ADTRAN

AOS

SSH Port Forwarding for Remote AOS Device Management

Basic Configuration Guide

October 2018
6AOSCG0067-29B

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

Revision History

Rev B	October 2018	Initial release of document in this format. Document updated to include new supported security ciphers for the AOS firmware R13.4.0 release.

Table of Contents

List of Figures

List of Tables

1 Overview

This configuration guide provides an overview of the secure shell (SSH) port forwarding feature for remote device management in the ADTRAN Operating System (AOS), and includes the Command Line Interface (CLI) configuration options available for configuring and using SSH port forwarding in multiple network situations. Additionally, troubleshooting information and additional documentation resources are also provided.

1.1 Intended Audience

The intended audience for this information is the network administrator using and configuring the AOS device. The instructions assume familiarity with the intended use of the equipment, basic required installation and configuration skills, and knowledge of local and accepted networking practices.

1.2 Document Structure

Table 1 lists the topics contained in this document

Table 1. Topic List

1.3 Hazard and Conventional Symbols

The following Hazard symbols are used throughout this guide:

WARNING!
Warning: Service affecting. Possible risk of system failure.

CAUTION!
Caution: Indicates that a failure to take or avoid a specific action could result in a loss of data.

NOTICE!
Notice: Provides information that is essential to the completion of a task.

NOTE
Note: Information that emphasizes or supplements important points of the main text.

1.4 Related Online Documents and Resources

Refer to Table 2 for additional information for this product.

Documentation for AOS products is available for viewing and download directly from the ADTRAN Support Community website, available online at https://supportforums.adtran.com.

Table 2. Related Online Documents and Resources

Title	Description
AOS Command Reference Guide	Document outlining all available AOS commands, their variations and parameters, and their uses.
Configuring SSH Public Key Authentication	Configuration guide outlining the necessary steps to configure SSH public key authentication in AOS products.

2 SSH Port Forwarding Overview

Port forwarding via SSH is a technology that uses a secure tunnel between two devices to relay data from other services. This secure tunnel can be used to forward data from services that are inherently insecure. SSH port forwarding on AOS devices supports tunneling of the following applications: Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), SSH, and Telnet. This feature can be used to manage an AOS device remotely.

When you create an SSH port forward instance on an AOS device, you open an SSH tunnel between a port on the AOS device and a port on the remote computer. Any traffic to the designated port on the remote computer forwards through the tunnel to the local port on the AOS device. Figure 1 illustrates SSH port forwarding connections.

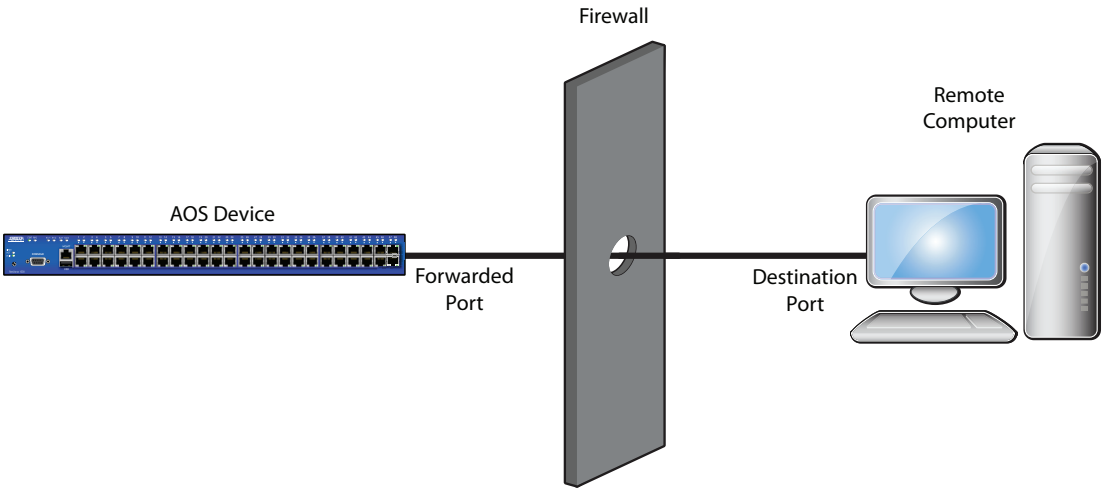

Figure 1. SSH Port Forwarding Traffic Flow

3 Hardware and Software Requirements and Limitations

The steps outlined in this guide are compatible with AOS switch products running AOS firmware version R11.4.0 or later.

NOTE

The maximum number of simultaneous SSH port forwards is 10. However, this number could be reduced if there are not enough Transmission Control Protocol (TCP) resources due to other applications using them. The SSH port forward maximum refers to the number of SSH ports that can be forwarded regardless of the number of sessions using the service associated with the forwarded port. For example, if port 22 is forwarded for Telnet, then Telnet will allow up to four simultaneous Telnet sessions. Even if four people Telnet in to the unit via the SSH port forward, the forward of port 22 uses only one of the 10 maximum SSH port forwards.

The SSH port forwarding feature has the following requirements:

- You must have an external SSH server to terminate the SSH sessions generated by the AOS device. The AOS device must have IP connectivity to the server, and the server must have one or more user accounts created that can be referenced by the AOS SSH client when initiating SSH port forwards. For more information regarding configuration of an SSH server, refer to the documentation for your particular server.
- Your network must allow encrypted outbound sessions to be created through your firewall. Most firewalls allow encrypted outbound sessions by default.

In AOS firmware release R13.4.0, support for the following SSH security algorithms and ciphers was added to AOS products:

- diffie-hellman-group14-sha1 KEX algorithm
- hmac-sha2-256 HMAC algorithm
- aes128-ctr cipher
- aes256-ctr cipher

4 Configuring SSH Port Forwarding Using the CLI

SSH port forwarding is configured using the CLI. The following sections outline the commands necessary for configuring and using SSH port forwarding.

5 Accessing the CLI

To configure SSH port forwarding using the CLI, connect to the AOS device using these steps:

1. Boot up the device.
2. Telnet to the device (**telnet** *<ip address>*), for example:

```
telnet 10.10.10.1
```

NOTE
If during the device's setup process you have changed the default IP address (10.10.10.1), use the configured IP address.

3. Enter your user name and password at the prompt.

NOTE
The AOS default user name is **admin** and the default password is **password**. If your device no longer has the default user name and password, contact your system administrator for the appropriate user name and password.

4. Enable your device by entering **enable** at the prompt as follows:

```
>enable
```

5. If configured, enter your Enable mode password at the prompt.

6 Enabling SSH Port Forwarding

Enable SSH port forwarding by entering the **ssh port-forward** *<port-forward port> <url>* **[port** *<port>***] [password** *<password>* **| privkey** *<filename>* **| myprivkey dsa]** command from the Enable Mode prompt. Use the **no** version of this command to disable the SSH port forwarding instance. The various parameters for this command are outlined and described in Table 3 on page 13.

Table 3. SSH Port Forwarding Enable Command Parameters

Parameter	Description
<port-forward port>	Specifies the forwarded port on the local unit. Services that correspond to the specified port will be forwarded. For example, if a unit uses TCP port 443 for HTTPS, using an SSH port forward port of 443 would forward the HTTPS process.
<url>	Specifies the uniform resource locator (URL) of the far end listening address. The format of the URL string must be **user@server:remote-port**, for example, MGARCIA@10.10.10.1:7000. Optionally, you may include the IP address of an interface on the remote machine using the format **user@server:remote-port:FarEndListenAddress**, for example, MGARCIA@10.10.10.1:7000:10.10.10.2. If a far end listening address is not included as part of the URL, **localhost** is assumed and only those users logged into the remote machine can use the tunnel.
port *<port>*	Optional. Specifies a destination port to use for underlying SSH protocol instead of the default SSH port 22. Valid range is **1** to **65535**.
privkey *<filename>*	Optional. Specifies a private key file to use for SSH authentication.
password *<password>*	Optional. Specifies a password to use for SSH authentication. If you do not specify a password when using this command, you will be prompted for a password for the far end machine after entering the command.
myprivkey dsa	Optional. Specifies to use the AOS unit's digital signature algorithm (DSA) private key for SSH authentication.

6.1 SSH Port Forwarding Command Usage Examples

The following sections illustrate different ways to use the **ssh port-forward** command to enable and configure SSH port forwarding.

6.1.1 SSH Port Forward Using Default Destination Port

The following example uses the **ssh port-forward** command to configure SSH port forwarding using a default destination port. An SSH port forward instance is created between the AOS device and machine 10.10.10.1, forwarding Telnet (port **23**) to the remote machine (**10.10.10.1**) using port **7000** on the remote machine. The user name on the remote machine is **MGARCIA**, and the command will prompt for a password. In this example, a user who logs into the remote machine and then telnets to **localhost** at port 7000 will receive a telnet prompt from the AOS device. To configure SSH port forwarding in this manner, enter the command from the Enable mode prompt as follows:

```
>enable
#ssh port-forward 23 MGARCIA@10.10.10.1:7000
```

6.1.2 SSH Port Forward Using DSA Private Key Authentication

The following example uses the **ssh port-forward** command to configure SSH port forwarding using DSA private key authentication. An SSH port forward instance is created between the AOS device and machine 10.10.10.1, forwarding Telnet (port **23**) to the remote

machine (**10.10.10.1**) using port **7000** on the remote machine. The user name on the remote machine is **MGARCIA**, and the SSH port forward will use the AOS unit's DSA private key for SSH authentication. For more information about configuring an AOS device for SSH public key authentication, refer to the configuration guide *Configuring SSH Public Key Authentication*, available online in ADTRAN's Support Community. In this example, a user who logs into the remote machine and then telnets to **localhost** at port 7000 will receive a telnet prompt from the AOS device.

```
>enable
#ssh port-forward 23 MGARCIA@10.10.10.1:7000 myprivkey dsa
```

6.1.3 SSH Port Forward Using Specified Destination Port

The following example uses the **ssh port-forward** command to configure SSH port forwarding using a specified destination port. An SSH port forward instance is created between the AOS device and machine 10.10.10.1 forwarding Telnet (port **23**) to the remote machine (**10.10.10.1**) using port **7000** on the remote machine. The user name on the remote machine is **MGARCIA**, and the command will prompt for a password. The SSH server on the remote machine is listening on port **8022** instead of the default port 22. In this example, a user who logs into the remote machine and then telnets to **localhost** at port 7000 will receive a telnet prompt from the AOS device.

```
>enable
#ssh port-forward 23 MGARCIA@10.10.10.1:7000 port 8022
```

7 Using SSH Port Forwarding

Once SSH port forwarding is enabled and configured, follow these steps to use SSH port forwarding:

1. Log into the remote computer.
2. From a command prompt on the remote computer, launch the service associated with the forwarded port on the AOS device. For example, if the forwarded port on the AOS device is the port used for Telnet, then Telnet from the remote computer to the designated port on the AOS device. Traffic using this connection will forward to the forwarded port on the AOS device.

8 Removing a Configured SSH Port Forward Instance

To remove any previously configured SSH port forwarding instances, enter the **clear ssh port-forward** *<port-forward port> <url>* **[port** *<port>***] [password** *<password>* **| privkey** *<filename>* **| myprivkey dsa]** command from the Enable mode prompt. The various parameters for this command are outlined and described in Table 4 on page 15.

Table 4. SSH Port Forwarding Clear Command Parameters

Parameter	Description
<port-forward port>	Specifies the forwarded port on the local unit. Services that correspond to the specified port will be forwarded. For example, if a unit uses TCP port 443 for HTTPS, using an SSH port forward port of 443 would forward the HTTPS process.
<url>	Specifies the uniform resource locator (URL) of the far end listening address. The format of the URL string must be **user@server:remote-port**, for example, MGARCIA@10.10.10.1:7000. Optionally, you may include the IP address of an interface on the remote machine using the format **user@server:remote-port:FarEndListenAddress**, for example, MGARCIA@10.10.10.1:7000:10.10.10.2. If a far end listening address is not included as part of the URL, **localhost** is assumed and only those users logged into the remote machine can use the tunnel.
port *<port>*	Optional. Specifies a destination port to use for underlying SSH protocol instead of the default SSH port 22. Valid range is **1** to **65535**.
privkey *<filename>*	Optional. Specifies a private key file to use for SSH authentication.
password *<password>*	Optional. Specifies a password to use for SSH authentication. If you do not specify a password when using this command, you will be prompted for a password for the far end machine after entering the command.
myprivkey dsa	Optional. Specifies to use the AOS unit's digital signature algorithm (DSA) private key for SSH authentication.

The following command example removes the SSH port forward of port **3300** on the AOS device for user **MGARCIA** using port **7000** on device **10.10.10.1**:

```
>enable
#clear ssh port-forward 3300 MGARCIA@10.10.10.1:7000 password PASSWORD
```

9 Troubleshooting

There are several **show** and **debug** commands that can be entered from the Enable mode prompt to assist with troubleshooting the SSH port forwarding feature.

9.1 Show Commands

The following **show ssh port-forward** command can be used to display a summary of secure SSH port forward information. Enter the command from the Enable mode prompt as follows:

```
>enable
#show ssh port-forward
Local Port: 22
URL of Remote User: AOS@10.10.10.1:5037
Status: Waiting for Connection
```

NOTE
If the SSH port forward has an active connection, the status will display as **Forwarding** instead of **Waiting for Connection**.

9.2 Debug Commands

The **debug ssh client port-forward** command activates debug messages associated with SSH port forwarding events. Debug messages are displayed in real time. Use the **no** form of this command to disable the debug messages.

WARNING!
Turning on a large amount of debug information can adversely affect the performance of your device.

The following is sample output from the **debug ssh client port-forward** command, issued after initiating an SSH port forward instance:

```
>enable
#ssh port-forward 23 mgarcia@10.10.10.1
#debug ssh client port-forward
08:08:37 SSH_PORT_FORWARD.PortForward Resolved 10.10.10.1 to an IP address
08:08:37 SSH_PORT_FORWARD.PortForward Connection made to 10.10.10.1
08:08:37 SSH_PORT_FORWARD [libssh2] 55247.438116 Transport: session_startup
for socket 35
08:08:37 SSH_PORT_FORWARD [libssh2] 55247.439131 Transport: Sending Banner:
SSH-2.0-libssh2_1.4.3
08:08:37 SSH_PORT_FORWARD [libssh2] 55247.440152 Socket: Sent 23/23 bytes at
17c9907+0
…
08:08:38 SSH_PORT_FORWARD.PortForward Server is listening on localhost:7000
08:08:38 SSH_PORT_FORWARD.PortForward Waiting for remote connection
08:08:38 SSH_PORT_FORWARD [libssh2] 55248.131466 Conn: Setting blocking mode
OFF1534P_1534DP001#
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.866092 Socket: Recved 100/16384
bytes to 3286144+0
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.867619 Transport: Packet type 90
received, length=66
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.868125 Conn: Remote received
connection from 127.0.0.1:56318 to localhost:7000
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.868631 Conn: Allocated new channel
ID#0
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.869137 Conn: Connection queued:
channel 0/2 win 2097152/262144 packet 32768/32768
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.870663 Socket: Sent 52/52 bytes at
328a16c
08:08:46 SSH_PORT_FORWARD.PortForward Accepted remote connection.
Connecting to local server 127.0.0.1:23
08:08:46 SSH_PORT_FORWARD.PortForward Forwarding connection from remote
localhost:7000 to local 127.0.0.1:23
08:08:46 SSH_PORT_FORWARD.PortForward Waiting for remote connection
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.888226 Conn: Setting blocking mode
OFF
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.898827 Conn: Writing 3 bytes on
channel 0/2, stream #0
```

```
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.899834 Conn: Sending 3 bytes on
channel 0/2, stream_id=0
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.900855 Socket: Sent 52/52 bytes at
328a16c
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.901874 Conn: channel_read() wants
16384 bytes from channel 0/2 stream #0
08:08:46 SSH_PORT_FORWARD [libssh2] 55256.902886 Socket: Sent 68/68 bytes at
328a16c
08:08:46 SSH_PORT_FORWARD.PortForward Waiting for remote connection
…
08:09:25 SSH_PORT_FORWARD [libssh2] 55295.563386 Conn: Setting blocking mode
OFF
08:09:25 SSH_PORT_FORWARD [libssh2] 55295.573495 Conn: Writing 2 bytes on
channel 0/2, stream #0
08:09:25 SSH_PORT_FORWARD [libssh2] 55295.574508 Conn: Sending 2 bytes on
channel 0/2, stream_id=0
08:09:25 SSH_PORT_FORWARD [libssh2] 55295.575517 Socket: Sent 52/52 bytes at
328a16c
08:09:25 SSH_PORT_FORWARD.PortForward Waiting for remote connection
08:09:25 SSH_PORT_FORWARD [libssh2] 55295.577036 Conn: Setting blocking mode
OFF
08:09:28 SSH_PORT_FORWARD.PortForward The local server at 127.0.0.1:23
disconnected!
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.583513 Conn: Setting blocking mode
OFF
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.584015 Conn: Freeing channel 0/2
resources
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.585030 Conn: Sending EOF on
channel 0/2
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.586040 Socket: Sent 36/36 bytes at
328a16c
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.586549 Conn: Closing channel 0/2
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.587561 Socket: Sent 36/36 bytes at
328a16c
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.588574 Conn: Setting blocking mode
ON
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.596661 Socket: Recved 36/16384
bytes to 3286144+0
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.597675 Transport: Packet type 97
received, length=5
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.598179 Conn: Close received for
channel 0/2
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.598688 Transport: Looking for
packet of type: 94
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.599701 Transport: Looking for
packet of type: 95
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.600211 Conn: Setting blocking mode
OFF
08:09:28 SSH_PORT_FORWARD.PortForward Waiting for remote connection
08:09:28 SSH_PORT_FORWARD [libssh2] 55298.601221 Conn: Setting blocking mode
OFF
```

The following is sample output from the **debug ssh client port-forward** command, issued after removing an SSH port forward instance:

```
>enable
#clear ssh port-forward 23 mgarcia@10.10.10.1:7000
#debug ssh client port-forward

08:12:35 SSH_PORT_FORWARD [libssh2] 55485.824949 Conn: Cancelling tcpip-
forward session for localhost:7000
08:12:35 SSH_PORT_FORWARD [libssh2] 55485.826465 Socket: Sent 84/84 bytes at
328a16c
08:12:35 SSH_PORT_FORWARD [libssh2] 55485.827851 Transport: Disconnecting:
reason=11, desc=Normal shutdown, lang=
08:12:35 SSH_PORT_FORWARD [libssh2] 55485.828866 Socket: Sent 68/68 bytes at
328a16c
08:12:35 SSH_PORT_FORWARD [libssh2] 55485.829880 Transport: Freeing session
resource
08:12:35 SSH_PORT_FORWARD [libssh2] 55485.830385 Transport: packet left with
id 82
08:12:35 SSH_PORT_FORWARD [libssh2] 55485.830890 Transport: packet left with
id 82
08:12:35 SSH_PORT_FORWARD [libssh2] 55485.831396 Transport: packet left with
id 82
08:12:35 SSH_PORT_FORWARD [libssh2] 55485.831903 Transport: packet left with
id 82
08:12:35 SSH_PORT_FORWARD [libssh2] 55485.832409 Transport: Extra packets
left 4
2014.10.03 08:12:35 SSH_PORT_FORWARD.PortForward SSH tunnel has been discon-
nected for mgarcia@10.10.10.1:7000
```

10 Warranty and Contact Information

10.1 Warranty

Warranty information can be found at:

www.adtran.com/warranty.

10.2 Contact Information

For all customer support inquiries, please contact ADTRAN Customer Care:

Contact	Support	Contact Information
Customer Care	From within the U.S. From outside the U.S. **Technical Support:** ■ Web: **Training:** ■ Email: ■ Web:	1.888.4ADTRAN (1.888.423.8726) + 1.256.963.8716 www.adtran.com/support training@adtran.com www.adtran.com/training www.adtranuniversity.com
Sales	Pricing and Availability	1.800.827.0807