


Handleiding IPsec instellen



Definities van opmerkingen

Overal in deze gebruikershandleiding wordt de volgende aanduiding gebruikt:

	Opmerking	Opmerkingen leggen uit wat u in een bepaalde situatie moet doen of hoe de bewerking met andere functies werkt.
---	-----------	--

Handelsmerken

Het Brother-logo is een gedeponeerd handelsmerk van Brother Industries, Ltd.

Alle andere merknamen en productnamen van bedrijven vermeld op Brother-producten, in gerelateerde documentatie en ander materiaal, zijn handelsmerken of wettig gedeponeerde handelsmerken van de desbetreffende bedrijven.

©2012 Brother Industries, Ltd. Alle rechten voorbehouden.

Inhoudsopgave

1	Inleiding	1
	Overzicht	1
	Configuratie met behulp van Beheer via een webbrowser	2
2	IPsec-instellingen	5
	Adressjabloon	5
	Servicesjabloon	7
	IPsec-servicesjabloon	7
	Service configureren	8
	IPsec-sjabloon	11
A	Appendix A	20
	Servicesjablonen	20
	Type/Code	21

Overzicht

IPsec (Internet Protocol Security) is een beveiligingsprotocol dat gebruikmaakt van een optionele IP-functie om manipulatie te voorkomen en de vertrouwelijkheid van de gegevens die als IP-pakketjes worden verzonden te garanderen. IPsec versleutelt gegevens die via het netwerk worden verzonden, zoals afdrukgegevens die van computers naar een printer worden verzonden. Omdat de gegevens op de netwerklaag worden versleuteld, gebruiken toepassingen die een protocol op een hoger niveau gebruiken IPsec, zelfs als de gebruiker hier geen weet van heeft.

IPsec ondersteunt de volgende functies:

■ Verzendingen via IPsec

Op basis van de IPsec-instellingen ontvangt en verstuurt de netwerkcomputer via IPsec gegevens van en naar het opgegeven apparaat. Wanneer de apparaten via IPsec met elkaar beginnen te communiceren, worden eerst via IKE (Internet Key Exchange) sleutels uitgewisseld en worden de versleutelde gegevens vervolgens met behulp van deze sleutels verzonden.

IPsec heeft twee modi: de transportmodus en de tunnelmodus. De transportmodus wordt voornamelijk voor communicatie tussen apparaten gebruikt en de tunnelmodus wordt in omgevingen zoals een VPN (Virtual Private Network) gebruikt.

Opmerking

- Voor verzending via IPsec is het volgende nodig:
 - Een op het netwerk aangesloten computer die via IPsec kan communiceren.
 - De printer of MFC is geconfigureerd voor communicatie via IPsec.
 - De op de printer of MFC aangesloten computer is geconfigureerd voor IPsec-verbindingen.
 - IPsec ondersteunt geen groepsverzending of multicastcommunicatie.
-

■ IPsec-instellingen

De instellingen die nodig zijn voor verbindingen via IPsec. Deze instellingen kunnen worden geconfigureerd via Beheer via een webbrowser. (Zie *Configuratie met behulp van Beheer via een webbrowser* >> pagina 2.)


Opmerking

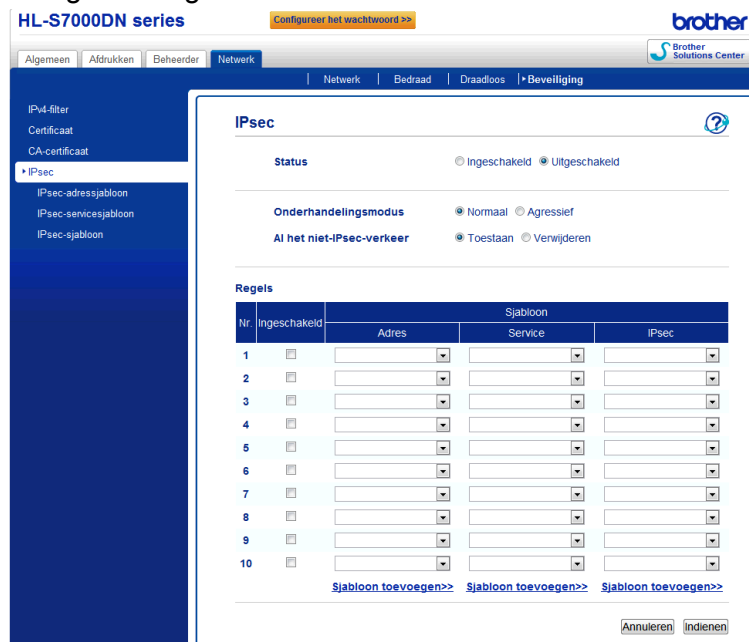
Om de IPsec-instellingen te configureren, dient een voor de browser geschikte computer op het netwerk te zijn aangesloten.

Configuratie met behulp van Beheer via een webbrowser

Gebruik het IPsec-instellingenschermb van Beheer via een webbrowser om de IPsec-verbindingsvoorwaarden op te geven.

De IPsec-verbindingsvoorwaarden bestaan uit drie **Sjabloon**-typen: **Adres**, **Service** en **IPsec**. U kunt maximaal 10 verbindingsvoorwaarden configureren.


- 1 Start uw webbrowser.
- 2 Typ "http://IP-adres van machine/" in uw browser (hierbij staat "IP-adres van machine" voor het IP-adres van de machine).
 - Bijvoorbeeld:
http://192.168.1.2/
- 3 Standaard hoeft geen wachtwoord te worden ingevoerd. Voer een wachtwoord in als u dit hebt ingesteld en druk op .
- 4 Klik op het tabblad **Netwerk**.
- 5 Klik op **Beveiliging**.
- 6 Klik op **IPsec**.
- 7 U kunt de IPsec-instellingen configureren in het onderstaande scherm.



HL-S7000DN series Configureer het wachtwoord >> **brother**
 Brother Solutions Center

Algemeen | Afdrukken | Beheerder | **Netwerk** | Netwerk | Bedraad | Draadloos | Beveiliging

IPv4-filter
 Certificaat
 CA-certificaat
 *IPsec
 IPsec-adressjabloon
 IPsec-servicesjabloon
 IPsec-sjabloon

IPsec 

Status Ingeschakeld Uitgeschakeld

Onderhandelingsmodus Normaal Agressief

Al het niet-IPsec-verkeer Toestaan Verwijderen

Regels

Nr.	Ingeschakeld	Sjabloon		
		Adres	Service	IPsec
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

[Sjabloon toevoegen>>](#) [Sjabloon toevoegen>>](#) [Sjabloon toevoegen>>](#)

- **Status**
Selecteer **Ingeschakeld** of **Uitgeschakeld** bij IPsec.
- **Onderhandelingsmodus**
Selecteer de modus voor IKE Phase 1.

- **Normaal**: de hoofdmodus wordt gebruikt.
- **Agressief**: de agressieve modus wordt gebruikt.

 **Opmerking**

IKE is een protocol dat wordt gebruikt voor het uitwisselen van versleutelingssleutels om versleutelde communicatie via IPsec mogelijk te maken.

Als de modus **Normaal** is ingeschakeld, is de verwerkingssnelheid laag, maar het beveiligingsniveau hoog. Als de modus **Agressief** is geselecteerd, is de verwerkingssnelheid sneller dan wanneer de modus **Normaal** is geselecteerd, maar het beveiligingsniveau is dan laag.

■ Al het niet-IPsec-verkeer

Selecteer de actie die voor niet-IPsec-pakketten moet worden genomen.

- **Toestaan**: alle pakketten mogen worden ontvangen.
- **Verwijderen**: niet-IPsec-pakketten worden geweigerd.

 **Opmerking**

Bij gebruik van Webservices moet u **Toestaan** selecteren voor **Al het niet-IPsec-verkeer**. Als **Verwijderen** is geselecteerd, kunnen Webservices niet worden gebruikt.

■ Regels

U kunt maximaal 10 IPsec-verbindingvoorwaarden (sjabloonset) configureren.

■ Ingeschakeld

Wanneer dit selectievakje is ingeschakeld, wordt de sjabloonset voor dat nummer ingeschakeld.

 **Opmerking**

Wanneer meerdere selectievakjes zijn ingeschakeld, krijgen de selectievakjes met de laagste nummers voorrang als de instellingen voor de geselecteerde selectievakjes met elkaar conflicteren.

■ Sjabloon - Adres

Selecteer het **Adressjabloon** dat voor de IPsec-verbindingvoorwaarden moet worden gebruikt.

Om een **Adressjabloon** toe te voegen, klikt u op **Sjabloon toevoegen**. (Zie *Adressjabloon* >> pagina 5.)

■ Sjabloon - Service

Selecteer het **Servicesjabloon** dat voor de IPsec-verbindingvoorwaarden wordt gebruikt.

Om een **Servicesjabloon** toe te voegen, klikt u op **Sjabloon toevoegen**. (Zie *Servicesjabloon* >> pagina 7.)

 **Opmerking**

Als u gebruik wilt maken van DNS voor de naamresolutie bij gebruik van servicesjabloon 2, 3 of 4 in *Appendix A*, moeten de DNS-instellingen afzonderlijk worden geconfigureerd.

■ Sjabloon - IPsec

Selecteer het **IPsec-sjabloon** dat voor de IPsec-verbindingvoorwaarden wordt gebruikt.

Om een **IPsec-sjabloon** toe te voegen, klikt u op **Sjabloon toevoegen**. (Zie *IPsec-sjabloon* >> pagina 11.)

■ **Indienen**

Klik op deze knop om de instellingen te registreren. Als de computer na het wijzigen van de instellingen opnieuw moet worden opgestart, verschijnt hiervoor een bevestigingsscherm nadat op deze knop wordt geklikt.



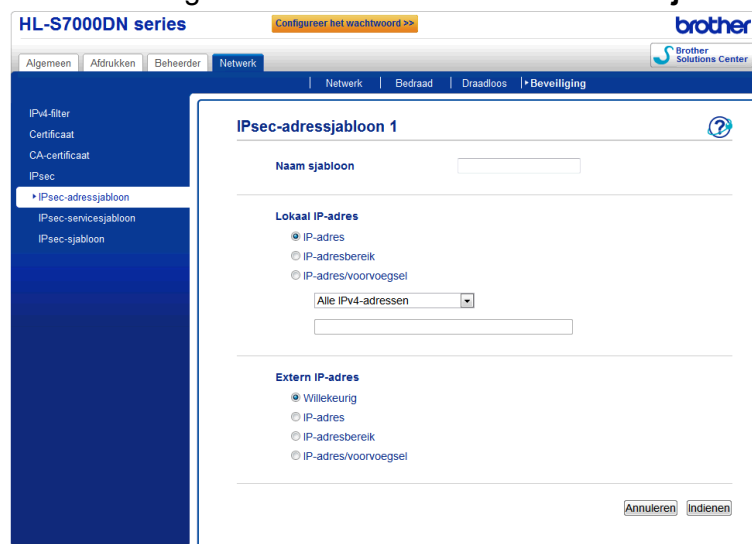
Opmerking

Als u het selectievakje **Ingeschakeld** inschakelt en op **Indienen** klikt, verschijnt een foutmelding als een van de opties voor het geselecteerde sjabloon niet is opgegeven.

Adressjabloon

Geef de IP-adressen op die voor de IPsec-verbingsvoorwaarden moeten worden gebruikt. Er kunnen maximaal 10 **Adressjablonen** worden gebruikt.

- 1 Start uw webbrowser.
- 2 Typ "http://IP-adres van machine/" in uw browser (hierbij staat "IP-adres van machine" voor het IP-adres van de machine).
 - Bijvoorbeeld:
http://192.168.1.2/
- 3 Standaard hoeft geen wachtwoord te worden ingevoerd. Voer een wachtwoord in als u dit hebt ingesteld en druk op .
- 4 Klik op het tabblad **Netwerk**.
- 5 Klik op **Beveiliging**.
- 6 Klik op **IPsec-adressjabloon**.
10 **Adressjablonen** worden weergegeven. Als het **Adressjabloon** niet is geconfigureerd, wordt **Niet geconfigureerd** weergegeven.
 - **Verwijderen**
Klik op deze knop om het geselecteerde **Adressjabloon** te verwijderen. Het huidige **Adressjabloon** kan echter niet worden verwijderd.
- 7 Klik op het nummer van het **Adressjabloon** dat u wilt aanmaken. Geef in het onderstaande venster het IP-adres op dat u voor IPsec wilt gebruiken en maak het **IPsec-adressjabloon** aan.



The screenshot shows the Brother HL-S7000DN series web interface. The top navigation bar includes 'Algemeen', 'Afdrukken', 'Beheerder', 'Netwerk', 'Bedraad', 'Draadloos', and 'Beveiliging'. The 'Beveiliging' tab is active, and the left sidebar shows 'IPsec' > 'IPsec-adressjabloon' selected. The main content area is titled 'IPsec-adressjabloon 1' and contains the following fields:

- Naam sjabloon**: A text input field.
- Lokaal IP-adres**:
 - IP-adres
 - IP-adresbereik
 - IP-adres/voorvoegsel
 - A dropdown menu labeled 'Alle IPv4-adressen' with a search input field below it.
- Extern IP-adres**:
 - Willekeurig
 - IP-adres
 - IP-adresbereik
 - IP-adres/voorvoegsel

At the bottom right of the form are two buttons: 'Annuleren' and 'Indienen'.

■ Naam sjabloon

Voer in dit veld een naam voor het sjabloon in. (Maximaal 16 tekens)

■ Lokaal IP-adres

Geef hier de IP-adresvoorwaarden van de afzender op.

• IP-adres

Geef het IP-adres op. Selecteer **Alle IPv4-adressen**, **Alle IPv6-adressen**, **Alle Link-local IPv6-adressen** of **Aangepast**.

Als u **Aangepast** selecteert, voert u het opgegeven IP-adres (IPv4 of IPv6) in het tekstveld in.

• IP-adresbereik

Geef het eerste en laatste IP-adres van het IP-adresbereik op. Als het eerste en laatste IP-adres niet worden gestandaardiseerd tot IPv4 of IPv6, of als het laatste IP-adres kleiner is dan het eerste, treedt een fout op.

• IP-adres/voorvoegsel

Geef het IP-adres op met een voorvoegsel.

Bijvoorbeeld: 192.168.1.1/24

Omdat het voorvoegsel wordt opgegeven in de vorm van een 24-bits subnetmasker (255.255.255.0) voor 192.168.1.1, zijn de adressen 192.168.1.xx geldig.

■ Extern IP-adres

Geef de IP-adresvoorwaarden van de ontvanger op.

• Willekeurig

Als u **Willekeurig** selecteert, worden alle IP-adressen geactiveerd.

• IP-adres

Geef het opgegeven IP-adres (IPv4 of IPv6) in het tekstveld op.

• IP-adresbereik

Geef het eerste en laatste IP-adres van het IP-adresbereik op. Als het eerste en laatste IP-adres niet worden gestandaardiseerd tot IPv4 of IPv6, of als het laatste IP-adres kleiner is dan het eerste, treedt een fout op.

• IP-adres/voorvoegsel

Geef het IP-adres op met een voorvoegsel.

Bijvoorbeeld: 192.168.1.1/24

Omdat het voorvoegsel wordt opgegeven in de vorm van een 24-bits subnetmasker (255.255.255.0) voor 192.168.1.1, zijn de adressen 192.168.1.xx geldig.

■ Indienen

Klik op deze knop om de instellingen te registreren.



Opmerking

Als u de instellingen van het huidige sjabloon wijzigt, wordt het IP-instellingenschermb van Beheer via een webbrowser gesloten en weer geopend.

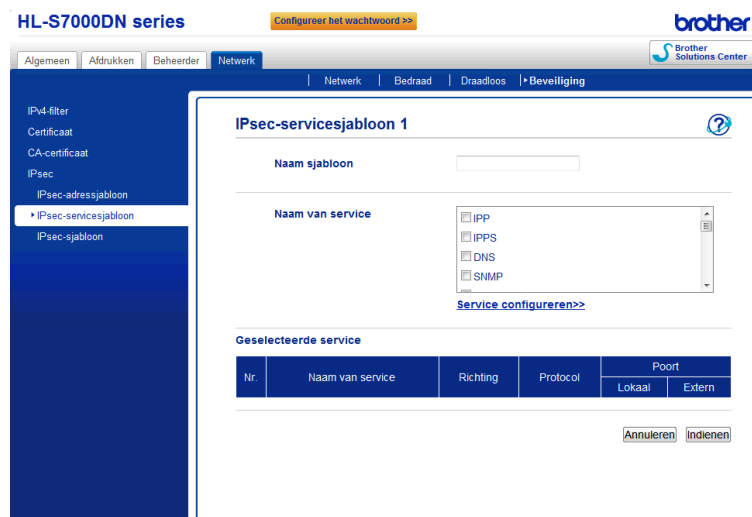
Servicesjabloon

IPsec-servicesjabloon

Geef het protocol en het poortnummer op die voor IPsec-verbindingen moeten worden gebruikt. Er kunnen maximaal 10 **Servicesjablonen** worden gebruikt.

2

- 1 Start uw webbrowser.
- 2 Typ "http://IP-adres van machine/" in uw browser (hierbij staat "IP-adres van machine" voor het IP-adres van de machine).
 - Bijvoorbeeld:
http://192.168.1.2/
- 3 Standaard hoeft geen wachtwoord te worden ingevoerd. Voer een wachtwoord in als u dit hebt ingesteld en druk op .
- 4 Klik op het tabblad **Netwerk**.
- 5 Klik op **Beveiliging**.
- 6 Klik op **IPsec-servicesjabloon**.
10 **Servicesjablonen** worden weergegeven. Als het **Servicesjabloon** niet is geconfigureerd, wordt **Niet geconfigureerd** weergegeven.
 - **Verwijderen**
Klik op deze knop om het geselecteerde **Servicesjabloon** te verwijderen. Het huidige **Servicesjabloon** kan echter niet worden verwijderd.
- 7 Klik op het nummer van het **Servicesjabloon** dat u wilt aanmaken. Geef in het onderstaande scherm de services op die u voor IPsec wilt gebruiken en maak het **IPsec-servicesjabloon** aan. Als u daarnaast eigen services wilt aanmaken, klikt u op **Service configureren**. (Zie *Service configureren* >> pagina 8.)



The screenshot shows the Brother HL-S7000DN series web interface. The top navigation bar includes 'Algemeen', 'Afdrukken', 'Beheerder', 'Netwerk', and 'Beveiliging'. The 'Beveiliging' section is expanded to show 'IPsec-servicesjabloon'. The main content area is titled 'IPsec-servicesjabloon 1' and contains the following fields and elements:

- Naam sjabloon:** A text input field.
- Naam van service:** A list box containing checkboxes for IPP, IPSPS, DNS, and SNMP. Below the list box is a link labeled 'Service configureren>>'.
- Geselecteerde service:** A table with columns for 'Nr.', 'Naam van service', 'Richting', 'Protocol', and 'Poort'. The 'Poort' column is further divided into 'Lokaal' and 'Extern'.
- At the bottom right of the table are buttons for 'Annuleren' and 'Indienen'.

■ Naam sjabloon

Voer in dit veld een naam voor het sjabloon in. (Maximaal 16 tekens)

■ Naam van service

De namen van standaardservices en eerder aangemaakte services worden weergegeven. Selecteer de services die u aan het sjabloon wilt toevoegen.

■ Service configureren

Klik op **Service configureren** om het sjabloon te configureren door services toe te voegen. (Zie *Service configureren* >> pagina 8.)

■ Geselecteerde service

De service-informatie (**Naam van service**, **Richting**, **Protocol** en **Poort**) die bij **Naam van service** is geselecteerd, wordt weergegeven.



Opmerking

- U kunt maximaal 32 services per keer toevoegen.
- Zie *Appendix A* voor meer informatie over de protocollen die u bij **IPsec-servicesjabloon** kunt opgeven.

■ Indienen

Klik op deze knop om de instellingen te registreren.



Opmerking

Als u de instellingen van het huidige sjabloon wijzigt, wordt het IP-instellingenschermb van Beheer via een webbrowser gesloten en weer geopend.

Service configureren

Maak een nieuwe service aan.

- 1 Klik in het scherm **IPsec-servicesjabloon** op **Service configureren**. 60 **Namen van service** worden weergegeven. Als **Naam van service** niet is geconfigureerd, wordt **Niet geconfigureerd** weergegeven.

■ Verwijderen

Klik op deze knop om de geselecteerde **Naam van service** te verwijderen. De huidige **Naam van service** kan echter niet worden verwijderd.

■ IPsec-servicesjabloon

Klik op deze knop om terug te keren naar het scherm **IPsec-servicesjabloon**.

- 2 Klik op het nummer van de **Naam van service** die u wilt aanmaken. Selecteer in het onderstaande scherm de services die u voor IPsec wilt gebruiken. De instellingsopties variëren afhankelijk van het geselecteerde **Protocol**.

(Protocol:ALLE)

The screenshot shows the Brother HL-S7000DN series web interface. The top navigation bar includes 'Algemeen', 'Afdrukken', 'Beheerder', and 'Netwerk'. The 'Netwerk' tab is active, with sub-tabs for 'Netwerk', 'Bedraad', 'Draadloos', and 'Beveiliging'. The left sidebar lists various configuration options, with 'IPsec-servicesjabloon' selected. The main content area is titled 'Service configureren 1' and contains the following fields:

- Naam van service:** An empty text input field.
- Richting:** Radio buttons for 'Initiator', 'Responder', and 'Beide', with 'Beide' selected.
- Protocol:** A dropdown menu set to 'ALLE'.
- Buttons:** 'Service configureren>>', 'Annuleren', and 'Indienen'.

(Protocol:TCP of UDP)

The screenshot shows the Brother HL-S7000DN series web interface. The top navigation bar includes 'Algemeen', 'Afdrukken', 'Beheerder', and 'Netwerk'. The 'Netwerk' tab is active, with sub-tabs for 'Netwerk', 'Bedraad', 'Draadloos', and 'Beveiliging'. The left sidebar lists various configuration options, with 'IPsec-servicesjabloon' selected. The main content area is titled 'Service configureren 1' and contains the following fields:

- Naam van service:** An empty text input field.
- Richting:** Radio buttons for 'Initiator', 'Responder', and 'Beide', with 'Beide' selected.
- Protocol:** A dropdown menu set to 'TCP'.
- Lokale poort:** Radio buttons for 'Eén' and 'Bereik', with 'Bereik' selected. Below it is a range input field showing '1' and '65535'.
- Externe poort:** Radio buttons for 'Eén' and 'Bereik', with 'Bereik' selected. Below it is a range input field showing '1' and '65535'.
- Buttons:** 'Service configureren>>', 'Annuleren', and 'Indienen'.

(Protocol: ICMP)

■ **Naam van service**

Voer in dit veld een naam voor de service in. (Maximaal 16 tekens)

■ **Richting**

Geef de communicatierichting op. Selecteer **Initiator**, **Responder** of **Beide**.

■ **Protocol**

Geef het protocol op dat is ingeschakeld. Selecteer **ALLE**, **TCP**, **UDP** of **ICMP**. De instellingsopties variëren afhankelijk van het geselecteerde **Protocol**.

- Als **TCP** of **UDP** is geselecteerd, registreert u de **Lokale poort** en **Externe poort**.
- Als **ICMP** is geselecteerd, registreert u het **Type** en de **Code**.

 **Opmerking**

ICMP is een protocol dat wordt gebruikt om IP-foutmeldingen en controlemeldingen te versturen. Dit protocol wordt door computers en netwerkapparaten die via TCP/IP zijn aangesloten gebruikt om wederzijdse statusinformatie te verwerken.

■ **Lokale poort/Externe poort** (Als **TCP** of **UDP** bij **Protocol** is geselecteerd.)

Voer het lokale poortnummer in. Als **Eén** is geselecteerd, voert u één poortnummer in. Als **Bereik** is geselecteerd, voert u het eerste poortnummer en vervolgens het laatste poortnummer in. Als u alle poortnummers wilt inschakelen, selecteert u **Bereik** en voert u "1-65535" zonder de dubbele aanhalingstekens in.

■ **ICMP(Lokaal)/ICMP(Extern)** (Als **ICMP** bij **Protocol** is geselecteerd.)

Configureer de ICMP-instellingen. Selecteer **Willekeurig** of voer het **Type** en de **Code** in. Zie *Appendix A* voor meer informatie over het **Type** en de **Code**.

■ **Service configureren**

Klik op deze knop om terug te keren naar het scherm **Service configureren**.

■ **Indienen**

Klik op deze knop om de instellingen te registreren.




Opmerking

Als u de instellingen van het huidige sjabloon wijzigt, wordt het IP-instellingenschermb van Beheer via een webbrowser gesloten en weer geopend.

IPsec-sjabloon

Configureer de IKE/IPsec-instellingen. Er kunnen maximaal 10 **IPsec-sjablonen** worden gebruikt.

- 1 Start uw webbrowser.
- 2 Typ "http://IP-adres van machine/" in uw browser (hierbij staat "IP-adres van machine" voor het IP-adres van de machine).
 - Bijvoorbeeld:
http://192.168.1.2/
- 3 Standaard hoeft geen wachtwoord te worden ingevoerd. Voer een wachtwoord in als u dit hebt ingesteld en druk op .
- 4 Klik op het tabblad **Netwerk**.
- 5 Klik op **Beveiliging**.
- 6 Klik op **IPsec-sjabloon**.
10 **IPsec-sjablonen** worden weergegeven. Als het **IPsec-sjabloon** niet is geconfigureerd, wordt **Niet geconfigureerd** weergegeven.
 - **Verwijderen**
Klik op deze knop om het geselecteerde **IPsec-sjabloon** te verwijderen. Het huidige **IPsec-sjabloon** kan echter niet worden verwijderd.

- 7 Klik op het nummer van het **IPsec-sjabloon** dat u wilt aanmaken. Configureer de IPsec-instellingen in het onderstaande scherm en maak het **IPsec-sjabloon** aan. Welke opties u kunt instellen, is afhankelijk van of u **Voorgeconfigureerde sjabloon gebruiken** of **Internet Key Exchange (IKE)** hebt geselecteerd.

(IKE: vooraf ingesteld)

The screenshot shows the configuration page for 'IPsec-sjabloon 1'. The 'Voorgeconfigureerde sjabloon gebruiken' dropdown is set to 'Streng beveiliging IKEv1'. The 'Internet Key Exchange (IKE)' is set to 'IKEv1'. Under 'Verificatietype', the Diffie-Hellman group is 'Groep 5' and 'Groep 14', encryption is 'AES-CBC 128' and 'AES-CBC 256', hash is 'SHA1', 'SHA256', and 'SHA512', lifetime is '28800 seconde(n) (240 - 63072000)', and key size is '32768 Kilobyte (10 - 2097152)'. Under 'Encapsulation-beveiliging', the protocol is 'ESP' and encryption is 'AES-CBC 128' and 'AES-CBC 256'.

(IKE:IKEv1)

The screenshot shows the configuration page for 'IPsec-sjabloon 1'. The 'Voorgeconfigureerde sjabloon gebruiken' dropdown is set to 'Aangepast'. The 'Internet Key Exchange (IKE)' has radio buttons for 'IKEv1' (selected), 'IKEv2', and 'Handmatig'. Under 'Verificatietype', the Diffie-Hellman group is 'Groep 1', encryption is 'DES', hash is 'MD5', lifetime is '86600 seconde(n) (240 - 63072000)', and key size is '32768 Kilobyte (10 - 2097152)'. The 'Encapsulation-beveiliging' section is visible but not fully detailed.

(IKE:IKEv2)

The screenshot shows the configuration page for an IPsec template. The main content area is titled 'IPsec-sjabloon 1'. It contains several sections:

- Naam sjabloon:** A text input field.
- Voorgeconfigureerde sjabloon gebruiken:** A dropdown menu currently set to 'Aangepast'.
- Internet Key Exchange (IKE):** Radio buttons for 'IKEv1', 'IKEv2' (selected), and 'Handmatig'.
- Verificatietype:**
 - Diffie-Hellman-groep:** Checkboxes for 'Groep 1' (checked), 'Groep 2', 'Groep 5', and 'Groep 14'.
 - Versleuteling:** Checkboxes for 'DES' (checked), '3DES', 'AES-CBC 128', and 'AES-CBC 256'.
 - Hekje:** Checkboxes for 'MD5' (checked), 'SHA1', 'SHA256', and 'SHA512'.
 - Levensduur beveiligingskoppeling:** Input fields for '86600' seconds and '32768' kilobytes.
- Encapsulation-beveiliging:**
 - Protocol:** Radio buttons for 'ESP' (selected) and 'AH'.
 - Versleuteling:** Checkboxes for 'DES' (checked), '3DES', 'AES-CBC 128', and 'AES-CBC 256'.
 - Hekje:** Checkboxes for 'MD5' (checked), 'SHA1', 'SHA256', and 'SHA512'.

■ Naam sjabloon

Voer in dit veld een naam voor het sjabloon in. (Maximaal 16 tekens)

■ Voorgeconfigureerde sjabloon gebruiken

Selecteer **Aangepast**, **Streng beveiliging IKEv1**, **Gemiddelde beveiliging IKEv1**, **Streng beveiliging IKEv2** of **Gemiddelde beveiliging IKEv2**. De instellingsopties variëren afhankelijk van het geselecteerde sjabloon.



Opmerking

Het standaardjabloon is afhankelijk van of u in het IPsec-instellingenschermbij Onderhandelingsmodus. Zie *Configuratie met behulp van Beheer via een webbrowser* >> pagina 2 voor meer informatie over het IPsec-instellingenschermbij.

■ Internet Key Exchange (IKE)

IKE is een communicatieprotocol dat wordt gebruikt voor het uitwisselen van versleutelingsleutels om versleutelde communicatie via IPsec mogelijk te maken. Om de versleutelde communicatie alleen voor die keer mogelijk te maken, wordt het versleutelingsalgoritme dat nodig is voor IPsec bepaald en worden de versleutelingsleutels gedeeld. Voor IKE worden de versleutelingsleutels uitgewisseld via de Diffie-Hellman-methode en wordt uitsluitend de versleutelde communicatie voor IKE uitgevoerd.

Als **Aangepast** is geselecteerd bij **Voorgeconfigureerde sjabloon gebruiken**, selecteert u **IKEv1**, **IKEv2** of **Handmatig**.

Als u een andere instelling dan **Aangepast** hebt geselecteerd, wordt het verificatietype weergegeven dat bij **Voorgeconfigureerde sjabloon gebruiken** is geselecteerd.

■ Verificatietype

Hier configureert u de IKE-verificatie en -versleuteling.

• Diffie-Hellman-groep

Met deze sleuteluitwisselingsmethode kunnen geheime sleutels veilig via een onbeveiligd netwerk verzonden worden. De Diffie-Hellman-methode voor het uitwisselen van sleutels gebruikt een discreet logaritme probleem, niet de geheime sleutel, om openbare informatie die met een willekeurig nummer en de geheime sleutel is gegenereerd te verzenden en ontvangen.

(Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **IKEv1** of **IKEv2** bij **IKE** is geselecteerd.) Selecteer **Groep 1**, **Groep 2**, **Groep 5** of **Groep 14**. Als **IKEv2** is geselecteerd, zijn er meerdere selecties mogelijk.

(Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **Handmatig** bij **IKE** is geselecteerd.) De groep wordt niet weergegeven.

(Als een andere instelling dan **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd.) De bovengenoemde geactiveerde groep wordt weergegeven.

• Versleuteling

(Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **IKEv1** of **IKEv2** bij **IKE** is geselecteerd.) Selecteer **DES**, **3DES**, **AES-CBC 128** of **AES-CBC 256**. Als **IKEv2** is geselecteerd, zijn er meerdere selecties mogelijk.

(Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **Handmatig** bij **IKE** is geselecteerd.) De versleuteling wordt niet weergegeven.

(Als een andere instelling dan **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd.) De bovengenoemde geactiveerde versleuteling wordt weergegeven.

• Hekje

(Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **IKEv1** of **IKEv2** bij **IKE** is geselecteerd.) Selecteer **MD5**, **SHA1**, **SHA256** of **SHA512**. Als **IKEv2** is geselecteerd, zijn er meerdere selecties mogelijk.

(Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **Handmatig** bij **IKE** is geselecteerd.) Het Hekje-algoritmetype wordt niet weergegeven.

(Als een andere instelling dan **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd.) Het bovengenoemde geactiveerde Hekje-algoritmetype wordt weergegeven.

• Levensduur beveiligingskoppeling

Geef de levensduur van de beveiligingskoppeling van de IKE op.

(Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **IKEv1** of **IKEv2** bij **IKE** is geselecteerd.) Voer de tijd (in seconden) en het aantal kilobytes (KByte) in.

(Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **Handmatig** bij **IKE** is geselecteerd.) De informatie over de levensduur van de beveiligingskoppeling wordt niet weergegeven.

(Als een andere instelling dan **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd.) De tijd (in seconden) en het aantal kilobytes (KByte) worden weergegeven.

■ Encapsulation-beveiliging

- **Protocol**

(Als **Aangepast** bij **Voorconfigureerde sjabloon gebruiken** is geselecteerd.) Selecteer **ESP** of **AH**. Als **IKEv2** bij **IKE** is geselecteerd, kan alleen **ESP** worden geselecteerd.

(Als een andere instelling dan **Aangepast** bij **Voorconfigureerde sjabloon gebruiken** is geselecteerd.) Het bovengenoemde geactiveerde protocol wordt weergegeven.

 **Opmerking**

- ESP is een protocol voor het uitvoeren van versleutelde communicatie via IPsec. ESP versleutelt de payload (inhoud van het verzonden pakket) en voegt aanvullende informatie toe. Het IP-pakket bestaat uit een kop en de versleutelde payload, die na de kop volgt. Naast de versleutelde gegevens bevat het IP-pakket ook informatie over de versleutelingsmethode en -sleutel, de verificatiegegevens, enzovoort.
- AH maakt onderdeel uit van het IPsec-protocol dat de afzender verifieert en manipulatie van de gegevens voorkomt (de volledigheid van de gegevens garandeert). De gegevens worden direct na de kop in het IP-pakket ingevoegd. Daarnaast bevat het pakket de hekjewwaarden, die worden berekend met een vergelijking die wordt samengesteld uit de verzonden inhoud, geheime sleutel, enzovoort, om vervalsing van de afzender en manipulatie van de gegevens te voorkomen. In tegenstelling tot ESP wordt de overgedragen inhoud niet versleuteld en worden de gegevens als onbewerkte tekst verzonden en ontvangen.

- **Versleuteling**

(Als **Aangepast** bij **Voorconfigureerde sjabloon gebruiken** is geselecteerd.) Selecteer **DES**, **3DES**, **AES-CBC 128** of **AES-CBC 256**. De versleuteling kan alleen worden geselecteerd als **ESP** is geselecteerd bij **Protocol**. Als **IKEv2** bij **IKE** is geselecteerd, zijn er meerdere selecties mogelijk.

(Als een andere instelling dan **Aangepast** bij **Voorconfigureerde sjabloon gebruiken** is geselecteerd.) De bovengenoemde geactiveerde versleuteling wordt weergegeven.

- **Hekje**

(Als **Aangepast** bij **Voorconfigureerde sjabloon gebruiken** is geselecteerd en **IKEv1** of **Handmatig** bij **IKE** is geselecteerd.) Selecteer **Geen**, **MD5**, **SHA1**, **SHA256** of **SHA512**. **Geen** kan alleen worden geselecteerd wanneer **ESP** bij **Protocol** is geselecteerd.

(Als **Aangepast** bij **Voorconfigureerde sjabloon gebruiken** is geselecteerd en **IKEv2** bij **IKE** is geselecteerd.) Selecteer **MD5**, **SHA1**, **SHA256** of **SHA512**. Er zijn meerdere selecties mogelijk.

(Als een andere instelling dan **Aangepast** bij **Voorconfigureerde sjabloon gebruiken** is geselecteerd.) Het bovengenoemde geactiveerde Hekje-algoritmetype wordt weergegeven.

- **Levensduur beveiligingskoppeling**

Geef de levensduur van de beveiligingskoppeling van de IKE op.

(Als **Aangepast** bij **Voorconfigureerde sjabloon gebruiken** is geselecteerd en **IKEv1** of **IKEv2** bij **IKE** is geselecteerd.) Voer de tijd (in seconden) en het aantal kilobytes (KByte) in.

(Als een andere instelling dan **Aangepast** bij **Voorconfigureerde sjabloon gebruiken** is geselecteerd.) De tijd (in seconden) en het aantal kilobytes (KByte) worden weergegeven.

- **Encapsulation-modus**

Selecteer **Transport** of **Tunnel**.

- **IP-adres externe router**

Geef het IP-adres (IPv4 of IPv6) van de verbindingbestemming op. U hoeft dit alleen te doen wanneer de modus **Tunnel** is geselecteerd.

 **Opmerking**

SA (Security Association) is een versleutelde communicatiemethode via IPsec of IPv6 die informatie, zoals de versleutelingsmethode en versleutelings sleutel, uitwisselt en deelt om een beveiligd communicatiekanaal op te zetten voordat de communicatie begint. SA kan ook verwijzen naar een virtueel versleuteld communicatiekanaal. De SA die voor IPsec wordt gebruikt, zorgt voor de versleutelingsmethode, wisselt de sleutels uit en voert wederzijdse verificatie volgens de IKE (Internet Key Exchange)-standaardprocedure uit. De SA wordt bovendien periodiek bijgewerkt.

- **Perfect Forward Secrecy (PFS)**

PFS leidt geen sleutels af van eerdere sleutels die voor het versleutelen van berichten zijn gebruikt. Als een sleutel die is gebruikt om een bericht te versleutelen is afgeleid van een hoofdsleutel, wordt die hoofdsleutel niet gebruikt om andere sleutels van af te leiden. Dus zelfs als een sleutel wordt aangetast, zal de schade beperkt blijven tot de berichten die met die betreffende sleutel waren versleuteld.

Selecteer **Ingeschakeld** of **Uitgeschakeld**. Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **Handmatig** bij **IKE** is geselecteerd, wordt de PFS-informatie niet weergegeven.

- **Authenticatiemethode**

Selecteer de authenticatiemethode. Selecteer **Vooraf gedeelde sleutel**, **Certificaten**, **EAP - MD5** of **EAP - MS-CHAPv2**.

EAP - MD5 en **EAP - MS-CHAPv2** kunnen alleen worden geselecteerd wanneer **IKEv2** bij **IKE** is geselecteerd. Als **Aangepast** bij **Vorgeconfigureerde sjabloon gebruiken** is geselecteerd en **Handmatig** bij **IKE** is geselecteerd, wordt de authenticatie-informatie niet weergegeven.

- **Vooraf gedeelde sleutel**

Bij het versleutelen van een bericht wordt de versleutelings sleutel uitgewisseld en van tevoren via een ander kanaal gedeeld.

Als **Vooraf gedeelde sleutel** bij **Authenticatiemethode** is geselecteerd, geeft u de **Vooraf gedeelde sleutel** op. (Maximaal 32 tekens)

- **Lokaal Type id/Id**

Selecteer het type id van de afzender en voer de id in.

Selecteer **IPv4-adres**, **IPv6-adres**, **FQDN**, **E-mailadres** of **Certificaat** voor het type.

Als u **Certificaat** selecteert, voert u de algemene naam van het certificaat in het veld **Id** in.

- **Extern Type id/Id**

Selecteer het type id van de ontvanger en voer de id in.

Selecteer **IPv4-adres**, **IPv6-adres**, **FQDN**, **E-mailadres** of **Certificaat** voor het type.

Als u **Certificaat** selecteert, voert u de algemene naam van het certificaat in het veld **Id** in.

■ Certificaten

Als u **Certificaten** bij **Authenticatiemethode** selecteert, selecteert u het certificaat.



Opmerking

U kunt alleen de certificaten selecteren die zijn aangemaakt op de pagina **Certificaat** van Beheer via een webbrowser. Zie Certificaten gebruiken ter beveiliging van de machine in de Netwerkhandleiding voor de beveiliging van apparaten.

■ EAP

EAP is een authenticatieprotocol dat een uitbreiding is van PPP. Door EAP samen met IEEE802.1x te gebruiken, wordt iedere sessie een andere sleutel voor gebruikersauthenticatie gebruikt.

De volgende instellingen zijn alleen nodig als **EAP - MD5** of **EAP - MS-CHAPv2** bij **Authenticatiemethode** is geselecteerd.

- **Modus**

Selecteer **Servermodus** of **Clientmodus**.

- **Certificaat**

Selecteer het certificaat.

- **Gebruikersnaam**

Voer de gebruikersnaam in. (Maximaal 32 tekens)

- **Wachtwoord**

Voer het wachtwoord in. Het wachtwoord moet tweemaal worden ingevoerd ter bevestiging. (Maximaal 32 tekens)

- **Certificaat>>**

Klik op deze knop om naar het certificaatinstellingsscherm te gaan.

(IKE:Handmatig)

■ Verificatiesleutel (ESP, AH)

Geef de sleutel op die voor authenticatie moet worden gebruikt. Geef de **In/Uit**-waarden op.

Deze instellingen zijn nodig wanneer **Aangepast** bij **Voorgeconfigureerde sjabloon gebruiken** is geselecteerd, **Handmatig** bij **IKE** is geselecteerd en een andere instelling dan **Geen** bij **Hekje** in het vak **Encapsulation-beveiliging** is geselecteerd.

Opmerking

Het aantal tekens dat u kunt gebruiken is afhankelijk van de instelling die u hebt gekozen bij Hekje in het vak Encapsulation-beveiliging.

Als de lengte van de opgegeven authenticatiesleutel afwijkt van het geselecteerde hekje-algoritme, treedt een fout op.

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

Als u de sleutel in ASCII-code specificeert, omsluit u de tekens met dubbele aanhalingstekens.

■ Codesleutel (ESP)

Geef de sleutel op die voor versleuteling moet worden gebruikt. Geef de **In/Uit**-waarden op.

Deze instellingen zijn nodig wanneer **Aangepast** bij **Voorgeconfigureerde sjabloon gebruiken** is geselecteerd, **Handmatig** bij **IKE** is geselecteerd en **ESP** bij **Protocol** in het vak **Encapsulation-beveiliging** is geselecteerd.

Opmerking

Het aantal tekens dat u kunt gebruiken is afhankelijk van de instelling die u hebt gekozen bij Versleuteling in het vak Encapsulation-beveiliging.

Als de lengte van de opgegeven codesleutel afwijkt van het geselecteerde versleutelingsalgoritme, treedt een fout op.

- **DES**: 64 bits (8 bytes)
- **3DES**: 192 bits (24 bytes)
- **AES-CBC 128**: 128 bits (16 bytes)
- **AES-CBC 256**: 256 bits (32 bytes)

Als u de sleutel in ASCII-code specificeert, omsluit u de tekens met dubbele aanhalingstekens.

■ **SPI**

Deze parameters worden gebruikt om de beveiligingsinformatie te bepalen. Over het algemeen beschikt een host over meerdere SA's (Security Associations) voor diverse typen IPsec-communicatie. Daarom is het nodig om bij ontvangst van een IPsec-pakket de geschikte SA te bepalen. De SPI-parameter, die de SA bepaalt, wordt meegezonden in de AH (Authentication Header)- en ESP (Encapsulating Security Payload)-kop.

Deze instellingen zijn nodig wanneer **Aangepast** bij **Voorgeconfigureerde sjabloon gebruiken** is geselecteerd en **Handmatig** bij **IKE** is geselecteerd.

Geef de **In/Uit**-waarden op. (3-10 tekens)

■ **Indienen**

Klik op deze knop om de instellingen te registreren.

Opmerking

Als u de instellingen van het huidige sjabloon wijzigt, wordt het IP-instellingenschermb van Beheer via een webbrowser gesloten en weer geopend.

Servicesjablonen

U kunt de volgende services gebruiken door de sjablonen te selecteren.

1 Alle services

IPsec wordt voor alle protocollen gebruikt.

2 Printservices

Naam service	Protocol	Lokale poort	Externe poort
IPP	TCP	631	Willekeurig
IPPS	TCP	443	Willekeurig
FTP (besturing)	TCP	21	Willekeurig
FTP (data)	TCP	20	Willekeurig
P9100	TCP	9100	Willekeurig
Webservices	TCP	80	Willekeurig
LPD	TCP	515	Willekeurig

3 Managementservices

Naam service	Protocol	Lokale poort	Externe poort
SNMP	UDP	161	Willekeurig
Telnet	TCP	23	Willekeurig
HTTP	TCP	80	Willekeurig
HTTPS	TCP	443	Willekeurig
Remote Setup	TCP	54922	Willekeurig

4 Printer/MFC-services ¹

Naam service	Protocol	Lokale poort	Externe poort
CIFS	TCP	Willekeurig	445
SMB	TCP	Willekeurig	139
LDAP	TCP	Willekeurig	389
SMTP	TCP	Willekeurig	25
POP3	TCP	Willekeurig	110
SNTP	UDP	Willekeurig	123
Netwerk scannen	TCP	54921	Willekeurig
PC-FAX	TCP	54923	Willekeurig

Naam service	Protocol	Lokale poort	Externe poort
Kerberos (TCP)	TCP	Willekeurig	88
Kerberos (UDP)	UDP	Willekeurig	88

¹ Als u gebruik wilt maken van Kerberos-authenticatie, dient u de DNS-instellingen dienovereenkomstig in te schakelen.

Type/Code

De volgende typen en codes worden ondersteund wanneer **ICMP** bij **Protocol** is geselecteerd.

IPv4		
Type		Ondersteunde 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		
Type		Ondersteunde 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

brother[®]

**Bezoek ons op het world wide web
<http://www.brother.com/>**



www.brotherearth.com