Sicherheitsprodukte

SSG 20 – Handbuch zur Hardwareinstallation und -konfiguration

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Teilenummer: 530-015646-01-GR, Revision 02

Copyright Notice

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

Inhaltsverzeichnis

Zu diesem Handbuch

Das Secure Services Gateway (SSG) 20-Gerät von Juniper Networks ist eine integrierte Router- und Firewallplattform, die Zweigstellen oder Einzelhandelsgeschäften Internet Protocol Security (IPSec) Virtual Private Network (VPN)- und Firewalldienste bietet.

Juniper Networks bietet zwei Ausführungen des SSG 20-Geräts an:

- SSG 20, das Auxiliary (AUX)-Verbindung unterstützt.
- SSG 20-WLAN, das integrierte 802.11a/b/g-Wireless-Standards unterstützt.

Beide SSG 20-Geräte unterstützen Universal Serial Bus (USB)-Speichergeräte und verfügen über zwei Mini Physical Interface Module (PIM)-Steckplätze, die mit sämtlichen Mini-PIMs kompatibel sind. Die Geräte ermöglichen zudem Protokollkonvertierungen zwischen Local Area Networks (LANs) und Wide Area Networks (WANs).

HINWEIS: Die Konfigurationsanweisungen und Beispiele in diesem Dokument basieren auf den Funktionen eines Geräts, auf dem ScreenOS 5.4 ausgeführt wird. Die Funktionsweise Ihres Gerätes unterscheidet sich möglicherweise abhängig von der verwendeten ScreenOS-Version. Die aktuellsten Gerätedokumentationen erhalten Sie auf der Juniper Networks-Website für technische Informationen unter http://www.juniper.net/techpubs/hardware. Die derzeit für Ihr Gerät verfügbaren ScreenOS-Versionen werden auf der Juniper Networks-Supportwebsite unter http://www.juniper.net/customers/support/ angezeigt.

Organisation

Dieses Handbuch ist in folgende Abschnitte gegliedert:

- In Kapitel 1, „Hardware – Überblick," werden das Gehäuse und die Komponenten eines SSG 20-Geräts beschrieben.
- In Kapitel 2, „Installieren und Anschließen des Geräts," werden die Montage eines SSG 20-Geräts sowie das Anschließen von Kabeln und der Stromversorgung an das Gerät beschrieben.
- In Kapitel 3, „Konfigurieren des Geräts," werden die Konfiguration und die Verwaltung eines SSG 20-Geräts sowie die Durchführung einiger grundlegender Konfigurationsaufgaben beschrieben.
- In Kapitel 4, „Warten des Geräts," werden die Wartungsmaßnahmen für SSG 20-Geräte erläutert.
- In Anhang A, „Technische Daten," finden Sie allgemeine technische Systemdaten für SSG 20-Geräte.
- In Anhang B bietet „Assistent für die Anfangskonfiguration," detaillierte Informationen zur Verwendung des Assistenten für die Anfangskonfiguration (Initial Configuration Wizard, ICW) für SSG 20-Geräte.

WebUI-Konventionen

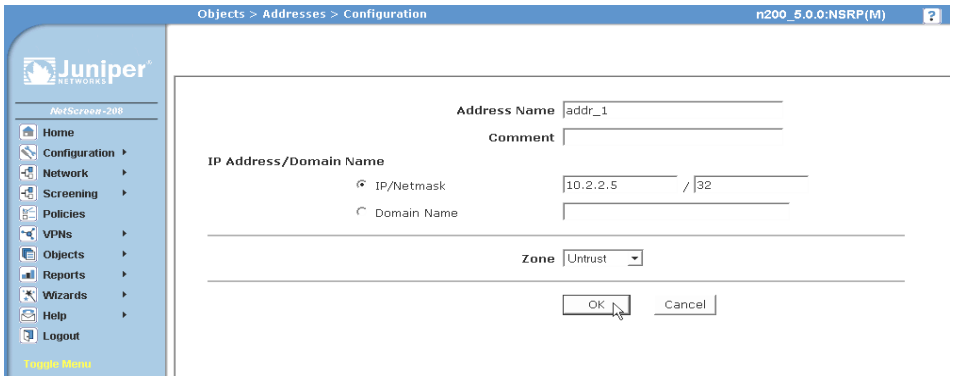
Navigieren Sie zum Ausführen einer Aufgabe mit der WebUI zuerst zum entsprechenden Dialogfeld, um dort Objekte zu definieren und Parameter festzulegen. Ein Rechtspfeil (>) zeigt die Schritte bei der Navigation durch die WebUI an, die durch Klicken auf Menüoptionen und Links ausgeführt werden. Die Anweisungen für jede Aufgabe werden in die Navigationspfad- und Konfigurationseinstellungen unterteilt.

Die folgende Abbildung zeigt den Pfad zum Adressenkonfigurations-Dialogfeld mit den folgenden Beispielkonfigurationseinstellungen:

Objects > Addresses > List > New: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

```
Address Name: addr_1
IP Address/Domain Name:
    IP/Netmask: (select), 10.2.2.5/32
Zone: Untrust
```

Abbildung 1: Navigationspfad- und Konfigurationseinstellungen



Konventionen für die Befehlszeilenschnittstelle

Die folgenden Konventionen dienen zur Darstellung der Syntax der Befehlszeilenbefehle in Beispielen und Text.

In Beispielen:

- Alle Angaben in eckigen Klammern [ ] sind optional.
- Alle Angaben in geschwungenen Klammern **{ }** sind erforderlich.
- Wenn mehreren Optionen möglich sind, sind diese durch einen senkrechten Strich (|) voneinander getrennt. Beispiel:

  set interface { ethernet1 | ethernet2 | ethernet3 } manage

  Dies bedeutet „Verwaltungsoptionen für die Schnittstelle ethernet1, ethernet2 *oder* ethernet3 einstellen“.

- Variablen werden *kursiv* dargestellt.

  set admin user *name1* password *xyz*

In Text:

- Befehle werden **fett** dargestellt.
- Variablen werden *kursiv* dargestellt.

HINWEIS: Beim Eingeben eines Schlüsselworts müssen Sie nur so viele Buchstaben eingeben wie zur eindeutigen Identifizierung des Wortes erforderlich sind. Die Eingabe **set adm u kath j12fmt54** ist z. B. ausreichend für den Befehl **set admin user kathleen j12fmt54**. Obwohl solche Abkürzungen zum Eingeben von Befehlen verwendet werden können, sind alle in diesem Handbuch dokumentierten Befehle vollständig dargestellt.

Abrufen von Dokumentationen und technischem Support

Technische Dokumentationen für Juniper Networks-Produkte stehen Ihnen auf unserer Website unter www.juniper.net/techpubs/ zur Verfügung.

Um technischen Support anzufordern, eröffnen Sie einen Support-Fall (Support Case) mit Hilfe des Links „Case Manager“ unter http://www.juniper.net/support/ , oder rufen Sie uns unter 1-888-314-JTAC (innerhalb der Vereinigten Staaten) oder unter +001-408-745-9500 (außerhalb der Vereinigten Staaten) an.

Wenn Sie Fehler oder Auslassungen in diesem Dokument entdecken, schreiben Sie an folgende E-Mail-Adresse:

techpubs-comments@juniper.net

Kapitel 1

Hardware – Überblick

Dieses Kapitel beinhaltet detaillierte Beschreibungen des SSG 20-Chassis und seiner Komponenten. Der Anhang umfasst die folgenden Abschnitte:

Verbindungs- und Netzanschlüsse

In diesem Abschnitt wird die Position der integrierten Anschlüsse und der Netzanschlüsse beschrieben und illustriert. Die folgende Abbildung enthält Darstellungen der Anschlusspositionen, und in Tabelle 1 sind die Netzanschlüsse beschrieben.

Abbildung 2: Position von integrierten Anschlüssen und Mini-PIM

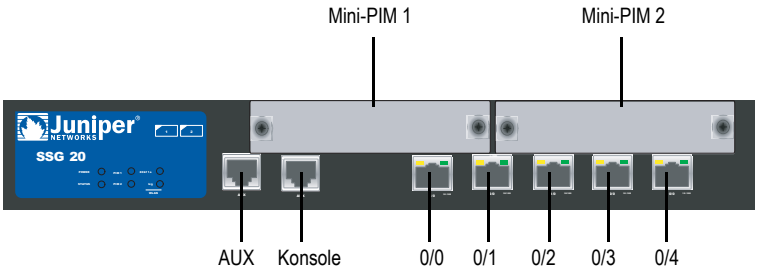


Tabelle 1: SSG 20-Anschlüsse und -Netzanschlüsse

Anschluss	Beschreibung	Stecker	Geschwindigkeit/Protokoll
0/0-0/4	Ermöglicht direkte Verbindungen mit Arbeitsstationen oder eine LAN-Verbindung über einen Switch oder Hub. Mithilfe dieser Verbindung kann das Gerät auch über eine Telnet-Sitzung oder die WebUI verwaltet werden.	RJ-45	Ethernet mit 10/100 MBit/s Automatische Erkennung von Duplex und automatischem MDI/MDIX
USB	Ermöglicht eine USB 1.1-Verbindung mit dem System.	Nicht zutreffend	12 MB (maximale Geschwindigkeit) oder 1,5 MB (minimale Geschwindigkeit)
Konsole	Ermöglicht eine serielle Verbindung mit dem System. Wird für Terminalemulationsverbindungen zum Starten von Befehlszeilenschnittstellen verwendet.	RJ-45	9.600 Bit/s/RS-232C seriell
AUX	Ermöglicht eine asynchrone serielle RS-232-Sicherungsverbindung zum Internet über ein externes Modem.	RJ-45	9.600 Bit/s-115 KBit/s/RS-232C seriell
Mini-PIM			
ADSL 2/2 +	Ermöglicht eine Internetverbindung über eine ADSL-Datenverbindung.	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Ausgabe 2 (nur Annex A) ITU G.992.1 (G.dmt) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2 +)
V.92-Modem	Ermöglicht eine Primär- oder Sicherungsverbindung zum Internet bzw. eine nicht vertrauenswürdige Netzwerkverbindung zu einem Dienstanbieter.	RJ-11	9.600 Bit/s-115 KBit/s/RS-232, serielle automatische Erkennung von Duplex und Polarität
T1	Ermöglicht eine Verbindung zur T1-Leitung des nicht vertrauenswürdigen Netzwerks.	RJ-45	1,544 MBit/s (Full-Time-Slots)
E1	Ermöglicht eine Verbindung zur E1-Leitung des nicht vertrauenswürdigen Netzwerks.	RJ-45	2,048 MBit/s (Full-Time-Slots)

Anschluss	Beschreibung	Stecker	Geschwindigkeit/Protokoll
ISDN	Ermöglicht die Verwendung der ISDN-Leitung als Untrust oder Sicherungsschnittstelle. (S/T)	RJ-45	B-Kanäle mit 64 KBit/s Geleaste Leitung mit 128 KBit/s
Antenne A und B (SSG 20-WLAN)	Ermöglicht eine direkte Verbindung mit Arbeitsstationen in der Nähe einer Wireless-Funkverbindung.	RPSMA	802.11a (54 MBit/s bei Nutzung eines Frequenzbandes von 5 GHz) 802.11b (11 MBit/s bei Nutzung eines Frequenzbandes von 4 GHz) 802.11g (54 MBit/s bei Nutzung eines Frequenzbereichs von 2,4 GHz) 802.11 superG (108 MBit/s bei Nutzung eines Frequenzbandes von 2,4 GHz und 5 GHz)

Bedienfeld

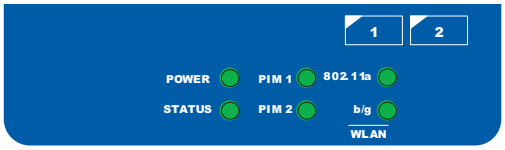
In diesem Abschnitt werden die folgenden Elemente auf dem Bedienfeld eines SSG 20-Geräts beschrieben:

- Systemstatus-LEDs
- Anschlüsse – Beschreibungen
- Mini Physical Interface Module – Anschlussbeschreibungen

Systemstatus-LEDs

Die Systemstatus-LEDs zeigen Informationen zu wichtigen Gerätefunktionen an. Abbildung 3 zeigt die Position jeder Status-LED auf der Vorderseite des SSG 20-WLAN-Geräts. Nur das SSG 20-WLAN-Gerät verfügt über WLAN-LEDs.

Abbildung 3: Status-LEDs



Beim Hochfahren des Systems blinkt die Strom-LED grün, und die Status-LED wechselt in dieser Abfolge: Rot, Grün, grün blinkend. Der Startvorgang nimmt etwa zwei Minuten in Anspruch. Möchten Sie das System aus- und anschließend wieder einschalten, wird empfohlen, nach dem Herunterfahren einige Sekunden zu warten, bevor das System wieder hochgefahren wird. Tabelle 2 beinhaltet den Namen, die Farbe, den Status und die Beschreibung jeder Systemstatus-LED.

Tabelle 2: Status-LED – Beschreibungen

Name	Farbe	Status	Beschreibung
POWER	Grün	Ständig leuchtend	Das System wird mit Strom versorgt.
		Aus	Das System wird nicht mit Strom versorgt.
	Rot	Ständig leuchtend	Das Gerät funktioniert nicht ordnungsgemäß.
		Aus	Das Gerät funktioniert ordnungsgemäß.
STATUS	Grün	Ständig leuchtend	Das System wird gestartet oder führt eine Diagnose durch.
		Blinkend	Das Gerät funktioniert ordnungsgemäß.
	Rot	Blinkend	Ein Fehler wurde festgestellt.
PIM 1	Grün	Ständig leuchtend	Das Mini-PIM funktioniert.
		Blinkend	Das Mini-PIM überträgt Datenverkehr.
		Aus	Das Mini-PIM ist außer Betrieb.
PIM 2	Grün	Ständig leuchtend	Das Mini-PIM funktioniert.
		Blinkend	Das Mini-PIM leitet Datenverkehr weiter.
		Aus	Das Mini-PIM ist außer Betrieb.
WLAN (nur WLAN-Gerät)			
802.11a	Grün	Ständig leuchtend	Die Wireless-Verbindung ist hergestellt, aber es liegt keine Verbindungsaktivität vor.
		Langsam blinkend	Eine Wireless-Verbindung ist hergestellt. Die Baudrate verhält sich proportional zur Verbindungsaktivität.
		Aus	Es ist keine Wireless-Verbindung hergestellt.
b/g	Grün	Ständig leuchtend	Die Wireless-Verbindung ist hergestellt, aber es liegt keine Verbindungsaktivität vor.
		Langsam blinkend	Eine Wireless-Verbindung ist hergestellt. Die Baudrate verhält sich proportional zur Verbindungsaktivität.
		Aus	Es ist keine Wireless-Verbindung hergestellt.

Anschlüsse – Beschreibungen

In diesem Abschnitt werden der Zweck und die Funktion folgender Elemente erläutert:

- Ethernet-Anschlüsse
- Konsolenanschluss
- AUX-Anschluss

Ethernet-Anschlüsse

Fünf 10/100-Ethernet-Anschlüsse ermöglichen LAN-Verbindungen zu Hubs, Switches, lokalen Servern und Arbeitsstationen. Zudem kann ein Ethernet-Anschluss für Verwaltungsdatenverkehr zugewiesen werden. Die Anschlüsse sind fortaufend mit **0/0** bis **0/4** beschriftet. Unter „Standardmäßige Geräteeinstellungen“ auf Seite 31 erhalten Sie Informationen zu den standardmäßigen Zonenbindungen für jeden Ethernet-Anschluss.

Achten Sie bei der Konfiguration eines der Anschlüsse auf den Schnittstellennamen, der der Position des Anschlusses entspricht. Auf dem Bedienfeld werden die Schnittstellennamen für die Anschlüsse von links nach rechts fortlaufend mit **ethernet0/0** bis **ethernet0/4** bezeichnet.

Abbildung 4 zeigt die Position der LEDs auf jedem Ethernet-Anschluss an.

Abbildung 4: Position der Activity Link-LEDs

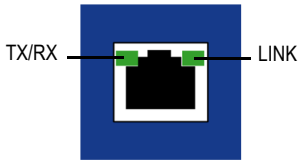


Tabelle 3 zeigt die Ethernet-Anschluss-LEDs an.

Tabelle 3: LAN-Anschluss-LEDs

Name	Farbe	Status	Beschreibung
LINK	Grün	Ständig leuchtend	Anschluss ist online.
		Aus	Anschluss ist offline.
TX/RX	Grün	Blinkend	Datenverkehr wird weitergeleitet. Die Baudrate verhält sich proportional zur Verbindungsaktivität.
		Aus	Der Anschluss ist möglicherweise aktiviert, empfängt jedoch keine Daten.

Konsolenanschluss

Beim Konsolenanschluss handelt es sich um einen seriellen RJ-45-Anschluss, der als zur lokalen Verwaltung verwendbares Data Circuit Terminating Equipment (DCE) verkabelt ist. Verwenden Sie bei einem Klemmanschluss ein Durchgangskabel und ein Crossoverkabel, wenn Sie eine Verbindung zu einem anderen DCE-Gerät herstellen. Ein Adapter für RJ-45 auf DB-9 wird mitgeliefert.

Informationen zu den Kontaktanordnungen der RJ-45-Stecker erhalten Sie unter „Stecker“ auf Seite 60.

AUX-Anschluss

Der Auxiliary (AUX)-Anschluss ist ein serieller RJ-45-Anschluss, der als Data Terminal Equipment (DTE) verkabelt ist. Durch Anschluss an ein Modem ist DTE für die Remoteverwaltung verwendbar. Dieser Anschluss sollte nicht regelmäßig für Remoteverwaltung verwendet werden. Der AUX-Anschluss wird normalerweise als serielle Sicherungsschnittstelle zugewiesen. Die Baudrate kann auf einen Wert zwischen 9.600 Bit/s und 115.200 Bit/s eingestellt werden und erfordert eine Hardwareflusssteuerung. Verwenden Sie beim Anschluss an ein Modem ein Durchgangskabel und beim Anschluss an ein anderes DTE-Gerät ein Crossoverkabel.

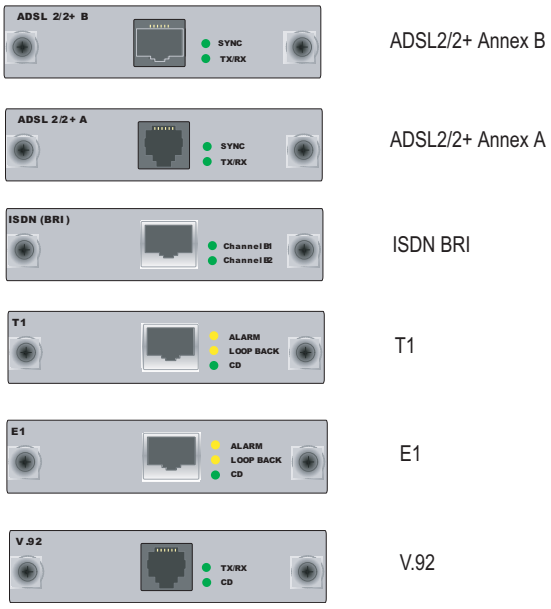
Informationen zu den Kontaktanordnungen der RJ-45-Stecker erhalten Sie unter „Stecker“ auf Seite 60.

Mini Physical Interface Module – Anschlussbeschreibungen

Jedes auf einem Gerät unterstützte Mini Physical Interface Module (PIM) verfügt über die folgenden Komponenten:

- Einen Kabelsteckeranschluss – Akzeptiert einen Netzwerkmedienstecker. Abbildung 5 enthält eine Darstellung der verfügbaren Mini-PIMs. In einem Gerät können maximal zwei Mini-PIMs installiert werden.

Abbildung 5: Mini-PIMs für das SSG 20



- Zwei bis drei Status-LEDs – Zeigt den Anschlussstatus an. In Tabelle 4 wird die Bedeutung der LED-Status erläutert.

Tabelle 4: LED-Status des Mini-PIM auf dem SSG 20

Typ	Name	Farbe	Status	Beschreibung
ADSL 2/2 + (Annex A und B)	SYNC	Grün	Ständig leuchtend	Eine Synchronisierung der ADSL-Schnittstelle wird durchgeführt.
			Blinkend	Die Synchronisierung ist in Bearbeitung.
			Aus	Die Schnittstelle ist nicht aktiv.
	TX/RX	Grün	Blinkend	Datenverkehr wird übertragen.
			Aus	Es wird kein Datenverkehr übertragen.
ISDN (BRI)	CH B1	Grün	Ständig leuchtend	B-Kanal 1 ist aktiv.
			Aus	B-Kanal 1 ist nicht aktiv.
	CH B2	Grün	Ständig leuchtend	B-Kanal 2 ist aktiv.
			Aus	B-Kanal 2 ist nicht aktiv.
T1/E1	ALARM	Gelb	Ständig leuchtend	Ein lokaler Alarm oder ein Remotealarm wurde ausgelöst; das Gerät hat einen Fehler festgestellt.
			Aus	Es ist kein Alarm oder Fehler ausgelöst worden bzw. aufgetreten.
	LOOP BACK	Gelb	Ständig leuchtend	Ein Loopback- oder Leitungsstatus wurde festgestellt.
			Aus	Das Loopback ist nicht aktiv.
	CD	Grün	Ständig leuchtend	Ein Trägersignal wurde festgestellt, und die interne DSU/CSU im Mini-PIM kommuniziert mit einer anderen DSU/CSU.
			Aus	Die Trägersignalerkennung ist nicht aktiv.
V.92	CD	Grün	Ständig leuchtend	Die Verbindung ist aktiv.
			Aus	Die serielle Schnittstelle ist außer Betrieb.
	TX/RX	Grün	Blinkend	Es wird kein Datenverkehr übertragen.
			Aus	Es wird kein Datenverkehr übertragen.

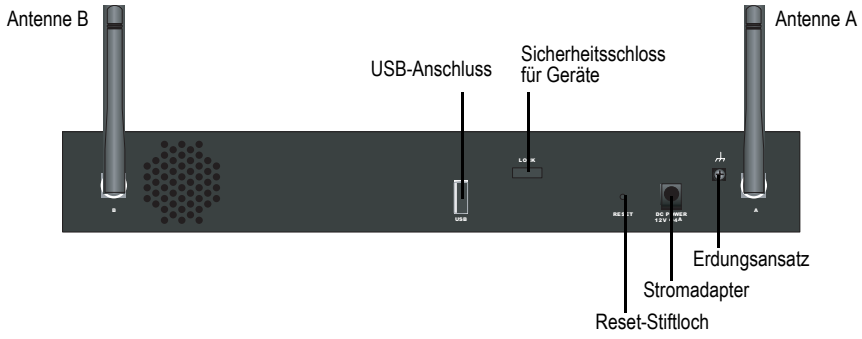
VORSICHT: Die Mini-PIMs sind nicht „hot-swappable“, d.h. der Austausch von Komponenten ist nicht möglich, während der Computer läuft. Die Mini-PIMs müssen vor Einschalten des Geräts in die Steckplätze auf dem Bedienfeld eingesetzt werden.

Rückseite

In diesem Abschnitt werden die folgenden Elemente auf der Rückseite eines SSG 20 Geräts beschrieben:

- Stromadapter
- Funktransceiver
- Erdungsansatz
- Antennentypen
- USB-Anschluss

Abbildung 6: Rückseite eines SSG 20-WLAN-Geräts



Stromadapter

Die Strom-LED auf dem Bedienfeld eines Geräts leuchtet entweder grün oder ist ausgeschaltet. Grün zeigt eine ordnungsgemäße Funktion an, wohingegen eine nicht leuchtende Strom-LED auf einen Stromadapterausfall oder auf den ausgeschalteten Zustand des Geräts hinweist.

Funktransceiver

Die SSG 20-WLAN-Gerät beinhaltet zwei Funktransceiver für Wireless-Verbindungen, die 802.11a/b/g-Standards unterstützen. Der erste Transceiver (WLAN 0) verwendet das 2,4 GHz-Frequenzband, das den 802.11b-Standard bei 11 MBit/s, den 802.11g-Standard bei 54 MBit/s sowie den 802.11 SuperG-Standard bei 108 MBit/s unterstützt. Der zweite Funktransceiver (WLAN 1) verwendet das 5 GHz-Frequenzband, das den 802.11a-Standard bei 54 MBit/s unterstützt. Informationen zur Konfiguration des Wireless-Frequenzbands erhalten Sie unter „Grundlegende Wireless-Konfiguration“ auf Seite 37.

Erdungsansatz

Auf der Rückseite des Chassis ist ein Ein-Loch-Erdungsansatz vorhanden, über den das Gerät geerdet wird (siehe Abbildung 6).

Stellen Sie mit einem Erdungskabel eine Erdung her, und bringen Sie anschließend das Kabel am Ansatz auf der Rückseite des Gehäuses an, um das Gerät vor Herstellung der Stromversorgung zu erden.

Antennentypen

Das SSG 20-WLAN-Gerät unterstützt drei Typen von speziell angefertigten Funkantennen:

- **Doppelantennen** – Die Doppelantennen ermöglichen eine Richtfunkübertragung mit 2 dBi und eine im Wesentlichen einheitliche Signalstärke im Bereich der Funkübertragung und sind für die meisten Installationen geeignet. Dieser Antennentyp wird zusammen mit dem Gerät geliefert.

- **Externe Rundstrahlantenne** – Die externe Antenne ermöglicht eine Rundstrahlübertragung mit 2 dBi. Im Gegensatz zu Doppelantennen, die paarweise eingesetzt werden, beseitigt eine externe Antenne Echoeffekte, die bei Verwendung von zwei Antennen gelegentlich aufgrund eines leicht verzögerten Signalempfangs auftreten.

- **Externe Richtantenne** – Die externe Richtantenne ermöglicht eine Funkübertragung mit 2 dBi in eine Richtung und ist für Orte wie Gänge und Außenmauern (dabei ist die Antenne nach innen gerichtet) geeignet.

USB-Anschluss

Der USB-Anschluss auf der Rückseite eines SSG 20-Geräts nimmt ein Universal Serial Bus (USB)-Speichergerät oder einen USB-Speichergeräteadapter auf, in dem ein Compact Flash-Datenträger installiert ist (siehe Definition in den von der CompactFlash Association veröffentlichten *technischen Angaben zu CompactFlash*. Ist das USB-Speichergerät installiert und konfiguriert, fungiert es automatisch als sekundäres Startgerät, falls beim Start ein Fehler beim primären Compact Flash-Datenträger auftritt.

Der USB-Anschluss ermöglicht Dateiübertragungen wie Gerätekonfigurationen, Benutzerzertifizierungen und die Aktualisierung von Versionsabbildern zwischen einem externen USB-Speichergerät und dem internen Flashspeicher im Sicherheitsgerät. Der USB-Anschluss unterstützt eine Dateiübertragung mit USB 1.1 entweder bei minimaler (1,5 MB) oder maximaler Geschwindigkeit (12 MB).

Führen Sie zur Übertragung von Dateien zwischen dem USB-Speichergerät und einem SSG 20 die folgenden Schritte aus:

1. Stecken Sie das USB-Speichergerät in den USB-Anschluss auf dem Sicherheitsgerät.

2. Speichern Sie die auf dem USB-Speichergerät enthaltenen Dateien mit dem Befehlszeilenbefehl **save {software config | image-key} from usb** *filename* **to flash** auf den internen Flashspeicher des Geräts.

3. Trennen Sie das USB-Speichergerät vor dem Entfernen mit dem Befehlszeilenbefehl **exec usb-device stop** vom USB-Anschluss.

4. Das USB-Speichergerät kann nun entfernt werden.

Möchten Sie vom USB-Speichergerät eine Datei löschen, verwenden Sie den Befehlszeilenbefehl **delete file** *usb:/filename* .

Möchten Sie Informationen zu den auf dem USB-Gerät oder dem internen Flashspeicher gespeicherten Dateien anzeigen, verwenden Sie den Befehlszeilenbefehl **get file**.

Kapitel 2

Installieren und Anschließen des Geräts

In diesem Kapitel wird die Montage eines SSG 20-Geräts sowie das Anschließen von Kabeln und der Stromversorgung an das Gerät beschrieben. Dieses Kapitel ist in folgende Abschnitte gegliedert:

HINWEIS: Sicherheitshinweise und Anweisungen finden Sie im *Security Products Safety Guide* von Juniper Networks. Bevor Sie mit der Arbeit an Geräten beginnen, informieren Sie sich über die Gefahren, die beim Umgang mit elektrischen Komponenten bestehen. Machen Sie sich außerdem mit den gängigen Vorkehrungen zur Vermeidung von Unfällen vertraut.

Einleitung

Die Position des Chassis, die Reihenfolge bei der Verwendung der Montagegeräte und die Sicherheit des Kabelraums sind für eine ordnungsgemäße des Systems von entscheidender Bedeutung.

WARNHINWEIS: Installieren Sie das SSG 20-Gerät in einer sicheren Umgebung, um Missbrauch und dem Eindringen Unbefugter in den Raum vorzubeugen.

Durch Einhalten der folgenden Vorsichtsmaßnahmen können das Herunterfahren des Geräts sowie Gerätefehler und Verletzungen verhindert werden:

- Überprüfen Sie vor jeder Installation, ob das Netzteil von allen Stromquellen getrennt ist.
- Stellen Sie sicher, dass der Raum, in dem das Gerät betrieben werden soll, ausreichend belüftet ist und dass die Raumtemperatur 40°C (104°F) nicht übersteigt.
- Stellen Sie das Gerät nicht in einem Gerätegestellrahmen auf, durch den die Ein- und Auslassöffnungen blockiert werden. Ein geschlossenes Gestell muss über Lüfter und Lüftungsschlitze verfügen.
- Beseitigen Sie vor jeder Installation die folgenden gefährlichen Umgebungsbedingungen: Feuchte oder nasse Böden, Lecks, ungeerdete oder schadhafte Netzkabel sowie Steckdosen ohne ausreichende Erdung.

Installieren der Geräte

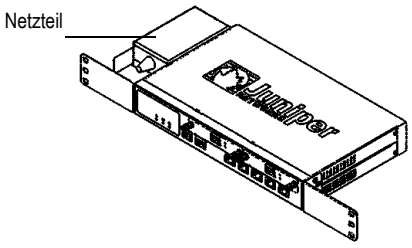
Für ein SSG 20-Gerät ist eine Front-, Wand- oder Schreibtischmontage möglich. Die Montagekits können einzeln gekauft werden.

Zum Montieren eines SSG 20-Geräts werden ein Kreuzschlitzschraubenzieher mittlerer Größe (nicht im Lieferumfang enthalten) und Schrauben benötigt, die mit dem Gerätegestell kompatibel sind (im Kit enthalten).

HINWEIS: Stellen Sie beim Montieren eines Geräts sicher, dass sich dieses nah genug an der Steckdose befindet.

Gehen Sie folgendermaßen vor, um die Frontmontage eines SSG 20-Geräts auf einem handelsüblichen 19 Zoll-Gerätegestell durchzuführen:

Abbildung 7: SSG 20-Frontmontage



1. Richten Sie die Öse des für eine Gestellmontage vorgesehenen Netzteils am linken vorderen Bereich des Geräts aus.

2. Fixieren Sie die Schrauben mit einem Kreuzschlitzschraubenzieher in den Öffnungen.

3. Richten Sie die andere Öse für die Gestellmontage am rechten vorderen Bereich des Geräts aus.

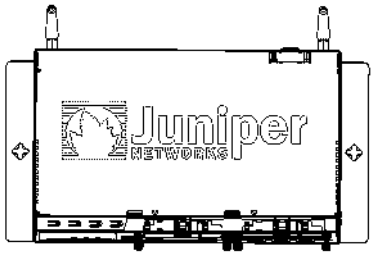
4. Fixieren Sie die Schrauben mit einem Kreuzschlitzschraubenzieher in den Öffnungen.

5. Montieren Sie das Gerät mit den mitgelieferten Schrauben auf dem Gestell.

6. Schließen Sie das Netzteil an die Steckdose an.

Führen Sie für die Wandmontage eines SSG 20-Geräts die folgenden Schritte aus:

Abbildung 8: Wandmontage des SSG 20



1. Richten Sie die Ösen für die Wandmontage am Gerät aus.

2. Stecken Sie die Schrauben in die Öffnungen, und fixieren Sie diese mit einem Kreuzschlitzschraubenzieher.

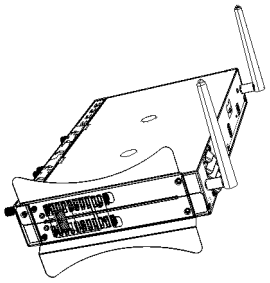
3. Die für die Montage vorgesehene Wand muss glatt, eben, trocken und massiv sein.

4. Montieren Sie das Gerät mit den mitgelieferten Schrauben an der Wand.

5. Schließen Sie das Netzteil an die Steckdose an.

Führen Sie für die Schreibtischmontage eines SSG 20-Geräts die folgenden Schritte aus:

Abbildung 9: SSG 20-Schreibtischmontage



1. Befestigen Sie die Vorrichtung zum Aufstellen auf dem Schreibtisch am Gerät. Verwenden Sie am besten die Seite, die dem Stromadapter am nächsten liegt.

2. Stellen Sie das montierte Gerät auf den Schreibtisch.

3. Stecken Sie den Stromadapter ein, und schließen Sie das Netzteil an die Steckdose an.

Anschließen von Schnittstellenkabeln an ein Gerät

Führen Sie zum Anschließen des Schnittstellenkabels an ein Gerät die folgenden Schritte aus:

1. Sie benötigen die für die Schnittstelle erforderliche Kabelart in ausreichender Länge.

2. Stecken Sie den Kabelstecker in den entsprechenden Anschluss auf der Frontscheibe der Schnittstelle.

3. Ordnen Sie das Kabel folgendermaßen an, um ein Herausgleiten des Kabels oder das Entstehen von Belastungsstellen zu verhindern:

    a. Bringen Sie das Kabel so an, dass es beim Herunterhängen nicht sein eigenes Gewicht stützen muss.

    b. Ist noch überschüssige Kabellänge vorhanden, legen Sie das Kabel sorgfältig zu einer Schleife zusammen, und räumen Sie diese beiseite.

    c. Fixieren Sie die Kabel mithilfe von Klemmen.

Anschließen der Stromversorgung

Führen Sie zum Herstellen einer Stromversorgung für das Gerät die folgenden Schritte aus:

1. Schließen Sie den Gleichstromstecker des Netzkabels an die Gleichstromnetzbuchse auf der Rückseite des Geräts an.

2. Schließen Sie den Wechselstromadapter des Netzkabels an eine Wechselstromquelle an.

WARNHINWEIS: Wir empfehlen die Verwendung eines Überspannungsschutzes für die Stromverbindung.

Anschließen eines Geräts an ein Netzwerk

Ein SSG 20-Gerät bietet eine Firewall und allgemeine Sicherheitsfunktionen für Ihre Netzwerke, wenn es zwischen internen Netzwerken und dem nicht vertrauenswürdigen Netzwerk platziert wird. In diesem Abschnitt werden insbesondere die folgenden Themen behandelt:

- Anschließen des Geräts an ein nicht vertrauenswürdiges Netzwerk
- Anschließen des Geräts an ein internes Netzwerk oder eine Arbeitsstation

Anschließen des Geräts an ein nicht vertrauenswürdiges Netzwerk

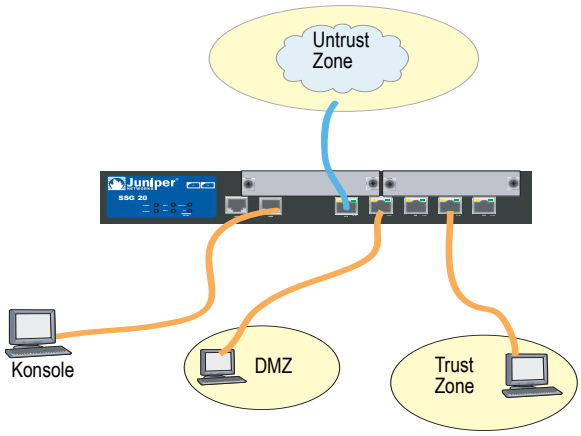
Folgende Möglichkeiten stehen zum Anschluss des SSG 20-Geräts an ein nicht vertrauenswürdiges Netzwerk zur Verfügung:

- Ethernet-Anschlüsse
- Serielle (AUX-/Konsol-) Anschlüsse
- Anschließen von Mini-PIMs an ein nicht vertrauenswürdiges Netzwerk

Abbildung10 zeigt das SSG 20 mit den grundlegenden Netzwerkkabelanschlüssen. Dabei sind zwei leere Mini-PIMs und die 10/100-Ethernet-Anschlüsse folgendermaßen verkabelt:

- Der mit „0/0“ gekennzeichnete Anschluss (Ethernet0/0-Schnittstelle) ist mit dem nicht vertrauenswürdigen Netzwerk verbunden.
- Der mit „0/1“ gekennzeichnete Anschluss (ethernet0/1-Schnittstelle) ist mit einer Arbeitsstation in der DMZ-Sicherheitszone verbunden.
- Der mit „0/3“ gekennzeichnete Anschluss (bgroup0-Schnittstelle) ist mit einer Arbeitsstation in der Trust Sicherheitszone verbunden.
- Der Konsolenanschluss ist zur Gewährleistung des Verwaltungszugriffs mit einem seriellen Terminal verbunden.

Abbildung 10: Grundlegender Netzwerkbetrieb – Beispiel



Ethernet-Anschlüsse

Schließen Sie zum Herstellen einer Hochgeschwindigkeitsverbindung das mitgelieferte Ethernet-Kabel für den Ethernet-Anschluss „0/0“ auf einem SSG 20-Gerät an den externen Router an. Das Gerät erkennt automatisch die erforderliche Geschwindigkeit, den Duplex und die MDI/MDIX-Einstellungen.

Serielle (AUX-/Konsol-) Anschlüsse

Eine Verbindung mit einem nicht vertrauenswürdigen Netzwerk kann mit einem seriellen RJ-45-Durchgangskabel und einem externen Modem hergestellt werden.

WARNHINWEIS: Schließen Sie nicht versehentlich die Konsolen-, AUX- oder Ethernet-Anschlüsse am Gerät an der Telefonanschlussdose an.

Anschließen von Mini-PIMs an ein nicht vertrauenswürdiges Netzwerk

In diesem Abschnitt wird das Verbinden des Mini-PIMs des Geräts mit einem nicht vertrauenswürdigen erläutert.

ADSL2/2+ Mini-PIM

Stellen Sie mit dem mitgelieferten ADSL-Kabel eine Verbindung zwischen der ADSL2/2 + -Mini-PIM und der Telefonbuchse her. Der ADSL-Anschluss der Annex A-Version des Geräts verwendet einen RJ-11-Stecker, während die Annex B-Version mit einem RJ-45-Stecker ausgestattet ist. Das zum Verbinden des ADSL-Anschlusses mit dem Telefonanschluss verwendete Kabel für Annex B-Modelle sieht identisch aus, und für die Verkabelung wird ein Straight-Through-10 Base-T Ethernet-Kabel verwendet.

Anschließen von Splittern und Mikrofiltern

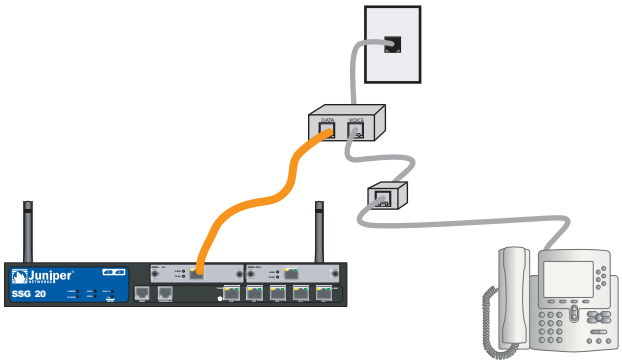
Ein *Signalsplitter* teilt das Telefonsignal in niederfrequente Sprachsignale für Telefonate und hochfrequente Datensignale für Datenverkehr auf. Der Dienstanbieter installiert den Splitter normalerweise zusammen mit dem Gerät, über das die Telefonleitungen an Ihrem Standort mit dem Netzwerk des Anbieters verbunden werden.

Abhängig von den vom Dienstanbieter bereitgestellten Geräten können Sie möglicherweise selbst Splitter installieren. In diesem Fall schließen Sie das ADSL-Kabel vom Gerät und die Telefonleitung an die entsprechenden Stecker (z.B. „Daten“ oder „Sprache“) am Splitter an. Das andere Ende des Splitters wird mit der Telefonanschlussdose verbunden.

Möglicherweise müssen Sie für alle mit der ADSL-Leitung verbundenen Telefone, Faxgeräte, Anrufbeantworter oder analogen Modems einen *Mikrofilter* installieren. Der Mikrofilter filtert hochfrequentes Rauschen in der Telefonleitung. Der Mikrofilter kann in der Telefonleitung zwischen dem Telefon, Faxgerät, Anrufbeantworter bzw. analogen Modem und dem Sprachstecker des Splitters installiert werden.

Abbildung 11 zeigt ein Beispiel für die Installation eines Mikrofilters und Splitters am Standort. (Die entsprechenden Mikrofilter oder Splitter erhalten Sie von Ihrem Dienstanbieter.)

Abbildung 11: Mikrofilter und Splitter in der Netzwerkverbindung



ISDN, T1, E1 und V.92-Mini-PIMs

Führen Sie zum Anschluss der Mini-PIMs an ein Gerät die folgenden Schritte aus:

1. Sie benötigen die für die Schnittstelle erforderliche Kabelart in ausreichender Länge.

2. Stecken Sie den Kabelstecker in den entsprechenden Anschluss auf der Frontscheibe der Schnittstelle.

3. Ordnen Sie das Kabel folgendermaßen an, um ein Herausgleiten des Kabels oder das Entstehen von Stresspunkten zu verhindern:

    a. Bringen Sie das Kabel so an, dass es beim Herunterhängen nicht sein eigenes Gewicht stützen muss.

    b. Ist noch überschüssige Kabellänge vorhanden, legen Sie das Kabel sorgfältig zu einer Schleife zusammen, und räumen Sie diese beiseite.

    c. Fixieren Sie die Kabel mithilfe von Klemmen.

Informationen zur Konfiguration von ISDN, E1, T1 oder V.92-Mini-PIM erhalten Sie unter „Konfiguration des Mini-PIM“ auf Seite 41.

Anschließen des Geräts an ein internes Netzwerk oder eine Arbeitsstation

Ein Local Area Network (LAN) oder eine Arbeitsstation kann mit den Ethernet- und/oder den Wireless-Schnittstellen verbunden werden.

Ethernet-Anschlüsse

Ein SSG 20-Gerät verfügt über sieben Ethernet-Anschlüsse. Sie können mindestens einen dieser Anschlüsse für die Herstellung einer Verbindung zu LANs über Switches oder Hubs verwenden. Die Anschlüsse können jedoch auch ohne Hubs oder Switches direkt mit Arbeitsstationen verbunden werden. Zum Anschließen der Ethernet-Anschlüsse an andere Geräte können Crossover- oder Durchgangskabel verwendet werden. Informationen zu den standardmäßigen Zone-zu-Schnittstelle-Bindungen erhalten Sie unter „Standardmäßige Geräteeinstellungen“ auf Seite 31.

Wireless-Antennen

Wenn Sie die Wireless-Schnittstelle verwenden, müssen Sie die mitgelieferten Antennen am Gerät anschließen. Wenn Sie über die standardmäßigen 2 dB-Doppelantennen verfügen, schrauben Sie diese an den mit A und B gekennzeichneten Anschlüssen auf der Geräterückseite fest. Biegen Sie jede Antenne jeweils am Gelenk, ohne dabei Druck auf die Stecker auszuüben.

Abbildung 12: SSG 20-WLAN – Position der Antennen

Führen Sie bei Verwendung der optionalen externen Antenne die beiliegenden Anweisungen für den Anschluss der Antenne aus.

Kapitel 3

Konfigurieren des Geräts

Die ScreenOS-Software ist auf einem SSG 20-Gerät vorinstalliert. Das Gerät wird in eingeschaltetem Zustand konfiguriert. Das Gerät verfügt über eine standardmäßige werkseitige Konfiguration, die den Erstanschluss an das Gerät ermöglicht. Für Ihre speziellen Netzwerkanforderungen müssen Sie jedoch eine Konfigurationen vornehmen.

Dieses Kapitel ist in folgende Abschnitte gegliedert:

HINWEIS: Nach der Konfiguration eines Geräts und der Überprüfung der Verbindung über das Remotenetzwerk, muss das Produkt unter www.juniper.net/support/ registriert werden, damit bestimmte ScreenOS-Dienste, wie z.B. der Deep Inspection-Signaturdienst und der Virenschutz (einzeln erhältlich) auf dem Gerät aktiviert werden. Nach der Registrierung des Produkts abonnieren Sie den Dienst über die WebUI. Weitere Informationen zur Produktregistrierung und zum Abonnieren bestimmter Dienste erhalten Sie im Band *Grundlagen* des *Concepts & Examples ScreenOS Reference Guide* für die auf dem Gerät installierte ScreenOS-Version.

Zugriff auf das Gerät

Ein Gerät kann auf verschiedene Arten konfiguriert werden:

- Konsole: Der Konsolenanschluss am Gerät ermöglicht Ihnen den Zugriff auf das Gerät über ein serielles an die Arbeitsstation oder das Terminal angeschlossenes Kabel. Zum Konfigurieren des Geräts geben Sie am Terminal oder in einem Terminalemulationsprogramm auf Ihrer Arbeitsstation ScreenOS-Befehlszeilenbefehle ein.

- WebUI: Bei der ScreenOS-Webbenutzerschnittstelle (WebUI) handelt es sich um eine über einen Browser verfügbare grafische Schnittstelle. Zur Erstverwendung der WebUI muss sich die Arbeitsstation, auf der der Browser ausgeführt wird, im selben Subnetz wie das Gerät befinden. Der Zugriff auf die WebUI über einen sicheren Server kann auch unter Verwendung von Secure Sockets Layer (SSL) mit Secure HTTP (S-HTTP) erfolgen.

- Telnet/SSH: Telnet und SSH sind Anwendungen, die Ihnen den Zugriff auf Geräte über ein IP-Netzwerk ermöglichen. Zum Konfigurieren des Geräts geben Sie in einer Telnet-Sitzung an Ihrer Arbeitsstation ScreenOS-Befehlszeilenbefehle ein. Weitere Informationen erhalten Sie im Band *Verwaltung* des *Concepts & Examples ScreenOS Reference Guide*.

- NetScreen-Security Manager: NetScreen-Security Manager ist eine von Juniper Networks entwickelte Verwaltungsanwendung für Unternehmen, mit der Firewall-/IPSec VPN-Geräte von Juniper Networks gesteuert und verwaltet werden. Anweisungen zur Verwaltung des Geräts mithilfe von NetScreen-Security Manager erhalten Sie im *NetScreen-Security Administrator's Guide*.

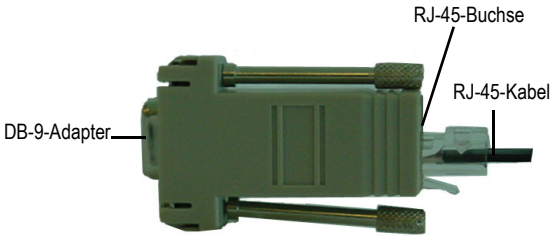
Verwenden einer Konsolenverbindung

HINWEIS: Verwenden Sie ein serielles RJ-45 CAT5-Durchgangskabel mit einem RJ-45-Stecker, um eine Verbindung mit dem Konsolenanschluss am Gerät herzustellen.

Führen Sie zum Herstellen einer Konsolenverbindung die folgenden Schritte aus:

1. Schließen Sie den Buchsenstecker des mitgelieferten DB-9-Adapters an den seriellen Anschluss der Arbeitsstation an. (Der DB-9-Stecker muss ordnungsgemäß eingesteckt und gesichert sein.) Abbildung13 zeigt den erforderlichen DB-9-Stecker.

Abbildung 13: DB-9-Adapter



2. Schließen Sie den Stecker des seriellen RJ-45 CAT5-Kabels am Konsolenanschluss am SSG 20 an. (Das andere Ende des CAT5-Kabels muss ordnungsgemäß an den DB-9-Adapter angeschlossen und gesichert sein.)

3. Starten Sie auf der Arbeitsstation ein serielles Terminalemulationsprogramm. Folgende Einstellungen sind zum Starten einer Konsolensitzung erforderlich:

   - Baudrate: 9600
   - Parität: Keine
   - Datenbits: 8
   - Stoppbit: 1
   - Flusssteuerung: Keine

4. Wenn Sie die Standardanmeldung für den Administratornamen und das Kennwort noch nicht geändert haben, geben Sie bei den Eingabeaufforderungen „login“ und „password“ **netscreen** ein. (Verwenden Sie nur Kleinbuchstaben. Für die Felder „login“ und „password“ muss die Groß-/Kleinschreibung beachtet werden.)

   Informationen zur Konfiguration des Geräts mithilfe der Befehlszeilenbefehle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

5. Standardmäßig tritt an der Konsole eine Zeitüberschreitung auf, und sie wird automatisch nach 10 Minuten ausbleibender Aktivität beendet (optional). Geben Sie zum Entfernen der Zeitüberschreitung **set console timeout 0** ein.

Verwenden der WebUI

Zur Verwendung der WebUI muss sich die Arbeitsstation, von der aus das Gerät verwaltet wird, zunächst im selben Subnetz wie das Gerät befinden. Führen Sie zum Zugriff auf das Gerät mit der WebUI die folgenden Schritte aus:

1. Stellen Sie für die Arbeitsstation eine Verbindung zum 0/2-0/4-Anschluss am Gerät her (bgroup0-Schnittstelle in der Trust Zone).

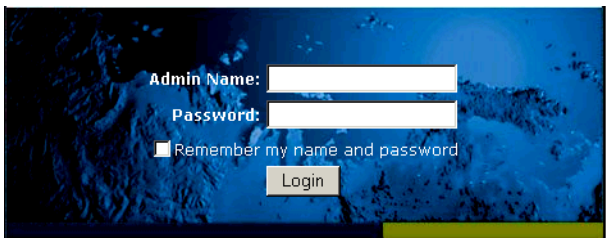
2. Stellen Sie sicher, dass die Arbeitsstation für Dynamic Host Configuration Protocol (DHCP) oder statisch mit einer IP-Adresse im Subnetz 192.168.1.0/24 konfiguriert ist.

3. Starten Sie den Browser, geben Sie die IP-Adresse für die bgroup0-Schnittstelle ein (die standardmäßige IP-Adresse lautet 192.168.1.1/24), und drücken Sie anschließend die **ENTER**.

HINWEIS: Beim ersten Zugriff auf das Gerät über die WebUI erscheint der Assistent für die Anfangskonfiguration (ICW). Möchten Sie Ihr Gerät mit diesem Assistenten konfigurieren, erhalten Sie unter „Assistent für die Anfangskonfiguration“ auf Seite 63 die entsprechenden Informationen.

Die WebUI-Anwendung zeigt die Anmeldeaufforderung entsprechend der Abbildung 14 an.

Abbildung 14: WebUI-Anmeldeaufforderung



4. Wenn Sie die Standardanmeldung für den Administratornamen und das Kennwort noch nicht geändert haben, geben Sie bei den Eingabeaufforderungen „admin name“ und „password“ **netscreen** ein. (Verwenden Sie nur Kleinbuchstaben. Für die Felder „login“ und „password“ muss die Groß-/Kleinschreibung beachtet werden.)

Verwenden von Telnet

Führen Sie zum Herstellen einer Telnet-Verbindung die folgenden Schritte aus:

1. Stellen Sie für die Arbeitsstation eine Verbindung zum 0/2-0/4-Anschluss am Gerät her (bgroup0-Schnittstelle in der Trust Zone).

2. Stellen Sie sicher, dass die Arbeitsstation für DHCP oder statisch mit einer IP-Adresse im Subnetz 192.168.1.0/24 konfiguriert ist.

3. Starten Sie mithilfe der IP-Adresse eine Telnet-Clientanwendung für die bgroup0-Schnittstelle (die standardmäßige IP-Adresse lautet 192.168.1.1). Geben Sie z.B. **telnet 192.168.1.1** ein.

   Die Telnet-Anwendung zeigt die Anmeldeaufforderung an.

4. Wenn Sie die Standardanmeldung für den Anmeldenamen und das Kennwort noch nicht geändert haben, geben Sie bei den Eingabeaufforderungen „login“ und „password“ **netscreen** ein. (Verwenden Sie nur Kleinbuchstaben. Für die Felder „login“ und „password“ muss die Groß-/Kleinschreibung beachtet werden.)

5. Standardmäßig tritt an der Konsole eine Zeitüberschreitung auf, und sie wird automatisch nach 10 Minuten ausbleibender Aktivität beendet (optional). Geben Sie zum Entfernen der Zeitüberschreitung **set console timeout 0** ein.

Standardmäßige Geräteeinstellungen

In diesem Abschnitt werden die standardmäßigen Einstellungen und der Betrieb eines SSG 20-Geräts erläutert.

Tabelle 5 zeigt die standardmäßigen Zonenbindungen für Anschlüsse an den Geräten.

Tabelle 5: Standardmäßige physikalische Schnittstelle zu Zonenbindungen

Anschlussbeschriftung	Schnittstelle	Zone
10/100-Ethernet-Anschlüsse:		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null
WAN-Mini-PIM-Anschlüsse (x = Mini-PIM-Steckplatz 1 oder 2):		
ADSL2/2 + (Annex A)	adsl(x/0)	Untrust
ADSL2/2 + (Annex B)	adsl(x/0)	Untrust
T1	serial(x/0)	Untrust
E1	serial(x/0)	Untrust
ISDN	bri(x/0)	Untrust
V.92	serial(x/0)	Null

Eine Bridge-Gruppe (bgroup) ermöglicht Netzwerkbenutzern das Wechseln zwischen per Kabel und drahtlos übertragenem Datenverkehr ohne Neukonfiguration oder Neustart des Geräts. Standardmäßig sind die ethernet0/2-ethernet0/4-Schnittstellen (die am Gerät als Anschlüsse 0/2-0/4 gekennzeichnet sind) zusammen als bgroup0-Schnittstelle gruppiert. Zudem verfügen die Schnittstellen über die IP-Adresse 192.168.1.1/24 und sind an die Trust Sicherheitszone gebunden. Bis zu vier bgroups können konfiguriert werden.

Soll eine Ethernet- oder Wireless-Schnittstelle in einer bgroup eingerichtet werden, muss sich die Ethernet- oder Wireless-Schnittstelle in der Null Sicherheitszone befinden. Nach dem Löschen der sich in einer bgroup befindenden Ethernet- bzw. Wireless-Schnittstelle wird die Schnittstelle in der Null Sicherheitszone angeordnet. Nach Zuweisung zur Null Sicherheitszone kann die Ethernet-Schnittstelle an eine Sicherheitszone gebunden und einer anderen IP-Adresse zugewiesen werden.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um ethernet0/3 aus bgroup0 zu löschen und diese Schnittstelle mit der statischen IP-Adresse 192.168.3.1/24 der Trust Zone zuzuweisen:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: Deaktivieren Sie **ethernet0/3**, und klicken Sie anschließend auf **Apply**.

List > Edit (ethernet0/3): Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

Zone Name: Trust (select)
IP Address/Netmask: 192.168.3.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

Tabelle 6: Wireless-Bindungen und Bindungen für logische Schnittstellen

SSG 20-WLAN	Schnittstelle	Zone
Wireless-Schnittstelle Gibt eine Wireless-Schnittstelle an, die für den Betrieb in einem Frequenzband mit 2,4 GHz und/oder 5GHz konfiguriert werden kann.	wireless0/0 (die Standard-IP-Adresse lautet 192.168.2.1/24).	Trust
	wireless0/1-0/3.	Null
Logische Schnittstellen		
Layer-2-Schnittstelle	vlan1 gibt die für die Verwaltung und die VPN-Datenverkehrbeendigung verwendeten logischen Schnittstellen an, während sich das Gerät im transparenten Modus befindet.	Nicht zutreffend
Tunnelschnittstellen	Tunnel.*n* gibt eine logische Tunnelschnittstelle an. Diese Schnittstelle ist für VPN-Datenverkehr vorgesehen.	Nicht zutreffend

Die Standard-IP-Adresse auf der bgroup0-Schnittstelle kann so geändert werden, dass sie den Adressen im LAN und WLAN entspricht. Unter „Grundlegende Wireless-Konfiguration“ auf Seite 37 erhalten Sie Informationen zur Konfiguration einer Wireless-Schnittstelle für eine bgroup.

HINWEIS: Die bgroup-Schnittstelle ist im transparenten Modus nicht verwendbar, wenn darin eine Wireless-Schnittstelle enthalten ist.

Zusätzliche Informationen und Beispiele zu bgroup erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

Auf anderen Ethernet- oder Wireless-Schnittstellen auf einem Gerät sind keine anderen Standard-IP-Adressen konfiguriert; IP-Adressen müssen den anderen Schnittstellen (einschließlich der WAN-Schnittstellen) zugewiesen werden.

Grundlegende Gerätekonfiguration

In diesem Abschnitt werden folgende grundlegende Konfigurationseinstellungen beschrieben:

- Administrator auf Stammebene – Name und Kennwort
- Datum und Uhrzeit
- Bridge-Gruppenschnittstellen
- Administratorzugriff
- Verwaltungsdienste
- Host- und Domänenname
- Standardroute
- Adresse der Verwaltungsschnittstelle
- Konfiguration der Untrust Sicherungsschnittstelle

Administrator auf Stammebene – Name und Kennwort

Der als Administrator auf Stammebene angemeldete Benutzer verfügt über vollständige Berechtigungen für die Konfiguration eines SSG 20-Geräts . Es wird empfohlen, den Standardnamen und das Kennwort des Administrators auf Stammebene umgehend zu ändern (beides **netscreen**).

Verwenden Sie zum Ändern des Namens und des Kennworts für den Administrator auf Stammebene die WebUI oder die Befehlszeilenschnittstelle folgendermaßen:

WebUI

Configuration > Admin > Administrators > Edit (für den NetScreen-Administratornamenwert): Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

```
Administrator Name:
Old Password: netscreen
New Password:
Confirm New Password:
```

HINWEIS: Kennwörter werden auf der WebUI nicht angezeigt.

CLI

```
set admin name name
set admin password pswd_str
save
```

Datum und Uhrzeit

Die auf einem SSG 20-Gerät festgelegte Uhrzeit nimmt beeinflusst Ereignisse wie die Einrichtung von VPN-Tunnels. Die einfachste Möglichkeit zum Festlegen des Datums und der Uhrzeit auf dem Gerät besteht darin, über die WebUI die Gerätesystemuhr mit der Arbeitsstationsuhr zu synchronisieren.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um das Datum und die Uhrzeit auf einem Gerät zu konfigurieren:

WebUI

1. Configuration > Date/Time: Klicken Sie auf die Schaltfläche **Sync Clock with Client**.

   Sie werden gefragt, ob Sie die Sommer-/Winterzeitoption auf Ihrer Arbeitsstation aktiviert haben.

2. Klicken Sie auf **Yes**, um die Systemuhr zu synchronisieren und entsprechend der Sommer-/Winterzeit anzupassen, oder klicken sie auf **No**, um die Systemuhr ohne Anpassung für die Sommer-/Winterzeit zu synchronisieren.

Sie können auch den Befehlszeilenbefehl **set clock** in einer Telnet- oder Konsolensitzung verwenden, um das Datum und die Uhrzeit für das Gerät manuell einzugeben.

Bridge-Gruppenschnittstellen

Standardmäßig verfügt das SSG 20-Gerät über die in der Trust Sicherheitszone zusammengruppierten Ethernet-Schnittstellen vom Typ ethernet0/2-ethernet0/4. Durch Gruppieren der Schnittstellen werden diese in einem Subnetz angeordnet. Eine Schnittstelle kann aus einer Gruppe gelöscht und einer anderen Sicherheitszone zugewiesen werden. Schnittstellen müssen sich in der Null Sicherheitszone befinden, bevor sie einer Gruppe zugewiesen werden können. Verwenden Sie zum Anordnen einer gruppierten Schnittstelle in der Null Sicherheitszone den Befehlszeilenbefehl **unset interface** *interface* **port** *interface*.

Die SSG 20-WLAN-Geräte ermöglichen die Gruppierung von Ethernet- und Wireless-Schnittstellen unter einem Subnetz.

HINWEIS: In einer bgroup können nur Wireless- und Ethernet-Schnittstellen festgelegt werden.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um eine Gruppe mit Ethernet- und Wireless-Schnittstellen zu konfigurieren:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: Deaktivieren Sie **ethernet0/3** und **ethernet0/4**, und klicken Sie anschließend auf **Apply**.

Edit (bgroup1) > Bind Port: Wählen Sie **ethernet0/3**, **ethernet0/4** und **wireless0/2** aus, und klicken Sie anschließend auf **Apply**.

> Basic: Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

Zone Name: DMZ (select)
IP Address/Netmask: 10.0.0.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```

Administratorzugriff

Standardmäßig kann jeder Benutzer im Netzwerk ein Gerät verwalten, sofern er den Anmeldenamen und das Kennwort kennt.

Verwenden Sie die WebUI und die Befehlszeilenschnittstelle folgendermaßen, um das Gerät so zu konfigurieren, dass es nur von einem bestimmten Host im Netzwerk verwaltet werden kann:

WebUI

Configuration > Admin > Permitted IPs: Geben Sie Folgendes ein, und klicken Sie dann auf **Add**:

IP Address/Netmask: *ip_addr/mask*

CLI

```
set admin manager-ip ip_addr/mask
save
```

Verwaltungsdienste

ScreenOS bietet Dienste für die Konfiguration und die Verwaltung des Geräts (z.B. SNMP, SSL und SSH), die für jede Schnittstelle einzeln aktiviert werden können.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um die Verwaltungsdienste im Gerät zu konfigurieren:

WebUI

Network > Interfaces > List > Edit (für ethernet0/0): Wählen Sie unter **Management Services** die auf der Schnittstelle zu verwendenden Dienste aus, bzw. löschen Sie diese, und klicken Sie anschließend auf **Apply**.

CLI

```
set interface ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```

Host- und Domänenname

Der Domänenname definiert das Netzwerk oder das Subnetzwerk, zu dem das Gerät gehört, wohingegen sich der Hostname auf ein bestimmtes Gerät bezieht. Anhand des Hostnamens und des Domänennamens wird das Gerät im Netzwerk eindeutig identifiziert.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um den Host- und den Domännenamen auf einem Gerät zu konfigurieren:

WebUI

Network > DNS > Host: Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

Host Name: *name*
Domain Name: *name*

CLI

set hostname *name*
set domain *name*
save

Standardroute

Bei der Standardroute handelt es sich um eine statische Route, über die Pakete weitergeleitet werden, die an nicht ausdrücklich in der Routentabelle aufgeführte Netzwerke adressiert sind. Geht ein Paket beim Gerät mit einer Adresse ein, für die dem Gerät keine Routeninformationen vorliegen, sendet das Gerät das Paket an das von der Standardroute angegebene Ziel.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um die Standardroute auf dem Gerät zu konfigurieren:

WebUI

Network > Routing > Destination > New (trust-vr): Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

IP Address/Netmask: 0.0.0.0/0.0.0.0
Next Hop
Gateway: (select)
Interface: ethernet0/2 (ausgewählt)
Gateway IP Address: *ip_addr*

Befehlszeilenschnittstelle

set route 0.0.0.0/0 interface ethernet0/2 gateway *ip_addr*
save

Adresse der Verwaltungsschnittstelle

Die Trust Schnittstelle besitzt die Standard-IP-Adresse 192.168.1.1/24 und ist für die Verwaltungsdienste konfiguriert. Werden die Anschlüsse 0/2-0/4 am Gerät mit einer Arbeitsstation verbunden, kann das Gerät über eine Arbeitsstation im Subnetzwerk 192.168.1.1/24 mithilfe eines Verwaltungsdienstes wie Telnet konfiguriert werden.

Die Standard-IP-Adresse kann auf der Trust Schnittstelle geändert werden. Möglicherweise möchten Sie die Schnittstelle ändern, um die Übereinstimmung mit den bereits im LAN vorhandenen IP-Adressen zu gewährleisten.

Konfiguration der Untrust Sicherungsschnittstelle

Das SSG 20-Gerät ermöglicht die Konfiguration einer Sicherungsschnittstelle für einen nicht vertrauenswürdigen Failover. Führen Sie zum Festlegen der Sicherungsschnittstelle bei Auftreten eines nicht vertrauenswürdigen Failovers folgende Schritte aus:

1. Legen Sie die Sicherungsschnittstelle in der Null Sicherheitszone mithilfe des Befehlszeilenbefehls **unset interface** *interface* [**port** *interface*] fest.

2. Binden Sie mithilfe des Befehlszeilenbefehls **set interface** *interface* **zone** *zone_name* die Sicherungsschnittstelle an dieselbe Sicherheitszone wie die Primärschnittstelle.

HINWEIS: Die Primär- und Sicherungsschnittstellen müssen sich in derselben Sicherheitszone befinden. Eine Primärschnittstelle verfügt nur über eine Sicherungsschnittstelle und umgekehrt.

Zum Festlegen der ethernet0/4-Schnittstelle als Sicherungsschnittstelle für die ethernet0/0-Schnittstelle muss die WebUI oder die Befehlszeilenschnittstelle folgendermaßen verwendet werden:

WebUI

Network > Interfaces > Backup > Geben Sie Folgendes ein, und klicken Sie anschließend auf **Apply**.

Primary: ethernet0/0
Backup: ethernet0/4
Type: track-ip (select)

CLI

```
unset interface bgroup0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

Grundlegende Wireless-Konfiguration

In diesem Abschnitt finden Sie Informationen zur Konfiguration der Wireless-Schnittstelle am SSG 20-WLAN-Gerät. Wireless-Netzwerke (Drahtlosnetzwerke) bestehen aus Namen, die als Service Set Identifiers (SSIDs) bezeichnet werden. Das Festlegen von SSIDs ermöglicht das Anordnen von mehreren Wireless-Netzwerken am selben Ort, ohne dass es zu Konflikten kommt. Ein SSID-Name darf aus maximal 32 Zeichen bestehen. Ist ein Leerzeichen Teil des SSID-Namens, muss die Zeichenfolge in Anführungszeichen gesetzt werden. Nach

Festlegung des SSID-Namens können weitere SSID-Attribute konfiguriert werden. Zur Verwendung von Wireless Local Area Network (WLAN)-Funktionen am Gerät muss zumindest eine SSID konfiguriert und an eine Wireless-Schnittstelle gebunden werden.

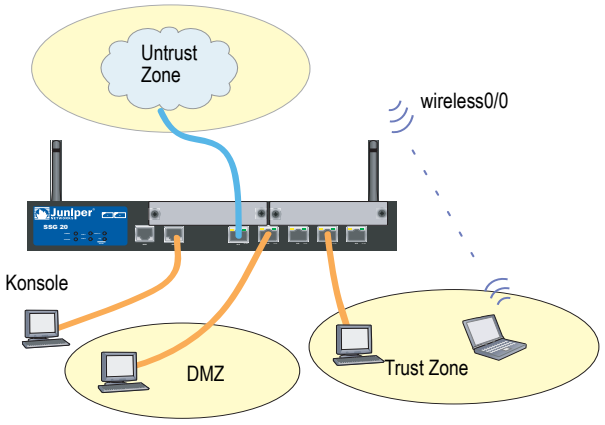
Das SSG 20-WLAN-Gerät ermöglicht das Erstellen von bis zu 16 SSIDs, von denen jedoch nur vier gleichzeitig verwendet werden können. Das Gerät kann für die Verwendung der vier 4 SSIDs auf einem der Transceiver oder für das Aufteilen der Verwendung auf beide Transceiver (z.B. drei WLAN 0 zugewiesene SSIDs und eine WLAN 1 zugewiesene SSID) konfiguriert werden. Legen Sie mit dem Befehlszeilenbefehl **set interface** *wireless_interface* **wlan** {0 | 1 | both} die Funktransceiver am SSG 20-WLAN-Gerät fest.

Sobald Sie eine SSID für die wireless0/0-Schnittstelle festgelegt haben, können Sie mithilfe der standardmäßigen IP-Adresse der wireless0/0-Schnittstelle auf das Gerät zugreifen (schrittweise Anleitungen hierzu finden Sie unter „Zugriff auf das Gerät“ auf Seite 28). Abbildung15 zeigt die Standardkonfiguration für das SSG 20-WLAN-Gerät.

HINWEIS: Wird das SSG 20-WLAN-Gerät außerhalb Japans, Kanadas, Chinas, Taiwans, Koreas, Israels, Singapurs oder der Vereinigten Staaten betrieben, benötigen Sie den Befehlszeilenbefehl **set wlan country-code**, oder Sie müssen das Gerät auf der Wireless-WebUI-Seite **>** General Settings einrichten, um eine WLAN-Verbindung herstellen zu können. Durch diesen Befehl wird der auswählbare Kanalbereich und die Übertragungsleistung festgelegt.

Lautet Ihr Regionalcode ETSI, muss der korrekte Ländercode festgelegt werden, der den örtlichen Bestimmungen zu Funkbereichen entspricht.

Abbildung 15: Standardmäßige SSG 20-WLAN-Konfiguration



Standardmäßig wird die wireless0/0-Schnittstelle mit der IP-Adresse 192.168.2.1/24 konfiguriert. Alle Wireless-Clients, für die eine Verbindung zur Trust Zone hergestellt werden muss, benötigen eine IP-Adresse im Wireless-Subnetzwerk. Das Gerät kann auch so konfiguriert werden, dass das Gerät mit DHCP Ihren Geräten automatisch IP-Adressen im Subnetzwerk 192.168.2.1/24 zuweist.

Standardmäßig werden die wireless0/1-wireless0/3-Schnittstellen als Null definiert. Den Schnittstellen sind keine IP-Adressen zugewiesen. Möchten Sie eine beliebige der anderen Wireless-Schnittstellen verwenden, müssen Sie für die Schnittstelle eine IP-Adresse konfigurieren, dieser eine SSID zuweisen und sie an eine Sicherheitszone binden. In Tabelle 7 sind die Methoden zur Wireless-Authentifizierung und –Verschlüsselung aufgeführt.

Tabelle 7: Wireless-Authentifizierung und Verschlüsselungsoptionen

Authentifizierung	Verschlüsselung
Offen	Ermöglicht einem beliebigen Wireless-Client den Zugriff auf das Gerät.
Shared-key	WEP shared-key
WPA-PSK	AES/TKIP mit Pre-Shared Key
WPA	AES/TKIP mit Schlüssel von RADIUS-Server
WPA2-PSK	802.11i-kompatibel mit einem Pre-Shared Key
WPA2	802.11i-kompatibel mit einem RADIUS-Server
WPA-Auto-PSK	Lässt einen WPA- und einen WPA2-Typ mit Pre-Shared Key zu.
WPA-Auto	Lässt einen WPA- und einen WPA2-Typ mit RADIUS-Server zu.
802.1x	WEP mit Schlüssel von RADIUS-Server

Im *Concepts & Examples ScreenOS Reference Guide* finden Sie Konfigurationsbeispiele, SSID-Attribute und Befehlszeilenbefehle bzgl. Wireless-Sicherheitskonfigurationen.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um eine Wireless-Schnittstelle für grundlegende Verbindung zu konfigurieren:

WebUI

1. Legen Sie den WLAN-Ländercode und die IP-Adresse fest.

   Wireless > General Settings > – Wählen Sie Folgendes aus, und klicken Sie anschließend auf **Apply**:

   Country code: Select your code
   IP Address/Netmask: *ip_add/netmask*

2. Legen Sie die SSID fest.

   Wireless > SSID > New: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

   SSID:
   Authentication:
   Encryption:
   Wireless Interface Binding:

3. Legen Sie den WEP-Schlüssel fest (optional).

   SSID > WEP Keys: Wählen Sie die Schlüssel-ID aus, und klicken Sie anschließend auf **Apply**:

4. Legen Sie den WLAN-Modus fest.

   Network > Interfaces > List > Edit (Wireless-Schnittstelle): Wählen Sie für den WLAN-Modus **Both** aus, und klicken Sie anschließend auf **Apply**.

5. Aktivieren Sie die Änderungen für die Wireless-Einstellungen.

   Wireless > General Settings > Klicken Sie auf **Activate Changes**.

CLI

1. Legen Sie den WLAN-Ländercode und die IP-Adresse fest.

   set wlan country-code { *code_id* }
   set interface *wireless_interface* ip *ip_addr/netmask*

2. Legen Sie die SSID fest.

   set ssid name *name_str*
   set ssid *name_str* authentication *auth_type* encryption *encryption_type*
   set ssid *name_str* interface *interface*
   set ssid *name_str* key-id *number* (optional)

3. Legen Sie den WLAN-Modus fest.

   set interface *wireless_interface* wlan both

4. Aktivieren Sie die Änderungen für die Wireless-Einstellungen.

   save
   exec wlan reactivate

Eine SSID kann so konfiguriert werden, dass er im selben Subnetz wie das verkabelte Subnetz arbeitet. Dadurch haben Clients die Möglichkeit, ohne Wiederherstellen einer Verbindung in einem anderen Subnetz auf beiden Schnittstellen zu arbeiten.

Verwenden Sie zum Festlegen einer Ethernet- und einer Wireless-Schnittstelle für dieselbe Bridge-Gruppenschnittstelle wie folgt die WebUI oder die Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (*bgroup_name*) > Bind Port: Wählen Sie die Wireless- und die Ethernet-Schnittstellen aus, und klicken Sie anschließend auf **Apply**:

CLI

set interface *bgroup_name* port *wireless_interface*
set interface *bgroup_name* port *wireless_interface*

HINWEIS: *Bgroup_name* kann bgroup0-bgroup3 sein.

Ethernet_interface kann ethernet0/0-ethernet0/4 sein.

Wireless_interface kann wireless0/0-wireless0/3 sein.

Ist eine Wireless-Schnittstelle konfiguriert, muss das WLAN mit dem Befehlszeilenbefehl **exec wlan reactivate** neu aktiviert werden. Alternativ dazu können Sie auch auf der WebUI-Seite „Wireless > General Settings“ auf **Activate Changes** klicken.

Konfiguration des Mini-PIM

In diesem Abschnitt wird die Konfiguration der Mini Physical Interface Modules (PIMs) erläutert:

- ADSL2/2 + -Schnittstelle
- ISDN ISDN-Schnittstelle
- T1-Schnittstelle
- E1-Schnittstelle
- V.92 Modemschnittstelle

ADSL2/2+-Schnittstelle

Ihr Netzwerk verwendet die ADSL2/2 + -Schnittstelle **adslx/0** (wobei x den Steckplatz des Mini-PIM (1 oder 2) bezeichnet) am Gerät, um über eine virtuelle Asynchronous Transfer Mode (ATM)-Verbindung eine Verbindung zum Dienstanbieter herzustellen. Zusätzliche virtuelle Verbindungen können durch Erstellen von ADSL2/2 + -Subschnittstellen konfiguriert werden. Weitere Informationen hierzu finden Sie unter „Virtuelle Verbindungen“ auf Seite 42.

Wechseln Sie auf der WebUI zur Seite Network > Interfaces > List um eine Liste der aktuellen Schnittstellen im NetScreen-Gerät anzuzeigen. Wenn Sie eine Telnet- oder Konsolensitzung verwenden, geben Sie den Befehlszeilenbefehl **get interface** ein. Die adslx/0-Schnittstelle ist an die Untrust Zone gebunden.

Bei Verwendung der ADSL2/2 + -Schnittstelle zur Herstellung einer Verbindung zum Dienstnetzwerk des Anbieters muss die adsl(x/0)-Schnittstelle konfiguriert werden. Hierzu benötigen Sie zunächst die folgenden Informationen von Ihrem Dienstanbieter:

- VPI- und VCI-Werte (virtuelle Pfad-ID/virtuelle Kanal-ID)
- ATM AAL5-Multiplexingmethode (Asynchronous Transfer Mode Adaptation Layer 5), hierbei kann es sich um Folgendes handeln:

  - Auf eine virtuelle Verbindung gestütztes Multiplexing. Hierbei wird jedes Protokoll über eine separate virtuelle ATM-Verbindung gesendet.

  - LLC-Einkapselung (Logical Link Control). Hierbei können mehrere Protokolle über dieselbe virtuelle ATM-Verbindung gesendet werden (dies ist die standardmäßige Multiplexingmethode).

- Vom Dienstanbieter zugeordneter Benutzername und Kennwort zum Herstellen einer Verbindung mit dem Netzwerk des Dienstanbieters mittels des PPPoE-Protokolls (Point-to-Point-Protokoll über Ethernet) oder PPPoA-Protokolls (Point-to-Point-Protokoll über ATM)

- Ggf. Authentifizierungsmethode für die PPPoE- oder PPPoA-Verbindung

- Optional eine statische IP-Adresse und ein Netzmaskenwert für Ihr Netzwerk

Virtuelle Verbindungen

Zum Hinzufügen von virtuellen Verbindungen erstellen Sie Subschnittstellen für die ADSL2/2+-Schnittstelle. Sie können bis zu zehn ADSL2/2+-Subschnittstellen erstellen. Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um z..B. eine neue Subschnittstelle mit der Bezeichnung **adsl1/0.1** zu erstellen, die an die vordefinierte Zone mit der Bezeichnung **Untrust** gebunden ist:

WebUI

Network > Interfaces > List > New ADSL Sub-IF: Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

Interface Name: adsl1/0.1
VPI/VCI: 0/35
Zone Name: Untrust (auswählen)

CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

Eine ADSL2/2+-Subschnittstelle muss auf die gleiche Weise konfiguriert werden wie die ADSL2/2+-Hauptschnittstelle, d.h., Sie müssen auch wie unter „ADSL2/2+-Schnittstelle“ auf Seite 41 beschrieben, die VPI/VCI-Werte einstellen. ADSL2/2+-Subschnittstellen können unabhängig von der ADSL2/2+-Hauptschnittstelle konfiguriert werden, d.h., Sie können für die Subschnittstelle eine andere Multiplexingmethode, andere VPI/VCI-Werte und einen anderen PPP-Client festlegen. Zudem können Sie auch dann eine statische IP-Adresse für eine Subschnittstelle konfigurieren, wenn die ADSL2/2+-Hauptschnittstelle nicht über eine statische IP-Adresse verfügt.

VPI/VCI und Multiplexingmethode

Ihr Dienstanbieter ordnet für jede virtuelle Verbindung ein VPI/VCI-Wertepaar zu. Sie können z.B. das VPI/VCI-Paar 1/32 erhalten. Dies bedeutet, dass der VPI-Wert und der VCI-Wert 1 lauten. Diese Werte müssen mit den Werten übereinstimmen, die der Dienstanbieter auf der Abonnentenseite des DSLAM (Digital Subscriber Line Access Multiplexer) konfiguriert hat.

Gehen Sie zum Konfigurieren des VPI/VCI-Paars 1/32 auf der adsl1/0-Schnittstelle mithilfe der WebUI oder der Befehlszeilenschnittstelle folgendermaßen vor:

WebUI

Network > Interfaces > List > Edit (für die adsl1/0-Schnittstelle): Geben Sie ins Feld VPI/VCI 1/32 ein, und klicken Sie auf **Apply**.

CLI

```
set interface adsl1/0 pvc 1 32
save
```

Standardmäßig verwendet das Gerät für jede virtuelle Verbindung Logical Link Control (LLC)-basiertes Multiplexing.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um das VPI/VCI 1/32 auf der adslx/0-Schnittstelle zu konfigurieren und die LLC-Einkapselung für die virtuelle Verbindung zu verwenden:

WebUI

Network > Interfaces > List > Edit (für die adsl1/0-Schnittstelle): Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

VPI/VCI: 1 / 32
Multiplexing Method: LLC (selected)

CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

PPPoE oder PPPoA

Das SSG 20-Gerät enthält sowohl PPPoE- als auch PPPoA-Clients zum Herstellen einer Verbindung mit dem Netzwerk des Dienstanbieters über die ADSL-Verbindung. PPPoE ist die am häufigsten verwendete Form der ADSL-Einkapselung und für die Beendigung an jedem Host im Netzwerk konzipiert. PPPoA wird in erster Linie für Geschäftsklassendienste verwendet, da PPP-Sitzungen am Gerät beendet werden können. Damit das Gerät eine Verbindung mit dem Netzwerk des Dienstanbieters herstellen kann, müssen Sie den vom Dienstanbieter zugeordneten Benutzernamen und das zugehörige Kennwort konfigurieren. Die Konfiguration für PPPoA ähnelt der Konfiguration für PPPoE.

HINWEIS: Das Gerät unterstützt nur eine PPPoE-Sitzung für jede virtuelle Verbindung.

Verwenden Sie die WebUI oder die Befehlszeilenschnittstelle folgendermaßen, um den Benutzernamen **roswell** und das Kennwort **area51** für PPPoE zu konfigurieren und die PPPoE-Konfiguration an die adsl1/0-Schnittstelle zu binden:

WebUI

Network > PPP > PPPoE Profile > New: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

PPPoE Instance: poe1
Bound to Interface: adsl1/0 (select)
Username: roswell
Password: area51

CLI

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

Sie können weitere PPPoE- oder PPPoA-Parameter im Gerät konfigurieren, z.B. die Authentifizierungsmethode (standardmäßig unterstützt das Gerät entweder CHAP, Challenge Handshake Authentication-Protokoll, oder PAP, Password Authentication-Protokoll), das Zeitlimit für Inaktivität usw. Fragen Sie Ihren Dienstanbieter, ob Sie weitere PPPoE- oder PPPoA-Parameter konfigurieren müssen, um eine einwandfreie Kommunikation mit dem Server des Dienstanbieters zu gewährleisten.

Statische IP-Adresse und Netzmaske

Wenn Sie von Ihrem Dienstanbieter eine spezifische statische IP-Adresse und eine Netzmaske für Ihr Netzwerk erhalten haben, konfigurieren Sie die IP-Adresse und die Netzmaske für das Netzwerk und die IP-Adresse des mit dem Gerät verbundenen Routeranschlusses. Zudem müssen Sie festlegen, dass das Gerät die statische IP-Adresse verwenden soll. (Das Gerät agiert normalerweise als PPPoE- oder PPPoA-Client und erhält durch Verhandlungen mit dem PPPoE- oder PPPoA-Server eine IP-Adresse für die ADSL-Schnittstelle.)

Sie müssen wie unter „PPPoE oder PPPoA“ auf Seite 43 beschrieben eine PPPoE- oder PPPoA-Instanz konfigurieren und an die adsl1/0-Schnittstelle binden. Achten Sie darauf, dass Sie **Obtain IP using PPPoE** oder **Obtain IP using PPPoA** sowie den Namen der PPPoE- oder PPPoA-Instanz auswählen.

So konfigurieren Sie mithilfe der WebUI oder der Befehlszeilenschnittstelle die statische IP-Adresse 1.1.1.1/24 für das Netzwerk:

WebUI

Network > Interfaces > List > Edit (für die adsl1/0-Schnittstelle): Geben Sie Folgendes ein, und klicken Sie dann auf **Apply**:

```
IP Address/Netmask: 1.1.1.1/24
Static IP: (select)
```

CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

oder

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

Wenn Sie das DNS (Domain Name System) für die Auflösung von Domänennamen und Adressen verwenden möchten, müssen die Computer in Ihrem Netzwerk die IP-Adresse von mindestens einem DNS-Server enthalten. Wenn dem Gerät über PPPoE oder PPPoA eine IP-Adresse für die ADSL2/2+-Schnittstelle zugewiesen wird, erhält es automatisch auch IP-Adressen für die DNS-Server. Weist der DHCP-Server im Gerät den Computern im Netzwerk ihre IP-Adressen zu, erhalten die Computer auch diese DNS-Serveradressen.

Wenn Sie der ADSL2/2 + -Schnittstelle eine statische IP-Adresse zuordnen, muss Ihnen der Dienstanbieter die IP-Adressen der DNS-Server zur Verfügung stellen. Sie können entweder die DNS-Serveradresse auf jedem Computer im Netzwerk konfigurieren, oder Sie können den DHCP-Server in der Trust Zonenschnittstelle so konfigurieren, dass er die DNS-Serveradresse für jeden Computer bereitstellt.

So konfigurieren Sie mithilfe der WebUI oder der Befehlszeilenschnittstelle den DHCP-Server auf der bgroup0-Schnittstelle zum Bereitstellen der DNS-Serveradresse 1.1.1.152 für Computer im Netzwerk:

WebUI

Network > DHCP > Edit (für die bgroup0-Schnittstelle) > DHCP Server: Geben Sie **1.1.1.152** für DNS1 ein, und klicken Sie dann auf **Apply**.

CLI

```
set interface bgroup0 dhcp server option dns1 1.1.1.152
save
```

Weitere Informationen zur Konfiguration der ADSL- und ADSL2/2 + -Schnittstellen erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

ISDN ISDN-Schnittstelle

Bei Integrated Services Digital Network (ISDN) handelt es sich um Standards für die digitale Übertragung über verschiedene vom Consultative Committee for International Telegraphy and Telephone (CCITT) und von der International Telecommunications Union (ITU) erstellte Medien. Als Dial-on-Demand-Dienst bietet ISDN einen schnellen Verbindungsaufbau sowie niedrige Latenz und ermöglicht zudem hochwertige Sprach-, Daten- und Videoübertragungen. ISDN ist überdies ein leitungsvermittelter Dienst, der sowohl für Multipoint- als auch auf Point-to-Point-Verbindungen verwendet werden kann. ISDN bietet einen Dienstrouter mit einer Multilink Point-to-Point Protocol (PPP)-Verbindung für Netzwerkschnittstellen. Die ISDN-Schnittstelle wird normalerweise zum Zugriff auf externe Netzwerke als Sicherungsschnittstelle der Ethernet-Schnittstelle konfiguriert.

So konfigurieren Sie die ISDN-Schnittstelle mithilfe der WebUI oder der Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (bri1/0): Geben Sie Folgendes ein (bzw. wählen Sie Folgendes aus), und klicken Sie dann auf **OK**:

BRI-Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile

CLI

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encap ppp
set interface bri1/0 ppp profile isdnprofile
save
```

Informationen zum Konfigurieren der ISDN-Schnittstelle als Sicherungsschnittstelle erhalten Sie unter „Konfiguration der Untrust Sicherungsschnittstelle“ auf Seite 37.

Weitere Informationen zur Konfiguration der ISDN-Schnittstelle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

T1-Schnittstelle

Die T1-Schnittstelle ist ein grundlegendes Physical Layer-Protokoll, das in Nordamerika von der Digital Signal Level 1 (DS-1)-Multiplexingmethode verwendet wird. Eine T1-Schnittstelle arbeitet mit einer Bitrate von 1,544 MBit/s oder erreicht eine Geschwindigkeit von 24 DS0-Kanälen.

Die Geräte unterstützen die folgenden T1 DS-1-Standards:

- ANSI TI.107, TI.102
- GR 499-core, GR 253-core
- AT&T Pub 54014
- ITU G.751, G.703

So konfigurieren Sie das T1-Mini-PIM mithilfe der WebUI oder der Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (serial1/0): Geben Sie Folgendes ein (bzw. wählen Sie Folgendes aus), und klicken Sie dann auf **OK**:

WAN Configure: main link (Hauptverknüpfung)
WAN Encapsulation: cisco-hdlc
Klicken Sie auf **Apply**.
Fixed IP: (select)
IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encap cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

Weitere Informationen zur Konfiguration der T1-Schnittstelle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

E1-Schnittstelle

Die E1-Schnittstelle ist ein standardmäßiges digitales Kommunikationsformat für Wide Area Network (WAN), das über Kupfervorrichtungen mit einer Rate von 2,048 MBit/s arbeitet. E1 ist ein grundlegendes Zeitmultiplexschema zum Übertragen digitaler Verbindungen, das sich außerhalb Nordamerikas großer Beliebtheit erfreut.

Die Geräte unterstützen die folgenden E1-Standards:

- ITU-T G.703
- ITU-T G0,751
- ITU-T G0,775

So konfigurieren Sie das E1-Mini-PIM mithilfe der WebUI oder der Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (serial1/0): Geben Sie Folgendes ein (bzw. wählen Sie Folgendes aus), und klicken Sie dann auf **OK**:

WAN Configure: main link
WAN Encapsulation: PPP
Binding a PPP Profile: junipertest
Klicken Sie auf **Apply**.
Fixed IP: (select)
IP Address/Netmask: 172.18.1.1/24

CLI

```
set interface serial1/0 encapsulation ppp
set ppp profile “junipertest” static-ip
set ppp profile “junipertest” auth type chap
set ppp profile “junipertest” auth local-name “juniper”
set ppp profile “junipertest” auth secret “password”
set interface serial1/0 ppp profile “junipertest”
set interface serial1/0 ip 172.18.1.1/24
set user “server” type wan
set user “server” password “server”
```

Weitere Informationen zur Konfiguration der E1-Schnittstelle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide.*

V.92 Modemschnittstelle

Die V.92-Schnittstelle verfügt über ein internes analoges Modem zum Herstellen einer PPP-Verbindung zu einem Dienstanbieter. Die serielle Schnittstelle kann als Primär- oder Sicherungsschnittstelle konfiguriert werden, die beim Failover einer Schnittstelle verwendet wird.

HINWEIS: Die V.92-Schnittstelle funktioniert im transparenten Modus nicht.

So konfigurieren Sie die V.92-Schnittstelle mithilfe der WebUI oder der Befehlszeilenschnittstelle:

WebUI

Network > Interfaces > List > Edit (for serial1/0): Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

Zone Name: untrust (select)

ISP: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

ISP Name: isp_juniper
Primary Number: 1234567
Login Name: juniper
Login Password: juniper

Modem: Geben Sie Folgendes ein, und klicken Sie dann auf **OK**:

```
Modem Name: mod1
Init String: AT&FS7=255S32=6
Active Modem setting
    Inactivity Timeout: 20
```

CLI

```
set interface serial1/0 zone untrust
set interface serial1/0 modem isp isp_juniper account login juniper password
juniper
set interface serial1/0 modem isp isp_juniper primary-number 1234567
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active
```

Weitere Informationen zur Konfiguration der V.92-Modemschnittstelle erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

Grundlegender Firewallschutz

Die Geräte werden mit einer Standardrichtlinie konfiguriert, die Arbeitsstationen in der Trust Zone des Netzwerks den Zugriff auf eine beliebige Ressource in der Untrust Sicherheitszone gestattet, wohingegen externe Computer mit den Arbeitsstationen nicht auf Sitzungen zugreifen oder diese starten dürfen. Sie können Richtlinien konfigurieren, damit das Gerät externen Computern das Starten bestimmter Sitzungstypen mit Ihren Computern erlaubt. Informationen zum Erstellen oder Ändern von Richtlinien erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

Das SSG 20-Gerät bietet verschiedene Erkennungsmethoden und Verteidigungsmechanismen zur Bekämpfung von Spionage und Angriffen, durch die ein Netzwerk oder eine Netzwerkressource gefährdet oder beschädigt werden soll.

- Die ScreenOS SCREEN-Optionen sichern eine Zone, indem sie alle über eine Schnittstelle laufenden Verbindungsversuche zu dieser Zone überprüfen und dann zulassen oder verweigern. Sie können in der Untrust Zone z.B. einen Port-Scan-Schutz anwenden, um eine Quelle aus einem Remotenetzwerk am Erkennen von Diensten zu hindern, die u. U. Gegenstand weiterer Angriffe werden sollen.

- Das Gerät wendet Firewallrichtlinien, die ggf. Komponenten für Inhaltsfilterung und Eindringungserkennung und -verhinderung (Intrusion Detection and Prevention, IDP) beinhalten, für den Datenverkehr an, der zonenübergreifend die SCREEN-Filter durchläuft. Standardmäßig darf durch das Gerät kein Datenverkehr zonenübergreifend geleitet werden. Erstellen Sie eine Richtlinie zum Deaktivieren des Standardverhaltens, um Datenverkehr ein zonenübergreifendes Durchlaufen des Geräts zu gestatten.

Legen Sie ScreenOS SCREEN-Optionen für eine Zone folgendermaßen mithilfe der WebUI oder der Befehlszeilenschnittstelle fest:

WebUI

Screening > Screen: Wählen Sie die Zone aus, für die die Optionen Gültigkeit besitzen. Wählen Sie die gewünschten SCREEN-Optionen aus, und klicken Sie anschließend auf **Apply**:

CLI

set zone *zone* screen *option*
save

Weitere Informationen zur Konfiguration der in ScreenOS verfügbaren Netzwerksicherheitsoptionen erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.

Überprüfen der externen Verbindung

Um zu überprüfen, ob die Arbeitsstationen in Ihrem Netzwerk auf Ressourcen im Internet zugreifen können, starten Sie auf einer Arbeitsstation im Netzwerk einen Browser, und geben Sie den folgenden URL ein: www.juniper.net.

Zurücksetzen eines Geräts auf die werkseitigen Standardeinstellungen

Wenn Sie das Administratorkennwort verlieren oder vergessen, können Sie das Gerät auf die Standardeinstellungen zurücksetzen. Dadurch gehen alle vorhandenen Konfigurationen verloren, der Zugriff auf das Gerät ist jedoch wieder möglich.

WARNHINWEIS: Durch das Zurücksetzen des Geräts werden alle vorhandenen Konfigurationseinstellungen gelöscht und alle vorhandenen Firewall- und VPN-Dienste deaktiviert.

Zum Wiederherstellen der Standardeinstellungen des Geräts stehen Ihnen folgende Methoden zur Auswahl:

- Verwenden einer Konsolenverbindung. Zusätzliche Informationen erhalten Sie im *Concepts & Examples ScreenOS Reference Guide*.
- Verwenden des Reset-Stiftlochs an der Rückseite des Geräts wie im folgenden Abschnitt beschrieben.

Sie können das Gerät zurücksetzen und die werkseitigen Standardeinstellungen wiederherstellen, indem Sie das Reset-Stiftloch betätigen. Hierzu müssen Sie entweder die Gerätestatus-LEDs am Bedienfeld überprüfen oder wie in „Verwenden einer Konsolenverbindung“ auf Seite 28 beschrieben eine Konsolensitzung starten.

Führen Sie zum Zurücksetzen und Wiederherstellen der Standardeinstellungen mithilfe des Reset-Stifts die folgenden Schritte aus:

1. Machen Sie das Reset-Stiftloch an der Rückseite des Geräts ausfindig. Drücken Sie einen dünnen festen Draht (z.B. eine Büroklammer) vier bis sechs Sekunden lang in das Stiftloch.

   Die Status-LED blinkt rot. Durch eine Meldung auf der Konsole wird angezeigt, dass die Löschung der Konfiguration gestartet wurde, und das System sendet eine SNMP/SYSLOG-Benachrichtigung.

2. Warten Sie ein bis zwei Sekunden.

   Nach dem ersten Zurücksetzen blinkt die Status-LED grün. Das Gerät wartet jetzt auf das zweite Zurücksetzen. In der Konsolenmeldung werden Sie nun darauf hingewiesen, dass das Gerät auf eine zweite Bestätigung wartet.

3. Betätigen Sie das Reset-Stiftloch erneut vier bis sechs Sekunden lang.

   Die Konsolenmeldung überprüft die zweite Zurücksetzung. Die Status-LED leuchtet kurz rot auf und blinkt anschließend wieder grün.

   Das Gerät wird dann auf seine ursprünglichen Werkseinstellungen zurückgesetzt. Beim Zurücksetzen des Geräts leuchtet die Status-LED kurz rot auf und leuchtet anschließend wieder grün. Die Konsole zeigt Gerätestartmeldungen an. Das System sendet SNMP- und SYSLOG-Benachrichtigungen an konfigurierte SYSLOG- oder SNMP-Trap-Hosts.

   Nachdem das Gerät neu gestartet wurde, zeigt die Konsole die Anmeldeaufforderung für das Gerät an. Die Status-LED blinkt grün. Der Anmeldename und das Kennwort lauten **netscreen**.

Wenn Sie nicht die vollständige Zurücksetzsequenz ausführen, wird der Vorgang ohne Konfigurationsänderung abgebrochen, und in der Konsolenmeldung werden Sie darauf hingewiesen, dass die Löschung der Konfiguration abgebrochen wird. Die Status-LED blinkt dann wieder grün. Wenn das Gerät nicht zurückgesetzt wurde, wird zur Bestätigung dieses Fehlers eine SNMP-Benachrichtigung gesendet.

Kapitel 4

Warten des Geräts

In diesem Kapitel werden die Wartungsmaßnahmen für SSG 20-Geräte erläutert. Der Anhang umfasst die folgenden Abschnitte:

- „Erforderliche Werkzeuge und Teile“ auf dieser Seite
- „Ersetzen eines Mini-Physical Interface Module“ auf dieser Seite
- „Erweitern des Arbeitsspeichers“ auf Seite 54

HINWEIS: Sicherheitshinweise und Anweisungen finden Sie im *Security Products Safety Guide* von Juniper Networks. Dieses Handbuch enthält Informationen zu Situationen, die zu Verletzungen führen können. Bevor Sie mit der Arbeit an Geräten beginnen, informieren Sie sich über die Gefahren, die beim Umgang mit elektrischen Komponenten bestehen. Machen Sie sich außerdem mit den gängigen Vorkehrungen zur Vermeidung von Unfällen vertraut.

Erforderliche Werkzeuge und Teile

Zum Ersetzen einer Komponente eines SSG 20-Geräts benötigen Sie folgende Werkzeuge und Teile:

- Abschirmbeutel zum Schutz vor elektrostatischer Entladung oder antistatische Matte
- Erdungsarmband zum Schutz vor elektrostatischer Entladung (Electrostatic Discharge, ESD)
- Kreuzschlitzschraubenzieher (3 mm)

Ersetzen eines Mini-Physical Interface Module

Beide SSG 20-Modelle verfügen am Bedienfeld über zwei Steckplätze für Wide Area Network Mini Physical Interface Modules (WAN-Mini-PIMs). Mini-PIMs in einem SSG 20-Gerät können eingebaut und ersetzt werden. Das Gerät muss vor dem Entfernen oder Einbauen eines Mini-PIM ausgeschaltet werden.

VORSICHT: Stellen Sie sicher, dass das Gerät beim Entfernen eines Mini-PIM ausgeschaltet ist. Die Mini-PIMs sind nicht „hot-swappable“, d.h. der Austausch von Komponenten ist nicht möglich, während der Computer läuft.

Entfernen einer unbeschrifteten Frontscheibe

Zur Gewährleistung einer ausreichenden Belüftung des SSG 20-Geräts sollten unbeschriftete Frontscheiben über Steckplätzen angebracht werden, die keine Mini-PIMs enthalten. Entfernen Sie eine unbeschriftete Frontscheibe nur, wenn Sie ein Mini-PIM in den leeren Steckplatz einbauen.

Führen Sie zum Entfernen einer unbeschrifteten Frontscheibe die folgenden Schritte aus:

1. Legen Sie einen Abschirmbeutel gegen elektrostatische Entladung oder eine antistatische Matte auf einen flachen, festen Untergrund, auf dem Sie das Mini-PIM abstellen möchten.

2. Schnallen Sie zum Schutz vor elektrostatischer Entladung ein Erdungsband um Ihr Handgelenk, und stellen Sie eine Verbindung zwischen dem Band und dem ESD-Punkt auf dem Gehäuse oder einem externen ESD-Punkt her, falls das SSG 20-Gerät nicht geerdet ist.

3. Entfernen Sie den Stromadapter vom Gerät. Überprüfen Sie, ob die Strom-LED aus ist.

4. Lösen Sie mit einem Schraubenzieher die Schrauben auf jeder Seite der Frontscheibe.

5. Entfernen Sie die Frontscheibe, und legen Sie die Frontscheibe anschließend in den Abschirmbeutel oder auf die antistatische Matte.

Entfernen eines Mini-PIM

Mini-PIMs werden im Bedienfeld des SSG 20-Geräts eingebaut. Ein Mini-PIM wiegt unter 110 g.

Führen Sie zum Entfernen eines Mini-PIM die folgenden Schritte aus:

1. Legen Sie einen Abschirmbeutel oder eine antistatische Matte auf einen flachen, festen Untergrund, auf dem Sie das Mini-PIM abstellen möchten.

2. Schnallen Sie zum Schutz vor elektrostatischer Entladung ein Erdungsband um Ihr Handgelenk, und stellen Sie eine Verbindung zwischen dem Band und dem ESD-Punkt auf dem Gehäuse oder einem externen ESD-Punkt her, falls das SSG 20-Gerät nicht geerdet ist.

3. Entfernen Sie den Stromadapter vom Gerät. Überprüfen Sie, ob die Strom-LED aus ist.

4. Beschriften Sie die an das Mini-PIM angeschlossenen Kabel, damit Sie später jedes Kabel wieder an das entsprechende PIM anschließen können.

5. Entfernen Sie die Kabel aus dem Mini-PIM.

6. Ordnen Sie das Kabel ggf. so an, dass ein Herausgleiten des Kabels oder das Entstehen von Stresspunkten verhindert wird:

    a. Bringen Sie die Kabel so an, dass sie beim Herunterhängen nicht ihr eigenes Gewicht stützen müssen.

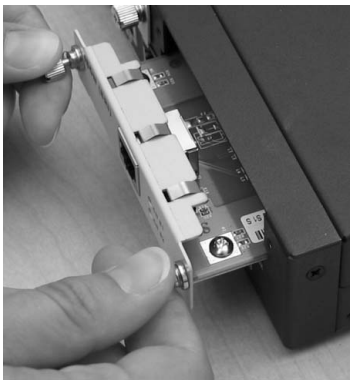
b. Legen Sie zu lange Kabel sorgfältig zu einer Schleife zusammen, und räumen Sie diese beiseite.

c. Fixieren Sie die Kabel mithilfe von Klemmen.

7. Lösen Sie auf jeder Seite der Mini-PIM-Frontscheibe die Schrauben mit einem Schraubenzieher.

8. Ergreifen Sie die Schrauben auf jeder Seite der Frontscheibe des Mini-PIM, und lassen Sie das Mini-PIM aus dem Gerät hinausgleiten. Legen Sie das Mini-PIM im Abschirmbeutel oder auf der antistatischen Matte ab.

Abbildung 16: Entfernen eines Mini-PIM



9. Wenn Sie das Mini-PIM nicht mehr in den leeren Steckplatz einbauen, bringen Sie über dem Steckplatz eine unbeschriftete Frontscheibe an, um eine ausreichende Belüftung zu gewährleisten.

Einbauen eines Mini-PIM

Führen Sie zum Einbauen eines Mini-PIM die folgenden Schritte aus:

1. Schnallen Sie zum Schutz vor elektrostatischer Entladung ein Erdungsband um Ihr Handgelenk, und stellen Sie eine Verbindung zwischen dem Band und dem ESD-Punkt auf dem Gehäuse oder einem externen ESD-Punkt her, falls das SSG 20-Gerät nicht geerdet ist.

2. Entfernen Sie den Stromadapter vom Gerät. Überprüfen Sie, ob die Strom-LED aus ist.

3. Ergreifen Sie die Schrauben auf jeder Seite der Frontscheibe des Mini-PIM, und richten Sie die Einkerbungen auf dem Stecker an der Hinterseite des Mini-PIM an den Einkerbungen im Steckplatz des Mini-PIM im SSG 20-Gerät aus. Schieben Sie das Mini-PIM anschließend hinein, bis es fest im Gerät einrastet.

Abbildung 17: Einbauen eines Mini-PIM

VORSICHT: Schieben Sie das Mini-PIM direkt in den Steckplatz, um die Komponenten der Mini-PIM nicht zu beschädigen.

4. Ziehen Sie die Schrauben auf jeder Seite der Frontscheibe des Mini-PIM mit einem 3 mm-Schlitzschraubenzieher fest.

5. Stecken Sie die entsprechenden Kabel in die Kabelanschlüsse am Mini-PIM ein.

6. Ordnen Sie das Kabel ggf. so an, dass ein Herausgleiten des Kabels oder das Entstehen von Stresspunkten verhindert wird:

   a. Bringen Sie die Kabel so an, dass sie beim Herunterhängen nicht ihr eigenes Gewicht stützen müssen.

   b. Legen Sie zu lange Kabel sorgfältig zu einer Schleife zusammen, und räumen Sie diese beiseite.

   c. Fixieren Sie die Kabel mithilfe von Klemmen.

7. Entfernen Sie den Stromadapter vom Gerät. Überprüfen Sie, ob die Strom-LED nach Drücken des Einschaltknopfs ständig grün leuchtet.

8. Überprüfen Sie, ob die PIM-Status-LED auf dem Systemdashboard ständig grün leuchtet. Dadurch wird angezeigt, dass das Mini-PIM online ist.

Erweitern des Arbeitsspeichers

Das einem SSG 20-Gerät zur Verfügung stehende 128 MB umfassende Dual Inline Memory Module (DIMM) Dynamic Random Access Memory (DRAM) kann auf 256 MB DIMM DRAM erweitert werden.

Gehen Sie zum Erweitern des Arbeitsspeichers eines SSG 20-Geräts folgendermaßen vor:

1. Schnallen Sie zum Schutz vor elektrostatischer Entladung ein Erdungsband um Ihr Handgelenk, und stellen Sie eine Verbindung zwischen dem Band und dem ESD-Punkt auf dem Chassis oder einem externen ESD-Punkt her, falls das Gerät nicht geerdet ist.

2. Stecken Sie das Wechselstromkabel aus.

3. Drehen Sie das Gerät um, damit die Oberseite auf einem ebenen Untergrund liegt.
4. Entfernen Sie die Schrauben mit einem Kreuzschlitzschraubenzieher von der Speicherkartenabdeckung. Legen Sie die Schrauben neben sich ab, um damit später wieder die Abdeckung zu fixieren.
5. Entfernen Sie die Speicherkartenabdeckung.

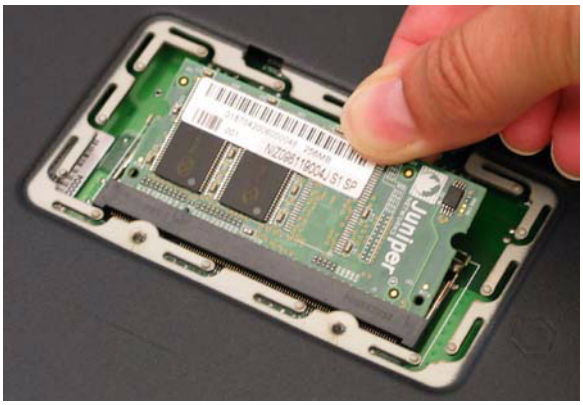
Abbildung 18: Unterseite des Geräts

6. Drücken Sie auf jeder Seite des Moduls mit den Daumen außen auf die Sperrriegel. Diese gleiten daraufhin vom Modul weg, und Sie können den 128 MB DIMM DRAM entnehmen.

Abbildung 19: Entriegeln des Arbeitsspeichermoduls

7. Ergreifen Sie die lange Kante des Arbeitsspeichermoduls, und lassen Sie dieses hinausgleiten. Legen Sie das Modul neben sich ab.

Abbildung 20: Entfernen der Modulsteckplätze



8. Setzen Sie den 256 MB DIMM DRAM in den Steckplatz ein. Üben Sie mit beiden Daumen einen gleichmäßigen Druck auf die obere Kante des Moduls aus, und drücken Sie das Modul nach unten, bis die Sperrriegel in der vorgesehenen Position einrasten.

Abbildung 21: Einsetzen des Arbeitsspeichermoduls

9. Platzieren Sie die Speicherkartenabdeckung über dem Steckplatz.

10. Ziehen Sie die Schrauben mit einem Kreuzschlitzschraubenzieher fest, und fixieren Sie die Abdeckung am Gerät.

Anhang A

Technische Daten

Dieser Anhang beinhaltet allgemeine technische Systemdaten für ein SSG 20-Gerät. Der Anhang umfasst die folgenden Abschnitte:

Physisch

Tabelle 8: SSG 20 – Physische Daten

Beschreibung	Wert
Chassisabmessungen	294 mm x 194,8 mm x 44 mm
Gewicht des Geräts	1,53 kg ohne eingebaute PIMs
ISDN-PIM	70 g
Annex A-PIM für ADSL	106 g
Annex B-PIM für ADSL	106 g
T1-PIM	75 g
E1-PIM	75 g
V.92-PIM	79 g

Elektrik

Tabelle 9: SSG 20 – Elektrische Daten

Physikalische Größe	Technische Daten
Eingangsgleichspannung	12 V
Zulässige Höchstspannung des Gleichspannungssystems	3 - 4,16 A

Umgebungstoleranz

Tabelle 10: SSG 20-Umgebungstoleranz

Beschreibung	Wert
Höhe über NN	Keine Beeinträchtigung der Leistung bis zu einer Höhe von 2.000 m
Relative Luftfeuchtigkeit	Bei einer relativen Luftfeuchtigkeit zwischen 10 und 90 Prozent (nicht kondensierend) ist eine ordnungsgemäße Funktion gesichert.
Temperatur	In einem Temperaturbereich zwischen 32°F (0°C) und 104°F (40°C) ist eine ordnungsgemäße Funktion sichergestellt. Zulässiger Temperaturbereich für die Lagerung des Geräts: -4°F (-20°C) bis 158°F (70°C)

Zertifizierungen

Sicherheit

- CAN/CSA-C22.2 Nr. 60950-1-03/UL 60950-1, Sicherheit von Informationstechnologiegeräten
- EN 60950-1 (2000) Dritte Ausgabe, Sicherheit von Informationstechnologiegeräten
- IEC 60950-1 (1999) Dritte Ausgabe, Sicherheit von Informationstechnologiegeräten

EMC-Emissionen

- FCC Teil 15 Klasse B (USA)
- EN 55022 Klasse B (Europa)
- AS 3548 Klasse B (Australien)
- VCCI Klasse B (Japan)

EMC-Störfestigkeit

- EN 55024
- EN-61000-3-2 – Netzoberwellen
- EN-61000-3-3 – Netzoberwellen
- EN-61000-4-2 – ESD (elektrostatische Entladung)
- EN-61000-4-3 – Störfestigkeit gegen Strahlung
- EN-61000-4-4 – EFT (schnelle transiente Störgrößen)
- EN-61000-4-5 – Stoßspannungen
- EN-61000-4-6 – Allgemeine Störfestigkeit gegen niedrige Frequenzen
- EN-61000-4-11 – Spannungseinbrüche und -schwankungen

ETSI

European Telecommunications Standards Institute (ETSI) EN-3000386-2: Netzwerkgeräte für Telekommunikation. Anforderungen für elektromagnetische Kompatibilität; (Gerätekategorie – Unterschied zu Telekommunikationscentern)

T1-Schnittstelle

- FCC Teil 68 – TIA 968
- Industry Canada CS-03
- UL 60950-1 – Geltende Anforderungen für TNV-Verbindungen mit einem externen Leitungsanschluss

Stecker

Abbildung 22 zeigt die Position der Pins auf einem RJ-45-Stecker.

Abbildung 22: RJ-45-Kontaktanordnungen

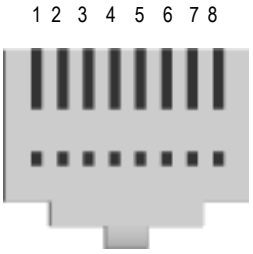


Tabelle 11 beinhaltet eine Auflistung der Kontaktanordnungen der RJ-45-Stecker.

Tabelle 11: Kontaktanordnungen der RJ-45-Stecker

Pin	Name	E/A	Beschreibung
1	RTS Out	O	Sendeaufforderung (Request To Send)
2	DTR Out	O	Endgerät betriebsbereit (Data Terminal Ready)
3	TxD	O	Daten übertragen (Transmit Data)
4	GND	Nicht zutreffend	Chassismasse (Chassis Ground)
5	GND	Nicht zutreffend	Chassismasse (Chassis Ground)
6	RxD	I	Daten empfangen (Receive Data)
7	DSR	I	Datensatz bereit (Data Set Ready)
8	CTS	I	Sendebereitschaft (Clear To Send)

Abbildung 23 zeigt die Position der Pins auf einer DB-9-Buchse.

Abbildung 23: DB-9-Buchse

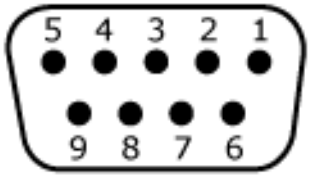


Tabelle 12 beinhaltet eine Auflistung der Kontaktanordnungen der DB-9-Stecker.

Tabelle 12: Kontaktanordnungen der DB-9-Stecker

Pin	Name	E/A	Beschreibung
1	DCD	I	Trägersignal erkannt (Carrier Detect)
2	RxD	I	Daten empfangen (Receive Data)
3	TxD	O	Daten übertragen (Transmit Data)
4	DTR	O	Endgerät betriebsbereit (Data Terminal Ready)
5	GND	Nicht zutreffend	Signalerde (Signal Ground)
6	DSR	I	Datensatz bereit (Data Set Ready)
7	RTS	O	Sendeaufforderung (Request To Send)
8	CTS	I	Sendebereitschaft (Clear To Send)
9	RING	I	Anrufanzeige (Ring Indicator)

Anhang B

Assistent für die Anfangskonfiguration

Dieser Anhang beinhaltet detaillierte Informationen zum Assistenten für die Anfangskonfiguration (Initial Configuration Wizard, ICW) für SSG 20-Geräte.

Verwenden Sie nach dem Anschluss des Geräts an das Netzwerk den ICW zur Konfiguration der auf dem Gerät installierten Schnittstellen.

In diesem Abschnitt werden die folgenden ICW-Fenster behandelt:

1. Fenster für die Schnellkonfiguration

Abbildung 24: Fenster für die Schnellkonfiguration

Arbeitet das Netzwerk mit NetScreen-Security Manager (NSM) kann das Configlet für die Schnellkonfiguration zur automatischen Konfiguration des Geräts eingesetzt werden. Sie erhalten ein Configlet vom NSM-Administrator, wählen Sie **Yes**, **Load Configlet from:**, und navigieren Sie zum Speicherort der Datei. Klicken Sie anschließend auf **Next**. Das Configlet richtet das Gerät für Sie ein, sodass Sie zum Konfigurieren des Geräts die folgenden Schritte nicht ausführen müssen.

Wenn Sie den ICW umgehen und direkt zur WebUI wechseln möchten, wählen Sie die letzte Option, und klicken Sie anschließend auf **Next**.

Wenn Sie zum Konfigurieren des Geräts kein Configlet, sondern den ICW verwenden möchten, wählen Sie die erste Option, und klicken Sie anschließend auf **Next**. Die ICW-Willkommensseite wird angezeigt. Klicken Sie auf **Next**. Das Fenster für die Administratoranmeldung wird angezeigt.

2. Fenster für die Administratoranmeldung

Geben Sie einen neuen Administratoranmeldenamen und ein neues Kennwort ein, und klicken Sie auf **Next**.

Abbildung 25: Fenster für die Administratoranmeldung

3. Fenster für den WLAN-Zugriffspunkt

Bei Verwendung des Geräts in der Regulierungsdomäne WORLD oder ETSI müssen Sie einen Ländercode auswählen. Wählen Sie die entsprechenden Optionen, und klicken Sie anschließend auf **Next**.

Abbildung 26: Fenster für die Konfiguration des Ländercodes für den Wireless-Zugriffspunkt

4. Fenster für die Konfiguration der physischen Schnittstelle

Auf dem Bildschirm für Schnittstellen-Zonenbindungen legen Sie die Schnittstelle fest, an die die Untrust Sicherheitszone gebunden werden soll. Bgroup0 ist vorab an die Trust Sicherheitszone gebunden. Eth0/1 ist an die DMZ-Sicherheitszone gebunden, dabei jedoch optional.

Abbildung 27: Fenster für die Angabe der physischen Schnittstelle

Sie können nach dem Binden einer Schnittstelle an eine Zone die Schnittstelle konfigurieren. Die auf dem Sicherheitsgerät installierten Mini-PIMs bestimmen darüber, welche Konfigurationsfenster anschließend angezeigt werden. Klicken Sie zum Fortsetzen der Konfiguration mithilfe des ICW auf **Next**.

5. ADSL2/2+ Interface – Fenster

Wenn auf dem Gerät das ADSL2/2 + -Mini-PIM installiert ist, können Sie über das folgende Fenster die adslx/0-Schnittstelle konfigurieren.

HINWEIS: Sind auf dem Gerät zwei ADSL2/2 + -Mini-PIMs installiert, kann die Mehrfachverbindungsfunktion mit dem ICW nicht verwendet werden. Informationen zum Konfigurieren von ML ADSL finden Sie im *Concepts & Examples ScreenOS Reference Guide*.

Abbildung 28: Fenster für die Konfiguration der ADSL-Schnittstelle

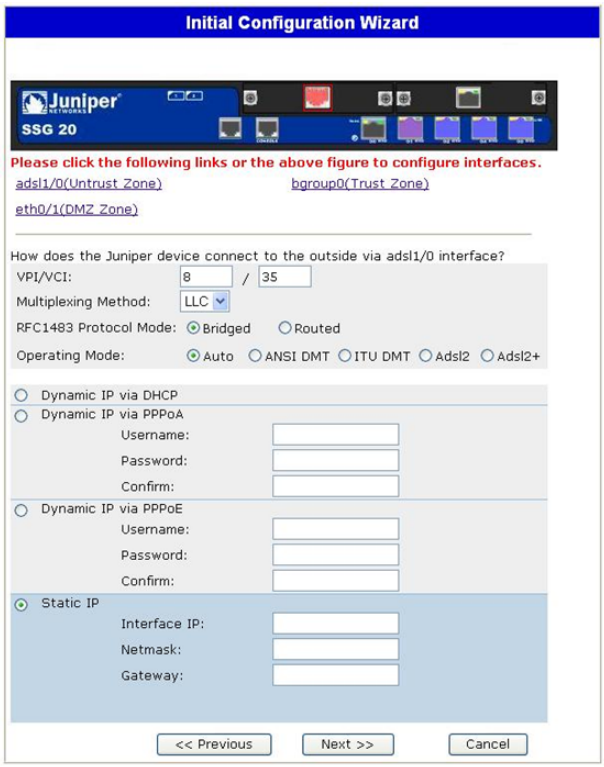


Tabelle 13: Felder im Fenster für die Konfiguration der ADSL-Schnittstelle

Feld	Beschreibung
Informationen vom Dienstanbieter:	
VPI/VCI	VPI/VCI-Werte zum Identifizieren der dauerhaften virtuellen Verbindung.
Multiplexing Method	ATM-Multiplexingmethode (Standardeinstellung: **LLC**).
RFC1483 Protocol Mode	Protokollmoduseinstellung (Standardeinstellung: **Bridged**).
Operating Mode	Betriebsmodus für die physische Leitung (Standardeinstellung: **Auto**).
IP-Konfigurationseinstellungen	■ Aktivieren Sie **Dynamic IP via DHCP**, damit das Gerät eine IP-Adresse für die ADSL-Schnittstelle von einem Dienstanbieter empfangen kann. ■ Aktivieren Sie **Dynamic IP via PPPoA**, damit das Gerät als PPPoA-Client arbeiten kann. Geben Sie den vom Dienstanbieter zugewiesenen Benutzernamen und das zugewiesene Kennwort ein. ■ Aktivieren Sie **Dynamic IP via PPPoE**, damit das Gerät als PPPoE-Client arbeiten kann. Geben Sie den vom Dienstanbieter zugewiesenen Benutzernamen und das zugewiesene Kennwort ein. ■ Wählen Sie zum Zuweisen einer eindeutigen und festen IP-Adresse zur ADSL-Schnittstelle die Option **Static IP** aus. Geben Sie die IP-Adresse der Schnittstelle, die Netzmaske und das Gateway ein (die Gateway-Adresse ist die IP-Adresse des mit dem Gerät verbundenen Routeranschlusses).

Sind Ihnen diese Einstellungen nicht bekannt, schlagen Sie in der mit dem Dienstanbietergerät mitgelieferten Dokument *Common Settings for Service Providers* nach.

6. Fenster für die Konfiguration der T1-Schnittstelle

Ist auf dem Gerät das T1-Mini-PIM installiert und wurde die Option **Frame Relay** ausgewählt, werden die folgenden Fenster angezeigt:

- Fenster für die Konfiguration der T1-Schnittstelle mit der Registerkarte „Physical Layer“
- Fenster für die Konfiguration der T1-Schnittstelle – Registerkarte „Frame Relay“

HINWEIS: Sind auf dem Gerät zwei T1-Mini-PIMs installiert und Sie wählen die Option für die Mehrfachverbindungen, werden zwei mit Physical Layer bezeichnete Registerkarten angezeigt.

Abbildung 29: Fenster für die Konfiguration der T1-Schnittstelle mit der Registerkarte „Physical Layer“

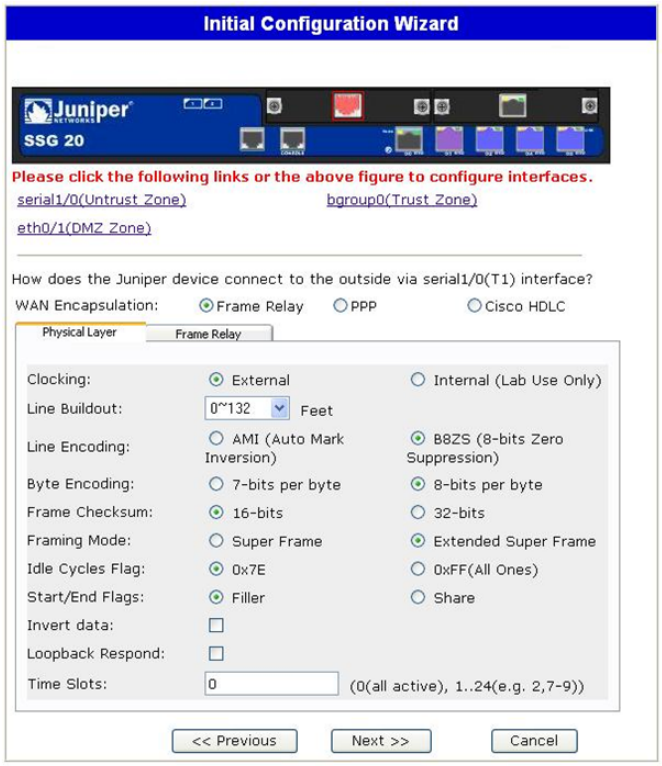


Tabelle 14: Felder im Fenster für die Konfiguration der T1-Schnittstelle mit der Registerkarte „Physical Layer“

Feld	Beschreibung
Clocking	Stellt den Übertragungstakt der Schnittstelle ein.
Line Buildout	Legt die Entfernung fest, bis zu der über eine Schnittstelle eine Verbindung aufrechterhalten werden kann. Die Standardeinstellung ist 0 - 132 Feet (ca. 0-40 m).
Line Encoding	Legt das Leitungsverschlüsselungsformat der Schnittstelle fest: ■ Auto Mark Inversion ■ 8-bits Zero Suppression
Byte Encoding	Legt die Byte-Verschlüsselung der T1-Schnittstelle auf 7 Bit/Byte oder 8 Bit/Byte fest. Standardmäßig sind 8 Bit/Byte ausgewählt.
Frame Checksum	Legt die Größe der Prüfsumme fest. Der Standardwert ist **16**.
Framing Mode	Legt das Rahmenformat fest. Standardmäßig ist der erweiterte Modus ausgewählt.
Idle Cycles Flag	Legt den Wert fest, der während Zyklen ohne Aktivität von der Schnittstelle übertragen wird. Standardmäßig ist **0x7E** ausgewählt: ■ 0x7E (Flags) ■ 0xFF (Einsen)
Start/End Flags	Für die Übertragung der Start- und Endflags kann Filler oder Shared ausgewählt werden. Standardmäßig ist **Filler** ausgewählt.
Invert Data – Kontrollkästchen	Ermöglicht die invertierte Übertragung nicht verwendeter Datenbits.
Loopback Respond – Kontrollkästchen	Ermöglicht das Loopback auf der T1-Schnittstelle von der Remote-CSU (Channel Service Unit).
Time Slots	Legt die Verwendung von Zeitsteckplätzen einer T1-Schnittstelle fest. Die Standardeinstellung ist **0**, alle 24 Zeitsteckplätze werden verwendet.

Abbildung 30: Fenster für die Konfiguration der T1-Schnittstelle – Registerkarte „Frame Relay“

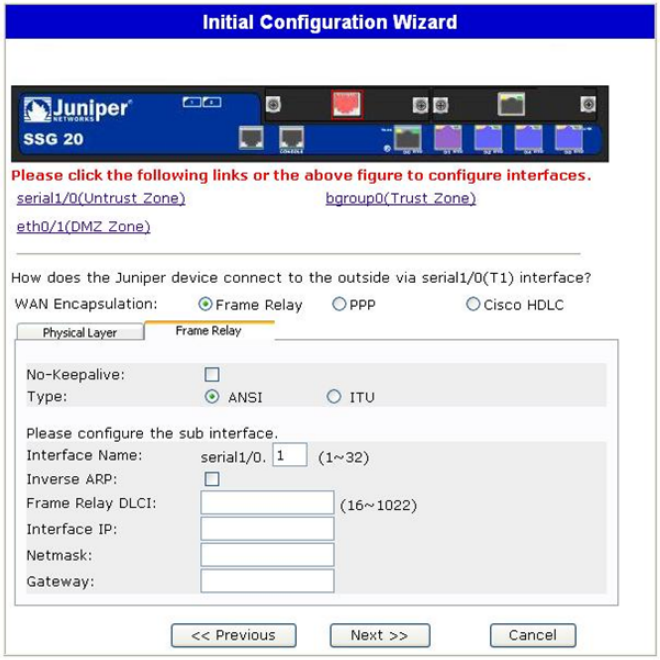


Tabelle 15: Felder auf der Registerkarte „Frame Relay“ im Fenster für die Konfiguration der T1-Schnittstelle

Feld	Beschreibung
No-Keepalive – Kontrollkästchen	Aktiviert No-Keepalives.
Type	Legt den Frame-Relay-LMI-Typ fest: ■ ANSI: American National Standards Institute unterstützt Downstream-Datenraten von bis zu 8 MBit/s und Upstream-Datenraten von bis zu 1 MBit/s. ■ ITU: International Telecommunications Union unterstützt Downstream-Datenraten von 6,144 MBit/s und Upstream-Datenraten von 640 KBit/s.
Interface Name	Legt den Namen der Subschnittstelle fest.
Inverse ARP	Ermöglicht das umgekehrte ARP (Address Resolution Protocol) für die Subschnittstelle.
Frame Relay DLCI	Weist der Subschnittstelle einen DLCI (Data Link Connection Identifier) zu.
Interface IP	Legt die IP-Adresse für die Subschnittstelle fest.
Netmask	Legt die Netzmaske für die Subschnittstelle fest.
Gateway	Legt die Gateway-Adresse für die Subschnittstelle fest.

Ist auf dem Gerät das T1-Mini-PIM installiert und wurde die Option „PPP“ ausgewählt, werden die folgenden zusätzlichen Fenster angezeigt:

- Fenster für die Option „PPP“ mit der Registerkarte „PPP“
- Fenster für die Option „PPP“ mit der Registerkarte „Peer User“

Abbildung 31: Fenster für die Option „PPP“ mit der Registerkarte „PPP“

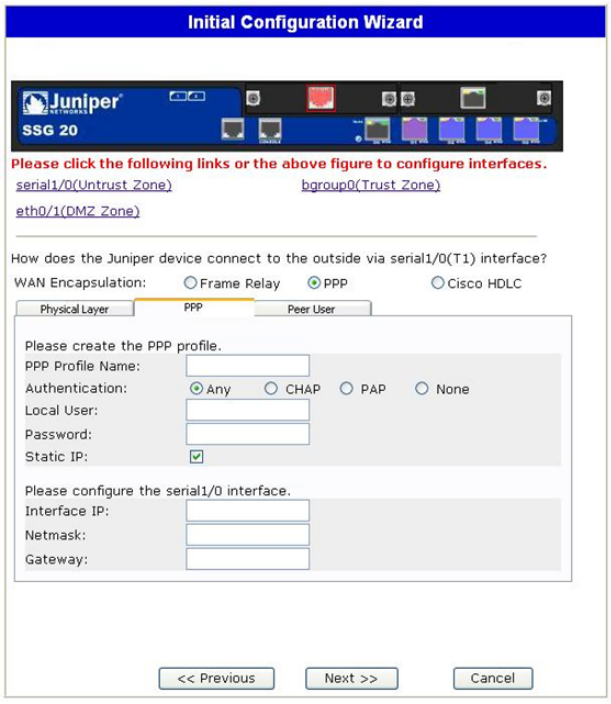


Tabelle 16: Felder im Fenster für die Option „PPP” mit der Registerkarte „PPP“

Feld	Beschreibung
PPP Profile Name	Legt den Namen des PPP-Profils fest.
Authentication	Legt den Authentifizierungstyp fest.
Local User	Legt den Namen des lokalen Benutzers fest.
Password	Legt das Kennwort für den lokalen Benutzer fest.
Static IP – Kontrollkästchen	Ermöglicht eine statische IP-Adresse.
Interface IP	Legt die IP-Adresse für die serialx/0-Schnittstelle fest.
Netmask	Legt die serialx/0-Netzmaske fest.
Gateway	Legt die serialx/0-Gateway-Adresse fest.

Abbildung 32: Fenster für die Option „PPP“ mit der Registerkarte „Peer User“

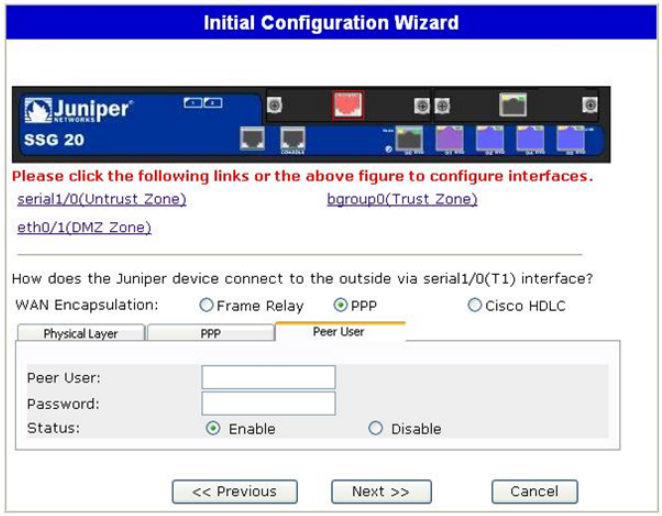


Tabelle 17: Felder im Fenster für die Option „PPP“ mit der Registerkarte „Peer User“

Feld	Beschreibung
Peer User	Legt den Namen des Peer-Benutzers fest.
Password	Legt das Kennwort für den im Textfeld Peer User angegebenen Peer-Benutzer fest.
Status	Aktiviert bzw. deaktiviert PPP.

Ist auf dem Gerät das T1-Mini-PIM installiert und wurde die Option Cisco HDLC ausgewählt, wird das folgende Fenster angezeigt:

Abbildung 33: Fenster für die Option „Cisco HDLC“ mit der Registerkarte „Cisco HDLC“

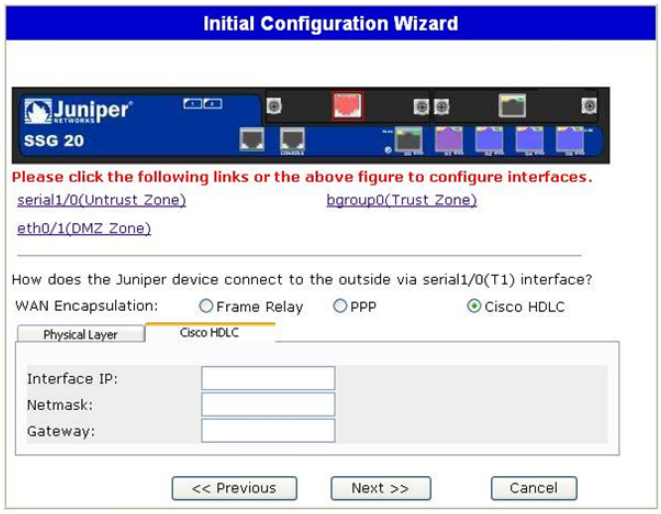


Tabelle 18: Felder im Fenster mit Option „Cisco HDLC“ und Registerkarte „Cisco HDLC“

Feld	Beschreibung
Interface IP	Legt die IP-Adresse für die T1 Cisco HDLC-Schnittstelle fest.
Netmask	Legt die Netzmaske für die T1 Cisco HDLC-Schnittstelle fest.
Gateway	Legt die Gateway-Adresse für die T1 Cisco HDLC-Schnittstelle fest.

7. Fenster für die Konfiguration der E1-Schnittstelle

Ist auf dem Gerät das E1-Mini-PIM installiert und wurde Option Frame Relay ausgewählt, werden die folgenden Fenster angezeigt:

- Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Physical Layer“
- Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Frame Relay“

HINWEIS: Sind auf dem Gerät zwei E1-Mini-PIMs installiert und wird die Option für die Mehrfachverbindungen ausgewählt, werden zwei der mit Physical Layer bezeichneten Registerkarten angezeigt.

Abbildung 34: Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Physical Layer“

Tabelle 19: Felder im Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Physical Layer“

Feld	Beschreibung
Clocking	Stellt den Übertragungstakt der Schnittstelle ein.
Frame Checksum	Legt die Größe der Prüfsumme fest. Der Standardwert ist **16**.
Framing Mode	Legt das Rahmenformat fest. Die Standardeinstellung ist **without CRC4**.
Idle Cycles Flag	Legt den Wert fest, der während Zyklen ohne Aktivität von der Schnittstelle übertragen wird. Standardmäßig ist **0x7E** ausgewählt: ■ 0x7E (Flags) ■ 0xFF (Einsen)
Start/End Flags	Für die Übertragung der Start- und Endflags kann Filler oder Shared ausgewählt werden. Standardmäßig ist **Filler** ausgewählt.
Invert Data – Kontrollkästchen	Ermöglicht die invertierte Übertragung nicht verwendeter Datenbits.
Time Slots	Legt die Verwendung von Zeitsteckplätzen einer T1-Schnittstelle fest. Die Standardeinstellung ist **0**, alle 32 Zeitsteckplätze werden verwendet.

Abbildung 35: Fenster für die Konfiguration der E1-Schnittstelle mit der Registerkarte „Frame Relay“

Tabelle 20: Felder auf der Registerkarte „Frame Relay“ im Fenster für die Konfiguration der E1-Schnittstelle

Feld	Beschreibung
No-Keepalive – Kontrollkästchen	Aktiviert No-Keepalives.
Type	Legt den Frame-Relay-LMI-Typ fest: ■ ANSI: American National Standards Institute unterstützt Downstream-Datenraten von bis zu 8 MBit/s und Upstream-Datenraten von bis zu 1 MBit/s. ■ ITU: International Telecommunications Union unterstützt Downstream-Datenraten von 6,144 MBit/s und Upstream-Datenraten von 640 Bit/s.
Interface Name	Legt den Namen der Subschnittstelle fest.
Inverse ARP – Kontrollkästchen	Ermöglicht das umgekehrte ARP (Address Resolution Protocol) für die Subschnittstelle.
Frame Relay DLCI	Weist der Subschnittstelle einenDLCI zu.
Interface IP	Legt die IP-Adresse für die Subschnittstelle fest.
Netmask	Legt die Netzmaske für die Subschnittstelle fest.
Gateway	Legt die Gateway-Adresse für die Subschnittstelle fest.

Informationen zum Konfigurieren der E1-Schnittstelle mit PPP-Optionen finden Sie unter „Fenster für die Option „PPP“ mit der Registerkarte „PPP““ auf Seite 71.

Informationen zum Konfigurieren der E1-Schnittstelle mit der Option Cisco HDLC finden Sie unter „Fenster für die Option „Cisco HDLC“ mit der Registerkarte „Cisco HDLC““ auf Seite 73.

8. Fenster für die Konfiguration der ISDN-Schnittstelle

Wenn auf dem Gerät das ISDN-Mini-PIM installiert ist, können Sie über das folgende Fenster die brix/0 (Untrust)-Schnittstelle konfigurieren.

HINWEIS: Sind auf dem Gerät zwei ISDN-Mini-PIMs installiert und wurde die Option für die Mehrfachverbindungen ausgewählt, werden zwei der mit Physical Layer bezeichneten Registerkarten angezeigt.

Abbildung 36: Fenster für die Konfiguration der ISDN-Schnittstelle mit der Registerkarte „Physical Layer“

Tabelle 21: Felder auf der Registerkarte „Physical Layer“ im Fenster für die Konfiguration der ISDN-Schnittstelle

Feld	Beschreibung
Switch Type	Legt den Vermittlungstyp des Dienstanbieters fest: ■ att5e: At&T 5ESS ■ ntdms100: Nortel DMS 100 ■ ins-net: NTT INS-Net ■ etsi: European variants ■ ni1: National ISDN-1
SPID1	Dienstanbieter-ID, normalerweise eine siebenstellige Telefonnummer mit einigen optionalen Nummern. Nur für die Vermittlungstypen DMS-100 und NI1 sind SPIDs erforderlich. Dem Vermittlungstyp DMS-100 sind zwei SPIDs zugewiesen, einer für jeden B-Kanal.
SPID2	Sicherungsdienstanbieter-ID.
TEI Negotiation	Gibt an, wann die TEI ausgehandelt werden soll (beim Start oder beim ersten Anruf). Diese Einstellung wird normalerweise für ISDN-Dienstangebote in Europa und Verbindungen zu DMS-100-Switches verwendet, die für das Initialisieren der TEI-Aushandlung vorgesehen sind.
Calling Number	Rechnungsnummer für das ISDN-Netzwerk.
Sending Complete – Kontrollkästchen	Ermöglicht das Senden vollständiger Informationen an ausgehende Installationsmeldung. Wird normalerweise nur in Hongkong und Taiwan verwendet.

Bei der bri1/0-Schnittstelle kann eine Verbindung mithilfe der Wählhilfe, der Wählhilfe für Mehrfachverbindungen, einer geleasten Leitung oder durch Einwahl mithilfe von BRI hergestellt werden. Wird keine oder eine Option oder werden beide Optionen ausgewählt, sieht das daraufhin angezeigte Fenster etwa folgendermaßen aus:

Abbildung 37: Fenster für die Konfiguration der ISDN-Schnittstelle mit der Registerkarte „Connection“

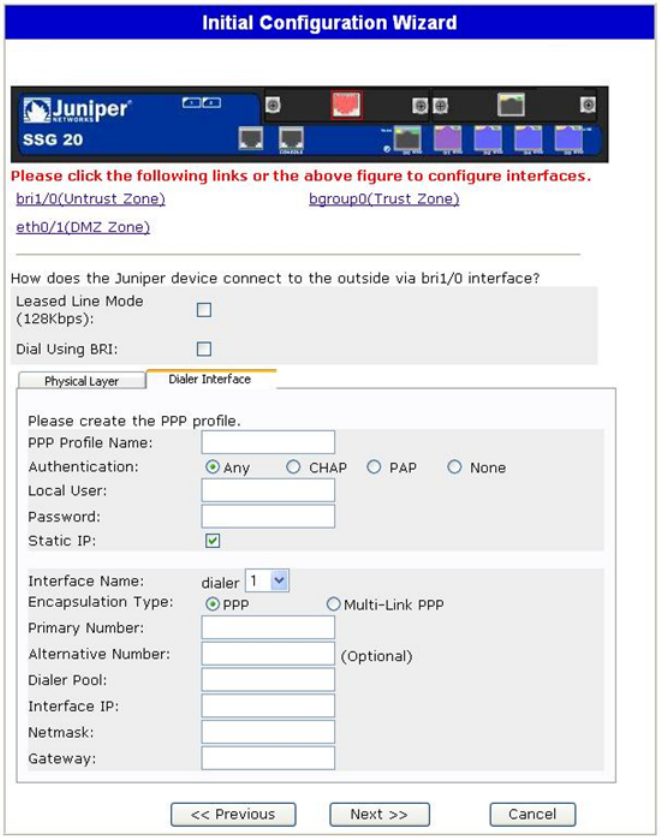


Tabelle 22: Felder auf der Registerkarte „Connection” im Fenster für die Konfiguration der ISDN-Schnittstelle

Feld	Beschreibung
PPP Profile Name	Legt für die ISDN-Schnittstelle einen PPP-Profilnamen fest.
Authentication	Legt den PPP-Authentifizierungstyp fest: ■ Any ■ CHAP: Challenge Handshake Authentication Protocol ■ PAP: Password Authentication Protocol ■ None
Local User	Legt den lokalen Benutzer fest.
Password	Legt das Kennwort für den lokalen Benutzer fest.
Static IP – Kontrollkästchen	Aktiviert eine statische IP-Adresse für die Schnittstelle.
Interface IP	Legt die IP-Adresse für die Schnittstelle fest.
Interface Name (nur Wählhilfe)	Legt den Schnittstellennamen der Wählhilfe fest. Der Standardwert ist **dialer.1**.
Encapsulation Type	Legt den Einkapselungstyp für die Wählhilfe und für BRI-Schnittstellen verwendende Wählhilfen fest. Der Standardwert ist **PPP**.
Primary Number	Legt die primäre Nummer für Wählhilfen und für BRI-Schnittstellen verwendende Wählhilfen fest.

Feld	Beschreibung
Alternative Number	Legt die alternative (sekundäre) Nummer fest, die verwendet werden soll, wenn die primäre Nummer für die Verbindungsherstellung nicht verwendet werden kann.
Dialer Pool (nur Wählhilfe)	Legt den Poolnamen der Wählhilfe für die Schnittstelle der Wählhilfe fest.
Netmask	Legt die Netzmaske fest.
Gateway	Legt die Gateway-Adresse fest.

9. Fenster für die Konfiguration der V.92-Modemschnittstelle

Wenn auf dem Gerät das V.92-Mini-PIM installiert ist, können Sie über das folgende Fenster die serialx/0 (Modem)-Schnittstelle konfigurieren:

Abbildung 38: Fenster für die Konfiguration der Modemschnittstelle

Tabelle 23: Felder im Fenster für die Konfiguration der Modemschnittstelle

Feld	Beschreibung
Modem Name	Legt den Namen für die Modemschnittstelle fest.
Init String	Legt die Initialisierungszeichenfolge für das Modem fest.
ISP Name	Weist dem Dienstanbieter einen Namen zu.
Primary Number	Gibt die Telefonnummer zum Zugreifen auf den Dienstanbieter an.
Alternative Number (optional)	Gibt eine alternative Telefonnummer zum Zugreifen auf den Dienstanbieter an, wenn mithilfe der primären Nummer keine Verbindung hergestellt werden kann.
Login Name	Legt den Anmeldenamen für das Dienstanbieterkonto fest.
Password	Legt das Kennwort für den Anmeldenamen fest.
Confirm	Bestätigt das ins Feld für das Kennwort eingegebene Kennwort.

10. Eth0/0 Interface (Untrust Zone) – Fenster

Der eth0/0-Schnittstelle kann über DHCP oder PPPoE eine statische oder dynamische IP-Adresse zugewiesen werden.

Abbildung 39: Fenster für die Konfiguration der Eth0/0-Schnittstelle

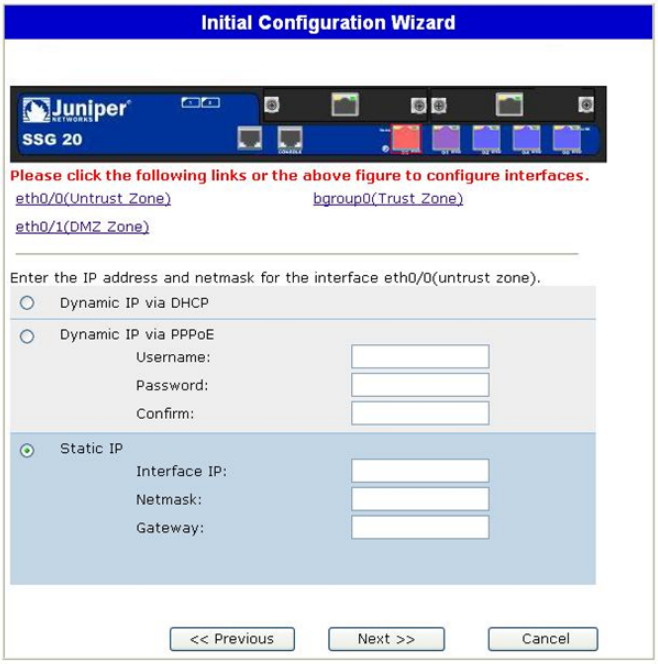


Tabelle 24: Felder im Fenster für die Konfiguration der Eth0/0-Schnittstelle

Feld	Beschreibung
Dynamic IP via DHCP	Ermöglicht den Empfang einer IP-Adresse für die Schnittstelle der Untrust Zone von einem Dienstanbieter.
Dynamic IP via PPPoE	Das Gerät kann als PPPoE-Client fungieren und empfängt eine IP-Adresse für die Schnittstelle der Untrust Zone von einem Dienstanbieter. Geben Sie den vom Dienstanbieter zugewiesenen Benutzernamen und das zugewiesene Kennwort ein.
Static IP	Weist der Schnittstelle der Untrust Zone eine eindeutige und feste IP-Adresse zu. Geben Sie die IP-Adresse der Schnittstelle der Untrust Zone, die Netzmaske und die Gateway-Adresse ein.

11. Eth0/1 Interface (DMZ Zone) – Fenster

Der eth0/1-Schnittstelle kann über DHCP eine statische oder dynamische IP-Adresse zugewiesen werden.

Abbildung 40: Fenster für die Konfiguration der Eth0/1-Schnittstelle

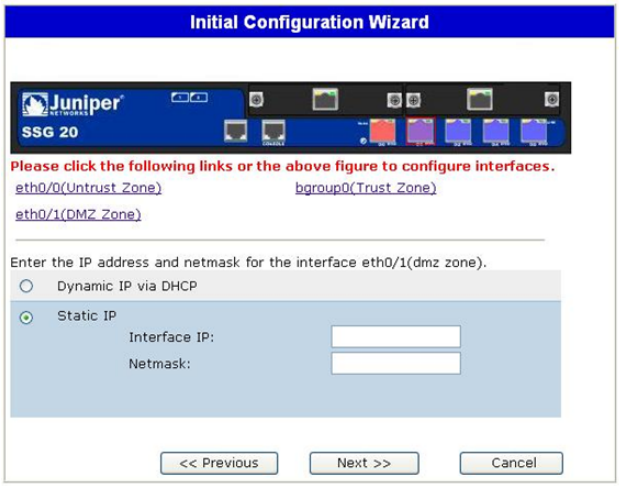


Tabelle 25: Felder im Fenster für die Konfiguration der Eth0/1-Schnittstelle

Feld	Beschreibung
Dynamic IP via DHCP	Ermöglicht den Empfang einer IP-Adresse für die DMZ-Schnittstelle von einem Dienstanbieter.
Static IP	Weist der DMZ-Schnittstelle eine eindeutige und feste IP-Adresse zu. Geben Sie die IP-Adresse der DMZ-Schnittstelle und eine Netzmaske ein.

12. Bgroup0 Interface (Trust Zone) – Fenster

Der bgroup0-Schnittstelle kann über DHCP eine statische oder dynamische IP-Adresse zugewiesen werden.

Die Standard-IP-Adresse für Schnittstellen ist **192.168.1.1**, und die Netzmaske lautet **255.255.255.0** oder **24**.

Abbildung 41: Fenster für die Konfiguration der Bgroup0-Schnittstelle

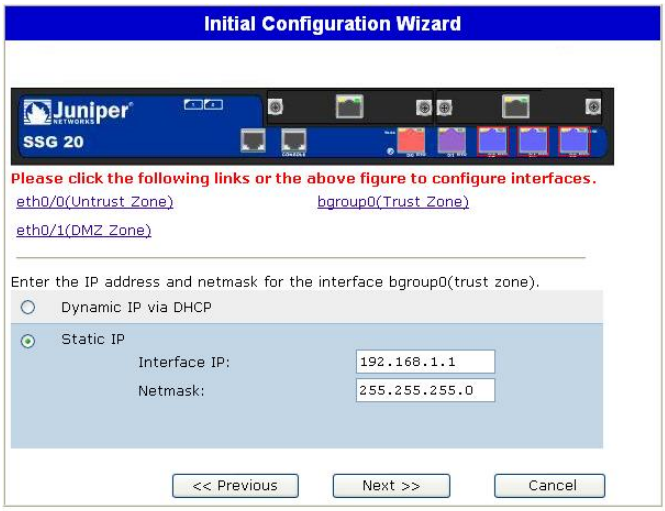


Tabelle 26: Felder im Fenster für die Konfiguration der Bgroup0-Schnittstelle

Feld	Beschreibung
Dynamic IP via DHCP	Ermöglicht den Empfang einer IP-Adresse für die Schnittstelle der Trust Zone von einem Dienstanbieter.
Static IP	Weist der Schnittstelle der Trust Zone eine eindeutige und feste IP-Adresse zu. Geben Sie die IP-Adresse der Schnittstelle der Trust Zone und eine Netzmaske ein.

13. Fenster für die Konfiguration der Wireless0/0-Schnittstelle (Trust Zone)

Beim Konfigurieren des SSG 20-WLAN-Geräts müssen Sie vor dem Aktivieren der wireless0/0-Schnittstelle eine Service Set Identifier (SSID) festlegen. Detaillierte Anweisungen zum Konfigurieren der Wireless-Schnittstellen finden Sie im *Concepts & Examples ScreenOS Reference Guide*.

Abbildung 42: Fenster für die Konfiguration der Wireless0/0-Schnittstelle

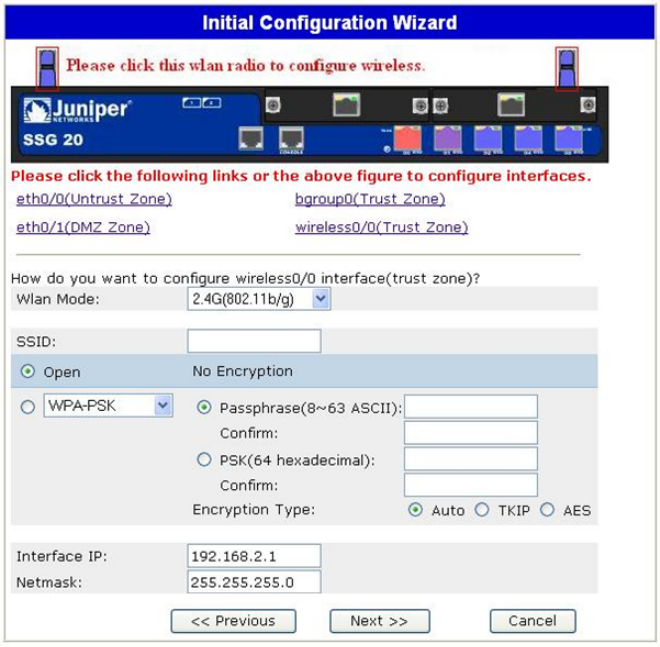


Tabelle 27: Felder im Fenster für die Konfiguration der Wireless0/0-Schnittstelle

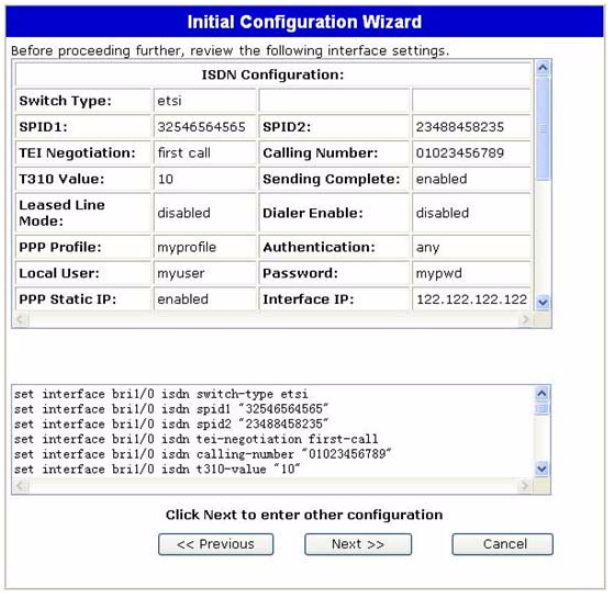
Feld	Beschreibung
Wlan Mode	Legt den WLAN-Funkmodus fest: ■ 5 G (802.11a) ■ 2.4 G (802.11b/g) ■ Both (802.11a/b/g)
SSID	Legt den SSID-Namen fest.

Feld	Beschreibung
Authentication and Encryption	Legt die Authentifizierung und Verschlüsselung der WLAN-Schnittstelle fest: ■ Mit der Standardeinstellung **Open** für die Authentifizierung kann jeder auf das Gerät zugreifen. Für diese Authentifizierungsoption steht keine Verschlüsselung zur Verfügung. ■ Der Authentifizierungstyp **WPA Pre-Shared Key** legt den Pre-Shared Key (PSK) oder die Passphrase fest, die beim Zugreifen auf eine Wireless-Verbindung eingegeben werden muss. Für den PSK können Sie einen HEX- oder ASCII-Wert eingeben. Für einen HEX PSK muss ein 256-Bit-HEX-Wert (64 Textzeichen) eingegeben werden. Eine ASCII-Passphrase muss zwischen 8 und 63 Textzeichen enthalten. Als Verschlüsselungstyp für diese Option muss Temporal Key Integrity Protocol (**TKIP**) oder Advanced Encryption Standard (**AES**) ausgewählt werden. Wählen Sie alternativ **Auto** aus, um beide Optionen zuzulassen. ■ WPA2 Pre-Shared Key. ■ WPA Auto Pre-Shared Key
Interface IP	Legt die IP-Adresse für die WLAN-Schnittstelle fest.
Netmask	Legt die Netzmaske für die WLAN-Schnittstelle fest.

14. Fenster für die Schnittstellenzusammenfassung

Nach dem Konfigurieren der WAN-Schnittstellen wird das Fenster für die Schnittstellenzusammenfassung angezeigt.

Abbildung 43: Fenster für die Schnittstellenzusammenfassung

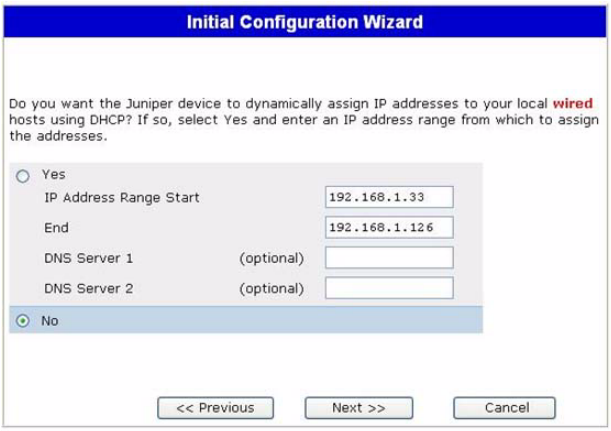


Überprüfen Sie die Schnittstellenkonfiguration, und klicken Sie anschließend zum Fortfahren auf **Next**. Das Fenster für Fenster für die Konfiguration der physischen Ethernet-DHCP-Schnittstelle wird angezeigt.

15. Fenster für die Konfiguration der physischen Ethernet-DHCP-Schnittstelle

Wählen Sie **Yes**, damit das Gerät dem verdrahteten Netzwerk über DHCP IP-Adressen zuweisen kann. Geben Sie den IP-Adressbereich ein, innerhalb dessen Clients im Netzwerk vom Gerät IP-Adressen zugewiesen werden können, und klicken Sie anschließend auf **Next**.

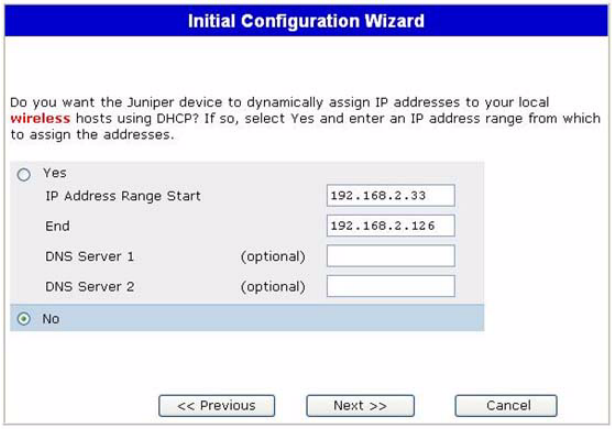
Abbildung 44: Fenster für die Konfiguration der physischen Ethernet-DHCP-Schnittstelle



16. Fenster für die Konfiguration der Wireless-DHCP-Schnittstelle

Wählen Sie **Yes**, damit das Gerät dem Wireless-Netzwerk über DHCP IP-Adressen zuweisen kann. Geben Sie den IP-Adressbereich ein, innerhalb dessen Clients im Netzwerk vom Gerät IP-Adressen zugewiesen werden können, und klicken Sie anschließend auf **Next**.

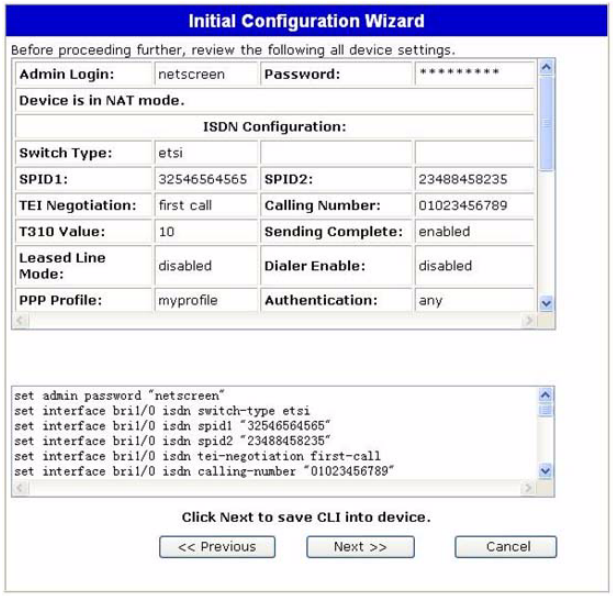
Abbildung 45: Fenster für die Konfiguration der Wireless-DHCP-Schnittstelle



17. Bestätigungsfenster

Bestätigen Sie die Gerätekonfiguration, und nehmen Sie ggf. Änderungen vor. Klicken Sie zum Speichern auf **Next**, starten Sie das Gerät neu, und führen Sie anschließend die Konfiguration aus.

Abbildung 46: Bestätigungsfenster



Nach dem Starten mit der gespeicherten Systemkonfiguration wird die WebUI-Anmeldeaufforderung angezeigt. Informationen zum Zugreifen auf das Gerät mithilfe der WebUI finden Sie unter „Verwenden der WebUI“ auf Seite 29.

Index

W

Z