spiele sowie der ausgehenden und eingehenden Ports, die jeweils geöffnet werden müssen. Sie können auch eine Portweiterleitungsregel angeben, indem Sie den Verkehrstyp (TCP oder UDP) und den Bereich der eingehenden und ausgehenden Ports definieren, die geöffnet werden sollen, wenn die Regel aktiviert ist.

Konfigurieren der Einzelportweiterleitung

So fügen Sie eine Regel für die Einzelportweiterleitung hinzu:

SCHRITT 1 Wählen Sie **Firewall** > **Einzelportweiterleitung** aus. Eine bereits vorhandene Liste mit Anwendungen wird angezeigt.

SCHRITT 2 Geben Sie in das Feld **Anwendung** den Namen der Anwendung ein, für die Sie die Portweiterleitung konfigurieren möchten.

SCHRITT 3 Geben Sie in das Feld **Externer Port** die Portnummer ein, die diese Regel auslöst, wenn eine Verbindungsanforderung von ausgehendem Verkehr gestellt wird.

SCHRITT 4 Geben Sie in das Feld **Interner Port** die Portnummer ein, die vom Remotesystem verwendet wird, um auf die empfangene Anforderung zu antworten.

SCHRITT 5 Wählen Sie im Dropdown-Menü **Schnittstelle** eine der Optionen **Beides (Ethernet und 3G)**, **Ethernet** oder **3G** aus.

SCHRITT 6 Wählen Sie im Dropdown-Menü **Protokoll** ein Protokoll aus (**TCP**, **UDP** oder **TCP** & **UDP**).

SCHRITT 7 Geben Sie in das Feld **IP-Adresse** die IP-Adresse des Hosts auf der LAN-Seite ein, an den der jeweilige IP-Verkehr weitergeleitet werden soll. Sie können beispielsweise HTTP-Verkehr an Port 80 der IP-Adresse eines Webservers auf der LAN-Seite weiterleiten.

SCHRITT 8 Aktivieren Sie im Feld **Aktivieren** das Kontrollkästchen **Aktivieren**, um die Regel zu aktivieren.

SCHRITT 9 Klicken Sie auf **Speichern**.

Konfigurieren der Portbereichsweiterleitung

So fügen Sie eine Regel für die Portbereichsweiterleitung hinzu:

SCHRITT 1 Wählen Sie **Firewall** > **Portbereichsweiterleitung** aus.

SCHRITT 2 Geben Sie in das Feld **Anwendung** den Namen der Anwendung ein, für die Sie die Portweiterleitung konfigurieren möchten.

SCHRITT 3 Geben Sie im Feld **Externer Port** die Portnummer an, die diese Regel auslöst, wenn eine Verbindungsanforderung von ausgehendem Verkehr gestellt wird.

SCHRITT 4 Geben Sie im Feld **Start** die Portnummer an, mit der der Bereich der weiterzuleitenden Ports beginnt.

SCHRITT 5 Geben Sie im Feld **Ende** die Portnummer an, mit der der Bereich der weiterzuleitenden Ports endet.

SCHRITT 6 Wählen Sie im Dropdown-Menü **Schnittstelle** eine der Optionen **Beides (Ethernet und 3G)**, **Ethernet** oder **3G** aus.

SCHRITT 7 Wählen Sie im Dropdown-Menü **Protokoll** ein Protokoll aus (**TCP**, **UDP** oder **TCP** & **UDP**).

SCHRITT 8 Geben Sie in das Feld **IP-Adresse** die IP-Adresse des Hosts auf der LAN-Seite ein, an den der jeweilige IP-Verkehr weitergeleitet werden soll.

SCHRITT 9 Aktivieren Sie im Feld **Aktivieren** das Kontrollkästchen **Aktivieren**, um die Regel zu aktivieren.

SCHRITT 10 Klicken Sie auf **Speichern**.

Konfigurieren der Auslösung des Portbereichs

Mithilfe der Portauslösung können Geräte im LAN oder in der DMZ anfordern, dass einer oder mehrere Ports an sie weitergeleitet werden. Die Portauslösung wartet auf ausgehende Anforderungen vom LAN bzw. von der DMZ an einem der definierten ausgehenden Ports und öffnet dann einen eingehenden Port für den angegebenen Verkehrstyp.

Die Portauslösung ist eine Form der dynamischen Portweiterleitung, während eine Anwendung Daten über die geöffneten ausgehenden oder eingehenden Ports überträgt. Die Portauslösung öffnet einen eingehenden Port für einen bestimmten Verkehrstyp an einem definierten ausgehenden Port. Die Portauslösung ist flexibler als die (beim Konfigurieren von Firewallregeln verfügbare) statische Portweiterleitung, da eine Regel nicht auf eine bestimmte IP-Adresse oder einen bestimmten IP-Adressbereich im LAN verweisen muss. Außerdem werden die Ports bei Nichtverwendung nicht offen gelassen, wodurch die Sicherheit gegenüber der Portweiterleitung erhöht wird.

HINWEIS Für Server im LAN ist die Portauslösung nicht geeignet, da die eingehenden Ports erst geöffnet werden, wenn das LAN-Gerät eine ausgehende Verbindung hergestellt hat.

Manche Anwendungen funktionieren beim Herstellen einer Verbindung durch externe Geräte nur dann ordnungsgemäß, wenn sie Daten über einen bestimmten Port oder Portbereich empfangen. Der Router darf alle eingehenden Daten für diese Anwendung nur über den erforderlichen Port oder Portbereich senden. Das Gateway verfügt über eine Liste gängiger Anwendungen und Spiele sowie der ausgehenden und eingehenden Ports, die jeweils geöffnet werden müssen. Sie können auch eine Portauslösungsregel angeben, indem Sie den Verkehrstyp (TCP oder UDP) und den Bereich der eingehenden und ausgehenden Ports definieren, die geöffnet werden sollen, wenn die Regel aktiviert ist.

So fügen Sie eine Portauslösungsregel hinzu:

SCHRITT 1 Wählen Sie **Firewall** > **Ausgelöste Portbereiche** aus.

SCHRITT 2 Geben Sie in das Feld **Anwendung** den Namen der Anwendung ein, für die Sie die Portweiterleitung konfigurieren möchten.

SCHRITT 3 Geben Sie in die Felder unter **Ausgelöster Bereich** die Portnummer bzw. den Portnummernbereich ein, die bzw. der diese Regel auslöst, wenn eine Verbindungsanforderung von ausgehendem Verkehr gestellt wird. Wenn die ausgehende Verbindung nur einen Port verwendet, geben Sie in beide Felder die gleiche Portnummer ein.

SCHRITT 4 Geben Sie in die Felder unter **Weitergeleiteter Bereich** die Portnummer bzw. den Portnummernbereich ein, die bzw. der vom Remotesystem verwendet wird, um auf die empfangene Anforderung zu antworten. Wenn die eingehende Verbindung nur einen Port verwendet, geben Sie in beiden Feldern die gleiche Portnummer an.

SCHRITT 5 Wählen Sie im Dropdown-Menü **Schnittstelle** eine der Optionen **Beides (Ethernet und 3G)**, **Ethernet** oder **3G** aus.

SCHRITT 6 Aktivieren Sie im Feld **Aktivieren** das Kontrollkästchen **Aktivieren**, um die Regel zu aktivieren.

SCHRITT 7 Klicken Sie auf **Speichern**.

6

Konfigurieren von VPN

VPN-Tunneltypen

Sie können VPN auf dem Gerät konfigurieren, um einen sicheren Kommunikationskanal (Tunnel) zwischen Geräten wie folgt bereitzustellen:

- Zwischen zwei Gatewayroutern
- Zwischen einem Remoteclientgerät und einem Gatewayrouter

Konfigurieren grundlegender Einstellungen für ein Site-to-Site-IPSec-VPN

Das Gerät unterstützt Site-to-Site-IPSec-VPN für einen einzelnen Gateway-to-Gateway-VPN-Tunnel. Nachdem Sie diese grundlegenden VPN-Einstellungen konfiguriert haben, können Sie eine sichere Verbindung mit einem anderen VPN-fähigen Router herstellen. Sie können beispielsweise das Gerät an einem Filialstandort so konfigurieren, dass eine Verbindung mit einem Router für Site-to-Site-VPN-Tunnel am Hauptstandort hergestellt wird und so vom Filialstandort aus ein sicherer Zugriff auf das Unternehmensnetzwerk möglich ist.

So konfigurieren Sie die grundlegenden VPN-Einstellungen für eine Site-to-Site-IPSec-Verbindung:

SCHRITT 1 Wählen Sie **VPN > Site-to-Site-IPSec-VPN > Grundlegende VPN-Einrichtung** aus.

SCHRITT 2 Geben Sie in das Feld **Neuer Verbindungsname** einen Namen für den VPN-Tunnel ein.

SCHRITT 3 Geben Sie im Feld **Pre-Shared Key** den Pre-Shared Key bzw. das Kennwort ein, den bzw. das die beiden Router austauschen sollen. Der Schlüssel muss zwischen 8 und 49 Zeichen lang sein.

SCHRITT 4 Geben Sie in den Feldern unter **Endpunktinformationen** die folgenden Informationen ein:

- **Remoteendpunkt**: Geben Sie an, ob der Router, mit dem eine Verbindung hergestellt wird, anhand der IP-Adresse oder eines voll qualifizierten Domänennamens ermittelt wird. Beispiel: eine IP-Adresse wie 192.168.1.1 oder ein voll qualifizierter Domänennamens wie „cisco.com“.
- **IP-Adresse des Remote-WAN**: Geben Sie die öffentliche IP-Adresse oder den Domänennamen des Remoteendpunkts ein.
- **Lokale WAN-IP-Adresse**: Geben Sie die öffentliche IP-Adresse oder den Domänennamen des Geräts ein.

SCHRITT 5 Geben Sie in den Feldern unter **Remotezugriff über sichere Verbindung** die folgenden Informationen ein:

- **Remote-LAN-IP-Adresse**: Die Adresse des Remoteendpunkts im privaten Netzwerk (LAN). Dies ist die IP-Adresse aus dem internen Netzwerk am Remotestandort.
- **Remote-LAN-Subnetzmaske**: Die Subnetzmaske des Remoteendpunkts im privaten Netzwerk (LAN).
- **Lokale LAN-IP-Adresse**: Die Adresse des lokalen Netzwerks im privaten Netzwerk (LAN). Dies ist die IP-Adresse des internen Netzwerks auf dem Gerät.
- **Lokale LAN-Subnetzmaske**: Die Subnetzmaske des lokalen Netzwerks im privaten Netzwerk (LAN).

Hinweis: Die Remote-WAN- und die Remote-LAN-IP-Adresse dürfen nicht zum selben Subnetz gehören. Wenn beispielsweise die Remote-LAN-IP-Adresse 192.168.1.100 und die lokale LAN-IP-Adresse 192.168.1.115 lauten würde, würde beim Routing von Verkehr über das VPN ein Konflikt entstehen. Das dritte

Oktett muss unterschiedlich sein, damit die IP-Adressen zu verschiedenen Subnetzen gehören. Eine Kombination aus der Remote-LAN-IP-Adresse 192.168.1.100 und der lokalen LAN-IP-Adresse 192.168.2.100 wäre beispielsweise zulässig.

SCHRITT 6 Klicken Sie auf **Speichern**.

Anzeigen von Standardwerten

Klicken Sie auf **Standardeinstellungen anzeigen**, um die Standardwerte der grundlegenden VPN-Einstellungen anzuzeigen. Bei diesen vom VPN Consortium (VPNC) empfohlenen Standardwerten wird davon ausgegangen, dass Sie einen vorinstallierten Schlüssel bzw. ein Kennwort verwenden, der bzw. das sowohl dem Gerät als auch dem Remoteendpunkt bekannt ist.

Konfigurieren der erweiterten Parameter für Site-to-Site-IPSec-VPNs

Über erweiterte VPN-Parameter wie IKE und andere VPN-Richtlinien wird gesteuert, wie das Gerät VPN-Verbindungen herstellt und empfängt.

Um erweiterte VPN-Parameter zu konfigurieren, wählen Sie **VPN > Site-to-Site-IPSec-VPN > Erweiterte VPN-Einrichtung** aus.

Verwalten von IKE-Richtlinien

Mit dem IKE-Protokoll (Internet Key Exchange) werden dynamisch Schlüssel zwischen zwei IPSec-Hosts ausgetauscht. Sie können IKE-Richtlinien erstellen, um die Sicherheitsparameter für den Datenaustausch mit dem Remoterouter über die IPSec-VPN-Verbindung zu definieren. Sie können beispielsweise IKE-Richtlinien erstellen, um die Parameter für die Peer-Authentifizierung und für Verschlüsselungsalgorithmen zu definieren. Vergewissern Sie sich, dass die Parameter für Verschlüsselung, Authentifizierung und Schlüsselgruppe in der VPN-Richtlinie mit den Einstellungen des Remoterouters kompatibel sind.

So fügen Sie eine IKE-Richtlinie hinzu:

SCHRITT 1 Klicken Sie auf der Seite **Erweiterte VPN-Einrichtung** auf **Hinzufügen**.

SCHRITT 2 Geben Sie einen eindeutigen Namen für die IKE-Richtlinie ein, um sie leicht erkennen und verwalten zu können.

SCHRITT 3 Wählen Sie im Feld **Austauschmodus** einen der folgenden Modi für die Richtlinie aus:

- **Haupt**: Aushandlung des Tunnels mit höherer Sicherheit, die Geschwindigkeit ist jedoch geringer.
- **Aggressiv**: Herstellung einer schnelleren Verbindung, die Sicherheit ist jedoch geringer.

SCHRITT 4 Geben Sie in den Feldern **Lokale Kennung** und **Remote-Kennung** an, ob das Gerät und der Remoterouter anhand ihrer tatsächlichen IP-Adresse oder ihrer öffentlichen IP-Adresse ermittelt werden sollen. Wenn Sie „IP-Adresse“ auswählen, geben Sie die tatsächliche IP-Adresse des Geräts und des Remoterouters ein.

SCHRITT 5 Konfigurieren Sie unter **IKE-SA-Parameter** die entsprechenden Parameter, um Stärke und Modus für die SA-Aushandlung (Security Association) zwischen Gerät und Remoterouter zu definieren:

a. Wählen Sie im Feld **Verschlüsselungsalgorithmus** den Algorithmus für die Datenverschlüsselung aus.

b. Geben Sie im Feld **Authentifizierungsalgorithmus** den Authentifizierungsalgorithmus für den VPN-Header an. Stellen Sie sicher, dass der Authentifizierungsalgorithmus auf beiden Seiten des VPN-Tunnels gleich konfiguriert ist.

c. Geben Sie in das Feld **Pre-Shared Key** den Schlüssel oder das Kennwort ein. Stellen Sie sicher, dass das Kennwort keine doppelten Anführungszeichen (") enthält.

d. Geben Sie im Feld **DH-Gruppe** den DH-Gruppenalgorithmus für den Austausch eines Pre-Shared Key an. Die DH-Gruppe legt die Stärke des Algorithmus in Bit fest. Stellen Sie sicher, dass die DH-Gruppe auf beiden Seiten der IKE-Richtlinie gleich konfiguriert ist.

e. Geben Sie in das Feld **SA-Gültigkeitsdauer** das Intervall (in Sekunden) ein, nach dem die Sicherheitsvereinbarung ungültig wird.

f. Um die Funktion **Dead Peer Detection (DPD)** zu aktivieren, aktivieren Sie das Kontrollkästchen **Aktivieren**. Mit Dead Peer Detection (DPD) wird erkannt, ob der Peer aktiv ist. Wenn erkannt wird, dass der Peer nicht aktiv ist, löscht das

Gerät die IPSec- und die IKE-Sicherheitsvereinbarung. Wenn Sie diese Funktion aktivieren, müssen Sie auch diese Einstellungen eingeben:

- **DPD-Verzögerung**: Das Intervall (in Sekunden) zwischen zwei aufeinanderfolgenden DPD R-U-THERE-Nachrichten. DPD R-U-THERE-Nachrichten werden nur gesendet, wenn sich der IPSec-Verkehr im Leerlauf befindet.
- **DPD-Zeitüberschreitung**: Die maximale Wartezeit für das Gerät bis zum Empfang einer Antwort auf die DPD-Nachricht, bevor der Peer für inaktiv erklärt wird.

SCHRITT 6 Klicken Sie auf **Speichern**.

HINWEIS Wenn bereits eine VPN-Verbindung konfiguriert ist, müssen Sie diese zunächst löschen, um eine neue hinzufügen zu können.

Verwalten von VPN-Richtlinien

HINWEIS Bevor Sie eine automatische VPN-Richtlinie erstellen, müssen Sie zunächst die IKE-Richtlinie erstellen, auf der die automatische VPN-Richtlinie basieren soll.

So verwalten Sie VPN-Richtlinien:

SCHRITT 1 Wählen Sie **VPN > Site-to-Site-IPSec-VPN > Erweiterte VPN-Einrichtung** aus. Klicken Sie auf **Hinzufügen**.

SCHRITT 2 Führen Sie unter **VPN-Richtlinienkonfiguration hinzufügen/bearbeiten** folgende Schritte aus:

a. Geben Sie in das Feld **IPSec-Name** einen eindeutigen Namen für die Richtlinie ein.

b. Wählen Sie im Feld **Richtlinientyp** eine der folgenden Optionen aus:

- **Automatische Richtlinie**: Einige Parameter für den VPN-Tunnel werden automatisch generiert. Hierzu müssen die Parameter zwischen den beiden VPN-Endpunkten unter Verwendung des IKE-Protokolls (Internet Key Exchange) ausgehandelt werden.
- **Manuelle Richtlinie**: Alle Parameter (einschließlich der Schlüssel) für den VPN-Tunnel werden für jeden Endpunkt manuell eingegeben. Es wird weder ein außenstehender Server noch eine außenstehende Organisation benötigt.

c. **Remoteendpunkt**: Wählen Sie den Typ der Kennung aus, die Sie für das Gateway am Remoteendpunkt bereitstellen möchten: **IP-Adresse** oder **FQDN** (voll qualifizierter Domänenname). Geben Sie die IP-Adresse oder den FQDN ein.

SCHRITT 3 Führen Sie unter **Lokale Datenverkehrauswahl** und **Remote-Datenverkehrauswahl** folgende Schritte aus:

- Geben Sie in den Feldern **Lokale IP und Remote-IP** an, wie viele Endpunkte an der VPN-Richtlinie teilnehmen:
  - **Einzeln**: Begrenzt die Richtlinie auf einen Host. Geben Sie in das Feld **IP-Adresse** die IP-Adresse des Hosts ein, der Mitglied des VPNs sein soll.
  - **Subnetz**: Lässt Verbindungen eines gesamten Subnetzes mit dem VPN zu. Geben Sie in das Feld **IP-Adresse** die Netzwerkadresse und in das Feld **Subnetzmaske** die Subnetzmaske ein. Geben Sie in das Feld **IP-Adresse** die IP-Netzwerkadresse des Subnetzes ein. Geben Sie in das Feld **Subnetzmaske** die Subnetzmaske ein, beispielsweise 255.255.255.0. Im Feld wird automatisch die auf der IP-Adresse basierende Standardsubnetzadresse angezeigt.

HINWEIS Verwenden Sie keine überlappenden Subnetze für die lokale oder Remote-Datenverkehrauswahl. Für die Verwendung dieser Subnetze müssten Sie statische Routen im Router und die zu verwendenden Hosts hinzufügen. Vermeiden Sie beispielsweise Folgendes:

Lokale Datenverkehrauswahl: 192.168.1.0/24

Remote-Datenverkehrauswahl: 192.168.0.0/16

SCHRITT 4 Geben Sie beim Richtlinientyp **Manuell** die Einstellungen im Abschnitt **Parameter für manuelle Richtlinien** ein:

- **SPI eingehend, SPI ausgehend**: Geben Sie einen hexadezimalen Wert aus 3 bis 8 Zeichen ein, beispielsweise 0x1234. Der Sicherheitsparameterindex (SPI) gibt die Sicherheitsvereinbarung der ein- und ausgehenden Verkehrsströme an.
- **Manueller Verschlüsselungsalgorithmus**: Wählen Sie den Algorithmus aus, der zum Verschlüsseln der Daten verwendet wird.
- **Schlüsseleingabe, Schlüsselausgabe**: Geben Sie den Verschlüsselungsschlüssel der Eingangs- und Ausgangsrichtlinie ein. Die Länge des Schlüssels hängt vom ausgewählten Verschlüsselungsalgorithmus ab:
  - DES: 8 Zeichen

- 3DES: 24 Zeichen
- AES-128: 16 Zeichen
- AES-192: 24 Zeichen
- AES-256: 32 Zeichen

- **Manueller Integritätsalgorithmus**: Wählen Sie den Algorithmus aus, der zum Überprüfen der Datenintegrität verwendet wird.
- **Schlüsseleingabe, Schlüsselausgabe**: Geben Sie den Integritätsschlüssel (für ESP mit Integritätsmodus) für die Eingangs- und Ausgangsrichtlinie ein. Die Länge des Schlüssels hängt vom ausgewählten Algorithmus ab:
  - MD5: 16 Zeichen
  - SHA-1: 20 Zeichen
  - SHA2-256: 32 Zeichen

SCHRITT 5 Legen Sie beim Richtlinientyp **Automatisch** die Einstellungen unter **Parameter für automatische Richtlinien** fest.

- **IPSec-SA-Gültigkeitsdauer**: Geben Sie die Dauer der Sicherheitsvereinbarung (in Sekunden) ein. Nach der angegebenen Anzahl von Sekunden wird die Sicherheitsvereinbarung erneut ausgehandelt. Der Standardwert beträgt 3.600 Sekunden. Der Mindestwert beträgt 300 Sekunden.
- **Verschlüsselungsalgorithmus**: Wählen Sie den Algorithmus aus, der zum Verschlüsseln der Daten verwendet wird.
- **Integritätsalgorithmus**: Wählen Sie den Algorithmus aus, der zum Überprüfen der Integrität der Daten verwendet wird.
- **PFS-Schlüsselgruppe**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um mithilfe von PFS (Perfect Forward Secrecy) die Sicherheit zu verbessern. Dieses Protokoll ist zwar langsamer, kann jedoch Abhören verhindern, da es sicherstellt, dass für alle Phase-2-Aushandlungen ein Diffie-Hellman-Schlüsselaustausch stattfindet.
- **DH-Gruppe**: Geben Sie den DH-Gruppenalgorithmus für den Austausch eines vorinstallierten Schlüssels an. Die DH-Gruppe legt die Stärke des Algorithmus in Bit fest. Stellen Sie sicher, dass die DH-Gruppe auf beiden Seiten der IKE-Richtlinie gleich konfiguriert ist.
- **IKE-Richtlinie auswählen**: Wählen Sie die IKE-Richtlinie aus, die die Merkmale der SA-Aushandlung definieren soll.

SCHRITT 6 Klicken Sie auf **Speichern**.

Konfigurieren des IPSec-VPN-Servers

IPSec-VPN ermöglicht den sicheren Remotezugriff auf Unternehmensressourcen mittels eines verschlüsselten Tunnels über das Internet. Das Gerät unterstützt die folgenden IPSec-VPN-Clients:

- TheGreenBow
- ShrewSoft

Konfigurieren des IPSec-VPN-Servers

So konfigurieren Sie den IPSec-VPN-Server:

SCHRITT 1 Wählen Sie **VPN > IPSec-VPN-Server > Einrichten** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Server aktivieren**.

SCHRITT 3 Konfigurieren Sie unter **Phase 1-Konfiguration** die Einstellungen zur gegenseitigen Authentifizierung der beiden VPN-Endpunkte und zur Aushandlung der IKE-Sicherheitsvereinbarung (SA), sodass ein sicherer Kanal zur Aushandlung von SAs in Phase 2 eingerichtet wird.

a. Geben Sie in das Feld **Pre-Shared Key** den Pre-Shared Key bzw. das Kennwort ein, das zwischen Gerät und Remoteendpunkt ausgetauscht werden soll. Das Kennwort muss zwischen 8 und 49 Zeichen lang sein.

b. Wählen Sie im Feld **Austauschmodus** einen der folgenden Modi für die IPSec-VPN-Verbindung aus:

- **Haupt**: Aushandlung des Tunnels mit höherer Sicherheit, die Geschwindigkeit ist jedoch geringer.
- **Aggressiv**: Herstellung einer schnelleren Verbindung, die Sicherheit ist jedoch geringer.

c. Wählen Sie den **Verschlüsselungsalgorithmus** für die Datenverschlüsselung und den **Authentifizierungsalgorithmus** für den VPN-Header aus. Stellen Sie sicher, dass der Authentifizierungsalgorithmus auf dem Gerät und dem Remoteendpunkt gleich konfiguriert ist.

d. Geben Sie im Feld **Diffie-Hellman-Gruppe (DH)** den Diffie-Hellman-Gruppenalgorithmus für den Austausch eines Pre-Shared Key an. Die DH-Gruppe bestimmt die Stärke des Algorithmus in Bits. Stellen Sie sicher, dass die DH-Gruppe auf dem Gerät und dem Remoteendpunkt gleich konfiguriert ist.

e. Geben Sie in das Feld **IKE-SA-Gültigkeitsdauer** die Dauer in Sekunden ein, nach der die Sicherheitsvereinbarung für die VPN-Verbindung erneut ausgehandelt wird.

SCHRITT 4 Konfigurieren Sie unter **Phase 2-Konfiguration** die Parameters für die Aushandlung der IPSec-Sicherheitsvereinbarung (SA) für den IPSec-Tunnel:

a. Geben Sie im Feld **Lokale IP** an, wie viele Endpunkte an der VPN-Richtlinie teilnehmen:

- **Einzeln**: Begrenzt die Richtlinie auf einen Host. Geben Sie in das Feld **IP-Adresse** die IP-Adresse des Hosts ein, der Mitglied des VPNs sein soll.
- **Subnetz**: Lässt Verbindungen eines gesamten Subnetzes mit dem VPN zu. Geben Sie in das Feld **IP-Adresse** die Netzwerkadresse und in das Feld **Subnetzmaske** die Subnetzmaske ein. Geben Sie in das Feld **IP-Adresse** die IP-Netzwerkadresse des Subnetzes ein. Geben Sie in das Feld **Subnetzmaske** die Subnetzmaske ein, beispielsweise 255.255.255.0. Im Feld wird automatisch die auf der IP-Adresse basierende Standardsubnetzadresse angezeigt.

b. Geben Sie in das Feld **IPSec-SA-Gültigkeitsdauer** die Dauer in Sekunden ein, nach der die IPSec-Sicherheitsvereinbarung für die VPN-Verbindung erneut ausgehandelt wird.

c. Wählen Sie den **Verschlüsselungsalgorithmus** für die Datenverschlüsselung und den **Authentifizierungsalgorithmus** für den VPN-Header aus. Stellen Sie sicher, dass der Authentifizierungsalgorithmus auf dem Gerät und dem Remoteendpunkt gleich konfiguriert ist.

d. Um eine sicherere IPSec-VPN-Verbindung zu erstellen, aktivieren Sie im Feld **PFS-Schlüsselgruppe** das Kontrollkästchen „Aktivieren“, wodurch ein neuer Diffie-Hellman-Schlüsselaustausch in Phase 2 stattfindet. Mit Perfect Forward Secrecy (PFS) entsteht eine weitere Sicherheitsschicht, indem die Daten mit einem neuen Schlüssel geschützt werden, falls der in Phase 1 generierte DH-Schlüssel bei der Übertragung kompromittiert wird. Stellen Sie sicher, dass bei beiden IPSec-Endpunkten PFS aktiviert ist.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von IPSec-VPN-Benutzerkonten

SCHRITT 1 Wählen Sie **VPN > IPSec-VPN-Server > Benutzer**.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie einen Benutzernamen und ein Kennwort ein.

Kennwörter sollten keine Wörter aus einem Wörterbuch irgendeiner Sprache enthalten. Außerdem sollten sie sowohl Buchstaben (Groß- und Kleinbuchstaben) als auch Ziffern und Symbole enthalten. Das Kennwort darf maximal 64 Zeichen enthalten.

SCHRITT 4 Um Benutzernamen und Kennwörter aus einer CSV-Datei zu importieren, klicken Sie auf **Importieren**. Die Seite **Administration > Benutzer** wird angezeigt. Klicken Sie unter **Benutzername und Kennwort importieren** auf **Durchsuchen**, wählen Sie die Datei aus, und klicken Sie auf **Importieren**.

SCHRITT 5 Speichern Sie die Benutzerkonten.

Konfigurieren von PPTP

PPTP (Point to Point Tunneling Protocol) ist ein Netzwerkprotokoll, das die sichere Übertragung von Daten von einem Remoteclient an ein Unternehmensnetzwerk ermöglicht, indem eine sichere VPN-Verbindung über öffentliche Netzwerke wie beispielsweise das Internet erstellt wird.

Konfigurieren des PPTP-Servers

So konfigurieren Sie den PPTP-VPN-Server:

SCHRITT 1 Wählen Sie **VPN** > **PPTP-Server** aus.

SCHRITT 2 Konfigurieren Sie unter **PPTP-Konfiguration** die PPTP-VPN-Einstellungen:

a. Aktivieren Sie im Feld **PPTP-Server** das Kontrollkästchen „Aktivieren“.

b. Geben Sie die IP-Adresse des PPTP-Servers ein.

c. Geben Sie den IP-Adressbereich für PPTP-Clients ein.

d. Wenn die Daten über die PPTP-VPN-Verbindung verschlüsselt werden sollen, aktivieren Sie im Feld **MPPE-Verschlüsselung** das Kontrollkästchen „Aktivieren“.

SCHRITT 3 Klicken Sie auf **Speichern**.

Erstellen und Verwalten von PPTP-Benutzern

So erstellen und aktivieren Sie PPTP-Benutzer:

SCHRITT 1 Wählen Sie **VPN > PPTP-Server** aus. Klicken Sie in der Tabelle **PPTP-Benutzerkonten** auf **Hinzufügen**.

SCHRITT 2 Geben Sie Benutzername und Kennwort für die Authentifizierung des PPTP-Benutzers ein. Die Werte müssen zwischen 4 und 32 Zeichen lang sein.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen **Aktivieren** für den Benutzer.

SCHRITT 4 Um Benutzernamen und Kennwörter aus einer CSV-Datei zu importieren, klicken Sie auf **Importieren**. Die Seite **Administration > Benutzer** wird angezeigt. Klicken Sie unter **Benutzername und Kennwort importieren** auf **Durchsuchen**, wählen Sie die Datei aus, und klicken Sie auf **Importieren**.

SCHRITT 5 Speichern Sie die Benutzerkonten.

Konfigurieren von VPN-Passthrough

Mithilfe von VPN-Passthrough kann VPN-Verkehr von VPN-Clients das Gerät passieren.

So konfigurieren Sie VPN-Passthrough:

SCHRITT 1 Wählen Sie **VPN** > **VPN-Passthrough** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um den Verkehrstyp auszuwählen, der das Gerät durchlaufen darf.

SCHRITT 3 Klicken Sie auf **Speichern**.

SSL-Zertifikat

Cisco RV130/RV130W unterstützt die Zertifikatauthentifizierung für VPN IPsec. Secure Socket Layer (SSL) Certificate bietet Datenverschlüsselung und Serverauthentifizierung vor der Erstellung der SSL-Sitzung.

Klicken Sie zum Verwalten des SSL-Zertifikats auf **VPN > SSL-Zertifikat**.

- **Tabelle zu vertrauenswürdigen Zertifikaten (Zertifizierungsstellenzertifikat)**
  - Klicken Sie auf **Upload**, um die Seite für **Zertifikate** aufzurufen. Klicken Sie auf **Durchsuchen**, um ein vertrauenswürdiges Zertifikat auf Ihrer Festplatte auszuwählen. Klicken Sie anschließend auf **Importieren**.
- **Aktives Selbstzertifikat**
  - Klicken Sie auf **Upload**, um die Seite für **Zertifikate** aufzurufen. Klicken Sie auf **Durchsuchen**, um ein aktives Selbstzertifikat auf Ihrer Festplatte auszuwählen. Klicken Sie anschließend auf **Importieren**.
- **Anforderungen Selbstzertifikat**

  Ein Selbstzertifikat ist ein von einer Zertifizierungsstelle ausgestelltes Zertifikat, das Ihr Gerät identifiziert (oder ein selbstsigniertes Zertifikat, wenn Sie den Identitätsschutz einer Zertifizierungsstelle nicht benötigen). Um die Signierung eines Selbstzertifikats durch eine Zertifizierungsstelle anzufordern, können Sie über das Gateway eine Zertifikatsignaturanforderung generieren, indem Sie Identifizierungsparameter eingeben und diese zum Signieren an die

Zertifizierungsstelle senden. Anschließend werden das vertrauenswürdige Zertifikat der Zertifizierungsstelle und das signierte Zertifikat von der Zertifizierungsstelle hochgeladen, um das Selbstzertifikat zu aktivieren, mit dem die Identität dieses Gateways überprüft wird. Das Selbstzertifikat wird dann bei IPSec-Verbindungen mit Peers zur Überprüfung der Authentizität des Gateways verwendet.

- **Zertifikat generieren:** Klicken Sie zum Erstellen eines SSL-Zertifikats auf **Zertifikat generieren**. Daraufhin wird die Seite für eine neue Anforderung von Zertifikatinformationen angezeigt.

  Name: Geben Sie den Namen des neuen Zertifikats ein.

  Betreff: Bitte folgen Sie bei der Eingabe dem Muster "CN=xxx", und verwenden Sie für "CN" Großbuchstaben.

  Hash-Algorithmus: Wählen Sie aus dem Drop-down-Menü den entsprechenden Hash-Algorithmus aus.

  Signaturalgorithmus: Wählen Sie aus dem Drop-down-Menü den entsprechenden Signaturalgorithmus aus.

  Signaturschlüssellänge: Wählen Sie aus dem Drop-down-Menü die entsprechende Signaturschlüssellänge aus.

  IP-Adresse (optional): Geben Sie die IP-Adresse des Routers ein.

  Domänenname (optional): Geben Sie den Domänennamen des Routers ein.

  E-Mail-Adresse (optional): Geben Sie die E-Mail-Adresse des Antragsstellers ein.

  - **Export für Admin:** Zum Exportieren der Zertifikatanforderungen auf die Festplatte.

- **Exportzertifikat:** Klicken Sie zum Herunterladen des Routerzertifikats auf die Schaltfläche **Export für Client.**

Klicken Sie auf **Speichern**, um die Konfiguration zu speichern, oder klicken Sie auf **Abbrechen**, um die Einstellungen abzurufen.

VPN-Setup-Assistent

So verwenden Sie den VPN-Setup-Assistenten:

SCHRITT 1 Klicken Sie auf **VPN > VPN-Setup-Assistent**.

Das Fenster des Assistenten wird angezeigt. Befolgen Sie die auf dem Bildschirm angezeigten Anweisungen zum Einrichten des Geräts.

7

Konfigurieren der Servicequalität

Servicequalität (Quality of Service, QoS) weist den verschiedenen Anwendungen, Benutzern oder Datenflüssen Prioritäten zu oder garantiert einem Datenfluss eine bestimmte Leistungsstufe. Diese Zusagen sind wichtig bei unzureichender Netzwerkkapazität. Dies gilt beispielsweise für das Streaming von Multimedia-Anwendungen in Echtzeit wie VoIP, Online-Spielen und IP-TV, da diese Anwendungen häufig eine feste Bitrate benötigen und anfällig für Verzögerungen sind. Außerdem sind die Zusagen in Netzwerken wichtig, in denen die Kapazität eine eingeschränkte Ressource ist.

Konfigurieren der Bandbreitenverwaltung

Mit dem Bandbreitenmanagement des Geräts können Sie die Bandbreite des Verkehrs verwalten, der vom sicheren Netzwerk (LAN) zum nicht sicheren Netzwerk (WAN) fließt.

Konfigurieren der Bandbreite

Sie können die Bandbreite begrenzen, um die Datenübertragungsrate des Geräts zu reduzieren. Außerdem können Sie mithilfe eines Bandbreitenprofils den ausgehenden Verkehr begrenzen und so verhindern, dass die LAN-Benutzer die gesamte Bandbreite der Internetverbindung verwenden.

So legen Sie die Upstream- und Downstream-Bandbreite fest:

SCHRITT 1 Wählen Sie **QoS** > **Bandbreitenverwaltung** aus.

SCHRITT 2 Aktivieren Sie im Feld **Bandbreitenverwaltung** das Kontrollkästchen **Aktivieren**. Im Abschnitt **Bandbreite** wird die vom ISP bereitgestellte maximale Bandbreite angezeigt.

SCHRITT 3 Geben Sie in die **Bandbreitentabelle** die folgenden Informationen für die WAN-Schnittstelle ein:

Upstream	Die Bandbreite (KBit/s), die zum Senden von Daten an das Internet verwendet wird.
Downstream	Die Bandbreite (KBit/s), die zum Empfangen von Daten aus dem Internet verwendet wird. **(Nur für Standard-VLAN anwenden)**

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren der Bandbreitenpriorität

In der **Bandbreitenprioritätstabelle** können Sie die Verwendung der Bandbreite verwalten, indem Sie Services Prioritäten zuweisen.

So konfigurieren Sie die Bandbreitenpriorität:

SCHRITT 1 Klicken Sie in der **Bandbreitenprioritätstabelle** auf **Hinzufügen**.

SCHRITT 2 Geben Sie in die folgenden Felder Informationen ein:

Aktivieren	Aktivieren Sie dieses Kontrollkästchen, um die Bandbreitenverwaltung für diesen Service zu aktivieren.
Richtung	Wählen Sie diese Option, um ein- oder ausgehenden Verkehr zu priorisieren.
Kategorie	Wählen Sie diese Option, um die Bandbreite für Services, VLANs/SSIDs, IP-Quelladressen (eingehender Verkehr) oder IP-Zieladressen (ausgehender Verkehr) zu priorisieren.
Service	Wählen Sie den Service aus, der priorisiert werden soll.
VLAN/SSID	Wählen Sie das VLAN oder die SSID aus, das bzw. die priorisiert werden soll.

IP-Adresse **Subnetzmaske**	Geben Sie im Feld **Kategorie**, je nachdem, ob Sie „Quell-IP“ oder „Ziel-IP“ ausgewählt haben, die IP-Adresse und die Subnetzmaske der Quelle oder des Ziels ein.
Priorität	Legen Sie die Priorität (**niedrig**, **mittel** oder **hoch**) für die ausgewählte Kategorie fest.
Remarking	Aktivieren Sie dieses Kontrollkästchen, um Remarking für DSCP (Differentiated Services Code Point) zu aktivieren. Wenn Sie diese Funktion aktivieren, wird der Netzwerkverkehr durch das LAN basierend auf den DSCP-Warteschlangenzuordnungen auf der Seite **DSCP-Einstellungen** priorisiert.
DSCP	Geben Sie den Remarking-Wert für Pakete in diesem Netzwerk ein.

SCHRITT 3 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen eines Eintrags in der Tabelle aktivieren Sie das entsprechende Kontrollkästchen, und klicken Sie auf **Bearbeiten**. Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Zum Löschen eines Eintrags aus der Tabelle aktivieren Sie das entsprechende Kontrollkästchen und klicken Sie auf **Löschen**. Klicken Sie auf **Speichern**.

Zum Hinzufügen eines neuen Serviceziels klicken Sie auf die Schaltfläche **Serviceverwaltung**. Sie können einen neuen Service definieren, der für alle Firewalldefinitionen und QoS-Definitionen verwendet werden soll. Weitere Informationen hierzu finden Sie unter **Konfigurieren der Serviceverwaltung**.

Konfigurieren der anschlussbasierten QoS-Einstellungen

Sie können QoS-Einstellungen für jeden Anschluss am Gerät konfigurieren. Das unterstützt vier Prioritätswarteschlangen, die eine Priorisierung des Verkehrs für die einzelnen Anschlüsse ermöglichen.

So konfigurieren Sie QoS-Einstellungen für die Anschlüsse des Geräts:

SCHRITT 1 Wählen Sie **QoS** > **Anschlussbasierte QoS-Einstellungen** aus.

SCHRITT 2 Geben Sie für jeden Anschluss in der Tabelle **Anschlussbasierte QoS-Einstellungen** folgende Informationen ein:

Vertrauensmodus	Wählen Sie im Dropdown-Menü eine der folgenden Optionen aus: • **Anschluss**: Die anschlussbasierten QoS-Einstellungen werden aktiviert. Anschließend können Sie die Verkehrspriorität für einen bestimmten Anschluss festlegen. Die Priorität der Verkehrswarteschlange beginnt mit der niedrigsten Priorität 1 und endet mit der höchsten Priorität 3. • **DSCP**: Differentiated Services Code Point (DSCP). Wenn Sie diese Funktion aktivieren, wird der Netzwerkverkehr durch das LAN basierend auf den DSCP-Warteschlangenzuordnungen auf der Seite **DSCP-Einstellungen** priorisiert. • **CoS**: Class of Service (CoS).
Standardmäßige Datenverkehrweiterleitungswarteschlange für nicht vertrauenswürdige Geräte	Wählen Sie eine Prioritätsstufe für ausgehenden Verkehr aus (1 bis 3).

SCHRITT 3 Klicken Sie auf **Speichern**.

Um die Standardeinstellungen für anschlussbasiertes QoS wiederherzustellen, klicken Sie auf **Standard wiederherstellen**, und speichern Sie Ihre Änderungen.

Konfigurieren der CoS-Einstellungen

Verwenden Sie den Link zur Seite „Anschlussbasierte QoS-Einstellungen“, um die CoS-Prioritätseinstellungen der QoS-Warteschlange zuzuordnen.

So ordnen Sie CoS-Prioritätseinstellungen der Warteschlange für die Datenverkehrweiterleitung zu:

SCHRITT 1 Wählen Sie **QoS** > **CoS-Einstellungen** aus.

SCHRITT 2 Wählen Sie für jede CoS-Prioritätsstufe in der **CoS-Einstellungstabelle** einen Prioritätswert im Dropdown-Menü **Datenverkehrweiterleitungswarteschlange** aus.

Diese Werte kennzeichnen Verkehrstypen mit je nach Verkehrstyp höherer oder niedrigerer Verkehrspriorität.

SCHRITT 3 Klicken Sie auf **Speichern**.

Um die Standardeinstellungen für anschlussbasiertes QoS wiederherzustellen, klicken Sie auf **Standard wiederherstellen** und anschließend auf **Speichern**.

Konfigurieren der DSCP-Einstellungen

Auf der Seite **DSCP-Einstellungen** können Sie die Zuordnung von DSCP-Warteschlangen zu QoS-Warteschlangen konfigurieren.

So konfigurieren Sie die Zuordnung von DSCP-Warteschlangen zu QoS-Warteschlangen:

SCHRITT 1 Wählen Sie **QoS** > **DSCP-Einstellungen** aus.

SCHRITT 2 Wählen Sie aus, ob nur RFC-Werte oder alle DSCP-Werte in der **DSCP-Einstellungstabelle** aufgelistet werden sollen, indem Sie auf die entsprechende Schaltfläche klicken.

SCHRITT 3 Wählen Sie für jeden DSCP-Wert in der **DSCP-Einstellungstabelle** im Dropdown-Menü **Queue Warteschlange** eine Prioritätsstufe aus.

Damit wird der DSCP-Wert der ausgewählten QoS-Warteschlange zugeordnet.

SCHRITT 4 Klicken Sie auf **Speichern**.

Zum Wiederherstellen der DSCP-Standardeinstellungen klicken Sie auf **Standard wiederherstellen** und anschließend auf **Speichern**.

8

Verwalten des Geräts

Festlegen von Geräteeigenschaften

Weisen Sie dem Gerät einen Namen und einen Domänennamen zu, damit es von anderen Geräten erkannt werden kann.

So legen Sie die Geräteeigenschaften fest:

SCHRITT 1 Wählen Sie **Administration > Geräteeigenschaften** aus.

SCHRITT 2 Geben Sie in das Feld **Hostname** einen Namen ein, anhand dessen das Gerät im Netzwerk eindeutig erkannt werden kann. Beispiel: „RTR141“.

SCHRITT 3 Geben Sie in das Feld **Domänenname** den Namen der Domäne ein, in der sich das Gerät befindet. Beispiel: „abcbusiness.com“. Den Namen der Domäne Ihres Unternehmens erfahren Sie bei Bedarf vom Netzwerkadministrator.

SCHRITT 4 Speichern Sie Ihre Änderungen.

Festlegen der Kennwortkomplexität

Sie können bei Kennwortänderungen Mindestanforderungen für die Kennwortkomplexität erzwingen.

So konfigurieren Sie die Einstellungen für die Kennwortkomplexität:

SCHRITT 1 Wählen Sie **Administration** > **Kennwortkomplexität** aus.

SCHRITT 2 Aktivieren Sie im Feld **Einstellungen für Kennwortkomplexität** das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Konfigurieren Sie die Einstellungen für die Kennwortkomplexität:

Kennwortmindestlänge	Geben Sie die Kennwortmindestlänge ein (0 – 64 Zeichen).
Mindestanzahl an Zeichenklassen	Geben Sie eine Zahl ein, die eine der folgenden Zeichenklassen darstellt: • Großbuchstaben • Kleinbuchstaben • Ziffern • Auf einer Standardtastatur verfügbare Sonderzeichen Kennwörter müssen standardmäßig Zeichen aus mindestens drei dieser Klassen enthalten.
Das neue Kennwort darf nicht mit dem aktuellen identisch sein	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um festzulegen, dass neue Kennwörter nicht mit dem aktuellen Kennwort identisch sein dürfen.
Kennwortfälligkeit	Aktivieren Sie das Kontrollkästchen **Aktivieren**, damit Kennwörter nach einem angegebenen Zeitraum ablaufen.
Kennwortfälligkeitszeit	Geben Sie ein, nach wie vielen Tagen das Kennwort abläuft (1 – 365). Der Standardwert beträgt 180 Tage.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von Benutzerkonten

Das Gerät unterstützt zwei Benutzerkonten zum Verwalten und Anzeigen von Einstellungen: Einen administrativen Benutzer (Standardbenutzername und -kennwort: „cisco“) und einen Gastbenutzer (Standardbenutzername: „guest“).

Das Gastkonto verfügt nur über Lesezugriff. Sie können den Benutzernamen und das Kennwort für das Administratorkonto und für das Gastkonto festlegen und ändern.

So konfigurieren Sie die Benutzerkonten:

SCHRITT 1 Wählen Sie **Administration** > **Benutzer** aus.

SCHRITT 2 Aktivieren Sie im Feld **Kontoaktivierung** die Kontrollkästchen für die Konten, die Sie aktivieren möchten. (Das Administratorkonto muss aktiv sein.)

SCHRITT 3 (Optional) Um das Administratorkonto zu bearbeiten, aktivieren Sie unter **Administratoreinstellungen** das Kontrollkästchen **Administratoreinstellungen bearbeiten**. Um das Gastkonto zu bearbeiten, aktivieren Sie unter Gasteinstellungen das Kontrollkästchen **Gasteinstellungen bearbeiten**. Geben Sie folgende Informationen ein:

Neuer Benutzername	Geben Sie einen neuen Benutzernamen ein.
Altes Kennwort	Geben Sie das aktuelle Kennwort ein.
Neues Kennwort	Geben Sie das neue Kennwort ein. Kennwörter sollten keine Wörter aus einem Wörterbuch irgendeiner Sprache enthalten. Außerdem sollten sie sowohl Buchstaben (Groß- und Kleinbuchstaben) als auch Ziffern und Symbole enthalten. Das Kennwort darf maximal 64 Zeichen enthalten.
Neues Kennwort erneut eingeben	Geben Sie das neue Kennwort erneut ein.

SCHRITT 4 Klicken Sie auf **Speichern**.

Importieren von Benutzerkonten

Sie können mehrere Benutzer auf einmal aus einer CSV-Datei importieren.

Die Daten in der CSV-Datei müssen wie in den folgenden Tabellen dargestellt angeordnet sein:

TYPE	USERNAME	PASSWORD
Admin	Admin123	Admin123

TYPE	USERNAME	PASSWORD
Guest	Gast123	Gast123

TYPE	USERNAME	PASSWORD	ENABLE
PPTP	PPTP-Benutzer-1	12345678	enable
PPTP	PPTP-Benutzer-2	345123678	disable

TYPE	USERNAME	PASSWORD
VPNServer	VPN-Benutzer-1	12345678
VPNServer	VPN-Benutzer-2	33245678

TYPE	USERNAME	PASSWORD	ACCESS_TIME
guestnet	Gastnetz-Benutzer-1	12345678	1440
guestnet	Gastnetz-Benutzer-2	33245678	60

HINWEIS Bei den Spaltennamen wird zwischen Groß- und Kleinschreibung unterschieden. Ändern Sie weder die Reihenfolge noch die Namen der Spalten.

So importieren Sie Benutzerkonten aus einer CSV-Datei:

SCHRITT 1 Klicken Sie im Feld **Benutzername und Kennwort importieren** auf **Durchsuchen**.

SCHRITT 2 Suchen Sie die Datei und klicken Sie auf **Öffnen**.

SCHRITT 3 Klicken Sie auf **Importieren**.

Festlegen des Sitzungs-Timeout-Werts

Der Timeout-Wert gibt an, wie lange (in Minuten) der Gerätemanager im inaktiven Zustand verbleiben kann, bis die Gerätemanagersitzung beendet wird. Sie können ein Timeout für das Administratorkonto und das Gastkonto konfigurieren.

So konfigurieren Sie ein Sitzungs-Timeout:

SCHRITT 1 Wählen Sie **Administration** > **Sitzungs-Timeout** aus.

SCHRITT 2 Geben Sie in das Feld **Administratorinaktivitäts-Timeout** ein, nach wie vielen Minuten ein Sitzungs-Timeout aufgrund von Inaktivität auftritt. Wählen Sie **Nie** aus, um zuzulassen, dass der Administrator dauerhaft angemeldet bleibt.

SCHRITT 3 Geben Sie in das Feld **Gastinaktivitäts-Timeout** ein, nach wie vielen Minuten ein Sitzungs-Timeout aufgrund von Inaktivität auftritt. Wählen Sie **Nie** aus, um zuzulassen, dass der Administrator dauerhaft angemeldet bleibt.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von SNMP (Simple Network Management)

Mit dem SNMP (Simple Network Management Protocol) können Sie den Router über einen SNMP-Manager überwachen und verwalten. SNMP ermöglicht die Remoteüberwachung und -steuerung von Netzwerkgeräten sowie die Verwaltung von Konfigurationen, Statistiken, Leistung und Sicherheit.

Konfigurieren von SNMP-Systeminformationen

HINWEIS Zum Verwenden von SNMP müssen Sie zuerst SNMP-Software auf dem Computer installieren. Das Gerät unterstützt nur SNMPv3 für die SNMP-Verwaltung und SNMPv1/2/3 für SNMP-Trap-Nachrichten.

So aktivieren Sie SNMP:

SCHRITT 1 Wählen Sie **Administration** > **SNMP** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um SNMP zu aktivieren.

SCHRITT 3 Klicken Sie auf **Aktivieren**, um **den Benutzerzugriff per Internet** oder **den Benutzerzugriff per VPN** zu erlauben.

SCHRITT 4 Wählen Sie im Feld **Modus** die SNMP-Version aus.

SCHRITT 5 Geben Sie folgende Informationen ein:

SysContact	Geben Sie den Namen der Kontaktperson für dieses Gerät ein. Beispiel: der Netzwerkadministrator.
SysLocation	Geben Sie den physischen Standort des Geräts ein. Beispiel: Rack Nr. 2, 4. Stock.
SysName	Geben Sie einen Namen zur einfachen Erkennung des Geräts ein. Beispiel: RTR 141“.

SCHRITT 6 Klicken Sie auf **Speichern**.

SCHRITT 7 Klicken Sie auf **Protokolle anzeigen**, um die Systemprotokolltabelle anzuzeigen.

Bearbeiten von SNMPv3-Benutzern

Sie können SNMPv3-Parameter für die beiden Standardbenutzerkonten des Geräts (Administrator und Gast) konfigurieren.

So konfigurieren Sie SNMPv3-Einstellungen:

SCHRITT 1 Wählen Sie **Administration** > **SNMP** aus.

SCHRITT 2 Konfigurieren Sie unter **SNMPv3-Benutzerkonfiguration** die folgenden Einstellungen:

Benutzername	Wählen Sie das zu konfigurierende Konto aus (**Administrator** oder **Gast**).
Zugriffsrecht	Zeigt die Zugriffsrechte des ausgewählten Benutzerkontos an.

Sicherheitsstufe	Wählen Sie die SNMPv3-Sicherheitsstufe aus: **Keine Authentifizierung und kein Datenschutz**: Erfordert keine Authentifizierung und keinen Datenschutz. **Authentifizierung und kein Datenschutz**: Es werden nur der Authentifizierungsalgorithmus und das Kennwort übermittelt. **Authentifizierung und Datenschutz**: Es werden der Authentifizierungs- und Datenschutzalgorithmus und das Kennwort übermittelt.
Authentifizierungs-algorithmusserver	Wählen Sie den Typ des Authentifizierungsalgorithmus aus (**MD5** oder **SHA**).
Authentifizierungs-kennwort	Geben Sie das Authentifizierungskennwort ein.
Datenschutzalgorithmus	Wählen Sie den Typ des Datenschutzalgorithmus aus (**DES** oder **AES**).
Datenschutzkennwort	Geben Sie das Datenschutzkennwort ein.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren der SNMP-Traps

In den Feldern im Abschnitt **SNMP-Trap-Konfiguration** können Sie einen SNMP-Agent konfigurieren, an den das Gerät Trap-Nachrichten (Benachrichtigungen) sendet.

So konfigurieren Sie die Traps:

SCHRITT 1 Wählen Sie **Administration** > **SNMP** aus.

SCHRITT 2 Nehmen Sie unter **Trap-Konfiguration** die folgenden Einstellungen vor:

IP-Adresse	Geben Sie die IP-Adresse des SNMP-Managers oder Trap-Agents ein.

Port	Geben Sie den SNMP-Trap-Port der IP-Adresse ein, an die Trap-Nachrichten gesendet werden sollen.
Community	Geben Sie die Community-Zeichenfolge für den Agent ein. Die meisten Agents sind so konfiguriert, dass Traps in der öffentlichen Community abgehört werden.
SNMP-Version	Wählen Sie die SNMP-Version aus: **v1**, **v2c** oder **v3**.
Schweregrad der SNMP-Trap	Wählen Sie den Schweregrad aus, für den das Gerät Trap-Nachrichten senden soll.

SCHRITT 3 Klicken Sie auf **Speichern**.

Verwenden von Diagnosetools

Das Gerät stellt verschiedene Diagnosetools bereit, die die Behebung von Netzwerkproblemen erleichtern sollen.

- **Netzwerktools**
- **Konfigurieren der Anschlussspiegelung**

Netzwerktools

Mit Netzwerktools können Sie Probleme im Netzwerk behandeln.

Verwenden von Ping

Mit dem Ping-Dienstprogramm können Sie die Konnektivität zwischen diesem Router und einem anderen Gerät im Netzwerk testen. Außerdem können Sie mit dem Ping-Tool die Konnektivität mit dem Internet testen, indem Sie einen Ping an einen voll qualifizierten Domänennamen (beispielsweise www.cisco.com) senden.

So verwenden Sie Ping:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Netzwerktools** aus.

SCHRITT 2 Geben Sie in das Feld **IP-Adresse/Domänenname** die IP-Adresse des Geräts oder einen voll qualifizierten Domänennamen wie beispielsweise „www.cisco.com“ ein, um einen Ping zu senden.

SCHRITT 3 Klicken Sie auf **Ping**. Die Ping-Ergebnisse werden angezeigt. Diesen Ergebnissen können Sie entnehmen, ob das Gerät erreichbar ist.

Verwenden der Routenverfolgung

Mit dem Dienstprogramm für die Routenverfolgung können Sie alle Router anzeigen, die sich zwischen der Ziel-IP-Adresse und diesem Router befinden. Der Router zeigt maximal 30 Hops (zwischengeschaltete Router) zwischen diesem Router und dem Ziel an.

So verwenden Sie die Routenverfolgung:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Netzwerktools** aus.

SCHRITT 2 Geben Sie in das Feld **IP-Adresse/Domänenname** die IP-Adresse ein, die Sie verfolgen möchten.

SCHRITT 3 Klicken Sie auf **Routenverfolgung**. Die Ergebnisse der Routenverfolgung werden angezeigt.

Ausführen einer DNS-Suche

Sie können das Suchtool verwenden, um die IP-Adresse des Hosts (beispielsweise eines Webservers, FTP-Servers oder Mailservers) im Internet zu ermitteln.

Um die IP-Adresse eines Webservers, FTP-Servers, Mailservers oder eines beliebigen anderen Servers im Internet abzurufen, geben Sie den Internetnamen in das Textfeld ein, und klicken Sie auf **Abfrage**. Wenn der Host- oder Domäneneintrag vorhanden ist, wird eine Antwort mit der IP-Adresse angezeigt. Wenn die Meldung „Unbekannter Host“ angezeigt wird, ist der angegebene Internetname nicht vorhanden.

So verwenden Sie das Suchtool:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Netzwerktools** aus.

SCHRITT 2 Geben Sie in das Feld **Internetname** den Internetnamen des Hosts ein.

SCHRITT 3 Klicken Sie auf **Suche**. Die nslookup-Ergebnisse werden angezeigt.

Konfigurieren der Anschlussspiegelung

Bei der Anschlussspiegelung wird der Netzwerkverkehr überwacht, indem Kopien aller ein- und ausgehenden Pakete von einem Anschluss an einen Überwachungsanschluss gesendet werden. Sie können die Anschlussspiegelung als Diagnose- und Fehlerbehebungstool verwenden, insbesondere wenn Sie einen Angriff abwehren oder den Benutzerverkehr vom LAN zum WAN anzeigen möchten, um herauszufinden, ob Benutzer auf Informationen oder Websites zugreifen, auf die sie nicht zugreifen sollen.

Der LAN-Host (PC) sollte eine statische IP-Adresse verwenden, um Probleme bei der Anschlussspiegelung zu vermeiden. DHCP-Leases für einen LAN-Host können ablaufen und zu Fehlern bei der Anschlussspiegelung führen, wenn für den LAN-Host keine statische IP-Adresse konfiguriert ist.

So konfigurieren Sie die Anschlussspiegelung:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Anschlussspiegelung** aus.

SCHRITT 2 Wählen Sie im Feld **Spiegelquelle** die zu spiegelnden Anschlüsse aus.

SCHRITT 3 Wählen Sie im Dropdown-Menü **Spiegelanschluss** einen Spiegelanschluss aus. Wenn Sie einen Anschluss für die Spiegelung verwenden, sollten Sie ihn nicht für anderen Verkehr verwenden.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von Protokoll- und E-Mail-Einstellungen

Konfigurieren Sie Protokolle, um Aktivitäten in Bezug auf Zustand und Leistung des Geräts zu überwachen.

Konfigurieren von Protokolleinstellungen

So konfigurieren Sie die Protokollierung:

SCHRITT 1 Wählen Sie **Administration** > **Protokollierung** > **Protokolleinstellungen** aus.

SCHRITT 2 Aktivieren Sie im Feld **Protokollmodus** das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Aktivieren Sie unter **E-Mail-Alarm** das Kontrollkästchen „Aktivieren“, um das Gerät so zu konfigurieren, dass bei Ereignissen oder Verhaltensweisen, die Leistung, Betrieb und Sicherheit des Geräts beeinträchtigen, oder zu Fehlerbehebungszwecken Alarm-E-Mails an eine bestimmte E-Mail-Adresse gesendet werden. Aktivieren Sie das entsprechende Kontrollkästchen, um E-Mail-Alarme für die folgenden Ereignisse zu aktivieren:

WAN gestartet/ heruntergefahren	Eine E-Mail wird gesendet, wenn die WAN-Verbindung heruntergefahren ist. Eine weitere E-Mail wird gesendet, wenn die Verbindung wieder gestartet ist.
Site-to-Site-IPSec-VPN-Tunnel gestartet/ heruntergefahren	Eine E-Mail wird gesendet, wenn der Site-to-Site-IPSec-VPN-Tunnel heruntergefahren ist. Eine weitere E-Mail wird gesendet, wenn der Tunnel wieder gestartet ist.
CPU-Auslastung	Eine Alarm-E-Mail wird gesendet, wenn die CPU-Auslastung den Schwellenwert überschreitet. Eine weitere Alarm-E-Mail wird gesendet, wenn sich die CPU-Auslastung wieder normalisiert hat.
Systemstart	Beim Systemstart des Geräts wird eine Alarm-E-Mail gesendet.
Neue Firmware verfügbar	Eine Alarm-E-Mail wird gesendet, wenn für das Gerät eine neue Firmware verfügbar ist.

SCHRITT 4 Klicken Sie auf **Hinzufügen**.

SCHRITT 5 Konfigurieren Sie die folgenden Einstellungen:

Remoteprotokollserver	Geben Sie die IP-Adresse des Protokollservers ein, auf dem die Protokolle verwaltet werden sollen.
Schweregrad für lokales und per E-Mail versendetes Protokoll	Wählen Sie den Schweregrad von Ereignissen aus, für die Sie Protokolle verwalten und an eine bestimmte E-Mail-Adresse senden möchten. Alle Protokolltypen mit einem höheren Schweregrad als der ausgewählte Protokolltyp werden automatisch berücksichtigt und können nicht ignoriert werden. Beispiel: Wenn Sie Protokolle des Typs „Fehler“ auswählen, werden die Typen „Notfall“, „Alarm“ und „Kritisch“ ebenfalls ausgewählt. Es stehen die folgenden Schweregrade für Ereignisse zur Verfügung (von der höchsten bis zur niedrigsten Gewichtung): • **Notfall**: Das System kann nicht verwendet werden. • **Alarm**: Es ist eine Aktion erforderlich. • **Kritisch**: Das System befindet sich in einem kritischen Zustand. • **Fehler**: Das System befindet sich im Fehlerzustand. • **Warnung**: Es ist eine Systemwarnung aufgetreten. • **Benachrichtigung**: Das System funktioniert ordnungsgemäß, es ist jedoch ein Systemhinweis aufgetreten. • **Informationen**: Geräteinformationen. • **Fehlerbehebung**: Detaillierte Ereignisinformationen. Die Auswahl dieses Protokollschweregrads führt zu einer langen Protokollliste und wird für den normalen Routerbetrieb nicht empfohlen.

Aktivieren	Zum Aktivieren dieser Protokollierungseinstellungen aktivieren Sie dieses Kontrollkästchen.

SCHRITT 6 Klicken Sie auf **Speichern**.

Zum Bearbeiten eines Eintrags in der **Tabelle für Protokollierungseinstellungen** wählen Sie den Eintrag aus, und klicken Sie auf **Bearbeiten**. Nehmen Sie die Änderungen vor, und klicken Sie dann auf **Speichern**.

Konfigurieren des E-Mail-Versands für Protokolle

Sie können das Gerät so konfigurieren, dass Protokolle per E-Mail gesendet werden. Wir empfehlen, zum Senden und Empfangen von Protokollen ein separates E-Mail-Konto einzurichten.

Zuerst müssen Sie den Schweregrad der zu erfassenden Protokolle einrichten (siehe **Konfigurieren von Protokolleinstellungen**).

So konfigurieren Sie den E-Mail-Versand für Protokolle:

SCHRITT 1 Wählen Sie **Administration** > **Protokollierung** > **E-Mail-Einstellungen** aus.

SCHRITT 2 Zum Aktivieren des E-Mail-Versands für Protokollereignisse aktivieren Sie das Kontrollkästchen **Aktivieren**.

Der Mindestschweregrad für den E-Mail-Versand der zu erfassenden Protokolle wird angezeigt. Um den Schweregrad zu ändern, klicken Sie auf **Schweregrad konfigurieren**.

SCHRITT 3 Konfigurieren Sie die folgenden Einstellungen:

Adresse des Mailservers	Geben Sie die IP-Adresse des SMTP-Servers ein. Dabei handelt es sich um den Mailserver, der dem von Ihnen eingerichteten E-Mail-Konto zugeordnet ist (Beispiel: mail.firmenname.com).

Port des Mailservers	Geben Sie den SMTP-Serverport ein. Wenn für den E-Mail-Anbieter ein spezieller Port für E-Mail erforderlich ist, geben Sie diesen hier ein. Verwenden Sie anderenfalls den Standardwert (25).
Antwort-E-Mail-Adresse	Geben Sie die Antwort-E-Mail-Adresse ein, an die das Gerät Nachrichten sendet, wenn Protokolle vom Router nicht an die unter „An E-Mail-Empfänger senden“ angegebene E-Mail-Adresse übermittelt werden können.
An E-Mail-Empfänger 1 senden	Geben Sie eine E-Mail-Adresse ein, an die Protokolle gesendet werden sollen (Beispiel: protokollierung@firmenname.com).
An E-Mail-Empfänger 2 senden (optional)	
An E-Mail-Empfänger 3 senden (optional)	
E-Mail-Verschlüsselung	Wählen Sie „SSL“ oder „TSL“ als E-Mail-Verschlüsselungsmethode aus. Wählen Sie „Deaktivieren“ aus, wenn Sie keine E-Mail-Verschlüsselungsmethode verwenden möchten.
Authentifizierung an SMTP-Server	Wenn der SMTP-Server (Mailserver) Verbindungen nur nach Authentifizierung akzeptiert, wählen Sie im Dropdown-Menü den Authentifizierungstyp aus: **Keine**, **Anmelden**, **Unverschlüsselt** oder **CRAM-MD5**.
E-Mail-Authentifizierungs-benutzername	Geben Sie den Benutzernamen für die E-Mail-Authentifizierung ein (Beispiel: protokollierung@firmenname.com).
E-Mail-Authentifizierungs-kennwort	Geben Sie das E-Mail-Authentifizierungskennwort ein (beispielsweise das Kennwort, das für den Zugriff auf das von Ihnen eingerichtete E-Mail-Konto verwendet wird, an das Protokolle gesendet werden sollen).
E-Mail-Authentifizierungstest	Klicken Sie auf **Testen**, um die E-Mail-Authentifizierung zu testen.

SCHRITT 4 Konfigurieren Sie im Abschnitt **Protokolle nach Zeitplan per E-Mail versenden** die folgenden Einstellungen:

Einheit	Wählen Sie die Zeiteinheit für die Protokolle aus (**Nie**, **Stündlich**, **Täglich** oder **Wöchentlich**). Wenn Sie **Nie** auswählen, werden keine Protokolle gesendet.
Tag	Wenn Sie für das Senden von Protokollen einen wöchentlichen Zeitplan ausgewählt haben, wählen Sie den Wochentag aus, an dem die Protokolle gesendet werden sollen.
Uhrzeit	Wenn Sie für das Senden von Protokollen einen täglichen oder wöchentlichen Zeitplan ausgewählt haben, wählen Sie die Tageszeit aus, zu der die Protokolle gesendet werden sollen.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von Bonjour

Bei Bonjour handelt es sich um ein Protokoll für die Ankündigung und Erkennung von Services. Die auf dem Gerät konfigurierten Standardservices werden nur dann von Bonjour angekündigt, wenn Bonjour aktiviert ist.

So aktivieren Sie Bonjour:

SCHRITT 1 Wählen Sie **Administration** > **Bonjour** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um Bonjour zu aktivieren.

SCHRITT 3 Zum Aktivieren von Bonjour für ein in der **Tabelle für Bonjour-Schnittstellensteuerung** aufgeführtes VLAN aktivieren Sie das entsprechende Kontrollkästchen **Bonjour aktivieren**.

Sie können Bonjour für bestimmte VLANs aktivieren. Wenn Sie Bonjour für ein VLAN aktivieren, können im VLAN vorhandene Geräte die im Router verfügbaren Bonjour-Services erkennen (beispielsweise HTTP/HTTPS).

Wenn beispielsweise ein VLAN mit der ID 2 konfiguriert ist, können Geräte und Hosts in VLAN 2 nur dann im Router ausgeführte Bonjour-Services erkennen, wenn Bonjour für VLAN 2 aktiviert ist.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von Datums- und Zeiteinstellungen

Sie können die Zeitzone konfigurieren, ob die Zeit an die Sommerzeit angepasst werden soll und mit welchem NTP-Server (Network Time Protocol) Datum und Uhrzeit synchronisiert werden sollen. Der Router erhält dann die Datums- und Zeitinformationen vom NTP-Server.

So konfigurieren Sie NTP und Zeiteinstellungen:

SCHRITT 1 Wählen Sie **Administration** > **Zeiteinstellungen** aus. Hier wird die aktuelle Zeit angezeigt.

SCHRITT 2 Geben Sie in die folgenden Felder Informationen ein:

Zeitzone	Wählen Sie die Zeitzone relativ zur Greenwich Mean Time (GMT) aus.
Automatisch auf Sommer-/Winterzeit umstellen	Aktivieren Sie das Kontrollkästchen **Automatisch auf Sommer-/Winterzeit umstellen**, wenn dies für Ihre Region unterstützt wird. Das Kontrollkästchen ist ausgegraut, wenn Sie im Feld **Datum und Uhrzeit festlegen** auf **Manuell** klicken.
Sommerzeit-Modus	Wenn Sie **Nach Datum** auswählen, geben Sie das Datum ein, an dem der Sommerzeit-Modus beginnt. Wenn Sie **Wiederkehrend** auswählen, geben Sie Monat, Woche, Wochentag und Uhrzeit für den Beginn der Sommerzeit ein. Geben Sie die entsprechenden Daten in die Felder **Von** und **Bis** ein.

Sommerzeitdifferenz	Wählen Sie im Dropdown-Menü die Differenz zur Coordinated Universal Time (UTC) aus.
Datum und Uhrzeit festlegen	Wählen Sie aus, ob Datum und Uhrzeit auf dem Gerät manuell oder automatisch eingestellt werden sollen. Wenn Sie **Manuell** auswählen, geben Sie Datum und Uhrzeit in die Felder **Datum und Uhrzeit eingeben** ein.
NTP-Server	Wenn Sie die Standard-NTP-Server verwenden möchten, klicken Sie auf die Schaltfläche **Standard verwenden**. Wenn Sie einen bestimmten NTP-Server verwenden möchten, klicken Sie auf **Benutzerdefinierter NTP-Server**, und geben Sie den voll qualifizierten Domänennamen oder die IP-Adresse des NTP-Servers in die zwei verfügbaren Felder ein.

SCHRITT 3 Klicken Sie auf **Speichern**.

Sichern und Wiederherstellen des Systems

Auf der Seite **Administration > Einstellungen sichern/wiederherstellen** können Sie benutzerdefinierte Konfigurationseinstellungen zur späteren Wiederherstellung sichern oder Einstellungen aus einer zuvor erstellten Sicherung wiederherstellen.

Wenn die Firewall mit den konfigurierten Einstellungen funktioniert, können Sie die Konfiguration sichern, damit Sie sie später wiederherstellen können. Bei der Sicherung werden die Einstellungen als Datei auf dem PC gespeichert. Aus dieser Datei können Sie die Einstellungen der Firewall wiederherstellen.

VORSICHT Versuchen Sie bei einer Wiederherstellung erst nach Abschluss des Vorgangs, eine Onlineverbindung herzustellen, die Firewall auszuschalten, den PC herunterzufahren oder die Firewall zu verwenden. Der Vorgang sollte ungefähr eine Minute dauern. Warten Sie nach dem Erlöschen der Test-LED noch ein paar Sekunden, bevor Sie die Firewall verwenden.

Sichern der Konfigurationseinstellungen

So sichern Sie die Konfiguration oder stellen sie wieder her:

SCHRITT 1 Wählen Sie **Administration** > **Konfiguration sichern/wiederherstellen** aus.

SCHRITT 2 Wählen Sie die Konfiguration aus, die Sie sichern oder löschen möchten:

Startkonfiguration	Wählen Sie diese Option aus, um die Startkonfiguration herunterzuladen. Die Startkonfiguration ist die aktuell ausgeführte Konfiguration, die vom Gerät verwendet wird. Wenn die Startkonfiguration des Routers verloren gegangen ist, verwenden Sie diese Seite, um die Sicherungskonfiguration in die Startkonfiguration zu kopieren. Dabei bleiben alle vorherigen Konfigurationsinformationen erhalten. Sie können die Startkonfiguration herunterladen, um sie problemlos auf anderen RV130/RV130W-Geräten bereitstellen zu können.
Spiegelkonfiguration	Wählen Sie diese Option aus, wenn das Gerät die Startkonfiguration nach 24 Betriebsstunden ohne Änderung an der Startkonfiguration sichern soll.
Sicherungskonfiguration	Wählen Sie diese Option aus, um die aktuellen Konfigurationseinstellungen zu sichern.

SCHRITT 3 Zum Herunterladen einer auf der ausgewählten Konfigurationsoption basierenden Sicherungsdatei klicken Sie auf **Herunterladen**.

Standardmäßig wird die Datei („startup.cfg“, „mirror.cfg“ oder „backup.cfg“) in den Standardordner für Downloads heruntergeladen, beispielsweise C:\Dokumente und Einstellungen\admin\Eigene Dokumente\Downloads\.

SCHRITT 4 Zum Löschen der ausgewählten Konfiguration klicken Sie auf **Löschen**.

Wiederherstellen der Konfigurationseinstellungen

So stellen Sie eine zuvor gespeicherte Konfigurationsdatei wieder her:

SCHRITT 1 Wählen Sie **Administration** > **Konfiguration sichern/wiederherstellen** aus.

SCHRITT 2 Wählen Sie im Feld zum Hochladen der Konfiguration die hochzuladende Konfiguration aus (**Startkonfiguration** oder **Sicherungskonfiguration**).

SCHRITT 3 Klicken Sie auf **Durchsuchen**, um die Datei zu suchen.

SCHRITT 4 Suchen Sie die Datei und klicken Sie auf **Öffnen**.

SCHRITT 5 Klicken Sie auf **Jetzt hochladen**.

Das Gerät lädt die Konfigurationsdatei hoch und verwendet die darin enthaltenen Einstellungen zum Aktualisieren der Startkonfiguration. Anschließend wird das Gerät neu gestartet und verwendet die neue Konfiguration.

Kopieren der Konfigurationseinstellungen

Kopieren Sie die Startkonfiguration in die Sicherungskonfiguration, um sicherzustellen, dass Sie über eine Sicherungskopie verfügen, falls Sie Ihren Benutzernamen und Ihr Kennwort vergessen und dann nicht auf den Gerätemanager zugreifen können. Um den Gerätemanager wieder aufrufen zu können, setzen Sie das Gerät auf die Werkseinstellungen zurück.

Die Sicherungskonfigurationsdatei bleibt im Speicher und Sie können die gesicherten Konfigurationsinformationen in die Startkonfiguration kopieren, wobei alle Einstellungen wiederhergestellt werden.

So kopieren Sie eine Konfiguration (um beispielsweise eine Startkonfiguration in die Sicherungskonfiguration zu kopieren):

SCHRITT 1 Wählen Sie **Administration** > **Einstellungen sichern/wiederherstellen** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü im Feld **Kopieren** die Quell- und Zielkonfiguration aus.

SCHRITT 3 Klicken Sie auf **Jetzt kopieren**.

Generieren eines Verschlüsselungsschlüssels

Sie können auf dem Router einen Verschlüsselungsschlüssel generieren, um die Sicherungsdateien zu schützen.

So generieren Sie einen Verschlüsselungsschlüssel:

SCHRITT 1 Wählen Sie **Administration** > **Einstellungen sichern/wiederherstellen** aus.

SCHRITT 2 Klicken Sie auf **Erweiterte Einstellungen anzeigen**.

SCHRITT 3 Geben Sie in das Feld den zum Generieren des Schlüssels verwendeten Seed-Wert ein.

SCHRITT 4 Klicken Sie auf **Speichern**.

Aktualisieren der Firmware oder Ändern der Sprache

Auf der Seite **Administration** > **Firmware-/Sprach-Upgrade** können Sie die Router-Firmware auf eine neuere Version aktualisieren oder auf dem Router die Sprache ändern.

VORSICHT Versuchen Sie bei einem Firmware-Upgrade nicht, vor Abschluss des Vorgangs eine Onlineverbindung herzustellen, das Gerät auszuschalten, den PC herunterzufahren oder den Vorgang auf irgendeine Weise zu unterbrechen. Der Vorgang dauert einschließlich des Neustarts ungefähr eine Minute. Wenn Sie den Upgrade-Vorgang an bestimmten Stellen unterbrechen, während Daten in den Flash-Speicher geschrieben werden, werden die Daten möglicherweise beschädigt und der Router kann nicht mehr verwendet werden.

Aktualisieren der Firmware

So aktualisieren Sie den Router auf eine neuere Version der Firmware:

SCHRITT 1 Wählen Sie **Administration** > **Firmware-/Sprach-Upgrade** aus.

SCHRITT 2 (Optional) Klicken Sie auf **Herunterladen**, um die aktuelle Version der Firmware herunterzuladen.

SCHRITT 3 Klicken Sie im Feld **Dateityp** auf die Schaltfläche **Firmware-Image**.

SCHRITT 4 Klicken Sie auf **Durchsuchen**, um die heruntergeladene Firmware zu suchen und auszuwählen.

SCHRITT 5 (Optional) Um das Gerät nach der Aktualisierung der Firmware auf die Werkseinstellungen zurückzusetzen, aktivieren Sie das Kontrollkästchen **Alle Konfigurationen/Einstellungen auf Werkseinstellungen zurücksetzen**.

VORSICHT Beim Zurücksetzen des Geräts auf die werkseitigen Einstellungen werden alle Konfigurationseinstellungen gelöscht.

SCHRITT 6 Klicken Sie auf **Upgrade starten**.

Nach der Überprüfung des neuen Firmware-Images wird das Image in den Flash-Speicher geschrieben und der Router wird automatisch mit der neuen Firmware neu gestartet.

SCHRITT 7 Wählen Sie **Status** > **Systemübersicht** aus, um sich zu vergewissern, dass die neue Firmwareversion im Router installiert wurde.

Ändern der Sprache

So ändern Sie die Sprache des Geräts:

SCHRITT 1 Wählen Sie **Administration** > **Firmware-/Sprach-Upgrade** aus.

SCHRITT 2 Klicken Sie im Feld **Dateityp** auf die Schaltfläche **Sprachdatei**.

SCHRITT 3 Klicken Sie auf **Durchsuchen**, um die heruntergeladene Sprachdatei zu suchen und auszuwählen.

SCHRITT 4 (Optional) Wenn Sie die Parameter der Gerätekonfiguration auf die werkseitigen Standardeinstellungen zurücksetzen möchten, wählen Sie **Alle Konfigurationen/ Einstellungen auf Werkseinstellungen zurücksetzen** aus.

SCHRITT 5 Klicken Sie auf **Upgrade starten**.

Neustarten des Geräts

So starten Sie den Router neu:

SCHRITT 1 Wählen Sie **Administration** > **Neustart** aus.

SCHRITT 2 Klicken Sie auf **Neustart**.

Wiederherstellen der Werkseinstellungen

VORSICHT Versuchen Sie bei einer Wiederherstellung erst nach Abschluss des Vorgangs, eine Onlineverbindung herzustellen, den Router auszuschalten, den PC herunterzufahren oder den Router zu verwenden. Der Vorgang sollte ungefähr eine Minute dauern. Warten Sie nach dem Erlöschen der Test-LED noch ein paar Sekunden, bevor Sie den Router verwenden.

So stellen Sie die Werkseinstellungen des Routers wieder her:

SCHRITT 1 Wählen Sie **Administration** > **Werkseinstellungen wiederherstellen** aus.

SCHRITT 2 Klicken Sie auf **Standard**.

B

Webfilter

Die Webfilterung ist eine Funktion auf dem Router, mit der Sie den Zugriff auf unerwünschte Websites verwalten können. Dies kann die Sicherheit eines bereits sicheren Netzwerks weiter verbessern und die Produktivität erhöhen, indem die Web-Zugriffs-Anfragen von Clients geprüft und der Zugriff auf die Website anschließend gewährt oder verweigert wird.

Administratoren verfügen über Richtlinien für die allgemeine Netzwerksicherheit, das Internet of Things und/oder Regeln, die sie im Netzwerk einer bestimmten Abteilung implementieren möchten. Administratoren können angepasste Zeitplanregeln erstellen und sie zu Ausnahmelisten hinzufügen, um beispielsweise bestimmten Benutzern zu bestimmten Zeiten den Zugriff auf bestimmte Websites zu gewähren.

Konfigurieren der Webfilterung

In diesem Abschnitt erfahren Sie, wie Sie die Webfilterung am Router konfigurieren und welche Bedeutung diese Funktion hat. Führen Sie die nachfolgenden Schritte aus, um die Webfilterung am Router zu konfigurieren und zu aktivieren:

SCHRITT 1 Klicken Sie auf **Web Filtering** (Webfilterung).

SCHRITT 2 Wählen Sie in diesem Abschnitt eine der folgenden Optionen aus:

- **Always On** (Immer aktiviert) – Die Webfilterung ist immer aktiviert.
- **Scheduled** (Geplant) – Sie können einen Zeitplan für die Implementierung der Webfilterung festlegen.
- **Always Off** (Immer deaktiviert) – Die Webfilterung ist immer deaktiviert.

HINWEIS Standardmäßig ist die Webfilterung immer deaktiviert.

SCHRITT 3 Wählen Sie im Abschnitt "Web Reputation" (Webreputation) die Option **Enable** (Aktivieren) aus, um die Filterung mit den ausgewählten Filterkategorien zu aktivieren.

SCHRITT 4 Klicken Sie auf "Categories" (Kategorien), und wählen Sie eine der folgenden Optionen aus, um die Filter zu verwalten und anzuwenden.

- **Low** (Niedrig) – Erotische Inhalte/Inhalte für Erwachsene und Sicherheit sind aktiviert. Wählen und prüfen Sie die verfügbaren Optionen, um Ihre Filter anzupassen.
- **Medium** (Mittel) – Erotische Inhalte/Inhalte für Erwachsene, Illegale/Fragwürdige Inhalte und Sicherheit sind aktiviert. Wählen und prüfen Sie die verfügbaren Optionen, um Ihre Filter anzupassen.
- **High** (Hoch) – Erotische Inhalte/Inhalte für Erwachsene, Business/Investment, Unterhaltung, Illegale/Fragwürdige Inhalte, IT-Ressourcen, Lifestyle/Kultur und Sicherheit sind aktiviert. Wählen und prüfen Sie die verfügbaren Optionen, um Ihre Filter anzupassen.
- **Custom** (Benutzerdefiniert) – Es wurden keine Optionen festgelegt, um eine benutzerdefinierte Webfilterung zu ermöglichen.

SCHRITT 5 Klicken Sie auf **Save** (Speichern) und **Back** (Zurück), um auf die Seite "Filter" (Filter) zurückzugelangen und mit der Einrichtung fortzufahren.

SCHRITT 6 Aktivieren Sie **Enable HTTPS Filtering** (HTTPS-Filterung aktivieren), um Inhalte basierend auf der Web-IP-Adresse anstatt auf der URL zu filtern. Websites mit sicherem HTTP oder HTTPS sind zugänglich. Aktivieren Sie **Enable HTTPS Filtering** (HTTPS-Filterung aktivieren) nicht, wenn Sie Websites unabhängig von einer sicheren URL blockieren möchten.

HINWEIS Die HTTPS-Filterung basiert auf der Webserver-IP-Adresse anstatt auf der URL, da die URL verschlüsselt ist. Oftmals verwenden mehrere Websites dieselbe Webserver-IP-Adresse. Ist dies der Fall, blockiert der Router die Seite nicht, wenn mit der IP-Adresse mehrere Website-Kategorien verknüpft sind. Der Router blockiert die Seite jedoch, wenn unter dieser IP-Adresse Inhalte für Erwachsene gehostet werden, oder wenn die IP-Adresse bekanntermaßen Malware hostet oder verteilt.

SCHRITT 7 Wenn Sie **Scheduled** (Geplant) für die Webfilterung ausgewählt haben, wird die Tabelle "Schedule" (Zeitplan) angezeigt. Klicken Sie unter dieser Tabelle auf **Add Row** (Zeile hinzufügen), um eine Zeitplanregel oder -richtlinie zu erstellen, die implementiert werden soll.

SCHRITT 8 Geben Sie in der Tabelle "Schedule" (Zeitplan) im Feld "Name" einen Namen und im Feld "Description" eine Beschreibung ein.

SCHRITT 9 Wählen Sie anschließend einen oder mehrere Tag(e) aus, um den Filter an den gewünschten Tagen anzuwenden.

SCHRITT 10 Geben Sie dann den Zeitraum im 24-Stunden-Format ein, in dem die Regel angewendet werden soll.

SCHRITT 11 Aktivieren Sie abschließend **Active** (Aktivieren), um die Zeitplanregel zu aktivieren.

HINWEIS Sie können beliebig viele Regeln implementieren.

SCHRITT 12 Klicken Sie auf **Save** (Speichern).

SCHRITT 13 (Optional). Erstellen Sie eine Liste, um Websites/Inhalte bei der Filterung zuzulassen, zu verweigern oder auszuschließen. Wählen Sie eine der folgenden Optionen aus:

- **White List** (Whitelist) – Klicken Sie auf **Add Row** (Zeile hinzufügen), und wählen Sie **Domain Name** (Domänenname) oder **Keyword** (Stichwort) aus der Dropdown-Liste aus. Geben Sie anschließend einen Namen ein, um die Richtlinie zu identifizieren.
- **Black List** (Blacklist) – Klicken Sie auf **Add Row** (Zeile hinzufügen), und wählen Sie **Domain Name** (Domänenname) oder **Keyword** (Stichwort) aus der Dropdown-Liste aus. Geben Sie anschließend einen Namen ein, um die Richtlinie zu identifizieren.
- **Exclusion List** (Ausschlussliste) – Klicken Sie auf **Add Row** (Zeile hinzufügen), und wählen Sie **Domain Name** (Domänenname) oder **Keyword** (Stichwort) aus der Dropdown-Liste aus. Geben Sie anschließend einen Namen ein, um die Richtlinie zu identifizieren.

SCHRITT 14 Wählen Sie die Webfilterungsrichtlinie aus der Liste aus, und klicken Sie auf **Edit** (Bearbeiten) oder **Delete** (Löschen), um die Richtlinie zu bearbeiten oder zu löschen.

SCHRITT 15 Klicken Sie auf **Save** (Speichern).

A

Weitere Informationen

Support	
Cisco Support-Community	www.cisco.com/go/smallbizsupport
Cisco Support und Ressourcen	www.cisco.com/go/smallbizhelp
Telefonischer Kundensupport	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Firmware-Downloads	www.cisco.com/cisco/software/navigator.html?i=!ch Wählen Sie einen Link zum Download der Firmware aus. Eine Anmeldung ist nicht erforderlich.
Cisco Open-Source-Anfragen	www.cisco.com/go/smallbiz_opensource_request
Cisco Partner Central (Partner-Anmeldung erforderlich)	www.cisco.com/web/partners/sell/smb
Produktdokumentation	
Cisco RV130/RV130W Wireless-Multifunktions-VPN-Router	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html

Ergebnisse im Zusammenhang mit EU-Lot 26 finden Sie unter www.cisco.com/go/eu-lot26-results.