Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for TRENDNET TW100-BRV214. You'll find the answers to all your questions on the TRENDNET TW100-BRV214 in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual TRENDNET TW100-BRV214
User guide TRENDNET TW100-BRV214
Operating instructions TRENDNET TW100-BRV214
Instructions for use TRENDNET TW100-BRV214
Instruction manual TRENDNET TW100-BRV214

You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide
http://yourpdfguides.com/dref/4129107

Manual abstract:

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

2 Application Diagram .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 4 Advanced Router Setup ...
.....
.....

.....
.....
.....
.....

.....
.....
. 36 Access your router management page ....
.....

.....
.....
.....
.....

.....
.....
.....
..... 36 Change your router login password ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

..... 32 © Copyright 2012 TRENDnet. All Rights Reserved. i TRENDnet User's Guide Enable route mode on your router ...

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

54 Using WoL (Wake on LAN) on your router .....

.....

.....
.....
.....
.....

.....
.....
.....

. 54 Table of Contents Router Maintenance & Monitoring.....

.....
.....
.....
.....

..... 55 Reset your router to factory defaults .

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

... 55 Router Default Settings .....

.....
.....
.....
.....

.....
.....
.....

. 67 © Copyright 2012 TRENDnet. All Rights Reserved. ii TRENDnet User's Guide TW100-BRV214 Features The 4-Port VPN Router, model TW100-BRV214, manages up to 80 Virtual Private Network (VPN) tunnels. IPSec, L2TP, and PPTP VPN pass-through sessions are supported and a configurable firewall ensures the highest level of security. Four Fast Ethernet ports on the back of the router help extend a wired network. Advanced Stateful Packet Inspection (SPI) and Network Address Translation (NAT) encryption protects your digital network. Advanced features include GRE tunneling, advanced Quality of Service (QoS) controls, Domain filtering, and packet filtering. · · · · 4 x 10/100 Mbps Auto-MDIX LAN ports 1 x 10/100 Mbps WAN port (Internet) On/off button Compatible with most popular cable/DSL Internet service providers using Dynamic/Static IP, PPPoE, PPTP and L2TP protocols Firewall protection with Network Address Translation (NAT), Stateful Packet Inspection (SPI), and Denial of Service (DoS) prevention Supports up to 80 PPTP/L2TP/IPsec tunnels Supports up to 100 PPTP/L2TP/IPsec VPN pass through sessions Supports up to 8 Generic Routing Encapsulation (GRE) tunnels Access Control: Virtual Servers, MAC/IP Packet Filters, URL/Keyword Filters, Demilitarized Zone (DMZ) host, and One-to-One NAT Set device time using Network Time Protocol (NTP) and define schedules for Virtual Server, Packet Filters, and Quality of Service (QoS) Quality of Service (QoS) traffic prioritization via IP/(TCP/UDP) ports with 3 priority queues Universal Plug and Play (UPnP) for auto discovery and support for device configuration of Internet applications Supports Internet Group Multicast Protocol IGMPv1/2 pass through for multicast applications Supports static and dynamic RIP v1/2 routing Dynamic DNS Client for dynamic Internet IP resolution Product Overview TW100-BRV214 · · Package Contents In addition to your router, the package includes: · · · · Muti-Language Quick Installation Guide CD-ROM (User's Guide) Network cable (1.5m / 5ft) Power adapter (12V DC, 1A) · · · · · · · · · If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor that the item was purchased.*

*© Copyright 2012 TRENDnet. All Rights Reserved. 1 TRENDnet User's Guide · · Device monitoring using the Internal System Log, External Syslog, E-mail Alert, and SNMPv1/2c Local/Remote management via Web browser, upgrade firmware, and backup/restore configuration TW100-BRV214 *The number of supported concurrent VPN tunnels is dependent upon available bandwidth. Product Hardware Features Rear Panel View · · LAN Ports Connect Ethernet cables (also called network cables) from your router LAN ports and to your wired network devices. WAN Port - Connect an Ethernet cable (also called network cable) from your router WAN port and to your xDSL/Cable modem.*

Power Port Connect the included power adapter from your router power port and to an available power outlet. Note: Use only the adapter that came with your router. On/Off Power Switch Push your router On/Off push button power switch to turn your router "On" (Inner position) or "Off" (Outer position). · · © Copyright 2012 TRENDnet. All Rights Reserved.

2 TRENDnet User's Guide Front Panel View TW100-BRV214 Front Panel Button and LEDs Reset Button Push and hold this button for 20 seconds and release to reset your router to its factory defaults. The LEDs will blink rapidly when the reset process is activated. WAN (Link/Activity) This LED indicator is solid green when your router WAN port is physically connected to the xDSL/Cable modem Ethernet port (also called network port) successfully with an Ethernet cable (also called network cable). The LED indicator will be blinking green while data is transmitted or received through the WAN port of your router. LAN 1-4 (Link/Activity) These LED indicators are solid green when the LAN ports are physically connected to your wired network devices successfully with an Ethernet cable (also called network cable). These LED indicators will be blinking green while data is transmitted or received through your router LAN ports. Status - This LED indicator is blinking green when your router is ready and working successfully. If this LED indicator is solid green on or off, your router is not receiving power or not working properly.


You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide
http://yourpdfguides.com/dref/4129107

© Copyright 2012 TRENDnet. All Rights Reserved.

3 TRENDnet User's Guide Application Diagram TW100-BRV214 The router is installed in a main office location which is connected to the Internet. Desktop computers are connected to the four LAN ports of the router using Ethernet ca_____ 6. L2TP Type (Dynamic IP or Static IP) My IP Address: _____. _____._____._____ (e.g. 215.24.24.
129) Subnet Mask:_____. _____._____._____ Gateway:_____. _____.
_____._____ Server IP: _____. _____._____._____ L2TP Account: _____ L2TP Password: _____ TW100-BRV214 © Copyright 2012 TRENDnet.
All Rights Reserved. 6 TRENDnet User's Guide Hardware Installation 1. Verify that you have an Internet connection when connecting your computer directly to the modem. Open your browser (e.g. Internet Explorer, Firefox, Chrome, Safari, or Opera) and type in a URL (e.g. http://trendnet.com) in the address bar. TW100-BRV214 5.

Connect one end of a network cable to one of your router LAN ports (1-4). Connect the other end of the network cable to the computer Ethernet port (also called network port). 2. Turn off your modem. 3. Disconnect the Ethernet cable (also called network cable) from your modem and your computer. 4. Connect one end of a network cable to your router WAN port. Connect the other end of the network cable to your Cable modem network port. 6.
Connect the included power adapter to your router Power Port and then to an available power outlet. Push the On/Off Power Switch on your router to the "On" (inner) position. 7. Turn on your modem. 8.
Verify that the following front panel LED indicators on your router (Status and WAN is solid green, and the LAN port for which your computer is connected is solid green. © Copyright 2012 TRENDnet. All Rights Reserved. 7 TRENDnet User's Guide Setup Wizard 1. Open your web browser (e.
g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to http://192.168.10.1. Your router will prompt you for a password. 4. Click Next.
TW100-BRV214 2. Enter the System Password and click Login.

Default System Password: admin 3. Make sure the Wizard option is selected and then click Enter. Note: If the Setup Wizard does not automatically appear, click Wizard at the top of the page. 5. Enter the Old Password (Default: admin), enter a New Password and enter the password again next to Reconfirm to verify the New Password. Note: 1. Setting a password prevents other users from accessing the router management page. 2. It is recommended that you enter a new password. If you decide to change the default password, please write down the new password.
3. Password is limited up to 9 characters. © Copyright 2012 TRENDnet. All Rights Reserved. 8 TRENDnet User's Guide 6.
Click the drop-down list and select your Time Zone. Click Next. TW100-BRV214 8. Configure the settings based on information provided by your Internet Service Provider (ISP). Follow the wizard instructions to complete your configuration.
Note: Each Internet connection type may have different options. 7. Select Auto Detecting WAN Type and the click Next. Note: When configuring your Internet connection settings. It is optional to change your LAN IP network settings. It is recommended to leave this setting at default. © Copyright 2012 TRENDnet. All Rights Reserved. 9 TRENDnet User's Guide 11. Click Apply Settings.

Note: You can check the network testing option to run an Internet connection test before applying the settings. 13. Click Finish. TW100-BRV214 12. Please wait until the router applies the changes and reboots. Note: If you checked the option to run network testing (Internet connection test), you will see the status message below. Note: If you checked the option to run network testing (Internet connection test) and the test is success, you will receive the message below along with your Internet connection settings. © Copyright 2012 TRENDnet. All Rights Reserved. 10 TRENDnet User's Guide Connect additional wired devices to your network You can connect an additional computer or device to your network by connecting one end of an Ethernet cable (also called network cable) from your computer or device Ethernet port (also called network port) to one of the available LAN ports labeled 1,2,3,4 on your router.
Check the status of the LED indicators (1, 2, 3, or 4) on the front panel of your router to ensure the physical cable connection from your computer or device. Note: If you encounter issues connecting to your network, there may be a problem with your computer or device network settings. Please ensure that your computer or device network settings (also called TCP/IP settings) are configured to obtain IP address settings automatically (also called dynamic IP address or DHCP) and to Obtain DNS Server address settings automatically. TW100-BRV214 © Copyright 2012 TRENDnet. All Rights Reserved.
11 TRENDnet User's Guide TW100-BRV214 Tunneling methods supported by your router: · IPsec (Internet Protocol Security) VPN This type of VPN can be used for either Site-to-Site VPN or Client-Server VPN however, the most common application for this type is a Site-to-Site VPN. This type of VPN can provide highest degree of security. For a Client-Server VPN, typically, a third party VPN client software is required to be installed and configured and can be difficult when installing and configuring on VPN client computers. This VPN type can provide the highest degree of security. PPTP (Point-to-Point Tunneling Protocol) VPN This type of VPN can be used for Client-Server VPN only however both server mode and client mode are supported on your router. Most computer operating systems already include a pre-installed PPTP VPN client software that can be easily configured which eliminates the need for an additional third party VPN client software to be purchased and installed. Since it provides less security overall than IPsec VPN, it is not recommended for a Site-to-Site VPN. L2TP (Layer 2 Tunneling Protocol) VPN This type of VPN is very similar to PPTP VPN as it is most commonly used for a Client-Server VPN, pre-installed on most computer operating systems and easy to configure, and provides less overall security than IPsec VPN. Most of the current operating systems with L2TP VPN client software pre-installed use L2TP VPN in conjunction with IPsec VPN to improve the overall security provided. This router does not support the L2TP over IPsec VPN method. GRE (Generic Routing Encapsulation) Tunneling This is strictly a tunneling protocol as it does not provide any security mechanisms and it can only be used for Site-to-Site tunneling to another router with GRE tunneling support but in most current implementations can be used in conjunction with IPsec or PPTP/L2TP to add security mechanisms. Because of the nature of how GRE works, the benefits include allow multicast traffic and allowing dynamic routing protocols to pass through the tunnel compared to IPsec VPN.


You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide
http://yourpdfguides.com/dref/4129107

This router does not support GRE over IPsec VPN or GRE over PPTP/L2TPVPN methods. Virtual Private Networking (VPN) Creating a Virtual Private Network What is a VPN? A VPN provides secure communications typically over the Internet by creating a secure tunnel between two or more VPN routers (gateways) also known as a site-to-site VPN or between a single client computer and a VPN router (gateway) also known as a clientserver VPN. On your VPN router, the following types of tunnels can be created: · Site-to-Site VPN Connects two or more VPN routers (gateways) allowing the LAN network from each router to securely communicate to each other over the Internet.

· · · Client-Server VPN A single client computer or device with VPN client software installed connects to a VPN router (gateway) allow the single client computer or device to securely communicate to the LAN network of the VPN router over the Internet. · Important Note: For any tunneling or VPN method used, to avoid IP address conflict and to ensure connectivity, it is required that each end (LAN IP network or single client) of the VPN tunnel is configured with a different IP network or subnet. © Copyright 2012 TRENDnet. All Rights Reserved. 12 TRENDnet User's Guide IPsec (Internet Protocol Security) Site-to-Site VPN Configuration > Security Setting >VPN-IPsec To configure an IPsec Site-to-Site VPN tunnel between two VPN routers: VPN Router A Configuration TW100-BRV214 · Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to both routers under the Status page. See page 59 for checking the status page. Example: VPN Router A WAN (Internet) IP Address: 10.10.10.10 VPN Router B WAN (Internet) IP Address: 10.
10.10.20 1. @@2. Click on Configuration at the top of the page, click on Security Setting, and click on VPN-IPsec.
3. Next to VPN-IPsec, check the Enable option to enable IPsec. Note: If Enable is not checked, then this will disable all IPsec functionality on your router. · Make sure the LAN IP network on each VPN router is different. Note: Changing the LAN IP address of your router will change the LAN IP network of your router.
See page 39 for changing the LAN IP address. Example: VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0 VPN Router B LAN IP Settings: 192.168.100.

1 / 255.255.255.0 4. For ID 1, check the Enable option and then click Edit. 5. Next to Tunnel Name, enter the tunnel name in the field. (e.g. Tunnel 1) © Copyright 2012 TRENDnet.
All Rights Reserved. 13 TRENDnet User's Guide 6. Enter the network settings for the IPsec Site-to-Site VPN tunnel. TW100-BRV214 7. Next to Preshare Key, enter the preshared key for your IPsec tunnel.
Note: The value 1234567890 is shown as an example. It is strongly recommended to enter your own preshared key for the IPsec VPN tunnel. Write down the preshared key you enter as it will also need to be entered when configuring VPN Router B. Note: The preshared key can consist of alphanumeric characters (a,b,C,?,, /,1,2, etc.) Note: Generally speaking if the LAN IP address setting of the router is 192.*
168.X.1 / 255.255.255.0, then the IP network will be identified as 192.168.X.0, X being any number from 0-254. · · · Local Subnet The local LAN IP subnet or network of your local VPN router.

(e.g. 192.168.10.0) Local Netmask The local LAN subnet mask of your local VPN router. (e.g. 255.255.
255.0) Remote Subnet The remote LAN IP subnet or network of your remote VPN router. (e.g. 192.
168.100.0) · · Remote Netmask The remote LAN subnet mask of your remote VPN router. (e.g.
255.255.255.0) Remote Gateway The remote WAN (Internet) IP address of your remote VPN router. (e.g. 10.10.10.20) Note: If the remote router is using dynamic DNS, you can enter domain for the remote gateway instead of the WAN IP address.

10. Next to IKE Proposal, check the Enable option. Next to ID 1, click the Encryption drop-down list and select AES-128 and click the DH Group drop-down list and select Group 2. Check the Enable option. Note: The IKE proposal settings must match the setting configured in VPN Router A. 9. Next to Dead Peer Detection (DPD), check the Enable option. 8. Click the PFS Group drop-down list, and select Same as Phase 1. Based on the example, the network settings will be the following: © Copyright 2012 TRENDnet.
All Rights Reserved. 14 TRENDnet User's Guide 11. Next to IPsec Proposal, check the Enable option. Next to ID 1, click the Encryption drop-down list and select AES-128. Check the Enable option.
Note: The IPsec proposal settings must match the setting configured in VPN Router A. TW100-BRV214 1. @@Note: If you changed router LAN IP address, you will need to log into the remote router using the new IP address instead of the default 192.168.10.
1. 2. Click on Configuration at the top of the page, click on Security Setting, and click on VPN-IPsec. 12. Click Save at the bottom of the page to save the changes. Note: If you would like to discard the changes, click Undo before you click Save. 3. Next to VPN-IPsec, check the Enable option to enable IPsec. Note: If Enable is not checked, then this will disable all IPsec functionality on your router. To view the status of the IPsec Site-to-Site VPN tunnel, click Back at the bottom of the page to go back to the main IPsec VPN configuration page.

VPN Router A Tunnel Status 4. For ID 1, check the Enable option and then click Edit. 5. Next to Tunnel Name, enter the tunnel name in the field. (e.g. Tunnel 1) VPN Router B Configuration 6. Enter the network settings for the IPsec Site-to-Site VPN tunnel. © Copyright 2012 TRENDnet. All Rights Reserved.
15 TRENDnet User's Guide Note: Generally speaking if the LAN IP address setting of the router is 192.168.X.1 / 255.255.
255.0, then the IP network will be identified as 192.168.X.0, X being any number from 0-254.
· · · Local Subnet The local LAN IP subnet or network of your local VPN router. (e.g. 192.168.100.0) Local Netmask The local LAN subnet mask of your local VPN router. (e.g. 255.

255.255.0) Remote Subnet The remote LAN IP subnet or network of your remote VPN router. (e.g. 192.168.10.0) · · Remote Netmask The remote LAN subnet mask of your remote VPN router. (e.
g. 255.255.255.0) Remote Gateway The remote WAN (Internet) IP address of your remote VPN router.
(e.g. 10.10.10.
10) Note: If the remote router is using dynamic DNS, you can enter domain for the remote gateway instead of the WAN IP address. TW100-BRV214 8. Click the PFS Group drop-down list, and select Same as Phase 1. 9. Next to Dead Peer Detection (DPD), check the Enable option. 10. Next to IKE Proposal, check the Enable option. Next to ID 1, click the Encryption drop-down list and select AES-128 and click the DH Group drop-down list and select Group 2.

[You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide]

http://yourpdfguides.com/dref/4129107

Check the Enable option. Note: The IKE proposal settings must match the setting configured in VPN Router A.

Based on the example, the network settings will be the following: 11. Next to IPsec Proposal, check the Enable option. Next to ID 1, click the Encryption drop-down list and select AES-128. Check the Enable option. Note: The IPsec proposal settings must match the setting configured in VPN Router A. 7. Next to Preshare Key, enter the preshared key for your IPsec tunnel. Note: The preshared key entered must be the same as the preshared key configured in VPN Router A. 12. Click Save at the bottom of the page to save the changes.
Note: If you would like to discard the changes, click Undo before you click Save. Note: The preshared key can consist of alphanumeric characters (a,b,C,?,, /,1,2, etc.) © Copyright 2012 TRENDnet. All Rights Reserved. 16 TRENDnet User's Guide To view the status of the IPsec Site-to-Site VPN tunnel, click Back at the bottom of the page to go back to the main IPsec VPN configuration page.*
Under Action, click Connect to establish the VPN tunnel. VPN Router B Tunnel Status TW100-BRV214 (UDP 500, UDP 4500, IP Protocol 50: ESP) may need to be forwarded to your VPN client computer. · If the single client computer is connecting to the Internet through a router with NAT enabled, make sure the LAN IP network of the router NAT enabled is different from the LAN IP network of your VPN router. Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 39 for changing the LAN IP address.
Example: VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0 Router with NAT enabled LAN IP Settings: 192.168.100.1 / 255.

255.255.0 For details on configuring additional IPsec VPN options, see the Appendix. · Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to your routers under the Status page. See page 59 for checking the status page. Example: VPN Router A WAN (Internet) IP Address: 10.10.10.10 Client-Server VPN (Server Mode) Configuration > Security Setting >VPN-IPsec To configure your router to allow IPsec VPN connections from remote VPN client computers or devices: 1. @@2.
Click on Configuration at the top of the page, click on Security Setting, and click on VPN-IPsec. 3. Next to VPN-IPsec, check the Enable option to enable IPsec. Note: If Enable is not checked, then this will disable all IPsec functionality on your router. · Typically, the single client computer is connecting to the Internet through a router with NAT enabled.
To establish an IPsec VPN tunnel when one of the VPN endpoints is behind a router with NAT enabled, enable NAT-T (NAT Traversal) to establish VPN connections through devices with NAT enabled. If the router with NAT enabled does not support IPsec VPN pass through, ports 4. Next to NAT Traversal, check the Enable option. © Copyright 2012 TRENDnet. All Rights Reserved.
17 TRENDnet User's Guide 5. Next to Dynamic VPN, check the Enable option and click Edit. TW100-BRV214 11. Next to IKE Proposal, check the Enable option. Next to ID 1, click the Encryption drop-down list and select AES-128 and click the DH Group drop-down list and select Group 2. Check the Enable option. 6. Next to Tunnel Name, enter the tunnel name in the field. (e.g.

Tunnel 1) 7. Enter the network settings for the IPsec VPN Server. 12. Next to IPsec Proposal, check the Enable option. Next to ID 1, click the Encryption drop-down list and select AES-128. Check the Enable option. · · Local Subnet The local LAN IP subnet or network of your local VPN router. (e.g. 192. 168.10.0) Local Netmask The local LAN subnet mask of your local VPN router. (e.g.
255.255.255.0) 13. Click Save at the bottom of the page to save the changes.
Note: If you would like to discard the changes, click Undo before you click Save. 8. Next to Preshare Key, enter the preshared key for your IPsec tunnel. Note: The preshared key entered must be the same as the preshared key configured in VPN Router A. Note: The preshared key can consist of alphanumeric characters (a,b,C,?,, /,1,2, etc.) 9. Click the PFS Group drop-down list, and select Same as Phase 1. 10. Next to Dead Peer Detection (DPD), check the Enable option. © Copyright 2012 TRENDnet.*

All Rights Reserved. 18 TRENDnet User's Guide Note: For the VPN client computer, you will require a third party IPsec VPN software to be installed configured matching the IPsec VPN settings on your router. Please refer to the your VPN software User's Guide/Manual for configuring the VPN settings. Below is your router VPN configuration based on the IPsec Client-Server VPN (Server Mode) procedure. · · · · · · · · · LAN IP Network: 192.168.10.0 / 255.255.255.
0 NAT-T (NAT Traversal): Enabled IPsec Mode: Main Tunnel Method: IKE Encapsulation: ESP Preshared Key: <preshared key you entered in VPN configuration> IKE Proposal: AES-128 / SHA1 / DH Group 2 IPsec Proposal: AES-128 / SHA1 PFS (Perfect Forward Secrecy): Enabled DH Group 2 · TW100-BRV214 PPTP (Point-to-Point Tunneling Protocol) Client-Server VPN (Server Mode) Configuration > Security Setting >VPN-PPTP Server To configure your router to allow PPTP VPN connections from remote VPN client computers or devices: To view the status of the IPsec Site-to-Site VPN tunnel, click Back at the bottom of the page to go back to the main IPsec VPN configuration page. When the client is connected, the Status will change from Wait for Traffic... to Connected.
Typically, the single client computer is connecting to the Internet through a router with NAT enabled. To establish a PPTP VPN tunnel when one of the VPN endpoints is behind a router with NAT enabled, PPTP VPN passthrough must be enabled on the router with NAT enabled. If the router with NAT enabled does not support PPTP VPN pass through, ports (TCP 1723, IP Protocol 47: GRE) may need to be forwarded to your VPN client computer. If the single client computer is connecting to the Internet through a router with NAT enabled, make sure the LAN IP network of the router NAT enabled is different from the LAN IP network of your VPN router. Note: Changing the LAN IP address of your router will change the LAN IP network of your router.
See page 39 for changing the LAN IP address. Example: VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0 Router with NAT enabled LAN IP Settings: 192.168.100.

1 / 255.255.255.0 · For details on configuring additional IPsec VPN options, see the Appendix. · Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to your routers under the Status page. See page 59 for checking the status page. Example: VPN Router A WAN (Internet) IP Address: 10.


You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide
http://yourpdfguides.com/dref/4129107

10.10.10 © Copyright 2012 TRENDnet.
All Rights Reserved. 19 TRENDnet User's Guide 1. @@2. Click on Configuration at the top of the page, click on Security Setting, and click on VPN-PPTP Server. 3.
Next to VPN-PPTP Server, check the Enable option to enable the PPTP server. 7. Next to MPPE Encryption Mode, check the Enable option. TW100-BRV214 8. Next to Encryption Length, to ensure highest compatibility, check 40 bits, 56 bits, and 128 bits.
4. Next to Server virtual IP, enter the LAN IP address of your router. Note: The LAN IP address of your router is automatically entered therefore, it is recommended to leave this setting unchanged. 9. Under User Accounts next to ID 1, enter the User Name and Password used by PPTP VPN clients to authenticate. Note: The same account can be used by multiple PPTP VPN clients. 5. Enter the IP address range to assign to PPTP VPN clients. Note: Please ensure that this range does not conflict with your DHCP server range. If you have not changed your LAN IP settings or DHCP server range, then you can leave hese settings at default.

Router default DHCP server range: 192.168.10.101-192.168.10.199 10. Click Save at the bottom of the page to save the changes. Note: If you would like to discard the changes, click Undo before you click Save. Clicking Refresh will reload the page.
Clicking PPTP Client will bring you to the PPTP Client mode configuration page. · · IP Pool Start Address Changes the starting address for the PPTP VPN server range. (e.g. 192.
168.10.10) IP Pool End Address Changes the last address for the PPTP VPN server range. (e.g.
192.168.10.100) Note: For the VPN client computer, you will require a third party PPTP VPN software to be installed configured matching the PPTP VPN settings on your router. Typically, PPTP VPN software is pre-installed with most operating systems. Please refer to the your operating system User's Guide/Manual for configuring the VPN settings. See Appendix. To view the status of connected PPTP VPN clients, check the Connection Status section. When a PPTP VPN client is connected, they will be listed under Connection Status. You can click Disconnect to disconnect the PPTP VPN client.

6. Next to Authentication Protocol, check MS_CHAP and MS_CHAPv2. © Copyright 2012 TRENDnet. All Rights Reserved. 20 TRENDnet User's Guide Client-Server VPN (Client Mode) Configuration > Security Setting >VPN-PPTP Client Your router can be configured as a PPTP VPN client to connect to a PPTP VPN server allowing your LAN IP network access to through the VPN tunnel. This method should only be used when experiencing compatibility or connectivity issues with establishing an IPsec Site-to-Site VPN. Note: For connecting LAN network through a VPN over the Internet, it is strongly recommended to use an IPsec Site-to-Site VPN. To configure a PPTP Client-Server VPN tunnel between two VPN routers: VPN Router A Configuration (Server Mode) Configuration > Security Setting >VPN-PPTP Server TW100-BRV214 1. @@· Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to both routers under the Status page. See page 59 for checking the status page.
Example: VPN Router A WAN (Internet) IP Address: 10.10.10.10 VPN Router B WAN (Internet) IP Address: 10.10.
10.20 · Make sure the LAN IP network on each VPN router is different. Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 39 for changing the LAN IP address. Example: VPN Router A LAN IP Settings: 192.
168.10.1 / 255.255.255.0 VPN Router B LAN IP Settings: 192.168.100.1 / 255.255.

255.0 4. Next to Server virtual IP, enter the LAN IP address of your router. Note: The LAN IP address of your router is automatically entered therefore, it is recommended to leave this setting unchanged. 2. Click on Configuration at the top of the page, click on Security Setting, and click on VPN-PPTP Server. 3. Next to VPN-PPTP Server, check the Enable option to enable the PPTP server. © Copyright 2012 TRENDnet. All Rights Reserved.
21 TRENDnet User's Guide 5. Enter the IP address range to assign to PPTP VPN clients. Note: Please ensure that this range does not conflict with your DHCP server range. If you have not changed your LAN IP settings or DHCP server range, then you can leave hese settings at default. Router default DHCP server range: 192.
168.10.101-192.168.10.
199 10. Click Save at the bottom of the page to save the changes. TW100-BRV214 Note: If you would like to discard the changes, click Undo before you click Save. Clicking Refresh will reload the page. Clicking PPTP Client will bring you to the PPTP Client mode configuration page. · · IP Pool Start Address Changes the starting address for the PPTP VPN server range. (e.g. 192.168.

10.10) IP Pool End Address Changes the last address for the PPTP VPN server range. (e.g. 192.168.10.100) Note: For the VPN client computer, you will require a third party PPTP VPN software to be installed configured matching the PPTP VPN settings on your router. Typically, PPTP VPN software is pre-installed with most operating systems. Please refer to the your operating system User's Guide/Manual for configuring the VPN settings.
See Appendix. To view the status of connected PPTP VPN clients, check the Connection Status section. When a PPTP VPN client is connected, they will be listed under Connection Status. You can click Disconnect to disconnect the PPTP VPN client. 6.
Next to Authentication Protocol, check MS_CHAP and MS_CHAPv2. 7. Next to MPPE Encryption Mode, check the Enable option. 8. Next to Encryption Length, to ensure highest compatibility, check 40 bits, 56 bits, and 128 bits.
VPN Router B Configuration (Client Mode) Configuration > Security Setting >VPN-PPTP Client 9. Under User Accounts next to ID 1, enter the User Name and Password used by PPTP VPN clients to authenticate. Note: The same account can be used by multiple PPTP VPN clients. © Copyright 2012 TRENDnet. All Rights Reserved. 22 TRENDnet User's Guide 1. @@Note: If you changed router LAN IP address, you will need to log into the remote router using the new IP address instead of the default 192.168.10.1.

2. Click on Configuration at the top of the page, click on Security Setting, and click on VPN-PPTP Client. 3. Next to VPN-PPTP Client, check the Enable option to enable the PPTP client. · o TW100-BRV214 Manual This mode will allow you to manually control if the VPN connection is established or disconnected by clicking Connect or Disconnect buttons. MPPE (Microsoft Point-to-Point Encryption) This will enable MPPE if required by the PPTP server. NAT (Network Address Translation) This will enable NAT over the VPN tunnel in order to access the Internet. If the LAN IP network of both VPN routers is the same (e.g. 192.
168.10.1 / 255.255.255.
0), then leave the NAT option disabled.

[You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide]

http://yourpdfguides.com/dref/4129107

Note: It is strongly recommended that the LAN IP networks on both VPN routers are different. If the LAN IP network of both VPN routers is different, then enable the NAT option. Option o o 4. Review the settings below.

Based on the example, the client settings will be the following: · · Name Enter a name for the tunnel. (e.g. Tunnel 1) Peer IP/Domain The remote WAN (Internet) IP address of your remote VPN router. (e.g. 10.10.10.10) Note: If the remote router is using dynamic DNS, you can enter domain for the remote gateway instead of the WAN IP address.

Username Enter the user name account info required by the remote VPN router. (e.g. trendnet1) Password Enter the password account info required by the remote VPN router (e.g. trendnet1) Peer Subnet The remote LAN IP subnet/netmask in CIDR (Classless InterDomain Routing) notation or network of your remote router. (e.g. 192.168.

10.0/24 where the /24 represents 255.255.255.0 subnet mask) Connect The mode which the VPN tunnel should be connected.

o On demand (Recommended) This mode will connect only when the traffic is sent through VPN tunnel and disconnect automatically after the Maximum Idle Time specified is reached. Auto This mode will keep the tunnel always established. 10. Click Save at the bottom of the page to save the changes. Note: If you would like to discard the changes, click Undo before you click Save.

Clicking Refresh will reload the page. · · · Under Connection Status, click Connect to connect the PPTP VPN client. You can also click Disconnect to disconnect the PPTP VPN client. · o © Copyright 2012 TRENDnet. All Rights Reserved. 23 TRENDnet User's Guide L2TP (Layer 2 Tunneling Protocol) Client-Server VPN (Server Mode) Configuration > Security Setting >VPN-L2TP Server To configure your router to allow L2TP VPN connections from remote VPN client computers or devices: TW100-BRV214 1. @@2. Click on Configuration at the top of the page, click on Security Setting, and click on VPN-L2TP Server. 3. Next to VPN-L2TP Server, check the Enable option to enable the L2TP server.

4. Next to Server virtual IP, enter the LAN IP address of your router. Note: The LAN IP address of your router is automatically entered therefore, it is recommended to leave this setting unchanged. · Typically, the single client computer is connecting to the Internet through a router with NAT enabled. To establish a L2TP VPN tunnel when one of the VPN endpoints is behind a router with NAT enabled, L2TP VPN passthrough must be enabled on the router with NAT enabled. If the router with NAT enabled does not support L2TP VPN pass through, ports (UDP 1701, IP Protocol 47: GRE) may need to be forwarded to your VPN client computer. If the single client computer is connecting to the Internet through a router with NAT enabled, make sure the LAN IP network of the router NAT enabled is different from the LAN IP network of your VPN router. Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 39 for changing the LAN IP address. Example: VPN Router A LAN IP Settings: 192.

168.10.1 / 255.255.255.

0 Router with NAT enabled LAN IP Settings: 192.168.100.1 / 255.255.

255.0 · Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to your routers under the Status page. See page 59 for checking the status page. Example: VPN Router A WAN (Internet) IP Address: 10.10.10.10 5. Enter the IP address range to assign to L2TP VPN clients. Note: Please ensure that this range does not conflict with your DHCP server range. If you have not changed your LAN IP settings or DHCP server range, then you can leave hese settings at default.

Router default DHCP server range: 192.168.10.101-192.168.10.199 · · · IP Pool Start Address Changes the starting address for the L2TP VPN server range. (e.g. 192.

168.10.10) IP Pool End Address Changes the last address for the L2TP VPN server range. (e.g.

192.168.10.100) 6. Next to Authentication Protocol, check MS_CHAP and MS_CHAPv2.

© Copyright 2012 TRENDnet. All Rights Reserved. 24 TRENDnet User's Guide 7. Next to MPPE Encryption Mode, check the Enable option. Client-Server VPN (Client Mode) Configuration > Security Setting >VPN-L2TP Client TW100-BRV214 8. Next to Encryption Length, to ensure highest compatibility, check 40 bits, 56 bits, and 128 bits. Your router can be configured as a L2TP VPN client to connect to a L2TP VPN server allowing your LAN IP network access to through the VPN tunnel. This method should only be used when experiencing compatibility or connectivity issues with establishing an IPsec Site-to-Site VPN. Note: For connecting LAN network through a VPN over the Internet, it is strongly recommended to use an IPsec Site-to-Site VPN. To configure a L2TP Client-Server VPN tunnel between two VPN routers: 9.

Under User Accounts next to ID 1, enter the User Name and Password used by L2TP VPN clients to authenticate. Note: The same account can be used by multiple L2TP VPN clients. 10. Click Save at the bottom of the page to save the changes. Note: If you would like to discard the changes, click Undo before you click Save. Clicking Refresh will reload the page. Clicking L2TP Client will bring you to the L2TP Client mode configuration page. · Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to both routers under the Status page. See page 59 for checking the status page. Example: VPN Router A WAN (Internet) IP Address: 10.

10.10.10 VPN Router B WAN (Internet) IP Address: 10.10.10.

20 · Make sure the LAN IP network on each VPN router is different. Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 39 for changing the LAN IP address. Example: VPN Router A LAN IP Settings: 192.168.

10.1 / 255.255.255.0 VPN Router B LAN IP Settings: 192.168.100.1 / 255.255.255.

0 Note: For the VPN client computer, you will require a third party L2TP VPN software to be installed configured matching the L2TP VPN settings on your router. Typically, L2TP VPN over IPsec is pre-installed with most operating systems which your router does not support. See Appendix. To view the status of connected L2TP VPN clients, check the Connection Status section. When a L2TP VPN client is connected, they will be listed under Connection Status. You can click Disconnect to disconnect the L2TP VPN client. © Copyright 2012 TRENDnet. All Rights Reserved. 25 TRENDnet User's Guide VPN Router A Configuration (Server Mode) Configuration > Security Setting >VPN-L2TP Server TW100-BRV214 Note: Please ensure that this range does not conflict with your DHCP server range. If you have not changed your LAN IP settings or DHCP server range, then you can leave hese settings at default.

You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide

http://yourpdfguides.com/dref/4129107

Router default DHCP server range: 192.168.10.101-192.168.
10.199 · · IP Pool Start Address Changes the starting address for the L2TP VPN server range. (e.g. 192.
168.10.10) IP Pool End Address Changes the last address for the L2TP VPN server range. (e.g. 192.168.10.100) 6. Next to Authentication Protocol, check MS_CHAP and MS_CHAPv2.

7. Next to MPPE Encryption Mode, check the Enable option. 1. @@2. Click on Configuration at the top of the page, click on Security Setting, and click on VPN-L2TP Server. 3. Next to VPN-L2TP Server, check the Enable option to enable the L2TP server. 8. Next to Encryption Length, to ensure highest compatibility, check 40 bits, 56 bits, and 128 bits. 9.
Under User Accounts next to ID 1, enter the User Name and Password used by L2TP VPN clients to authenticate. Note: The same account can be used by multiple L2TP VPN clients. 4. Next to Server virtual IP, enter the LAN IP address of your router. Note: The LAN IP address of your router is automatically entered therefore, it is recommended to leave this setting unchanged.
10. Click Save at the bottom of the page to save the changes. 5. Enter the IP address range to assign to L2TP VPN clients. Note: If you would like to discard the changes, click Undo before you click Save.
Clicking Refresh will reload the page. Clicking L2TP Client will bring you to the L2TP Client mode configuration page. © Copyright 2012 TRENDnet. All Rights Reserved. 26 TRENDnet User's Guide TW100-BRV214 2. Click on Configuration at the top of the page, click on Security Setting, and click on VPN-L2TP Client. Note: For the VPN client computer, you will require a third party L2TP VPN software to be installed configured matching the L2TP VPN settings on your router. Typically, L2TP VPN over IPsec is pre-installed with most operating systems which your router does not support. See Appendix. To view the status of connected L2TP VPN clients, check the Connection Status section.

When a L2TP VPN client is connected, they will be listed under Connection Status. You can click Disconnect to disconnect the L2TP VPN client. 3. Next to VPN-L2TP Client, check the Enable option to enable the L2TP client. 4. Review the settings below. · · VPN Router B Configuration (Client Mode) Configuration > Security Setting >VPN-L2TP Client Name Enter a name for the tunnel. (e.g. Tunnel 1) Peer IP/Domain The remote WAN (Internet) IP address of your remote VPN router.
(e.g. 10.10.10.
10) Note: If the remote router is using dynamic DNS, you can enter domain for the remote gateway instead of the WAN IP address. Username Enter the user name account info required by the remote VPN router. (e.g. trendnet1) Password Enter the password account info required by the remote VPN router (e. g. trendnet1) Peer Subnet The remote LAN IP subnet/netmask in CIDR (Classless InterDomain Routing) notation or network of your remote router. (e.g. 192.168.10.0/24 where the /24 represents 255.255.255.

0 subnet mask) Connect The mode which the VPN tunnel should be connected. o On demand (Recommended) This mode will connect only when the traffic is sent through VPN tunnel and disconnect automatically after the Maximum Idle Time specified is reached. Auto This mode will keep the tunnel always established. Manual This mode will allow you to manually control if the VPN connection is established or disconnected by clicking Connect or Disconnect buttons. MPPE (Microsoft Point-to-Point Encryption) This will enable MPPE if required by the PPTP server. · · · · o o 1. @@Note: If you changed router LAN IP address, you will need to log into the remote router using the new IP address instead of the default 192.168.10.1.
· Option o © Copyright 2012 TRENDnet. All Rights Reserved. 27 TRENDnet User's Guide o NAT (Network Address Translation) This will enable NAT over the VPN tunnel in order to access the Internet. If the LAN IP network of both VPN routers is the same (e.g.
192.168.10.1 / 255.255.
255.0), then leave the NAT option disabled. Note: It is strongly recommended that the LAN IP networks on both VPN routers are different. If the LAN IP network of both VPN routers is different, then enable the NAT option. TW100-BRV214 GRE (Generic Routing Encapsulation)Tunneling Site-to-Site GRE Tunnel Configuration > Security Setting > GRE Tunnel To configure a Site-to-Site GRE tunnel between two routers: Based on the example, the client settings will be the following: · 10. Click Save at the bottom of the page to save the changes. Note: If you would like to discard the changes, click Undo before you click Save. Clicking Refresh will reload the page. Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to both routers under the Status page. See page 59 for checking the status page.

Example: Router A WAN (Internet) IP Address: 10.10.10.10 Router B WAN (Internet) IP Address: 10.10.10.20 Under Connection Status, click Connect to connect the L2TP VPN client. · Make sure the LAN IP network on each router is different. Note: Changing the LAN IP address of your router will change the LAN IP network of your router. See page 39 for changing the LAN IP address.
Example: Router A LAN IP Settings: 192.168.10.1 / 255.255.
255.0 Router B LAN IP Settings: 192.168.100.1 / 255.
255.255.0 You can also click Disconnect to disconnect the L2TP VPN client. © Copyright 2012 TRENDnet. All Rights Reserved. 28 TRENDnet User's Guide Router A Configuration · · TW100-BRV214 TTL Enter the Time to Live value. (Range 1-255, Recommended: 100) Subnet The remote LAN IP subnet/netmask in CIDR (Classless Inter-Domain Routing) notation or network of your remote router. (e.g. 192.

168.100.0/24 where the /24 represents 255.255.255.0 subnet mask) Enable Check this option to enable the tunnel. · Based on the example, the GRE settings will be the following: 4. Click Save at the bottom of the page to save the changes. 1. @@2.
Click on Configuration at the top of the page, click on Security Setting, and click on GRE Tunnel. 3. Review and configure the GRE Tunnel settings: Note: If you would like to discard the changes, click Undo before you click Save. If you are prompted to reboot, reboot the device to apply the changes. Router B Configuration · · · · Name Enter a name for the tunnel (e.
g. Tunnel1) Note: Do not use spaces in the name. The name must match on both routers. Tunnel IP Enter the tunnel virtual IP address. (e.
g. 1.1.1.1) Peer IP The remote WAN (Internet) IP address of your router. (e.g. 10.10.10.

10) Key Enter the key for the tunnel. (e.g. 12345) Note: The value 12345 is shown as an example. It is strongly recommended to enter your own key. Write down the key you enter as it will also need to be entered when configuring Router B.


You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide

http://yourpdfguides.com/dref/4129107

The preshared key can consist of up to five alphanumeric characters (a,b,C,?,, /,1,2, etc.) 1. @@Note: If you changed router LAN IP address, you will need to log into the remote router using the new IP address instead of the default 192.168.*
10.1. © Copyright 2012 TRENDnet. All Rights Reserved. 29 TRENDnet User's Guide 2.
Click on Configuration at the top of the page, click on Security Setting, and click on GRE Tunnel. 3. Review and configure the GRE Tunnel settings: TW100-BRV214 · · · · Name Enter a name for the tunnel (e.g. Tunnel1) Note: Do not use spaces in the name.
The name must match on both routers. Tunnel IP Enter the tunnel virtual IP address. (e.g. 1.1.1.2) Peer IP The remote WAN (Internet) IP address of your router. (e.g.

10.10.10.20) Key Enter the key for the tunnel.(e.g. 12345 Note: The value 12345 is shown as an example. It is strongly recommended to enter your own key. Write down the key you enter as it will also need to be entered when configuring Router B. The preshared key can consist of up to five alphanumeric characters (a,b,C,?,, /,1,2, etc.*
) · · TTL Enter the Time to Live value. (Range 1-255, Recommended: 100) Subnet The remote LAN IP subnet/netmask in CIDR (Classless Inter-Domain Routing) notation or network of your remote router. (e.g. 192.
168.10.0/24 where the /24 represents 255.255.255.
0 subnet mask) Enable Check this option to enable the tunnel. · Based on the example, the GRE settings will be the following: 4. Click Save at the bottom of the page to save the changes. Note: If you would like to discard the changes, click Undo before you click Save. If you are prompted to reboot, reboot the device to apply the changes. © Copyright 2012 TRENDnet. All Rights Reserved. 30 TRENDnet User's Guide TW100-BRV214 Access Control Filters Access control basics Configuration > Security Setting MAC Control Configuration > Security Setting > MAC Control Every network device has a unique, 12-digit MAC (Media Access Control) address. Using MAC filters, you can allow only known MAC addresses to connect your network and deny all other unknown MAC addresses from connecting to your network. Note: Denied MAC addresses will not be able to connect to your router management page, or access the Internet.

1. @@2. Click on Configuration at the top of the page, click on Security Setting, and click on MAC Control. 3. Add the MAC addresses to the MAC Table first before applying the MAC filter function. Note: MAC filter can be configured to allow access to the listed MAC address and deny all others unlisted or vice versa. The recommended function is to choose to only allow access to the MAC addresses listed and deny all others unlisted because it is easier to determine the MAC addresses of devices in your network then to determine which MAC addresses you do not want to allow access. To simplify configuration, click the DHCP clients drop-down list to select and computer or device that is currently connected to your router. Once you have selected the computer or device, click the ID drop-down list to select which entry to copy the selected DHCP client information and click Copy To. You can choose a DHCP client from the drop down list or you can manually enter the MAC/IP address information.
6. Click Save at the bottom of the page to save the changes. Note: If you would like to discard the changes, click Undo before you click Save. Note: If you are manually entering the MAC/IP address information, refer to your computer or device documentation to find the MAC address. 4.
After the MAC address (e.g. 00:11:22:AA:BB:CC) and IP address (e.g. 192.
168.10.101) information is entered, check the Allow option next to the entry to allow network access to this MAC address. Note: Any unspecified MAC/IP addresses or entries without the Allow option checked will be denied network access. 5. Next to MAC Address Control at the top of the page, check the Enable option to enable MAC filtering. Note: Please add MAC/IP address entries first before enabling. · · Next Displays the next page to the current page of MAC filtering entries. Previous Displays the previous page to the current page of MAC filtering entries. © Copyright 2012 TRENDnet.

All Rights Reserved. 31 TRENDnet User's Guide URL Filters Configuration > Security Setting > URL Filters You may want to allow or block computers or devices on your network access to specific websites (e.g. www.trendnet.com, etc.), also called domains or URLs (Uniform Resource Locators). 1. @@2. Click on Configuration at the top of the page, click on Security Setting, and click on URL Filters.
3. Next to URL Filter, check the Enable option to enable URL filtering. Additional URL filter options: 5. To save changes, click Save at the bottom of the page. TW100-BRV214 Note: If you would like to discard the changes, click Undo before you click Save.
Log DNS Query Checking the Enable optin will log all URL or domain queries in the router log. 4. In the entry list, choose an entry and under URL, enter the URL or domain name (e.g. www.
trendnet.com) you would like to block access. Privilege IP Addresses Range Enter the IP address range (use last IP address number only such as 192.168.10.101-192.168.10.110) to exclude from Domain/URL filtering. IP addresses included in the range will not be blocked from accessing any of the URLs specified.

· · Drop Checking the option will drop or block access to the specific URL or domain. Log Checking the option will log the access requests to the specific URL or domain in the router log. Note: Checking the Log option only will not block access. You will need to check the Drop option to block access. Enable Check the enable option to enable the URL/domain filter. · © Copyright 2012 TRENDnet. All Rights Reserved. 32 TRENDnet User's Guide Keyword Blocking Configuration > Security Setting > Keyword Blocking You may want to allow or block computers or devices on your network access to web content with specific keywords instead of complete URL to generally allow or block computers or devices access to websites that may contain the keyword in the URL or on the web page. 1. @@2.
Click on Configuration at the top of the page, click on Security Setting, and click on Keyword Blocking. 3. Next to Keyword Blocking, check the Enable option to enable keyword blocking. Packet Outbound/Inbound Filters Configuration > Security Setting > Packet Filters TW100-BRV214 You may want specify inbound or outbound access control to allow/deny sources (or Internet IP addresses) to your network from the Internet or from computers or devices on your network to the Internet. Firewall rules may allow for more granular control of specific inbound and outbound access between your network and the Internet. It is recommended that these settings remain set to default unless you are knowledgeable about the effects of changing the firewall rule configuration.


You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide
http://yourpdfguides.com/dref/4129107

It is possible to have undesirable functionality from your router if these settings are improperly modified. 1. @@2. Click on Configuration at the top of the page, click on Security Setting, and click on Packet Filters.
Outbound Packet Filter 4. In the entry list, choose an entry and under keyword, enter the keyword you would like to block access and check the Enable option. You may want apply outbound packet filters to allow or deny access of specific traffic from computers or devices on your local network to the Internet. To configure outbound packet filters: Next to Outbound Packet Filter, check the Enable option to enable outbound filtering. 5. To save changes, click Save at the bottom of the page. Note: If you would like to discard the changes, click Undo before you click Save. · · Select Allow all to pass except those match the following rules to allow all traffic and deny only the filters specified in the list. Select Deny all to pass except those match the following rules to deny all traffic and allow only the filter specified in the list. © Copyright 2012 TRENDnet.

All Rights Reserved. 33 TRENDnet User's Guide Review the outbound packet filter settings. Inbound Packet Filter TW100-BRV214 You may want apply inbound packet filters to allow or deny access of specific traffic from the Internet to computers or devices on your local network. To configure inbound packet filters: Click Inbound Filter at the bottom of the outbound packet filter page. · · Source IP Enter the source IP address or computer/device IP address on your local network to apply the filter. (e.g. 192.168.10.
101) Destination IP : Ports Enter the destination IP address of the computer/device located on the Internet and port number to apply the filter. To specify all port numbers, do not specify any value for Ports field. For specific port numbers, enter a port number or range within the range of 1-65535 (e.g. 21 or 21-30) in the Ports field.
Note: Typically, you can specify 0.0.0.0 for any destination IP address located on the Internet or enter the specific IP address. (e.g. 10.10.10.200) · · · Protocol Select the protocol type to filter. TCP, UDP, or you can select Both to choose both protocol types. Enable Check the option to enable the filter. Use rule# - Click the drop-down list to select a pre-defined schedule. The filter will only be active during the time period defined in the pre-defined schedule. Note: Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule.

See page 37 to configure Time Settings and see page 51 to create a schedule. Review the inbound packet filter settings. To save changes, click Save at the bottom of the page. Note: If you would like to discard the changes, click Undo before you click Save. Next to Inbound Packet Filter, check the Enable option to enable inbound filtering. · · Select Allow all to pass except those match the following rules to allow all traffic and deny only the filters specified in the list. Select Deny all to pass except those match the following rules to deny all traffic and allow only the filter specified in the list. Clicking MAC Level will bring you to the MAC Control configuration page. See MAC Control section. · Source IP Enter the source IP address or computer/device IP address on your located on the Internet to apply the filter.
(e.g. 192.168.10.
101) Note: Typically, you can specify 0.0.0.0 for any source IP address located on the Internet or enter the specific IP address. (e.g. 10.10.10.200) © Copyright 2012 TRENDnet. All Rights Reserved. 34 TRENDnet User's Guide · Destination IP : Ports Enter the destination IP address of the computer/device located on your local network and port number to apply the filter. To specify all port numbers, do not specify any value for Ports field. For specific port numbers, enter a port number or range within the range of 165535 (e.g.

21 or 21-30) in the Ports field. Protocol Select the protocol type to filter. TCP, UDP, or you can select Both to choose both protocol types. Enable Check the option to enable the filter. Use rule# - Click the drop-down list to select a pre-defined schedule. The filter will only be active during the time period defined in the pre-defined schedule. Note: Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 37 to configure Time Settings and see page 51 to create a schedule. To save changes, click Save at the bottom of the page. Note: If you would like to discard the changes, click Undo before you click Save.
TW100-BRV214 · · · Clicking MAC Level will bring you to the MAC Control configuration page. See MAC Control section. © Copyright 2012 TRENDnet. All Rights Reserved. 35 TRENDnet User's Guide TW100-BRV214 Change your router login password Configuration > Basic Setting > Password 1.
@@2. Click on Configuration at the top of the page, click on Basic Setting, and click on Password. Advanced Router Setup Access your router management page Note: Your router management page http://192.168.10.
1 is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide. 1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to http://192.168.10.1.

Your router will prompt you for a password. 3. In the Old Password field, enter the current password (default: admin). New Password field, enter the new password and in the New Password field, and in the Reconfirm field, retype the new password again to confirm. 2. Enter the default user name and password and then click Login. Default System Password: admin 4. To save changes, click Save at the bottom of the page. Note: If you would like to discard the changes, click Undo before you click Save. Note: If you change the router login password, you will need to access the router management page using the new password instead of the default password "admin".
© Copyright 2012 TRENDnet. All Rights Reserved. 36 TRENDnet User's Guide Set your router date and time Configuration > Advanced Setting > System Time 1. @@2. Click on Configuration at the top of the page, click on Advanced Setting, and click on System Time.
3. Next to Time Zone, click the drop-down list to select your time zone. · TW100-BRV214 Click Save at the bottom of the page to save the changes, then click Sync with Time Server and wait for a status result. Note: If you would like to discard the changes, click Undo before you click Save. OR Sync with your computer time - Click Sync with my PC (Date & Time of your computer) and wait for a status result, then click Save to save the changes.
5. To verify the current system time, click on Configuration, click on Advanced Setting, and click Setting Overview to check the system time.


You're reading an excerpt. Click here to read official TRENDNET TW100-BRV214 user guide
http://yourpdfguides.com/dref/4129107