Manual de Configuração de Ipsec

Versão 0

BRA-POR

Definições de observações

Utilizamos o ícone a seguir ao longo deste Manual do Usuário:

 Observação	Os ícones de Observação ensinam como agir em determinada situação ou fornecem dicas sobre como a operação funciona com outros recursos.

Marcas registradas

A logomarca Brother é uma marca registrada da Brother Industries, Ltd.

Todos os nomes comerciais e de produtos de empresas que apareçam nos produtos Brother, documentos relacionados e outros materiais são marcas comerciais ou marcas registradas dessas respectivas empresas.

Índice

1 Introdução

Visão geral

O IPsec (Internet Protocol Security) é um protocolo de segurança que utiliza uma função opcional do protocolo de Internet para evitar a manipulação e garantir a confidencialidade dos dados transmitidos como pacotes de IP. O IPsec criptografa os dados transportados pela rede, tal como os dados de impressão enviados de computadores para uma impressora. Como os dados são criptografados na camada de rede, os aplicativos que utilizam um protocolo de nível mais alto usam IPsec mesmo se o usuário não estiver ciente do seu uso.

O IPsec suporta as funções a seguir:

■ Transmissões IPsec

De acordo com as condições de configuração do IPsec, o computador conectado à rede envia e recebe dados do dispositivo especificado usando o IPsec. Quando o dispositivo começa a se comunicar usando o IPsec, as chaves são trocadas primeiro usando o IKE (Internet Key Exchange) e, em seguida, os dados criptografados são transmitidos usando as chaves.

Além disso, o IPsec possui dois modos de operação: o modo de Transporte e o modo de Túnel. O modo de Transporte é usado principalmente para a comunicação entre os dispositivos e o modo de Túnel é usado em ambientes como o VPN (Virtual Private Network).

Observação

- Para as transmissões IPsec, são necessárias as condições a seguir:
  - Um computador que possa se comunicar usando IPsec está conectado à rede.
  - A impressora ou multifuncional está configurado para a comunicação IPsec.
  - O computador conectado à impressora ou multifuncional está configurado para conexões IPsec.
- O IPsec não aceita comunicações ‘broadcast’ ou ‘multicast’.

■ Configurações de IPsec

Configurações que são necessárias para as conexões que usam IPsec. Estas configurações podem ser ajustadas usando o Gerenciamento via Web. (Consulte *Configuração usando o Gerenciamento via Web (navegador da web)* ➤➤ página 2).

Observação

Para ajustar as configurações de IPsec, um computador que possa operar o navegador deve estar conectado à rede.

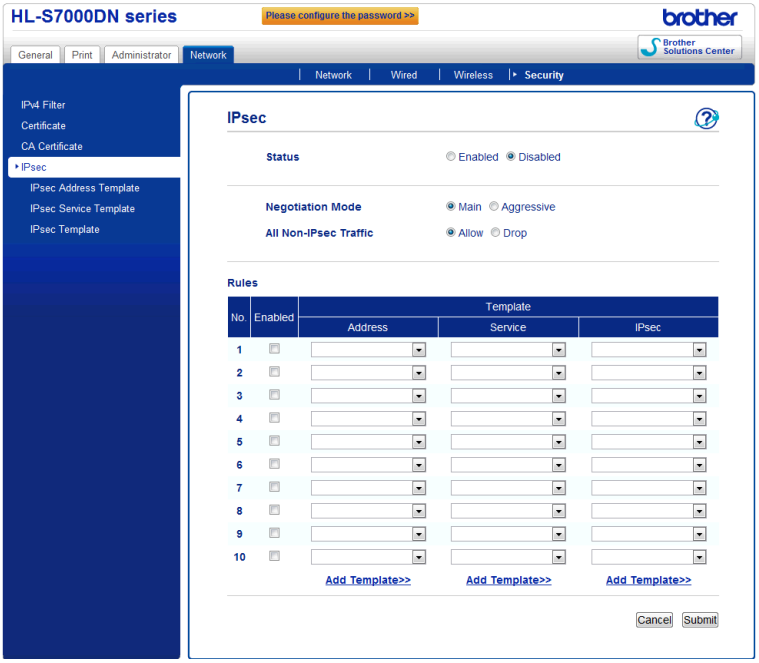
Configuração usando o Gerenciamento via Web (navegador da web)

Use a tela de configuração de IPsec no Gerenciamento via Web para especificar as condições de conexão do IPsec.

As condições de conexão IPsec são compostas de três tipos de **Template** (Modelo): **Address** (Endereço), **Service** (Serviço) e **IPsec**; podem ser configuradas no máximo 10 condições de conexão.

1. Inicie o seu navegador da Web.
2. Digite “http://endereço IP do aparelho/” no navegador (onde “endereço IP do aparelho” é o endereço IP do aparelho).
   - Por exemplo:

     http://192.168.1.2/
3. Por padrão, não há necessidade de senha. Insira a senha, se tiver definido uma, e pressione .
4. Clique na guia **Network** (Rede).
5. Clique em **Security** (Segurança).
6. Clique em **IPsec**.
7. Você pode ajustar as configurações do IPsec na tela abaixo.



- **Status**

  Selecione **Enabled** (Habilitado) ou **Disabled** (Desabilitado) para o IPsec.
- **Negotiation Mode** (Modo de negociação)

  Selecione o modo para a fase 1 do IKE.

- **Main** (Principal): é utilizado o modo principal.
- **Aggressive** (Agressivo): é utilizado o modo agressivo.

Observação

IKE é um protocolo usado para a troca de chaves de criptografia para efetuar comunicação criptografada usando o IPsec.

Se for selecionado o modo **Main** (Principal), a velocidade de processamento é lenta, mas a segurança é alta. Se for selecionado o modo **Aggressive** (Agressivo), a velocidade é maior do que quando o modo **Main** (Principal) está selecionado, mas a segurança é menor.

■ **All Non-IPsec Traffic** (Todo o tráfego não IPsec)

Selecione a ação para os pacotes não IPsec.

- **Allow** (Permitir): todos os pacotes podem ser recebidos.
- **Drop** (Descartar): todos os pacotes não IPsec são descartados.

Observação

Ao usar Serviços Web, você deve selecionar **Allow** (Permitir) em **All Non-IPsec Traffic** (Todo o tráfego não IPsec). Se for selecionado **Drop** (Descartar), os Serviços Web não podem ser usados.

■ **Rules** (Regras)

No máximo podem ser configuradas 10 condições de conexão IPsec (conjunto de modelos).

■ **Enabled** (Habilitado)

Quando esta caixa de seleção está marcada, o conjunto de modelos para aquele número está habilitado.

Observação

Quando várias caixas de seleção estão marcadas, as caixas de seleção com menos números têm prioridade caso as configurações das caixas de seleção marcadas estiverem em conflito.

■ **Template** (Modelo) - **Address** (Endereço)

Selecione o **Address Template** (Modelo de endereço) que é usado para as condições de conexão IPsec.

Para adicionar um **Address Template** (Modelo de endereço), clique em **Add Template** (Adicionar modelo). (Consulte *Modelo de endereço* ➤➤ página 5).

■ **Template** (Modelo) - **Service** (Serviço)

Selecione o **Service Template** (Modelo de serviço) que é usado para as condições de conexão IPsec.

Para adicionar um **Service Template** (Modelo de serviço), clique em **Add Template** (Adicionar modelo). (Consulte *Modelo de serviço* ➤➤ página 7).

Observação

Se você desejar usar DNS para a resolução de nomes ao usar os modelos de serviço 2, 3 e 4 em *Apêndice A*, as configurações de DNS devem ser ajustadas separadamente.

■ **Template** (Modelo) - **IPsec**

Selecione o **IPsec Template** (Modelo IPsec) que é usado para as condições de conexão IPsec.

Para adicionar um **IPsec Template** (Modelo IPsec), clique em **Add Template** (Adicionar modelo). (Consulte *Modelo IPsec* ➤➤ página 11).

■ **Submit** (Enviar)

Clique neste botão para registrar as configurações. Se o computador precisar ser reiniciado para alterar as configurações, a tela de confirmação de reinício será exibida quando este botão for clicado.

Observação

Se você marcar a caixa de seleção **Enabled** (Habilitado) e clicar em **Submit** (Enviar), ocorrerá um erro se houver um item em branco no modelo selecionado.

2 Configurações de IPsec

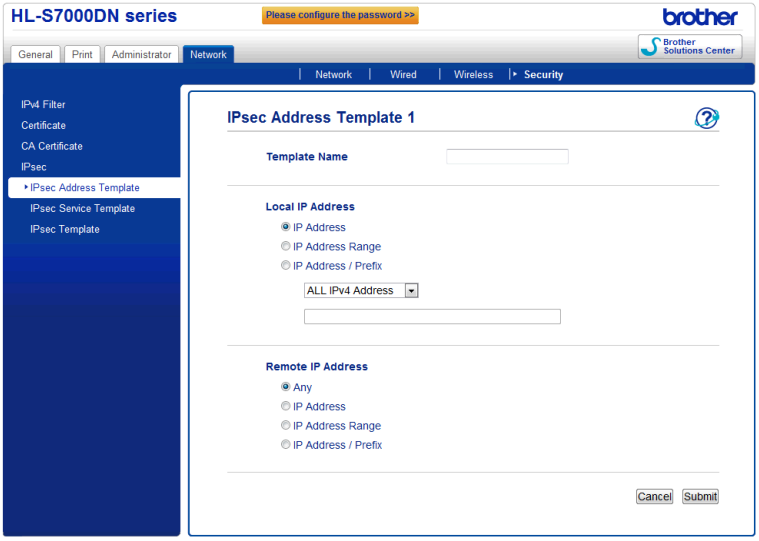
Modelo de endereço

Especifique os endereços IP que serão usados para as condições de conexão IPsec. Podem ser usados no máximo 10 modelos **Address Template** (Modelo de endereço).

1. Inicie o seu navegador da Web.
2. Digite “http://endereço IP do aparelho/” no navegador (onde “endereço IP do aparelho” é o endereço IP do aparelho).
   - Por exemplo:

     http://192.168.1.2/
3. Por padrão, não há necessidade de senha. Insira a senha, se tiver definido uma, e pressione .
4. Clique na guia **Network** (Rede).
5. Clique em **Security** (Segurança).
6. Clique em **IPsec Address Template** (Modelo de endereço IPsec).
   Serão exibidos 10 modelos **Address Template** (Modelo de endereço). Se o **Address Template** (Modelo de endereço) não foi configurado, será exibido **Not Configured** (Não configurado).
   - **Delete** (Excluir)

     Clique neste botão para excluir o **Address Template** (Modelo de endereço) selecionado. Entretanto, o **Address Template** (Modelo de endereço) atualmente em uso não pode ser excluído.
7. Clique no número do **Address Template** (Modelo de endereço) que você deseja criar. Especifique o endereço IP que você deseja usar para o IPsec na tela abaixo e crie o **IPsec Address Template** (Modelo de endereço IPsec).



- **Template Name** (Nome do modelo)

  Insira um nome para o modelo nesta caixa (com no máximo 16 caracteres).

■ **Local IP Address** (Endereço IP local)

Especifique as condições de endereço IP para o remetente.

- **IP Address** (Endereço IP)

  Especifique o endereço IP. Selecione **ALL IPv4 Address** (TODOS os endereços IPv4), **ALL IPv6 Address** (TODOS os endereços IPv6), **ALL Link Local IPv6** (TODOS os links locais IPv6) ou **Custom** (Personalizado).

  Se for selecionado **Custom** (Personalizado), insira o endereço IP especificado (IPv4 ou IPv6) na caixa de texto.

- **IP Address Range** (Intervalo de endereços IP)

  Insira os endereços IP inicial e final para o intervalo de endereços IP. Se os endereços IP inicial e final não estiverem padronizados para IPv4 ou IPv6, ou se o endereço IP final for menor que o endereço inicial, ocorrerá um erro.

- **IP Address / Prefix** (Endereço IP / Prefixo)

  Especifique o endereço IP usando um prefixo.

  Por exemplo: 192.168.1.1/24

  Já que o prefixo é especificado na forma de uma máscara de sub-rede com 24 bits (255.255.255.0) para 192.168.1.1, os endereços 192.168.1.xx são válidos.

■ **Remote IP Address** (Endereço IP remoto)

Especifique as condições de endereço IP para o destinatário.

- **Any** (Qualquer)

  Quando **Any** (Qualquer) estiver selecionado, todos os endereços IP estão habilitados.

- **IP Address** (Endereço IP)

  Insira o endereço IP especificado (IPv4 ou IPv6) na caixa de texto.

- **IP Address Range** (Intervalo de endereços IP)

  Insira os endereços IP inicial e final para o intervalo de endereços IP. Se os endereços IP inicial e final não estiverem padronizados para IPv4 ou IPv6, ou se o endereço IP final for menor que o endereço inicial, ocorrerá um erro.

- **IP Address / Prefix** (Endereço IP / Prefixo)

  Especifique o endereço IP usando um prefixo.

  Por exemplo: 192.168.1.1/24

  Já que o prefixo é especificado na forma de uma máscara de sub-rede com 24 bits (255.255.255.0) para 192.168.1.1, os endereços 192.168.1.xx são válidos.

■ **Submit** (Enviar)

Clique neste botão para registrar as configurações.

Observação

Quando você altera as configurações do modelo atualmente em uso, a tela de configurações de IPsec do Gerenciamento via Web irá fechar e abrir novamente.

Modelo de serviço

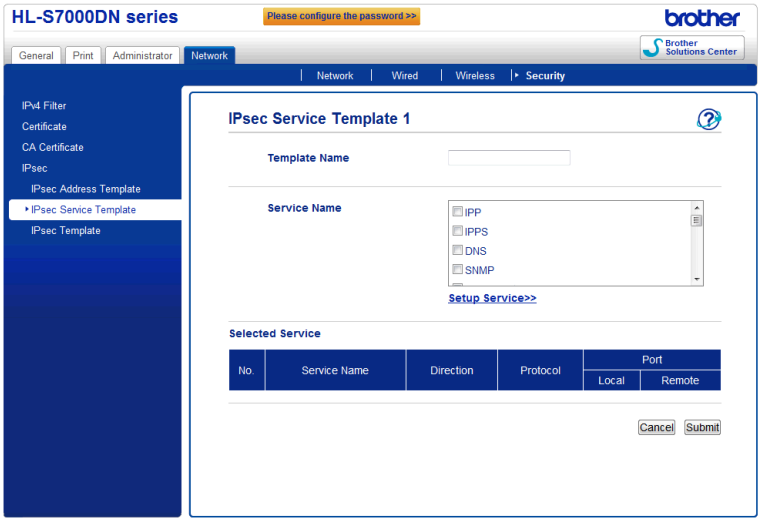
Modelo de serviço IPsec

Especifique o protocolo e o número da porta para utilizar nas conexões IPsec. Podem ser usados no máximo 10 modelos **Service Template** (Modelo de serviço).

1. Inicie o seu navegador da Web.
2. Digite “http://endereço IP do aparelho/” no navegador (onde “endereço IP do aparelho” é o endereço IP do aparelho).
   - Por exemplo:

     http://192.168.1.2/
3. Por padrão, não há necessidade de senha. Insira a senha, se tiver definido uma, e pressione .
4. Clique na guia **Network** (Rede).
5. Clique em **Security** (Segurança).
6. Clique em **IPsec Service Template** (Modelo de serviço IPsec).
   Serão exibidos 10 modelos **Service Template** (Modelo de serviço). Se o **Service Template** (Modelo de serviço) não foi configurado, será exibido **Not Configured** (Não configurado).
   - **Delete** (Excluir)

     Clique neste botão para excluir o **Service Template** (Modelo de serviço) selecionado. Entretanto, o **Service Template** (Modelo de serviço) atualmente em uso não pode ser excluído.
7. Clique no número do **Service Template** (Modelo de serviço) que você deseja criar. Selecione os serviços que deseja usar para o IPsec na tela abaixo e crie o **IPsec Service Template** (Modelo de serviço IPsec).
   Além disso, se você deseja criar serviços originais, clique em **Setup Service** (Configurar serviço). (Consulte *Configurar serviço* ➤➤ página 8).



■ **Template Name** (Nome do modelo)

Insira um nome para o modelo nesta caixa (com no máximo 16 caracteres).

■ **Service Name** (Nome do serviço)

São exibidos os nomes dos serviços predefinidos e dos serviços criados anteriormente. Selecione os serviços que você deseja adicionar ao modelo.

■ **Setup Service** (Configurar serviço)

Clique em **Setup Service** (Configurar serviço) para configurar o modelo através da adição de serviços. (Consulte *Configurar serviço* ➤➤ página 8).

■ **Selected Service** (Serviço selecionado)

As informações do serviço (**Service Name** (Nome do serviço), **Direction** (Direção), **Protocol** (Protocolo) e **Port** (Porta)) selecionadas para o **Service Name** (Nome do serviço) são exibidas.

Observação

- Podem ser adicionados 32 serviços de uma vez.
- Para obter detalhes sobre os protocolos que você pode especificar em **IPsec Service Template** (Modelo de serviço IPsec), consulte *Apêndice A*.

■ **Submit** (Enviar)

Clique neste botão para registrar as configurações.

Observação

Quando você altera as configurações do modelo atualmente em uso, a tela de configurações de IPsec do Gerenciamento via Web irá fechar e abrir novamente.

Configurar serviço

Crie um novo serviço.

1. Na tela **IPsec Service Template** (Modelo de serviço IPsec), clique em **Setup Service** (Configurar serviço).
   Serão exibidos 60 nomes **Service Name** (Nome do serviço). Se o **Service Name** (Nome do serviço) não foi configurado, será exibido **Not Configured** (Não configurado).

   ■ **Delete** (Excluir)

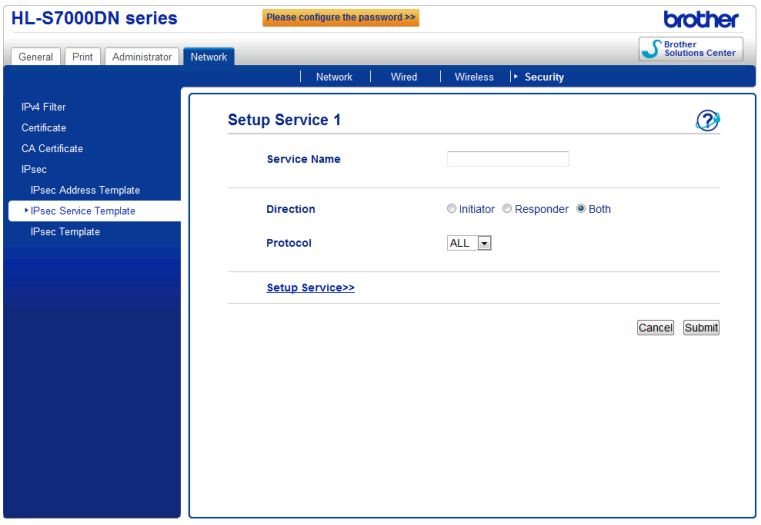
   Clique neste botão para excluir o **Service Name** (Nome do serviço) selecionado. Entretanto, o **Service Name** (Nome do serviço) atualmente em uso não pode ser excluído.

   ■ **IPsec Service Template** (Modelo de serviço IPsec)

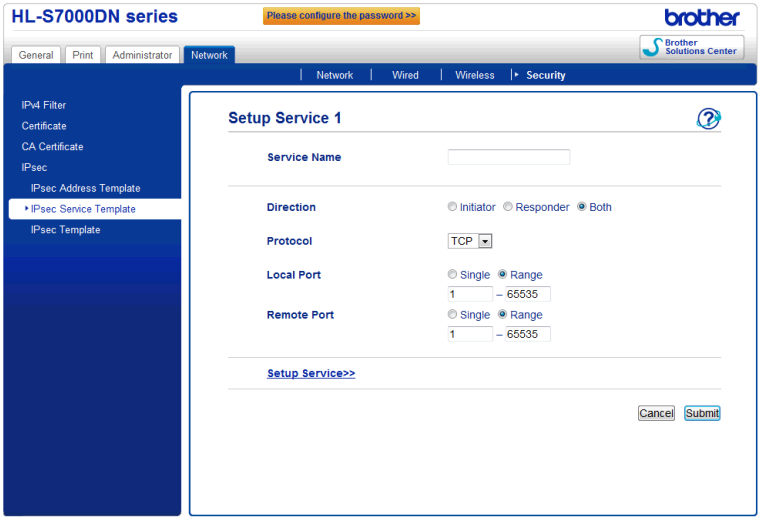
   Clique neste botão para retornar à tela **IPsec Service Template** (Modelo de serviço IPsec).

2 Clique no número do **Service Name** (Nome do serviço) que você deseja criar. Selecione os serviços que deseja usar para o IPsec na tela abaixo. Os itens de configuração são diferentes, dependendo do **Protocol** (Protocolo) selecionado.

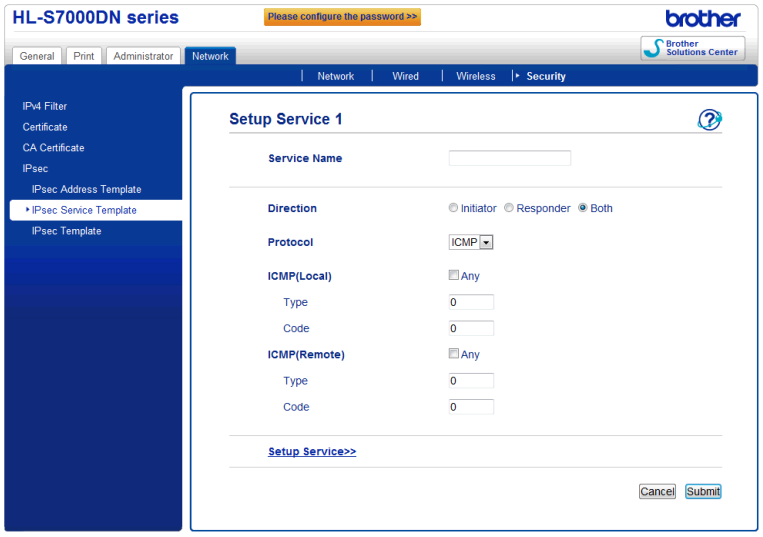
(**Protocol** (Protocolo):**ALL** (TODOS))



(**Protocol** (Protocolo):**TCP** ou **UDP**)



(**Protocol** (Protocolo): **ICMP**)



■ **Service Name** (Nome do serviço)

Insira um nome para o serviço nesta caixa (com no máximo 16 caracteres).

■ **Direction** (Direção)

Especifique a direção da comunicação. Selecione **Initiator** (Iniciador), **Responder** (Respondente) ou **Both** (Ambos).

■ **Protocol** (Protocolo)

Especifique o protocolo que está habilitado. Selecione **ALL** (TODOS), **TCP**, **UDP** ou **ICMP**. Os itens de configuração são diferentes, dependendo do **Protocol** (Protocolo) selecionado.

- Quando **TCP** ou **UDP** for selecionado, registre a **Local Port**/**Remote Port** (Porta Local/Porta Remota).
- Quando **ICMP** for selecionado, registre o **Type**/**Code** (Tipo/Código).

Observação

ICMP é um protocolo usado para enviar mensagens de erro e de controle de IP. Este protocolo é usado por computadores e dispositivos de rede conectados usando TCP/IP para transportar confirmações de status mútuas.

■ **Local Port**/**Remote Port** (Porta Local/Porta Remota) (Quando **TCP** ou **UDP** estiver selecionado em **Protocol** (Protocolo)).

Insira o número da porta local. Se **Single** (Única) estiver selecionado, insira um número de porta. Se **Range** (Intervalo) estiver selecionado, insira o número de porta inicial e depois insira o número de porta final. Quando você desejar habilitar todos os números de porta, selecione **Range** (Intervalo) e insira "1-65535" sem as aspas.

■ **ICMP(Local)**/**ICMP(Remote)** (ICMP(Local)/ICMP(Remoto)) (Quando **ICMP** estiver selecionado em **Protocol** (Protocolo)).

Ajuste as configurações de ICMP. Selecione **Any** (Qualquer) ou insira o **Type**/**Code** (Tipo/Código). Para obter detalhes sobre o **Type**/**Code** (Tipo/Código), consulte *Apêndice A*.

■ **Setup Service** (Configurar serviço)

Clique neste botão para retornar à tela **Setup Service** (Configurar serviço).

■ **Submit** (Enviar)

Clique neste botão para registrar as configurações.

Observação

Quando você altera as configurações do modelo atualmente em uso, a tela de configurações de IPsec do Gerenciamento via Web irá fechar e abrir novamente.

Modelo IPsec

Ajuste as configurações de IKE/IPsec. Podem ser usados no máximo 10 modelos **IPsec Template** (Modelo IPsec).

1. Inicie o seu navegador da Web.
2. Digite “http://endereço IP do aparelho/” no navegador (onde “endereço IP do aparelho” é o endereço IP do aparelho).

   ■ Por exemplo:

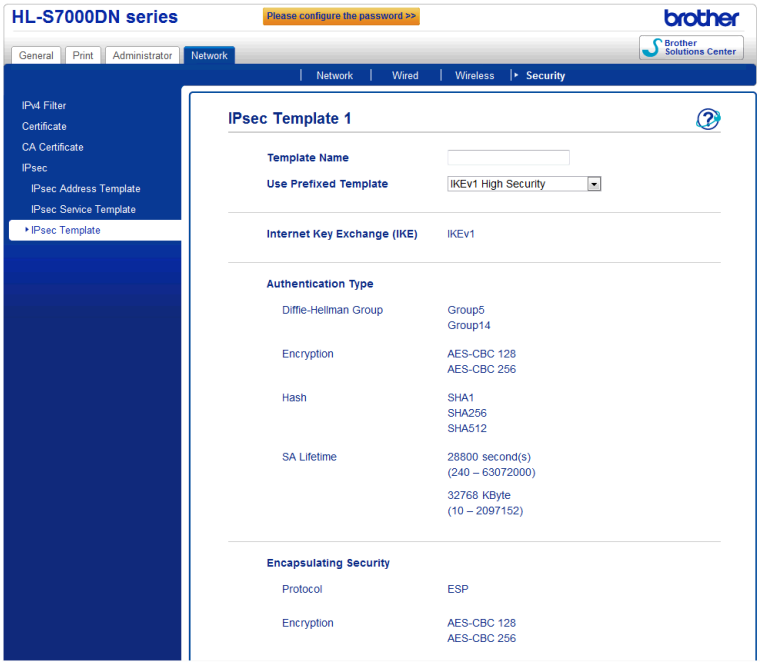
   http://192.168.1.2/
3. Por padrão, não há necessidade de senha. Insira a senha, se tiver definido uma, e pressione .
4. Clique na guia **Network** (Rede).
5. Clique em **Security** (Segurança).
6. Clique em **IPsec Template** (Modelo IPsec).
   Serão exibidos 10 modelos **IPsec Template** (Modelo IPsec). Se o **IPsec Template** (Modelo IPsec) não foi configurado, será exibido **Not Configured** (Não configurado).

   ■ **Delete** (Excluir)

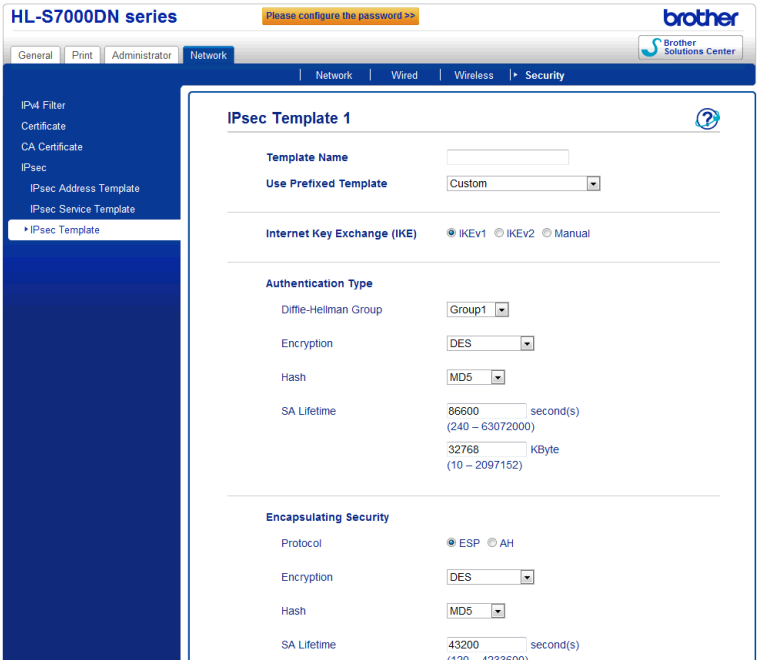
   Clique neste botão para excluir o **IPsec Template** (Modelo IPsec) selecionado. Entretanto, o **IPsec Template** (Modelo IPsec) atualmente em uso não pode ser excluído.

7 Clique no número do **IPsec Template** (Modelo IPsec) que você deseja criar. Ajuste as configurações de IPsec na tela abaixo e crie o **IPsec Template** (Modelo IPsec). As configurações são diferentes dependendo do **Use Prefixed Template** (Usar modelo com prefixo) e da **Internet Key Exchange (IKE)** selecionados.

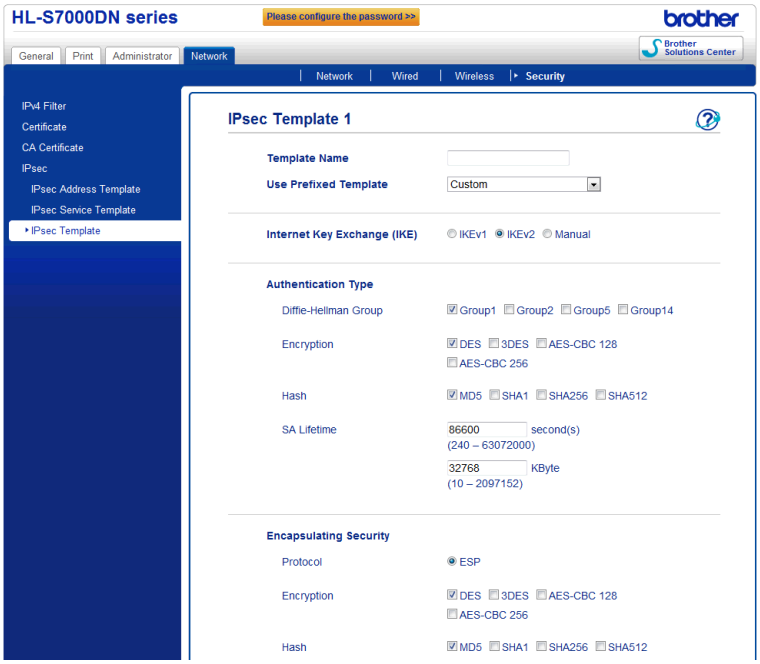
(**IKE**:**Predefinição**)



(**IKE**:**IKEv1**)



(**IKE**:**IKEv2**)



■ **Template Name** (Nome do modelo)

Insira um nome para o modelo nesta caixa (com no máximo 16 caracteres).

■ **Use Prefixed Template** (Usar modelo com prefixo)

Selecione **Custom** (Personalizado), **IKEv1 High Security** (IKEv1 de alta segurança), **IKEv1 Medium Security** (IKEv1 de média segurança), **IKEv2 High Security** (IKEv2 de alta segurança) ou **IKEv2 Medium Security** (IKEv2 de média segurança). Os itens de configuração são diferentes, dependendo do modelo selecionado.

Observação

O modelo predefinido pode diferir dependendo da escolha Principal ou Agressivo no Modo de negociação na tela de configuração de IPsec. Para obter detalhes sobre a tela de configuração de IPsec, consulte *Configuração usando o Gerenciamento via Web (navegador da web)* ➤➤ página 2.

■ **Internet Key Exchange (IKE)**

IKE é um protocolo de comunicação usado para a troca de chaves de criptografia para efetuar comunicação criptografada usando o IPsec. Para conduzir a comunicação criptografada apenas uma vez, o algoritmo de criptografia necessário para IPsec é determinado e as chaves de criptografia são compartilhadas. Para o IKE, as chaves de criptografia são trocadas usando o método de troca de chave Diffie-Hellman e a comunicação criptografada limitada ao IKE é conduzida.

Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo), selecione **IKEv1**, **IKEv2** ou **Manual**.

Se uma configuração diferente de **Custom** (Personalizado) estiver selecionada, o tipo de autenticação selecionado em **Use Prefixed Template** (Usar modelo com prefixo) será exibido.

■ **Authentication Type** (Tipo de autenticação)

Configura a autenticação e a criptografia de IKE.

- **Diffie-Hellman Group** (Grupo Diffie-Hellman)

  Este método de troca de chaves permite que chaves secretas sejam trocadas de forma segura em uma rede não protegida. O método de troca de chaves Diffie-Hellman usa um problema de logaritmo discreto, não a chave secreta, para enviar e receber informações abertas que são geradas com um número aleatório e a chave secreta.

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **IKEv1** ou **IKEv2** estiver selecionado em **IKE**) Selecione **Group1** (Grupo1), **Group2** (Grupo2), **Group5** (Grupo5) ou **Group14** (Grupo14). Se **IKEv2** estiver selecionado, são possíveis várias seleções.

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **Manual** estiver selecionado em **IKE**) O grupo não será exibido.

  (Se uma configuração diferente de **Custom** (Personalizado) estiver selecionada em **Use Prefixed Template** (Usar modelo com prefixo)) O grupo habilitado mencionado acima será exibido.

- **Encryption** (Criptografia)

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **IKEv1** ou **IKEv2** estiver selecionado em **IKE**) Selecione **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. Se **IKEv2** estiver selecionado, são possíveis várias seleções.

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **Manual** estiver selecionado em **IKE**) A criptografia não será exibida.

  (Se uma configuração diferente de **Custom** (Personalizado) estiver selecionada em **Use Prefixed Template** (Usar modelo com prefixo)) A criptografia habilitada mencionada acima será exibida.

- **Hash**

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **IKEv1** ou **IKEv2** estiver selecionado em **IKE**) Selecione **MD5**, **SHA1**, **SHA256** ou **SHA512**. Se **IKEv2** estiver selecionado, são possíveis várias seleções.

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **Manual** estiver selecionado em **IKE**) O tipo de algoritmo de hash não será exibido.

  (Se uma configuração diferente de **Custom** (Personalizado) estiver selecionada em **Use Prefixed Template** (Usar modelo com prefixo)) O tipo de algoritmo de hash habilitado mencionado acima será exibido.

- **SA Lifetime** (Tempo de vida de SA)

  Especifique o tempo de vida de SA do IKE.

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **IKEv1** ou **IKEv2** estiver selecionado em **IKE**) Insira o tempo (em segundos) e o número de kilobytes (KByte).

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **Manual** estiver selecionado em **IKE**) As informações de tempo de vida de SA não serão exibidas.

(Se uma configuração diferente de **Custom** (Personalizado) estiver selecionada em **Use Prefixed Template** (Usar modelo com prefixo)) O tempo (em segundos) e o número de kilobytes (KByte) serão exibidos.

■ **Encapsulating Security** (Segurança encapsulada)

- **Protocol** (Protocolo)

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo)) Selecione **ESP** ou **AH**. Se **IKEv2** estiver selecionado em **IKE**, somente **ESP** pode ser selecionado.

  (Se uma configuração diferente de **Custom** (Personalizado) estiver selecionada em **Use Prefixed Template** (Usar modelo com prefixo)) O protocolo habilitado mencionado acima será exibido.

Observação

- ESP é o protocolo para a condução de comunicação criptografada usando IPsec. ESP criptografa a carga (conteúdo comunicado) a acrescenta informações adicionais. O pacote de IP é composto do cabeçalho e da carga criptografada que acompanha o cabeçalho. Além dos dados criptografados, o pacote de IP também inclui informações relacionadas ao método de criptografia e à chave de criptografia, os dados de autenticação e assim por diante.
- AH é a parte do protocolo IPsec que autentica o remetente e evita manipulação dos dados (garante a integridade dos dados). No pacote de IP, os dados são inseridos imediatamente após o cabeçalho. Além disso, os pacotes incluem valores de hash que são calculados usando uma equação a partir do conteúdo comunicado, da chave secreta e assim por diante, de modo a evitar a falsificação do remetente e a manipulação dos dados. Diferentemente do ESP, o conteúdo comunicado não é criptografado e os dados são enviados e recebidos como texto simples.

- **Encryption** (Criptografia)

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo)) Selecione **DES**, **3DES**, **AES-CBC 128** ou **AES-CBC 256**. A criptografia somente pode ser selecionada quando **ESP** está selecionado em **Protocol** (Protocolo). Se **IKEv2** estiver selecionado em **IKE**, são possíveis várias seleções.

  (Se uma configuração diferente de **Custom** (Personalizado) estiver selecionada em **Use Prefixed Template** (Usar modelo com prefixo)) A criptografia habilitada mencionada acima será exibida.

- **Hash**

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **IKEv1** ou **Manual** estiver selecionado em **IKE**) Selecione **None** (Nenhum), **MD5**, **SHA1**, **SHA256** ou **SHA512**. **None** (Nenhum) somente pode ser selecionado quando **ESP** está selecionado em **Protocol** (Protocolo).

  (Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **IKEv2** estiver selecionado em **IKE**) Selecione **MD5**, **SHA1**, **SHA256** ou **SHA512**. São possíveis várias seleções.

  (Se uma configuração diferente de **Custom** (Personalizado) estiver selecionada em **Use Prefixed Template** (Usar modelo com prefixo)) O tipo de algoritmo de hash habilitado mencionado acima será exibido.

- **SA Lifetime** (Tempo de vida de SA)

  Especifique o tempo de vida de SA do IKE.

(Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **IKEv1** ou **IKEv2** estiver selecionado em **IKE**) Insira o tempo (em segundos) e o número de kilobytes (KByte).

(Se uma configuração diferente de **Custom** (Personalizado) estiver selecionada em **Use Prefixed Template** (Usar modelo com prefixo)) O tempo (em segundos) e o número de kilobytes (KByte) serão exibidos.

- **Encapsulation Mode** (Modo de encapsulamento)

  Selecione **Transport** (Transporte) ou **Tunnel** (Túnel).

- **Remote Router IP-Address** (Endereço IP do roteador remoto)

  Especifique o endereço IP (IPv4 ou IPv6) do destino da conexão. Insira somente quando o modo **Tunnel** (Túnel) estiver selecionado.

Observação

SA (Associação de Segurança) é um método de comunicação criptografada usando IPsec ou IPv6 que troca e compartilha informações, como o método de criptografia e a chave de criptografia, para estabelecer um canal seguro de comunicação antes que a comunicação inicie. SA pode também se referir a um canal de comunicação criptografado virtual que tenha sido estabelecido. A SA usada para IPsec estabelece o método de criptografia, troca as chaves e conduz a autenticação mútua de acordo com o procedimento padrão do IKE (Internet Key Exchange). Além disso, a SA é atualizada periodicamente.

■ **Perfect Forward Secrecy (PFS)**

O PFS não deriva chaves das chaves anteriores que foram usadas para criptografar mensagens. Além disso, se uma chave que é usada para criptografar uma mensagem foi derivada de uma chave pai, essa chave pai não é usada para derivar outras chaves. Desta forma, mesmo se uma chave for comprometida, o dano estará limitado às mensagens que foram criptografas usando aquela chave.

Selecione **Enabled** (Habilitado) ou **Disabled** (Desabilitado). Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **Manual** estiver selecionado em **IKE**, as informações de PFS não serão exibidas.

■ **Authentication Method** (Método de autenticação)

Selecione o método de autenticação. Selecione **Pre-Shared Key** (Chave pré-compartilhada), **Certificates** (Certificados), **EAP - MD5** ou **EAP - MS-CHAPv2**.

EAP - MD5 e **EAP - MS-CHAPv2** somente podem ser selecionados quando **IKEv2** está selecionado em **IKE**. Se **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **Manual** estiver selecionado em **IKE**, as informações de método de autenticação não serão exibidas.

■ **Pre-Shared Key** (Chave pré-compartilhada)

Ao criptografar a comunicação, a chave de criptografia é trocada e compartilhada antes de usar outro canal.

Se **Pre-Shared Key** (Chave pré-compartilhada) estiver selecionado em **Authentication Method** (Método de autenticação), insira a **Pre-Shared Key** (Chave pré-compartilhada) (com no máximo 32 caracteres).

- **Local ID Type** (Tipo de ID local)/**ID**

  Selecione o tipo de ID do remetente e insira a ID.

Selecione **IPv4 Address** (Endereço IPv4), **IPv6 Address** (Endereço IPv6), **FQDN**, **E-mail Address** (Endereço de e-mail) ou **Certificate** (Certificado) para o tipo.

Se **Certificate** (Certificado) estiver selecionado, insira o nome comum do certificado em **ID**.

- **Remote ID Type** (Tipo de ID remota)/**ID**

  Selecione o tipo de ID do destinatário e insira a ID.

  Selecione **IPv4 Address** (Endereço IPv4), **IPv6 Address** (Endereço IPv6), **FQDN**, **E-mail Address** (Endereço de e-mail) ou **Certificate** (Certificado) para o tipo.

  Se **Certificate** (Certificado) estiver selecionado, insira o nome comum do certificado em **ID**.

■ **Certificates** (Certificados)

Se **Certificates** (Certificados) estiver selecionado em **Authentication Method** (Método de autenticação), selecione o certificado.

Observação

Somente é possível selecionar certificados que foram criados usando a página **Certificate** (Certificado) dos recursos de segurança do Gerenciamento via Web. Para obter detalhes, consulte o Manual do Usuário de Rede: Usar certificados para segurança do dispositivo.

■ **EAP**

EAP é um protocolo de autenticação que é uma extensão do PPP. Ao usar EAP junto com IEEE802.1x, uma chave diferente é usada para a autenticação do usuário e cada sessão.

As configurações a seguir somente são necessárias quando **EAP - MD5** ou **EAP - MS-CHAPv2** estiverem selecionados em **Authentication Method** (Método de autenticação).

- **Mode** (Modo)

  Selecione **Server-Mode** (Modo servidor) ou **Client-Mode** (Modo cliente).

- **Certificate** (Certificado)

  Selecione o certificado.

- **User Name** (Nome de usuário)

  Insira o nome do usuário (com no máximo 32 caracteres).

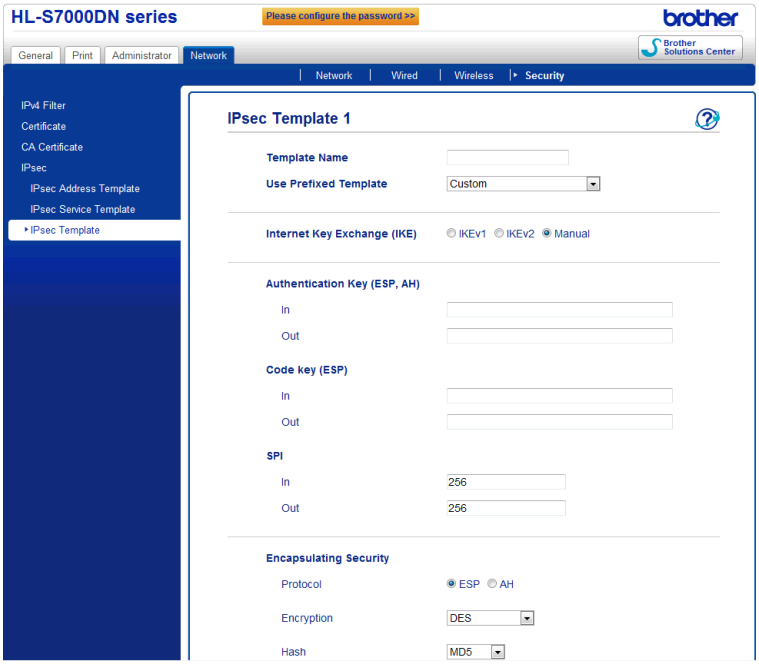
- **Password** (Senha)

  Insira a senha. A senha deve ser inserida duas vezes para confirmação (com no máximo 32 caracteres).

- **Certificate** (Certificado)>>

  Clique neste botão para ir para a tela de configuração de certificado.

(**IKE**:**Manual**)



■ **Authentication Key (ESP,AH)** (Chave de autenticação (ESP,AH))

Especifique a chave a ser usada para autenticação. Insira os valores **In**/**Out** (Entrada/Saída).

Estas configurações são necessárias quando **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo), **Manual** estiver selecionado em **IKE** e uma configuração diferente de **None** (Nenhum) estiver selecionada em **Hash** na **Encapsulating Security** (Segurança encapsulada).

Observação

O número de caracteres que você pode definir difere dependendo da configuração escolhida em Hash na Segurança encapsulada.

Se o comprimento da chave de autenticação especificada for diferente do algoritmo de hash selecionado, ocorrerá um erro.

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

Ao especificar a chave em código ASCII, coloque os caracteres entre aspas duplas.

■ **Code key (ESP)** (Chave de código (ESP))

Especifique a chave a usar para criptografia. Insira os valores **In**/**Out** (Entrada/Saída).

Estas configurações são necessárias quando **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo), **Manual** estiver selecionado em **IKE** e **ESP** estiver selecionado em **Protocol** (Protocolo) na **Encapsulating Security** (Segurança encapsulada).

Observação

O número de caracteres que você pode definir difere dependendo da configuração escolhida em Criptografia na Segurança encapsulada.

Se o comprimento da chave de código especificada for diferente do algoritmo de criptografia selecionado, ocorrerá um erro.

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

Ao especificar a chave em código ASCII, coloque os caracteres entre aspas duplas.

■ **SPI**

Estes parâmetros são usados para identificar as informações de segurança. Geralmente, um host possui várias SAs (Associações de Segurança) para diversos tipos de comunicação IPsec. Desta forma, é necessário identificar a SA aplicável quando um pacote IPsec é recebido. O parâmetro SPI, que identifica a SA, é incluído no AH (Cabeçalho de autenticação) e no cabeçalho de ESP (Carga de segurança encapsulada).

Estas configurações são necessárias quando **Custom** (Personalizado) estiver selecionado em **Use Prefixed Template** (Usar modelo com prefixo) e **Manual** estiver selecionado em **IKE**.

Insira os valores **In**/**Out** (Entrada/Saída) (3-10 caracteres).

■ **Submit** (Enviar)

Clique neste botão para registrar as configurações.

Observação

Quando você altera as configurações do modelo atualmente em uso, a tela de configurações de IPsec do Gerenciamento via Web irá fechar e abrir novamente.

A Apêndice A

Modelos de serviços

Você pode usar os serviços a seguir selecionando os modelos.

1 Todos os serviços

IPsec é usado para todos os protocolos.

2 Serviços de impressão

Nome do serviço	Protocolo	Porta local	Porta remota
IPP	TCP	631	Any (Qualquer)
IPPS	TCP	443	Any (Qualquer)
FTP (Control) (FTP (Controle))	TCP	21	Any (Qualquer)
FTP (Data) (FTP (Dados))	TCP	20	Any (Qualquer)
P9100	TCP	9100	Any (Qualquer)
Web Services (Serviços Web)	TCP	80	Any (Qualquer)
LPD	TCP	515	Any (Qualquer)

3 Serviços de gerenciamento

Nome do serviço	Protocolo	Porta local	Porta remota
SNMP	UDP	161	Any (Qualquer)
Telnet	TCP	23	Any (Qualquer)
HTTP	TCP	80	Any (Qualquer)
HTTPS	TCP	443	Any (Qualquer)
Remote Setup (Configuração remota)	TCP	54922	Any (Qualquer)

4 Serviços de impressora/multifuncional [1]

Nome do serviço	Protocolo	Porta local	Porta remota
CIFS	TCP	Any (Qualquer)	445
SMB	TCP	Any (Qualquer)	139
LDAP	TCP	Any (Qualquer)	389
SMTP	TCP	Any (Qualquer)	25
POP3	TCP	Any (Qualquer)	110
SNTP	UDP	Any (Qualquer)	123
Network Scan (Escaneamento em rede)	TCP	54921	Any (Qualquer)
PC-FAX	TCP	54923	Any (Qualquer)
Kerberos (TCP)	TCP	Any (Qualquer)	88
Kerberos (UDP)	UDP	Any (Qualquer)	88

[1] Se você deseja usar a autenticação Kerberos, deve habilitar as configurações de DNS de acordo.

Tipo/Código

Os tipos e códigos a seguir são suportados quando **ICMP** estiver selecionado em **Protocol** (Protocolo).

IPv4		
Tipo		**Códigos suportados**
0	Resposta de eco	0
3	Destino não alcançável	0,1,2,3,4,5,6,7,8,9,10,11,12
4	Extinção de fonte	0
5	Redireção	0,1,2,3
8	Solicitação de eco	0
9	Anúncio de roteador	0
10	Solicitações de roteador	0

Código IPv4

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

IPv6		
Tipo		**Códigos suportados**
1	Destino não alcançável	0,1,2,3,4
3	Tempo ultrapassado	0,1
4	Problema de parâmetro	0,1,2
128	Solicitação de eco	0
129	Resposta de eco	0
133	Solicitação de roteador	0
134	Anúncio de roteador	0
135	Solicitação de vizinho	0
136	Anúncio de vizinho	0
137	Redireção	0

Código IPv6

0,1,2,3,4

brother

Visite-nos na Internet
http://www.brother.com/

Brother Earth

www.brotherearth.com