Handbuch für IPsec-Einstellungen

Version 0

GER

Definition der Hinweise

In diesem Handbuch wird das folgende Symbol verwendet:

Hinweis	Hinweise informieren Sie, wie auf eine bestimmte Situation reagiert werden sollte, oder geben Ihnen hilfreiche Tipps zur beschriebenen Funktion.

Warenzeichen

Das Brother-Logo ist ein eingetragenes Warenzeichen von Brother Industries, Ltd.

Alle auf Brother-Produkten gezeigten oder in den dazugehörigen Dokumenten bzw. in anderen Materialien erwähnten Marken- und Produktnamen von Firmen sind Warenzeichen oder eingetragene Warenzeichen der entsprechenden Firmen.

©2012 Brother Industries, Ltd. Alle Rechte vorbehalten.

Inhaltsverzeichnis

1 Einführung 1

Übersicht 1
Konfiguration mit Web Based Management (Webbrowser) 2

2 IPsec-Einstellungen 5

Adressvorlage 5
Dienstvorlage 7
IPsec-Dienstvorlage 7
Einrichtungsdienst 9
IPsec-Vorlage 11

A Anhang A 20

Dienstvorlagen 20
Typ/Code 21

1 Einführung

Übersicht

IPsec (Internet Protocol Security) ist ein Sicherheitsprotokoll, das eine optionale Internet-Protokollfunktion verwendet, um Manipulationen zu verhindern und die Vertraulichkeit von Daten, die als IP-Pakete übertragen werden, zu gewährleisten. IPsec verschlüsselt Daten, die über das Netzwerk transportiert werden, wie zum Beispiel Druckdaten, die von Computern an einen Drucker gesendet werden. Da die Daten auf Netzwerkebene verschlüsselt werden, wird IPsec von Anwendungen verwendet, die Protokolle höherer Ebenen nutzen, ohne dass der Benutzer es wahrnimmt.

IPsec unterstützt die folgenden Funktionen:

■ IPsec-Übertragungen

Entsprechend den IPsec-Einstellungsbedingungen sendet ein mit dem Netzwerk verbundener Computer über IPsec Daten an das angegebene Gerät und empfängt davon Daten. Wenn die Geräte beginnen über IPsec zu kommunizieren, werden mit IKE (Internet Key Exchange) zunächst Schlüssel ausgetauscht und dann die verschlüsselten Daten mit den Schüsseln übertragen.

Darüber hinaus verfügt IPsec über zwei Betriebsarten: den Transport-Modus und den Tunnel-Modus. Der Transport-Modus wird hauptsächlich für die Kommunikation zwischen Geräten verwendet, der Tunnel-Modus wird in Umgebungen wie zum Beispiel einem VPN (Virtual Private Network) eingesetzt.

Hinweis

- Für IPsec-Übertragungen müssen die folgenden Bedingungen erfüllt sein:
  - Ein Computer, der Kommunikation über IPsec unterstützt, ist mit dem Netzwerk verbunden.
  - Der Drucker oder das MFC ist für IPsec-Kommunikation konfiguriert.
  - Der an den Drucker oder das MFC angeschlossene Computer ist für IPsec-Verbindungen konfiguriert.
- IPsec unterstützt keine Broadcast- oder Multicast-Kommunikation.

■ IPsec-Einstellungen

Die Einstellungen, die für Verbindungen über IPsec erforderlich sind. Diese Einstellungen können mit Web Based Management konfiguriert werden. (Siehe *Konfiguration mit Web Based Management (Webbrowser)* ➤➤ Seite 2.)

Hinweis

Zur Konfiguration der IPsec-Einstellungen muss ein Computer, auf dem der Browser installiert ist, mit dem Netzwerk verbunden sein.

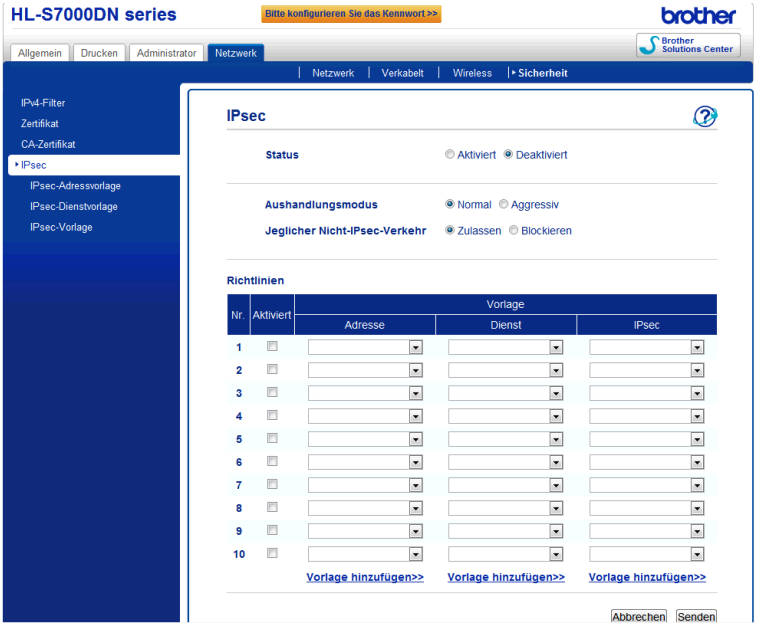
Konfiguration mit Web Based Management (Webbrowser)

Legen Sie im IPsec-Einstellungsbildschirm für Web Based Management die IPsec-Verbindungsbedingungen fest.

Die IPsec-Verbindungsbedingungen bestehen aus drei **Vorlage**-Typen: **Adresse**, **Dienst** und **IPsec**, und maximal 10 Verbindungsbedingungen können konfiguriert werden.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes steht).
   - Zum Beispiel:

     http://192.168.1.2/
3. Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eines eingerichtet haben, und drücken Sie →.
4. Klicken Sie auf die Registerkarte **Netzwerk**.
5. Klicken Sie auf **Sicherheit**.
6. Klicken Sie auf **IPsec**.
7. Nun können Sie die IPsec-Einstellungen im unten gezeigten Bildschirm vornehmen.



- **Status**

  Wählen Sie **Aktiviert** oder **Deaktiviert** für IPsec.
- **Aushandlungsmodus**

  Wählen Sie den Modus für IKE Phase 1.
  - **Normal**: Der Hauptmodus wird verwendet.

- **Aggressiv**: Der Aggressiv-Modus wird verwendet.

Hinweis

IKE ist ein Protokoll zum Austauschen von Verschlüsselungsschlüsseln für die verschlüsselte Kommunikation über IPsec.

Im **Normal**-Modus ist die Verarbeitungsgeschwindigkeit langsam, aber die Sicherheit hoch. Im **Aggressiv**-Modus ist die Verarbeitungsgeschwindigkeit schneller als im **Normal**-Modus, aber die Sicherheit geringer.

■ **Jeglicher Nicht-IPsec-Verkehr**

Wählen Sie, welche Aktion für Nicht-IPsec-Pakete ausgeführt werden soll.

- **Zulassen**: Alle Pakete werden empfangen.
- **Blockieren**: Nicht-IPsec-Pakete werden verworfen.

Hinweis

Wenn Sie Webdienste verwenden, müssen Sie **Zulassen** für **Jeglicher Nicht-IPsec-Verkehr** verwenden. Wenn **Blockieren** ausgewählt ist, können Webdienste nicht verwendet werden.

■ **Richtlinien**

Es können maximal 10 IPsec-Verbindungsbedingungen (Vorlagensatz) konfiguriert werden.

■ **Aktiviert**

Wenn dieses Kontrollkästchen ausgewählt ist, ist der Vorlagensatz für diese Nummer aktiviert.

Hinweis

Bei Auswahl mehrerer Kontrollkästchen haben die Kontrollkästchen mit kleineren Nummern im Falle von Einstellungskonflikten zwischen den ausgewählten Kontrollkästchen Vorrang.

■ **Vorlage** - **Adresse**

Wählen Sie die **Adressvorlage**, die für die IPsec-Verbindungsbedingungen verwendet wird.

Zum Hinzufügen einer **Adressvorlage** klicken Sie auf **Vorlage hinzufügen**. (Siehe *Adressvorlage* ➤➤ Seite 5.)

■ **Vorlage** - **Dienst**

Wählen Sie die **Dienstvorlage**, die für die IPsec-Verbindungsbedingungen verwendet wird.

Zum Hinzufügen einer **Dienstvorlage** klicken Sie auf **Vorlage hinzufügen**. (Siehe *Dienstvorlage* ➤➤ Seite 7.)

Hinweis

Wenn Sie DNS für die Namenauflösung bei Verwendung der Dienstvorlagen 2, 3 und 4 in *Anhang A* verwenden möchten, müssen die DNS-Einstellungen getrennt konfiguriert werden.

■ **Vorlage** - **IPsec**

Wählen Sie die **IPsec-Vorlage**, die für die IPsec-Verbindungsbedingungen verwendet wird.

Zum Hinzufügen einer **IPsec-Vorlage** klicken Sie auf **Vorlage hinzufügen**. (Siehe *IPsec-Vorlage* ➤➤ Seite 11.)

■ Senden

Klicken Sie auf diese Schaltfläche, um die Einstellungen zu registrieren. Falls der Computer zum Ändern der Einstellungen neu gestartet werden muss, wird nach dem Klicken auf diese Schaltfläche der Bestätigungsbildschirm für den Neustart angezeigt.

Hinweis

Wenn Sie das Kontrollkästchen **Aktiviert** auswählen und auf **Senden** klicken, wird im Falle eines leeren Feldes im ausgewählten Vorlagensatz ein Fehler angezeigt.

2 IPsec-Einstellungen

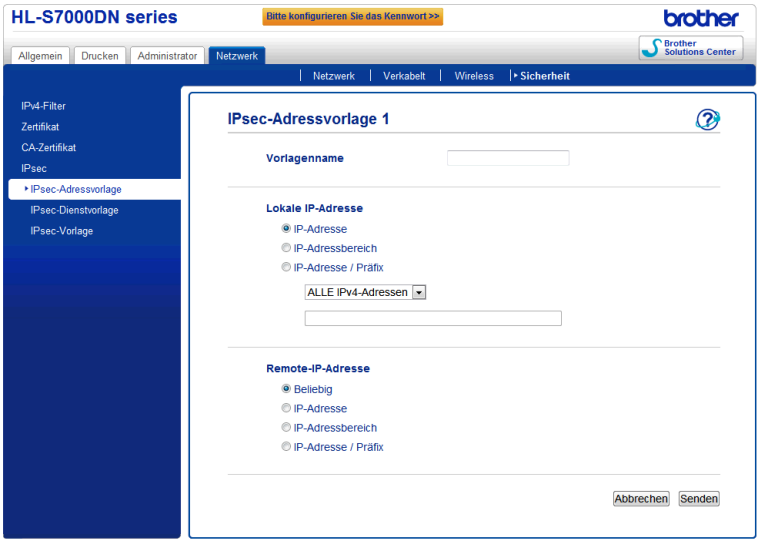
Adressvorlage

Geben Sie die IP-Adressen an, die für die IPsec-Verbindungsbedingungen verwendet werden. Es können maximal 10 **Adressvorlagen** verwendet werden.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes steht).
   - Zum Beispiel:

     http://192.168.1.2/
3. Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eines eingerichtet haben, und drücken Sie →.
4. Klicken Sie auf die Registerkarte **Netzwerk**.
5. Klicken Sie auf **Sicherheit**.
6. Klicken Sie auf **IPsec-Adressvorlage**.
   10 **Adressvorlagen** werden angezeigt. Wenn keine **Adressvorlage** konfiguriert wurde, wird **Nicht konfiguriert** angezeigt.
   - **Löschen**

     Klicken Sie auf diese Schaltfläche, um die ausgewählte **Adressvorlage** zu löschen. Die aktuell verwendete **Adressvorlage** kann jedoch nicht gelöscht werden.
7. Klicken Sie auf die Nummer für die **Adressvorlage**, die Sie erstellen möchten. Geben Sie im Bildschirm unten die IP-Adresse an, die für IPsec verwendet werden soll, und erstellen Sie die **IPsec-Adressvorlage**.



■ **Vorlagenname**

Geben Sie in diesem Feld einen Namen für die Vorlage ein. (Maximal 16 Zeichen)

■ **Lokale IP-Adresse**

Geben Sie die IP-Adressbedingungen für den Sender an.

- **IP-Adresse**

  Geben Sie die IP-Adresse an. Wählen Sie **ALLE IPv4-Adressen**, **ALLE IPv6-Adressen**, **ALLE Link Local IPv6** oder **Benutzerdefiniert** aus.

  Wenn **Benutzerdefiniert** ausgewählt ist, geben Sie die gewünschte IP-Adresse (IPv4 oder IPv6) im Textfeld ein.

- **IP-Adressbereich**

  Geben Sie die Anfangs- und End-IP-Adressen für den IP-Adressbereich an. Wenn die Anfangs- und End-IP-Adressen nicht dem Format nach IPv4 oder IPv6 entsprechen oder die End-IP-Adresse kleiner als die Anfangs-IP-Adresse ist, wird ein Fehler angezeigt.

- **IP-Adresse / Präfix**

  Geben Sie die IP-Adresse mit einem Präfix an.

  Zum Beispiel: 192.168.1.1/24

  Da das Präfix in Form einer 24-Bit-Subnetzmaske (255.255.255.0) für 192.168.1.1 angegeben wird, sind die Adressen 192.168.1.xx gültig.

■ **Remote-IP-Adresse**

Geben Sie die IP-Adressbedingungen für den Empfänger an.

- **Beliebig**

  Wenn **Beliebig** ausgewählt ist, sind alle IP-Adressen aktiviert.

- **IP-Adresse**

  Geben Sie die gewünschte IP-Adresse (IPv4 oder IPv6) im Textfeld ein.

- **IP-Adressbereich**

  Geben Sie die Anfangs- und End-IP-Adressen für den IP-Adressbereich an. Wenn die Anfangs- und End-IP-Adressen nicht dem Format nach IPv4 oder IPv6 entsprechen oder die End-IP-Adresse kleiner als die Anfangs-IP-Adresse ist, wird ein Fehler angezeigt.

- **IP-Adresse / Präfix**

  Geben Sie die IP-Adresse mit einem Präfix an.

  Zum Beispiel: 192.168.1.1/24

  Da das Präfix in Form einer 24-Bit-Subnetzmaske (255.255.255.0) für 192.168.1.1 angegeben wird, sind die Adressen 192.168.1.xx gültig.

■ **Senden**

Klicken Sie auf diese Schaltfläche, um die Einstellungen zu registrieren.

Hinweis

Wenn Sie die Einstellungen der aktuell verwendeten Vorlage ändern, wird der IPsec-Einstellungsbildschirm für Web Based Management geschlossen und dann wieder geöffnet.

Dienstvorlage

IPsec-Dienstvorlage

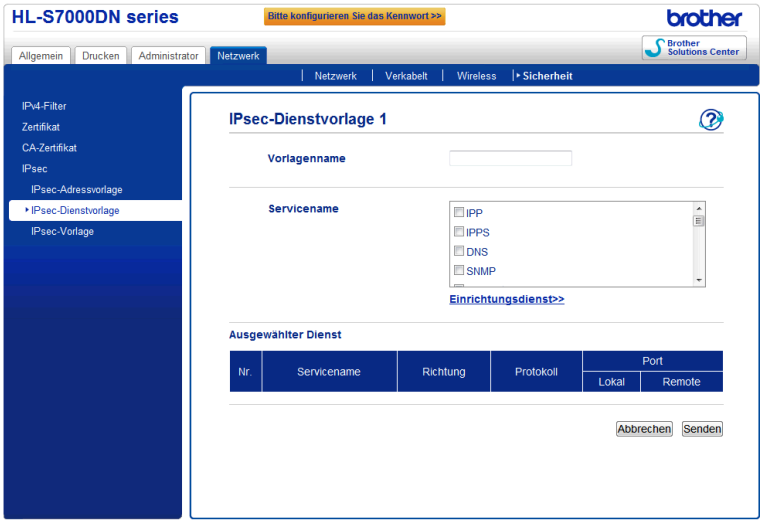
Geben Sie das Protokoll und die Portnummer an, die für IPsec-Verbindungen verwendet werden sollen. Es können maximal 10 **Dienstvorlagen** verwendet werden.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes steht).
   - Zum Beispiel:

     http://192.168.1.2/
3. Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eines eingerichtet haben, und drücken Sie →.
4. Klicken Sie auf die Registerkarte **Netzwerk**.
5. Klicken Sie auf **Sicherheit**.
6. Klicken Sie auf **IPsec-Dienstvorlage**.
   10 **Dienstvorlagen** werden angezeigt. Wenn keine **Dienstvorlage** konfiguriert wurde, wird **Nicht konfiguriert** angezeigt.
   - **Löschen**

     Klicken Sie auf diese Schaltfläche, um die ausgewählte **Dienstvorlage** zu löschen. Die aktuell verwendete **Dienstvorlage** kann jedoch nicht gelöscht werden.

7 Klicken Sie auf die Nummer für die **Dienstvorlage**, die Sie erstellen möchten. Wählen Sie im Bildschirm unten die Dienste, die Sie für IPsec verwenden möchten, und erstellen Sie die **IPsec-Dienstvorlage**. Wenn Sie zusätzlich eigene Dienste erstellen möchten, klicken Sie auf **Einrichtungsdienst**. (Siehe *Einrichtungsdienst* ➤➤ Seite 9.)



■ **Vorlagenname**

Geben Sie in diesem Feld einen Namen für die Vorlage ein. (Maximal 16 Zeichen)

■ **Servicename**

Die Standardservicenamen und zuvor erstellte Servicenamen werden angezeigt. Wählen Sie die Dienste aus, die Sie zur Vorlage hinzufügen möchten.

■ **Einrichtungsdienst**

Klicken Sie auf **Einrichtungsdienst**, um die Vorlage durch Hinzufügen von Diensten zu konfigurieren. (Siehe *Einrichtungsdienst* ➤➤ Seite 9.)

■ **Ausgewählter Dienst**

Die Dienstinformationen (**Servicename**, **Richtung**, **Protokoll** und **Port**), die für **Servicename** ausgewählt sind, werden angezeigt.

Hinweis

- Es können maximal 32 Dienste gleichzeitig hinzugefügt werden.
- Einzelheiten zu den Protokollen, die Sie unter **IPsec-Dienstvorlage** angeben können, finden Sie unter *Anhang A*.

■ **Senden**

Klicken Sie auf diese Schaltfläche, um die Einstellungen zu registrieren.

Hinweis

Wenn Sie die Einstellungen der aktuell verwendeten Vorlage ändern, wird der IPsec-Einstellungsbildschirm für Web Based Management geschlossen und dann wieder geöffnet.

Einrichtungsdienst

Erstellen Sie einen neuen Dienst.

1. Klicken Sie im Bildschirm **IPsec-Dienstvorlage** auf **Einrichtungsdienst**.
   60 **Servicenamen** werden angezeigt. Wenn kein **Servicename** konfiguriert wurde, wird **Nicht konfiguriert** angezeigt.

   - **Löschen**

     Klicken Sie auf diese Schaltfläche, um den ausgewählten **Servicenamen** zu löschen. Der aktuell verwendete **Servicename** kann jedoch nicht gelöscht werden.

   - **IPsec-Dienstvorlage**

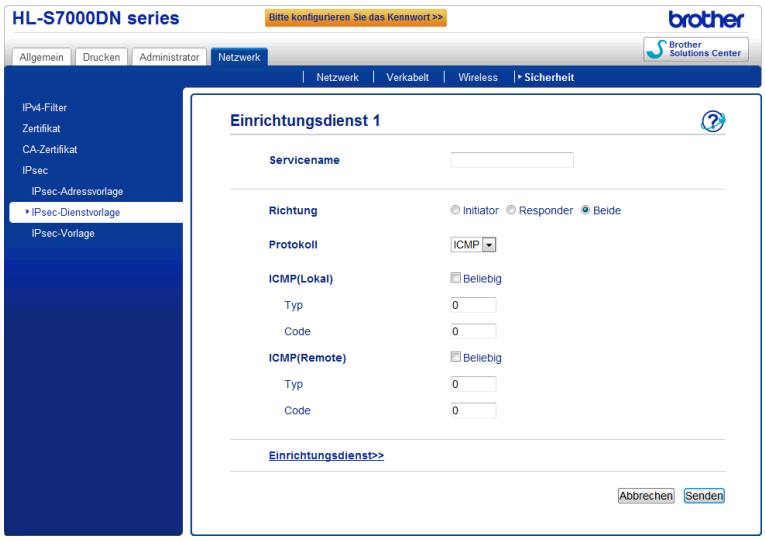
     Klicken Sie auf diese Schaltfläche, um zum Bildschirm **IPsec-Dienstvorlage** zurückzukehren.

2. Klicken Sie auf die Nummer für den **Servicenamen**, den Sie erstellen möchten. Wählen Sie im Bildschirm unten die Dienste aus, die Sie für IPsec verwenden möchten. Die Einstellungsoptionen sind je nach ausgewähltem **Protokoll** unterschiedlich.

(**Protokoll**:**ALLE**)

(**Protokoll**:**TCP** oder **UDP**)

(**Protokoll**: **ICMP**)



■ Servicename

Geben Sie in diesem Feld einen Namen für den Dienst ein. (Maximal 16 Zeichen)

■ Richtung

Geben Sie die Kommunikationsrichtung an. Wählen Sie **Initiator**, **Responder** oder **Beide**.

■ Protokoll

Geben Sie das Protokoll an, das aktiviert wird. Wählen Sie **ALLE**, **TCP**, **UDP** oder **ICMP**. Die Einstellungsoptionen sind je nach ausgewähltem **Protokoll** unterschiedlich.

- Wenn **TCP** oder **UDP** ausgewählt ist, registrieren Sie **Lokaler Port**/**Remote-Port**.
- Wenn **ICMP** ausgewählt ist, registrieren Sie **Typ**/**Code**.

Hinweis

ICMP ist ein Protokoll zum Senden von IP-Fehlermeldungen und IP-Informationsmeldungen. Das Protokoll wird von Computern und Netzwerkgeräten, die über TCP/IP verbunden sind, verwendet, um die gegenseitige Statusüberprüfung auszuführen.

- **Lokaler Port**/**Remote-Port** (Wenn **TCP** oder **UDP** als **Protokoll** ausgewählt ist.)

  Geben Sie die lokale Portnummer ein. Wenn **Einzel** ausgewählt ist, geben Sie eine Portnummer ein. Wenn **Bereich** ausgewählt ist, geben Sie die Anfangsportnummer und dann die Endportnummer ein. Wenn Sie alle Portnummern aktivieren möchten, wählen Sie **Bereich** und geben Sie „1-65535“ ohne die doppelten Anführungszeichen ein.

- **ICMP(Lokal)**/**ICMP(Remote)** (Wenn **ICMP** als **Protokoll** ausgewählt ist.)

  Konfigurieren Sie die ICMP-Einstellungen. Wählen Sie **Beliebig** oder geben Sie den **Typ**/**Code** ein. Einzelheiten zu **Typ**/**Code** finden Sie unter *Anhang A*.

- **Einrichtungsdienst**

  Klicken Sie auf diese Schaltfläche, um zum Bildschirm **Einrichtungsdienst** zurückzukehren.

- **Senden**

  Klicken Sie auf diese Schaltfläche, um die Einstellungen zu registrieren.

Hinweis

Wenn Sie die Einstellungen der aktuell verwendeten Vorlage ändern, wird der IPsec-Einstellungsbildschirm für Web Based Management geschlossen und dann wieder geöffnet.

IPsec-Vorlage

Konfigurieren Sie die IKE/IPsec-Einstellungen. Es können maximal 10 **IPsec-Vorlagen** verwendet werden.

1. Starten Sie Ihren Webbrowser.
2. Geben Sie in Ihren Browser „http://IP-Adresse des Gerätes/“ ein (wobei „IP-Adresse des Gerätes“ für die IP-Adresse des Gerätes steht).
   - Zum Beispiel:

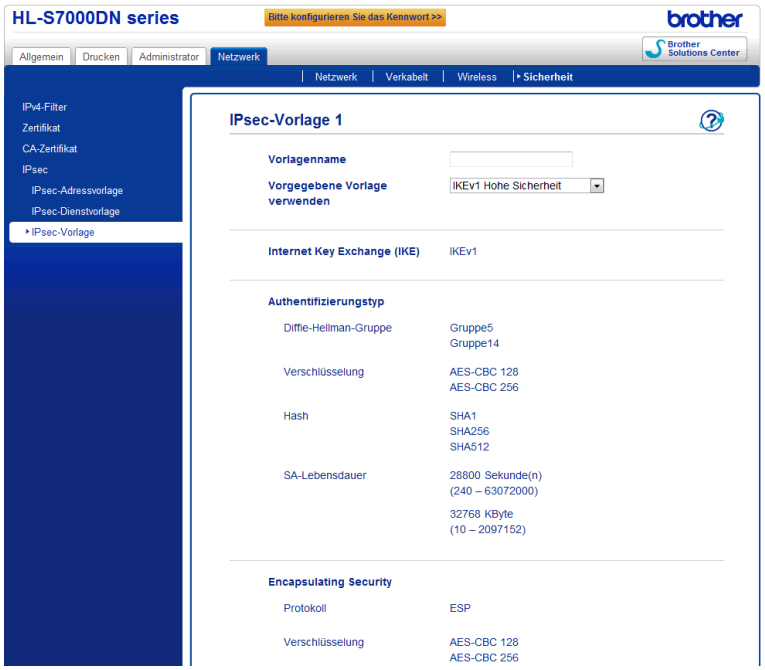
     http://192.168.1.2/
3. Standardmäßig ist kein Kennwort erforderlich. Geben Sie ein Kennwort ein, wenn Sie eines eingerichtet haben, und drücken Sie →.
4. Klicken Sie auf die Registerkarte **Netzwerk**.
5. Klicken Sie auf **Sicherheit**.
6. Klicken Sie auf **IPsec-Vorlage**.
   10 **IPsec-Vorlagen** werden angezeigt. Wenn keine **IPsec-Vorlage** konfiguriert wurde, wird **Nicht konfiguriert** angezeigt.

■ Löschen

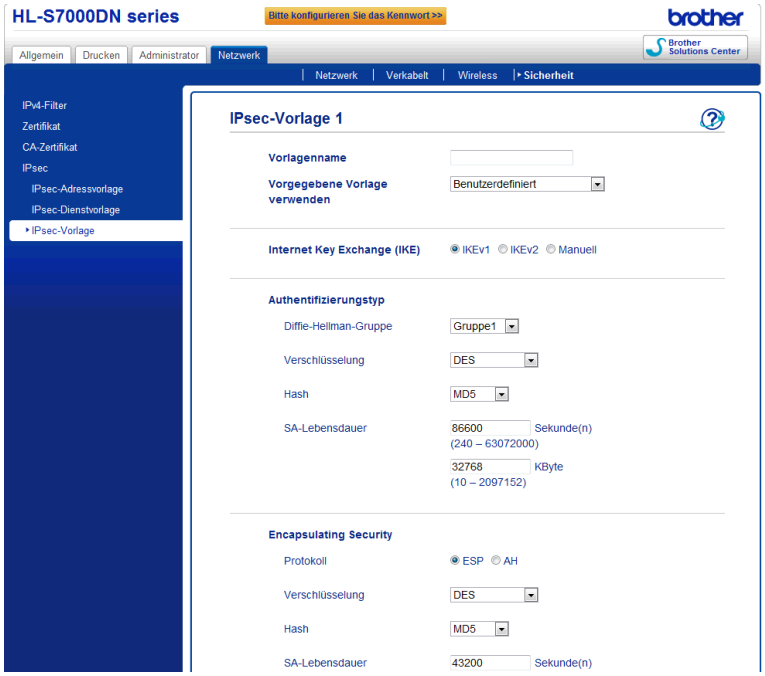
Klicken Sie auf diese Schaltfläche, um die ausgewählte **IPsec-Vorlage** zu löschen. Die aktuell verwendete **IPsec-Vorlage** kann jedoch nicht gelöscht werden.

7 Klicken Sie auf die Nummer für die **IPsec-Vorlage**, die Sie erstellen möchten. Konfigurieren Sie im Bildschirm unten die IPsec-Einstellungen und erstellen Sie die **IPsec-Vorlage**. Die Einstellungsoptionen sind je nach ausgewählter Option **Vorgegebene Vorlage verwenden** und **Internet Key Exchange (IKE)** unterschiedlich.

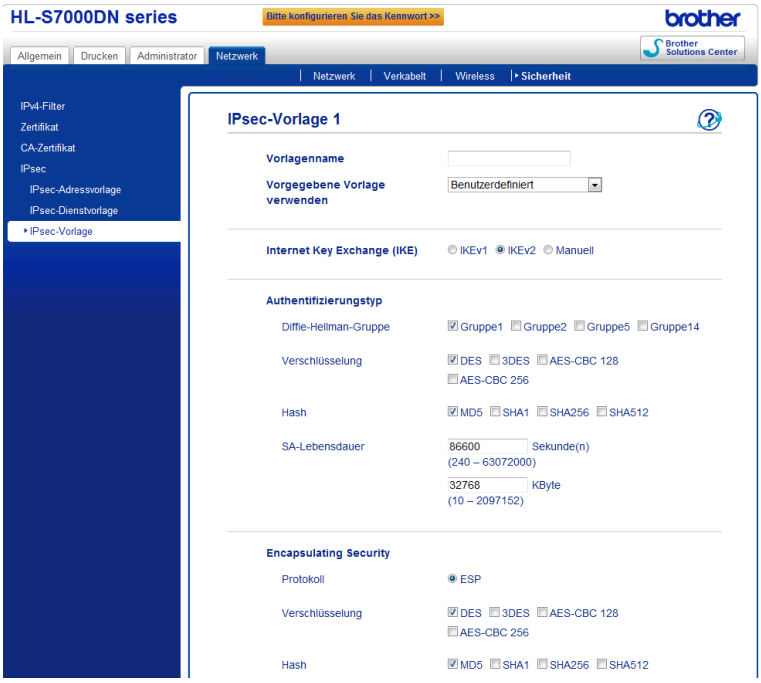
(**IKE**:**Voreinstellung**)



(IKE:IKEv1)



(IKE:IKEv2)



■ Vorlagenname

Geben Sie in diesem Feld einen Namen für die Vorlage ein. (Maximal 16 Zeichen)

Vorgegebene Vorlage verwenden

Wählen Sie **Benutzerdefiniert**, **IKEv1 Hohe Sicherheit**, **IKEv1 Mittlere Sicherheit**, **IKEv2 Hohe Sicherheit** oder **IKEv2 Mittlere Sicherheit**. Die Einstellungsoptionen sind je nach ausgewählter Vorlage unterschiedlich.

Hinweis

Die Standardvorlage ist je nach Auswahl von „Normal“ oder „Aggressiv“ im Aushandlungsmodus auf dem IPsec-Einstellungsbildschirm unterschiedlich. Einzelheiten zum IPsec-Einstellungsbildschirm finden Sie unter *Konfiguration mit Web Based Management (Webbrowser)* ➤➤ Seite 2.

Internet Key Exchange (IKE)

IKE ist ein Kommunikationsprotokoll zum Austauschen von Verschlüsselungsschlüsseln für die verschlüsselte Kommunikation über IPsec. Um die verschlüsselte Kommunikation in diesem Fall einmalig auszuführen, wird der Verschlüsselungsalgorithmus, den IPsec benötigt, festgelegt und die Verschlüsselungsschlüssel werden ausgetauscht. Bei IKE werden die Verschlüsselungsschlüssel mit dem Diffie-Hellman-Schlüsselaustauschverfahren ausgetauscht und verschlüsselte Kommunikation, die auf IKE beschränkt ist, wird ausgeführt.

Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist, wählen Sie **IKEv1**, **IKEv2** oder **Manuell**.

Wenn eine andere Einstellung als **Benutzerdefiniert** ausgewählt ist, wird der unter **Vorgegebene Vorlage verwenden** ausgewählte Authentifizierungstyp angezeigt.

Authentifizierungstyp

Konfiguriert die IKE-Authentifizierung und -Verschlüsselung.

- **Diffie-Hellman-Gruppe**

  Mit diesem Schlüsselaustauschverfahren können geheime Schlüssel über ein ungeschütztes Netzwerk sicher ausgetauscht werden. Das Diffie-Hellman-Schlüsselaustauschverfahren setzt ein Diskreter-Logarithmus-Problem ein, nicht den geheimen Schlüssel, um Informationen, die mit einer Zufallszahl und einem geheimen Schlüssel erzeugt wurden, offen zu senden und zu empfangen.

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **IKEv1** oder **IKEv2** unter **IKE** ausgewählt ist.) Wählen Sie **Gruppe1**, **Gruppe2**, **Gruppe5** oder **Gruppe14**. Wenn **IKEv2** ausgewählt ist, ist eine Mehrfachauswahl möglich.

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **Manuell** unter **IKE** ausgewählt ist.) Die Gruppe wird nicht angezeigt.

  (Wenn eine andere Einstellung als **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Die oben genannte aktivierte Gruppe wird angezeigt.

- **Verschlüsselung**

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **IKEv1** oder **IKEv2** unter **IKE** ausgewählt ist.) Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**. Wenn **IKEv2** ausgewählt ist, ist eine Mehrfachauswahl möglich.

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **Manuell** unter **IKE** ausgewählt ist.) Die Verschlüsselung wird nicht angezeigt.

  (Wenn eine andere Einstellung als **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Die oben genannte aktivierte Verschlüsselung wird angezeigt.

- **Hash**

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **IKEv1** oder **IKEv2** unter **IKE** ausgewählt ist.) Wählen Sie **MD5**, **SHA1**, **SHA256** oder **SHA512**. Wenn **IKEv2** ausgewählt ist, ist eine Mehrfachauswahl möglich.

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **Manuell** unter **IKE** ausgewählt ist.) Der Hash-Algorithmustyp wird nicht angezeigt.

  (Wenn eine andere Einstellung als **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Der oben genannte aktivierte Hash-Algorithmustyp wird angezeigt.

- **SA-Lebensdauer**

  Geben Sie die IKE-SA-Lebensdauer an.

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **IKEv1** oder **IKEv2** unter **IKE** ausgewählt ist.) Geben Sie die Zeit (Sekunden) und die Anzahl der Kilobytes (KB) an.

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **Manuell** unter **IKE** ausgewählt ist.) Die SA-Lebensdauerinformationen werden nicht angezeigt.

  (Wenn eine andere Einstellung als **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Die Zeit (Sekunden) und die Anzahl der Kilobytes (KB) werden angezeigt.

■ **Encapsulating Security**

- **Protokoll**

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Wählen Sie **ESP** oder **AH**. Wenn **IKEv2** unter **IKE** ausgewählt ist, kann nur **ESP** ausgewählt werden.

  (Wenn eine andere Einstellung als **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Das oben genannte aktivierte Protokoll wird angezeigt.

Hinweis

- ESP ist ein Protokoll zur verschlüsselten Kommunikation über IPsec. ESP verschlüsselt die Nutzdaten (übermittelter Inhalt) und fügt zusätzliche Informationen hinzu. Das IP-Paket besteht aus den Kopfdaten und den verschlüsselten Nutzdaten, die nach den Kopfdaten folgen. Zusätzlich zu den verschlüsselten Daten enthält ein IP-Paket auch Informationen zur Verschlüsselungsmethode und zum Verschlüsselungsschlüssel, zu den Authentifizierungsdaten usw.
- AH ist ein Teil des IPsec-Protokolls, der den Sender authentifiziert und Manipulation der Daten verhindert (Vollständigkeit der Daten gewährleistet). Im IP-Paket werden die Daten direkt nach den Kopfdaten eingefügt. Darüber hinaus enthalten die Pakete Hashwerte, die mit einer Gleichung aus dem übermittelten Inhalt berechnet werden, einen geheimen Schlüssel usw., um eine Verfälschung des Senders und die Manipulation der Daten zu verhindern. Im Gegensatz zu ESP wird der übermittelte Inhalt nicht verschlüsselt, sondern die Daten werden in Klartext gesendet und empfangen.

- **Verschlüsselung**

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Wählen Sie **DES**, **3DES**, **AES-CBC 128** oder **AES-CBC 256**. Die Verschlüsselung kann nur ausgewählt werden, wenn **ESP** unter **Protokoll** ausgewählt ist. Wenn **IKEv2** unter **IKE** ausgewählt ist, ist eine Mehrfachauswahl möglich.

(Wenn eine andere Einstellung als **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Die oben genannte aktivierte Verschlüsselung wird angezeigt.

- **Hash**

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **IKEv1** oder **Manuell** unter **IKE** ausgewählt ist.) Wählen Sie **Keine**, **MD5**, **SHA1**, **SHA256** oder **SHA512**. **Keine** kann nur ausgewählt werden, wenn **ESP** unter **Protokoll** ausgewählt ist.

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **IKEv2** unter **IKE** ausgewählt ist.) Wählen Sie **MD5**, **SHA1**, **SHA256** oder **SHA512**. Eine Mehrfachauswahl ist möglich.

  (Wenn eine andere Einstellung als **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Der oben genannte aktivierte Hash-Algorithmustyp wird angezeigt.

- **SA-Lebensdauer**

  Geben Sie die IKE-SA-Lebensdauer an.

  (Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **IKEv1** oder **IKEv2** unter **IKE** ausgewählt ist.) Geben Sie die Zeit (Sekunden) und die Anzahl der Kilobytes (KB) an.

  (Wenn eine andere Einstellung als **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist.) Die Zeit (Sekunden) und die Anzahl der Kilobytes (KB) werden angezeigt.

- **Encapsulation-Modus**

  Wählen Sie **Transport** oder **Tunnel**.

- **IP-Adresse des Remote-Routers**

  Geben Sie die IP-Adresse (IPv4 oder IPv6) des Verbindungsziels an. Eingabe nur, wenn der **Tunnel**-Modus ausgewählt ist.

Hinweis

SA (Security Association) ist ein Verfahren zur verschlüsselten Kommunikation über IPsec oder IPv6, bei dem Informationen ausgetauscht und verwendet werden, wie zum Beispiel die Verschlüsselungsmethode und der Verschlüsselungsschlüssel, um einen sicheren Kommunikationskanal einzurichten, bevor die Kommunikation beginnt. SA kann auch einen virtuellen verschlüsselten Kommunikationskanal verwenden, der bereits eingerichtet wurde. SA für IPsec legt die Verschlüsselungsmethode fest, tauscht die Schlüssel aus und führt die gegenseitige Authentifizierung nach dem IKE-Standardverfahren (Internet Key Exchange) aus. Zusätzlich wird SA regelmäßig aktualisiert.

Perfect Forward Secrecy (PFS)

PFS leitet keine Schlüssel aus Schlüsseln ab, die zuvor für die Verschlüsselung von Daten verwendet wurden. Darüber hinaus wird, wenn ein Schlüssel zur Datenverschlüsselung aus einem Parent-Schlüssel abgeleitet wurde, dieser Parent-Schlüssel nicht zur Ableitung weiterer Schlüssel verwendet. Daher ist der Schaden, selbst wenn ein Schlüssel beschädigt wurde, nur auf die Daten begrenzt, die mit diesem Schlüssel verschlüsselt wurden.

Wählen Sie **Aktiviert** oder **Deaktiviert**. Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **Manuell** unter **IKE** ausgewählt ist, werden die PFS-Informationen nicht angezeigt.

Authentifizierungsmethode

Wählen Sie die Authentifizierungsmethode. Wählen Sie **Pre-Shared Key**, **Zertifikate**, **EAP - MD5** oder **EAP - MS-CHAPv2**.

EAP - MD5 und **EAP - MS-CHAPv2** können nur ausgewählt werden, wenn **IKEv2** unter **IKE** ausgewählt ist. Wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **Manuell** unter **IKE** ausgewählt ist, werden die Informationen zur Authentifizierungsmethode nicht angezeigt.

Pre-Shared Key

Bei Verschlüsselung der Kommunikation wird der Verschlüsselungsschlüssel im Voraus über einen anderen Kanal ausgetauscht und verwendet.

Wenn **Pre-Shared Key** unter **Authentifizierungsmethode** ausgewählt ist, geben Sie den **Pre-Shared Key** ein. (Maximal 32 Zeichen)

- **Lokal ID-Typ/ID**

  Wählen Sie den ID-Typ des Senders und geben Sie die ID ein.

  Wählen Sie **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** als Typ.

  Wenn **Zertifikat** ausgewählt ist, geben Sie den allgemeinen Namen des Zertifikats unter **ID** ein.

- **Remote ID-Typ/ID**

  Wählen Sie den ID-Typ des Empfängers und geben Sie die ID ein.

  Wählen Sie **IPv4-Adresse**, **IPv6-Adresse**, **FQDN**, **E-Mail-Adresse** oder **Zertifikat** als Typ.

  Wenn **Zertifikat** ausgewählt ist, geben Sie den allgemeinen Namen des Zertifikats unter **ID** ein.

Zertifikate

Wenn **Zertifikate** unter **Authentifizierungsmethode** ausgewählt ist, wählen Sie das Zertifikat.

Hinweis

Sie können nur Zertifikate auswählen, die über die **Zertifikat**-Seite von Web Based Management Sicherheitsfunktionen erstellt wurden. Einzelheiten finden Sie im Netzwerkhandbuch: Zertifikate für Gerätesicherheit verwenden.

EAP

EAP ist ein Authentifizierungsprotokoll, das eine Erweiterung von PPP ist. Bei Verwendung von EAP zusammen mit IEEE802.1x wird für jede Benutzerauthentifizierung und für jede Sitzung jeweils ein anderer Schlüssel verwendet.

Die folgenden Einstellungen sind nur erforderlich, wenn **EAP - MD5** oder **EAP - MS-CHAPv2** unter **Authentifizierungsmethode** ausgewählt ist.

- **Modus**

  Wählen Sie **Server-Modus** oder **Client-Modus**.

- **Zertifikat**

  Wählen Sie das Zertifikat aus.

- **Benutzername**

  Geben Sie den Benutzernamen ein. (Maximal 32 Zeichen)

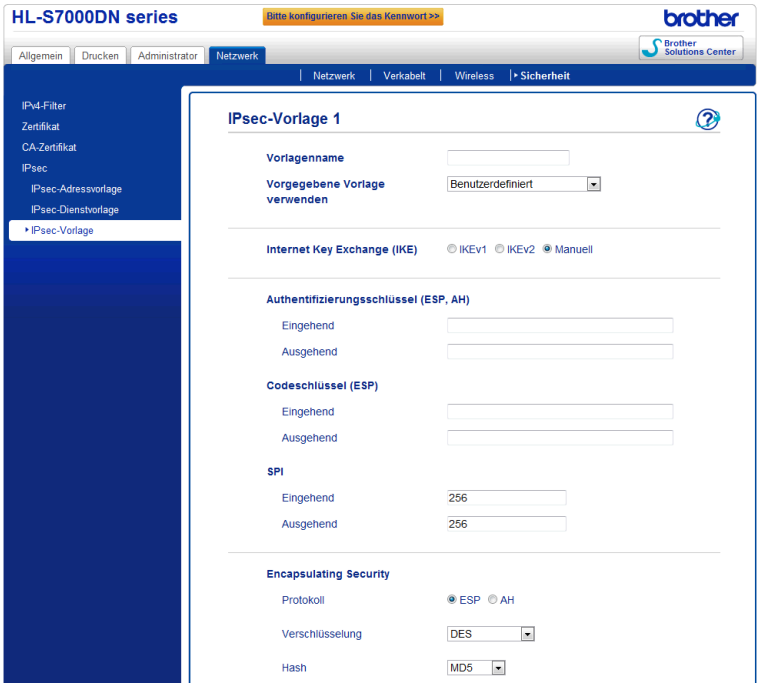
- **Kennwort**

  Geben Sie das Kennwort ein. Das Kennwort muss zur Bestätigung zwei Mal eingegeben werden. (Maximal 32 Zeichen)

- **Zertifikat>>**

  Klicken Sie auf diese Schaltfläche, um auf den Bildschirm für die Zertifikateinstellungen zuzugreifen.

(**IKE**:**Manuell**)



■ Authentifizierungsschlüssel (ESP, AH)

Geben Sie den Schlüssel an, der für die Authentifizierung verwendet werden soll. Geben Sie die Werte **Eingehend**/**Ausgehend** ein.

Diese Einstellungen sind erforderlich, wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist, **Manuell** unter **IKE** ausgewählt ist und eine andere Einstellung als **Keine** für **Hash** unter **Encapsulating Security** ausgewählt ist.

Hinweis

Die Anzahl der Zeichen, die Sie festlegen können, ist abhängig von Ihrer Einstellung für Hash unter Encapsulating Security.

Wenn die Länge des angegebenen Authentifizierungsschlüssels vom ausgewählten Hashalgorithmus abweicht, wird ein Fehler angezeigt.

- **MD5**: 128 Bits (16 Bytes)
- **SHA1**: 160 Bits (20 Bytes)
- **SHA256**: 256 Bits (32 Bytes)
- **SHA512**: 512 Bits (64 Bytes)

Wenn Sie den Schlüssel in ASCII-Code angeben, schließen Sie die Zeichen in doppelte Anführungszeichen ein.

■ **Codeschlüssel (ESP)**

Geben Sie den Schlüssel an, der für die Verschlüsselung verwendet werden soll. Geben Sie die Werte **Eingehend**/**Ausgehend** ein.

Diese Einstellungen sind erforderlich, wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist, **Manuell** unter **IKE** ausgewählt ist und **ESP** für **Protokoll** unter **Encapsulating Security** ausgewählt ist.

Hinweis

Die Anzahl der Zeichen, die Sie festlegen können, ist abhängig von Ihrer Einstellung für Verschlüsselung unter Encapsulating Security.

Wenn die Länge des angegebenen Codeschlüssels vom ausgewählten Verschlüsselungsalgorithmus abweicht, wird ein Fehler angezeigt.

- **DES**: 64 Bits (8 Bytes)
- **3DES**: 192 Bits (24 Bytes)
- **AES-CBC 128**: 128 Bit (16 Byte)
- **AES-CBC 256**: 256 Bit (32 Byte)

Wenn Sie den Schlüssel in ASCII-Code angeben, schließen Sie die Zeichen in doppelte Anführungszeichen ein.

■ **SPI**

Diese Parameter werden zur Kennzeichnung der Sicherheitsinformationen verwendet. Im Allgemeinen verfügt ein Host über mehrere SAs (Security Associations) für verschiedene Typen der IPsec-Kommunikation. Daher muss das geltende SA gekennzeichnet werden, wenn ein IPsec-Paket empfangen wird. Der SPI-Parameter, der das SA kennzeichnet, ist in den AH- (Authentication Header) und ESP-Kopfdaten (Encapsulating Security Payload) enthalten.

Diese Einstellungen sind erforderlich, wenn **Benutzerdefiniert** unter **Vorgegebene Vorlage verwenden** ausgewählt ist und **Manuell** unter **IKE** ausgewählt ist.

Geben Sie die Werte **Eingehend**/**Ausgehend** ein. (3-10 Zeichen)

■ **Senden**

Klicken Sie auf diese Schaltfläche, um die Einstellungen zu registrieren.

Hinweis

Wenn Sie die Einstellungen der aktuell verwendeten Vorlage ändern, wird der IPsec-Einstellungsbildschirm für Web Based Management geschlossen und dann wieder geöffnet.

A Anhang A

Dienstvorlagen

Sie können die folgenden Dienste durch Auswählen der Vorlagen verwenden.

1 Alle Dienste

IPsec wird für alle Protokolle verwendet.

2 Druckdienste

Servicename	Protokoll	Lokaler Port	Remote-Port
IPP	TCP	631	Beliebig
IPPS	TCP	443	Beliebig
FTP (Steuerung)	TCP	21	Beliebig
FTP (Daten)	TCP	20	Beliebig
P9100	TCP	9100	Beliebig
Webdienst	TCP	80	Beliebig
LPD	TCP	515	Beliebig

3 Verwaltungsdienste

Servicename	Protokoll	Lokaler Port	Remote-Port
SNMP	UDP	161	Beliebig
Telnet	TCP	23	Beliebig
HTTP	TCP	80	Beliebig
HTTPS	TCP	443	Beliebig
Remote Setup	TCP	54922	Beliebig

4 Drucker/MFC-Dienste [1]

Servicename	Protokoll	Lokaler Port	Remote-Port
CIFS	TCP	Beliebig	445
SMB	TCP	Beliebig	139
LDAP	TCP	Beliebig	389
SMTP	TCP	Beliebig	25
POP3	TCP	Beliebig	110
SNTP	UDP	Beliebig	123
Netzwerk-Scan	TCP	54921	Beliebig
PC-FAX	TCP	54923	Beliebig

Servicename	Protokoll	Lokaler Port	Remote-Port
Kerberos (TCP)	TCP	Beliebig	88
Kerberos (UDP)	UDP	Beliebig	88

[1] Wenn Sie Kerberos-Authentifizierung verwenden möchten, müssen Sie die DNS-Einstellungen entsprechend aktivieren.

Typ/Code

Die folgenden Typen und Codes werden unterstützt, wenn **ICMP** unter **Protokoll** ausgewählt ist.

IPv4		
Typ		**Unterstützte Codes**
0	Echo Reply	0
3	Destination Unreachable	0,1,2,3,4,5,6,7,8,9,10,11,12
4	Source Quench	0
5	Redirect	0,1,2,3
8	Echo Request	0
9	Router Advertisement	0
10	Router Solicitations	0

IPv4-Code

0,1,2,3,4,5,6,7,8,9,10,11,12

IPv6		
Typ		**Unterstützte Codes**
1	Destination Unreachable	0,1,2,3,4
3	Time Exceeded	0,1
4	Parameter Problem	0,1,2
128	Echo Request	0
129	Echo Reply	0
133	Router Solicitation	0
134	Router Advertisement	0
135	Neighbor Solicitation	0
136	Neighbor Advertisement	0
137	Redirect	0

IPv6-Code

0,1,2,3,4

Besuchen Sie uns im Internet
http://www.brother.com/

Brother Earth

www.brotherearth.com