

Quick Note 19

Manage a Router Securely with HTTP over SSH Tunnel

Digi Technical Support

September 2016

Contents

1	Inti	roduction	3
	1.1	Outline	3
	1.2	Assumptions	3
	1.3	Corrections	3
	1.4	Version	3
2	Coi	nfiguration	4
	2.1	Generate a New SSH Private Key	4
	2.2	Configure the SSH Server	4
	2.3	Test SSH Connectivity	5
	2.4	Configure the SSH Client for Port Forwarding	6
	2.5	Port Forwarding Test	8
3	Ge	nerate the Key Pair	9
	3.1	Configure a User with the Public Key File	. 12
	3.2	Configure the SSH Client Software	. 14
4	Tes	st SSH Access	. 16
5	Sav	ve Configuration	17

1 INTRODUCTION

1.1 Outline

To securely administer a Digi TransPort router, SSH, VPN or SSL can be used. The document explains how to use SSH to secure the router HTTP (web GUI) management traffic. It is possible to transport HTTP traffic in the SSH tunnel and have ease of management through the web interface without compromising on security. Security can be increased further by using an RSA key pair to handle the authentication of the connection. When using public and private keys, the regular user passwords configured on the router are not used, the client must have the private key configured within the SSH software that can be verified by the public key on the router.

Management of a TransPort via HTTP is used in this Quick Note (QN) by way of an example. It may be that the reader wishes to use an SSH tunnel to connect to some third party equipment on port 80 or some other TCP port via SSH. This can be achieved by following this QN and making changes to the destination IP address and port number in section 2.4.

1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. This QN applies only to:

Model: All Digi TransPort routers

Firmware versions: 5.123 and later

NOTE: This QN has been specifically rewritten for firmware release 5.123 and later but the original QN was testing as working for TransPorts running 5.050 and later. TransPorts running earlier firmware may find that the screenshots do not accurately reflect what will be seen.

Configuration: This QN assumes that the TransPort is set to its factory default. Most configuration commands are only shown if they differ from the factory default.

1.3 Corrections

Requests for corrections or amendments to this QN are welcome and should be addressed to: <u>tech.support@digi.com</u>

Requests for new QNs can be sent to the same address.

1.4 Version

Version Number	Status
1.0	Published
2.0	Updated for New Web Gui after 5123
	Updated screenshots and
2.1	instructions for new web interface,
	rebranding (Sept 2016)

2 CONFIGURATION

This process involves generating a private key on the TransPort then configuring the SSH to use the key for SSH connections.

All new TransPorts have a factory generated private key named privSSH.pem and SSH access is pre-configured. If you wish to use this key rather than generating a new one, skip to section 2.3

2.1 Generate a New SSH Private Key

ADMINISTRATION > X.509 CERTIFICATE MANAGEMENT > KEY GENERATION

Browse to the link above and enter the following values:

Parameter	Setting	Description
Key Filename	<name_of_key>.pem</name_of_key>	Enter a name for the private key that will be generated.
Key Size	<key_size></key_size>	Select a key size in bits.

NOTE: The larger the key, the more secure the connection, but also the larger the key, the slower the connection.

Click on the 'Generate Key' button to start the creation of the private key. After a few seconds, the browser will start updating with the progress of the key generation. When the key has been generated, the information below the 'Generate Key' button in the screenshot below will be shown.

The private key has now been generated and saved to FLASH as "privSSH.pem".

Administration - X.509 Certificate Management > Key Generation

 Certificate Authorities (CAs) IPsec/SSH/HTTPS Certificates
Key files
▼ Key Generation
Key filename: privSSH.pem ▼ Key size: 2048 ▼ bits
Save in SSHv1 format
Generate Key

Figure 1: Generate SSH Key

2.2 Configure the SSH Server

CONFIGURATION > NETWORK > SSH SERVER > SSH SERVER o

Browse to the above link; if the default values are correct, just enter the name of the private key generated in the previous step into the 'Host key 1 filename' field and enable Port Forwarding:

Parameter	Setting	Description
Enable SSH Server	Ticked	Option to enable SSH Server
Host Key 1 Filename	<ssh_key_file_name></ssh_key_file_name>	SSH Key file name generated in section 2.1
Enable Port Forwarding	Ticked	Allows access through the tunnel to the router

<u>Configuration - Network > SSH Serv</u>	<u>ver</u> > <u>SSI</u>	H Server 0		
▼ SSH Server 0				
Enable SSH Server				
Use TCP port:	22			
Allow up to	5	connections		
Host Key 1 Filename:	privSSH.	pem		
Host Key 2 Filename:				
Maximum login time:	60	seconds		
Maximum login attempts:	3			
Use Deflate compression:	No			
	Yes,	level 6 🔻		
Enable Port Forwarding				
Command Session IP Address:			Port:	0

Figure 2: SSH Server Configuration

Then click the '**Apply**' button.

NOTE: Depending on the running TransPort firmware version, these may be the default settings.

2.3 Test SSH Connectivity

A normal SSH connection to the router should now be possible without RSA authentication.

2.4 Configure the SSH Client for Port Forwarding

Configure Putty or any other SSH client to listen on a local port and forward this to the TransPort on port 80.

🕵 PuTTY Configuratio	n	
Category:		
Terminal Keyboard Hell Features Window Window	•	Options controlling SSH port forwarding Port forwarding Local ports accept connections from other hosts Remote ports do the same (SSH-2 only) Forwarded ports: Remove
Behaviour Translation Selection Colours Data Proxy Table t	ш	Add new forwarded port: Source port 81 Add Destination 10.1.51.2:80
Flogin Rlogin SSH Kex Auth TTY X11 Tunnels Bugs	+	 ● Local ● Remote ● Dynamic ● Auto ● IPv4 ● IPv6
About		Open Cancel

Figure 3: Putty Port Forwarding Configuration

In the Putty menu, expand the menus to **Connection > SSH > Tunnels**

Configure the '**Source port**'; this is the local port that PuTTY will listen on.

Configure the '**Destination**'; this is the LAN IP address and TCP port of the router that needs to be managed.

Click the **Add** button to confirm the configuration and the data entered will move into the top box titled **`Forwarded ports:**'.

RuTTY Configuration	1	
Putty Configuration Category: - Terminal - Keyboard - Bell - Features - Window - Appearance - Behaviour - Translation - Selection - Colours - Connection - Data - Proxy - Telnet - Rlogin - SSH - Kex - Auth - Try - X11 - Turansla	E	Options controlling SSH port forwarding Port forwarding Local ports accept connections from other hosts Remote ports do the same (SSH-2 only) Forwarded ports: Remove L81 10.1.51.2:80 Add new forwarded port: Source port Add Destination Image: Destination
About	Ŧ	Open Cancel

Figure 4: Putty Port Forwarding Configured

In the PuTTY menu, click on '**Session**', enter the public IP address of the router to manage, and select SSH. The port will change to 22.

Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Selection	
Close window on exit: Always Only on clean exit	

Figure 5: Putty Session Configuration

Click on "Open" and log in to the TransPort using SSH, the normal username and password.



Figure 6: Successful Connection Using Putty

PuTTY is now listening on port 81 for local connections.

2.5 Port Forwarding Test

Open the web browser and enter the following address to manage the router:

http://127.0.0.1:81



Figure 7: Digi TransPort Configuration via SSH Port Forwarding

HTTP will be forwarded to the router over the SSH tunnel for secure management.

If higher security is required, public and private key pairs can be used. The rest of this QN configures the key pair.

3 GENERATE THE KEY PAIR

Download a copy of PuTTYgen. This will be used to create the public and private keys.

PuTTY Key Generator	$\overline{\mathbf{X}}$
ile Key Conversions Help	
∕ Key No key.	
Actions Generate a public/private key pair	Generate
Load an existing private key file	Load
Save the generated key	Save public key Save private key
Parameters	
Type of key to generate: O SSH-1 (RSA)	◯ SSH-2 DSA
Number of bits in a generated key:	1024

Figure 8: Putty Generate Key

Click on 'Generate' to start the key generation process:

Full I key belief ator		_
ile Key Conversions Help		
Key		
Please generate some randomness by moving	the mouse over the bla	nk area.
Astron		
~ Actions		
Actions Generate a public/private key pair		Generate
Actions Generate a public/private key pair Load an existing private key file		Generate
Actions Generate a public/private key pair Load an existing private key file Save the generated key	Save public key	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters	Save public key	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate: OSSH-1 (RSA)	Save public key	Generate Load Save private key

Figure 9: Putty Key Generation in Progress

Move the mouse pointer around below the white bar to generate randomness and the bar will fill up with green blocks. When the process is complete, the following screen will be shown:

Key		
Public key for pasting	; into OpenSSH authorized_ke	/s file:
ssh-rsa AAAAB3NzaC1yc2E /kaLzCXt1uu5ELdK3 dRz0U/poTxvawW1 rsa-key-20071127	AAAABJQAAAIBwpPmB4g0Jfr JIQgj45KXJjlgsdAmQDNvnDTY MgvnhLwYAJUXiAkiejG9TYn1	kkoro3PzBz10R4VM92oFRyP903k MijZ7962ljYthQPLD4FNKaCO35Eq dd1SltRRPhN5kMX3smhCviTUw==
Key fingerprint:	ssh-rsa 1023 2d:09:cd:0b:4	7:b3:85:da:14:f0:87:3a:d7:06:c8:04
Key comment:	rsa-key-20071127	
Key passphrase:		
Confirm passphrase:		
Actions		
Generate a public/pr	ivate key pair	Generate
Load an existing priva	ate key file	Load
Save the generated I	key Sa	ve public key Save private key
Parameters		
	-1	

Figure 10: Putty Key Generated

Copy the text in the top part of PuTTYgen, headed "Public key for pasting into OpenSSH authorized_keys file" to the clipboard:

PuTTY Key	Generator			2
ile Key Conve	ersions Help			
Key				
Public key for p	basting into OpenSS	H authorized_	keys file:	
ssh-rsa AAAAB3NzaC /kaLzCXtluu5 dRz0U/poTxv rsa-key-20071	1yc2EAAAABJQAA ELdK9lQgj45KXJjlgs rawWMgvnhLwYAJ 127	AlBwpPmB4g(₃dAmQDNvnD UXiAkieljG9TY	Dyfnkkoro3PzBzI0F ITYMijZ7962ljYthQ ín1dd1SltRRPhN5	AVW92oFRyP903k PLD4FNKaC035Eq kMX3smhCviTUw==
Key fingerprint:	ssh-rsa 102	23 2d:09:cd:0b	o:47:b3:85:da:14:f0):87:3a:d7:06:c8:04
Key comment:	rsa-key-20	071127		
Key passphras	e:			
Confirm passph	nrase:			
Actions				
Generate a put	blic/private key pair			Generate
Load an existin	ig private key file			Load
Save the gene	rated key		Save public key	Save private key
Parameters				
Type of key to OSSH-1 (RS)	generate: A) ()	SSH-2 RSA	⊖ s:	SH-2 DSA
Number of bits	in a generated key:			1024

Figure 11: Copy Public Key

Open Notepad; paste the text from the clipboard and save the document as "public.pem":

🕞 public.pem - Notepad	
File Edit Format View Help	
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIBwpPmB4g0Jfnkkoro3PzB	zIOR4VM92oFRyP903k/kaLzCXtIuu5ELdK9IQgj45KXJj1gsdAmQDNvnt
×)

Figure 12: Save Public Key to Text File

NOTE: The pasted text should occupy one (1) line only.

Transfer the public.pem file onto the TransPort using an FTP Client.

Enter a Key passphrase and confirm it in the fields shown, then click the '**Save private key**' button. Save it with the name "private.ppk":

PuTTY Key Ge	nerator	
e Key Conversio	ns Help	
Key		
Public key for past	ng into OpenSSH authorized_keys	file:
sshrsa AAAAB3NzaC1yc /kaLzCXtluu5ELd dRz0U/poTxvaw rsa-key-20071127	2EAAAABJQAAAIBwpPmB4g0Jfnk K9lQgj45KXJjlgsdAmQDNvnDTYN WMgvnhLwYAJUXJAkieljG9TYn1d	koro3PzBzI0R4VM92oFRyP903k lijZ7962ljYthQPLD4FNKaC035Eq d1SltRRPhN5kMX3smhCviTUw==
Key fingerprint:	ssh-rsa 1023 2d:09:cd:0b:47:	b3:85:da:14.f0:87:3a:d7:06:c8:04
Key comment:	rsa-key-20071127	
Key passphrase: -	→	
Confirm passphras	•••••	
Actions		
Generate a public/	private key pair	Generate
Load an existing p	ivate key file	Load
Save the generate	d key Sav	e public key Save private key
Parameters		
Type of key to gen OSSH-1 (RSA)	erate:	◯ SSH-2 DSA
Number of bits in a	generated key:	1024

Figure 13: Save Putty Private Key

3.1 Configure a User with the Public Key File

CONFIGURATION - SECURITY > USERS > USER o - 9 > USER <N>

Navigate to the above link; enter a name for the user in the 'Username' field.

Enter a random, non-dictionary based password into the **Password** fields. This password will not be used, but should the RSA authentication fail, the user will be displayed a password prompt.

Select the Public Key from the dropdown list. This is the one that was created and FTP'd onto the TransPort in the previous steps.

Parameter	Setting	Description			
Licername	diser names	Login username for the user to access the			
Usemanie		router			
Password	disor Passwords	Password for user to use if the SSH public			
Passworu		private key authentication fails			
Confirm Decoverd	d lear Decoverds	Confirm password for user to use if the SSI			
Commin Password	<usei_passworu></usei_passworu>	public private key authentication fails			
Dublic Kov file	den file names nam	Name of the public key file for this user			
Public Key file:	<key_me_name>.pem</key_me_name>	generated above and FTP'd to the TransPor			

Configuration - Security > Users > User 0 - 9 > User 1



Figure 14: Configure User to Authenticate with Public Key

Click the 'Apply' button.

3.2 Configure the SSH Client Software

The SSH client software (e.g. PuTTY) will need to be configured to use the private key generated in the previous steps.

In PuTTY, this is done by expanding **Connection > SSH > Auth** and entering the location of the private key file in the field titled 'Private key file for authentication':

🕵 PuTTY Configuratio	n	?
Category:		
Category: Session Category: Category: Category: Session Category: Category: Session Sell Sel	* III	Options controlling SSH authentication Bypass authentication entirely (SSH-2 only) Authentication methods Authentication methods Attempt authentication using Pageant Attempt TIS or CryptoCard auth (SSH-1) Attempt "keyboard-interactive" auth (SSH-2) Authentication parameters Allow agent forwarding Allow attempted changes of usemame in SSH-2 Private key file for authentication: C: 'private.ppk
Rilogin SSH Kex Auth TTY X11 About	Ŧ	Open Cancel

Figure 15: Configure Putty to use the Private Key

Expand **Connection > Data** and enter the username to be used for this connection:

🕵 PuTTY Configuration	n		?
Category:			
Session		Data to ser	nd to the server
Logging		Login details	
Ierminal Keyboard		Auto-login usemame	ssh-user
Eeatures		Terminal details	
		Terminal-type string	xterm
Appearance Behaviour		Terminal speeds	38400,38400
Translation Selection	Ε	Environment variables	
Colours		Variable	Add
		Value	Remove
Data			
Telnet			
Rlogin			
SSH Ker			
Auth			
TTY			
×11	Ŧ		
About	Help		Open Cancel

Figure 16: Configure Putty to Automatically Use the Correct Username for this Connection

Return to **Session** and name the connection by typing something meaningful into the blank text box below 'Saved Sessions' and click 'Save':

Real Putty Configuration	1	? ×
Category: Session Logging Category: Logging Category: Logging Category: Selection Colours Colours Connection Data Proxy Telnet Rlogin SSH Connection Connection Connection Colours Colours Colours Connection Colours Colours Colours Connection Colours Connection Colours Colours Colours Colours Colours Colours Colours Connection Colours Colours Colours Connection Colours Colours Colours Connection Colours C		Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Pot 217.34.13.12 22 Connection type: Raw Raw Telnet Rlogin Tensport QN19 SSH Serial Load, save or delete a stored session Saved Sessions Digi Transport QN19 Load Default Settings Load 1306712 Save BP > Radiator Save BP > MASTER VC Save BP > SLAVE VC Delete MASTER VC> BP Close window on exit: Always Never Only on clean exit
About	Help	Open Cancel

Figure 17: Save the Putty Setup for Future Connection to Remote Router

4 TEST SSH ACCESS

Click the 'Open' button in PuTTY to connect:

😵 PuTTY Configuration			? ×
Category:			
	_	Basic options for your PuTTY se	ssion
Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin SSH Kex Auth TTY X11		Specify the destination you want to conner Host <u>Name</u> (or IP address) 217.34.13.12 Connection type: <u>Raw</u> <u>Telnet</u> Rlogin <u>SSF</u> Load, save or delete a stored session Sav <u>ed</u> Sessions Digi Transport QN19 Default Settings 1306712 BP > Radiator BP > MASTER VC BP > SLAVE VC MASTER VC> BP MASTER VC> BP MASTER VC> Test Lab Close window on exit: Aways Never <u>O</u> Only on cl	ct to <u>Port</u> 22 Serial <u>Load</u> <u>Save</u> <u>Delete</u>
<u>A</u> bout <u>H</u>	lelp	Open	<u>C</u> ancel

Figure 18: Use Saved Configuration to Connect to Remote Digi TransPort

The first time you connect to the remote router and the private key is loaded into PuTTY, you will be prompted to enter the passphrase that was configured for the private key previously in PuTTYgen. Access to the CLI will now be granted.



Figure 19: Successful Connection to Remote Digi TransPort Router

5 SAVE CONFIGURATION

ADMINISTRATION > SAVE CONFIGURATION

Browse to the link above and then click 'Save'.

Administration - Save configuration

Save current configuration to Config 0 (power up) 🔻
Save
Save all configuration. This includes the following
 Save the current configuration to config 0 Save the current firewall
 Save all sregisters on all ports to profile 0 Save all PAD parameters on all PADs to profile 0
Save All

Figure 20: Save TransPort Configuration