Frequently Asked Questions

Firewall Setup & Network Protection of a Scan2Net Scanner

Abstract

All Scan2Net scanners, as well as all Bookeye and WideTEK scanners and their OEM versions, have a network connection to communicate with local hosts and resources on the end user's corporate network. Since all resources connected to a network are potentially vulnerable to viruses, malware, phishing and other hacking attacks, the user must be aware of this and should consult the network administrator to protect the scanners from attacks. This FAQ document is intended to provide a simple step-by-step process for setting up the Scan2Net Firewall and the network protection of a Scan2Net scanner.

Title	Firewall Setup & Network Protection of a Scan2Net Scanner
Revision	1.1
Date	03.07.2023
Category	Network
Owner	Support
Authors	knuejo

1. Confidentiality

Status	Interested Party	Source	PDF
Public Information	Image Access Support	Yes	Yes
	Authorized Service Providers	No	Yes
	Image Access Customers	No	Yes

2. Revision History

Date	Rev.	Name	Description of Change	Reason of Change
28.02.2023	1.0		Initial Version	
03.07.2023	1.1		Updated Version	

3. Table of Contents

4. Table of Figures

5. References

Ref.	Link	Content
[1]	www.debian.org/	Debian is an operating system and a distribution of free software. It is maintained and updated through the work of many users.
[2]	https://www.youtube.com/watch?v=UH-yZVweZkY&t=5s	IT-security of Scan2Net Scanners. YouTube video describing the security concept of Scan2Net scanners.

6. Purpose

The purpose of this document is to answer frequently asked questions about how to setup the Scan2Net Firewall and the network protection of a Scan2Net scanner.

7. Scope

This document will describe how the Scan2Net scanners network security setup should be performed and maintained. The scope of the document includes all Scan2Net, Bookeye or WideTEK scanners as well as OEM versions of these scanners. The firmware versions covered by this document are 6.xx and higher. The Windows versions covered in the documentation are Windows 7 and higher.

8. Terms and Definitions

Term	Description, Meaning
Scan2Net	Technology from Image Access implemented in many scanners. More at: www.imageaccess.de/?page=SoftwareScan2Net
SMB	SMB, which stands for Server Message Block, is a protocol for sharing files, printers, serial ports and other resources between computers.
Bookeye	Book scanners. More at: www.imageaccess.de/?page=ScannersBookscanner
WideTEK	Wide format scanner. More at: www.imageaccess.de/?page=ScannersWideformat
https://www.imageaccess.de/_WhitePapers/PDF/WhitePaper_Security.pdf	This white paper will outline the security features Scan2Net scanners have and will also explain why some penetration tools might report security risks that are not accurate

9. Introduction

The target audience for this FAQ document is the administrator of a Scan2Net scanner and the administrator of the customer PCs. The administrator should have experience setting up and configuring Windows PCs, network, firewalls and virus checkers.

All Scan2Net scanners, WideTEK, Bookeye and OEM brands, have one thing in common: The core of the scanner's internal firmware is a Linux-based system. Today (02/2023) the current version of the Linux is a Debian-based distribution. This version is a stable version and is fully supported in respect to security fixes and the user can patch it via the Debian website at any time with an internet connected scanner. Whenever the support of a stable Linux distribution ends, we will upgrade to a newer distribution after extensive testing.
It should be noted that the scanners are very fast and therefore the Linux and all other software must be thoroughly tested for its real time behavior and performance. This implies that we will not always install the latest and greatest software but only fully tested and specified versions of the Linux system.

The document will offer a guideline to:

- Setup the Scan2Net Firewall
- Update the scanners Scan2Net Debian Linux
- Update the Client Certificates

10. Difference between a Scanner and a PC

In a PC environment, there will be at least one user with admin permissions and maybe other users with limited permissions. Since these users actively go into the Internet and can also actively download malicious code through e-mails extensions, infected web sites, USB sticks and other means, they themselves and their conscious or unconscious behavior pose a security risk. If you run a Linux PC, the risk is significantly reduced because most attacks are run against Windows based systems. A PC environment whether Windows or Linux based is in stark contrast to the architecture of the Scan2Net-scanners firmware.
The scanner basically behaves like a web server, of which there are hundreds of millions found on the Internet. It can be accessed through the network using standard TCP/IP protocols and its HTML based graphical user interface called GUI. All scanner functions are accessible this way. In contrast to a PC, you cannot login to the scanner´s Linux under normal circumstances. The software that is presented to a user like the ScanWizard has the lowest user permissions on the Linux system.
The scanner being a web server also allows users to login like a User, Poweruser and Admin. This is not the same as login into Linux because these users are shielded through the software from any access to Linux. It can be thought of as the login to an internet store with your personal credentials which does not mean that you are logged into the operating system.

This architecture greatly reduces the risk to open any backdoors into the scanner, as compared to standard workstations. Almost all exploits need a user interaction with access permissions to the operation system, which does not happen in the scanner firmware. Also, a typical Scan2Net scanner will only be visible in the Intranet and all attacks can typically only come from inside the network that the scanner is connected to.

NOTE!	**Scan2Net scanners are like web servers and not like PCs. There is no login into Linux from the outside, reducing the risk of injecting malicious code by users into the system to almost zero.**

11. Scan2Net Firewall Setup

- Connect your Scan2Net scanner via web browser.

Figure 1: Scan2Net Start Page

- Go to Setup Device / Poweruser (LG: Poweruser / PW: Poweruser) / Base Settings / Network Configuration / Firewall

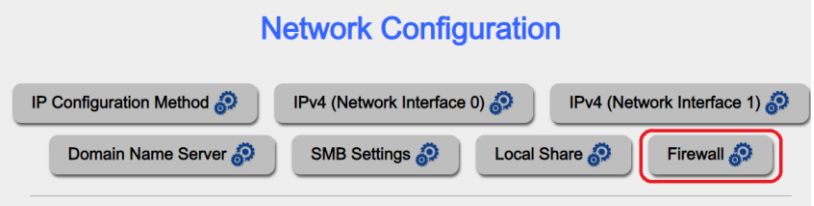

Figure 2: Setup Scan2Net Firewall

This section is used to set the firewall parameters. It is divided in incoming and outgoing connections. The standard ports for the protocols are displayed in brackets. allow all: No restriction for the use of the protocol allow only for: Enter the IP address or the address range in CIDR notation for the devices which are allowed to use the protocol. CIDR notation means e.g. 192.168.0.x/24 or 172.16.x.x/16. block all: Blocks all communication for this protocol.

NOTE!	**If HTTP (port 80) is blocked for all addresses, only HTTPS (port 443) connections will be enabled for web administration / ScanWizard or vice versa.**

NOTE!	**The selection of available ports, listed in each case for incoming and outgoing connections, corresponds to the respective active services on the scanner. Ports that are not listed do not support an active service on the scanner.**

1. Firewall: Incoming Connections

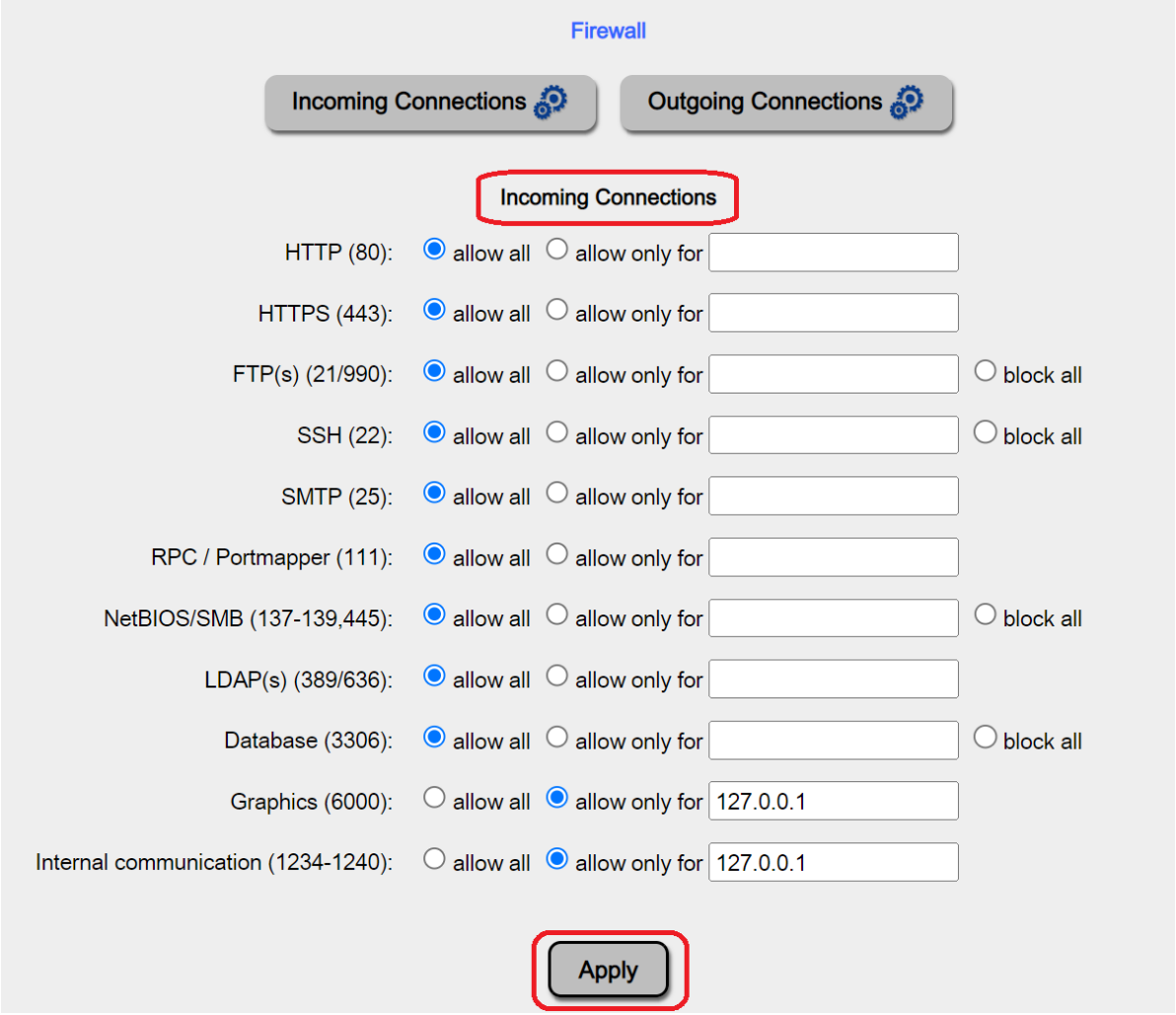

Figure 3: Firewall: Incoming Connections

Protocol (Port): Service	Description, Meaning
HTTP (80)	Web administration, ScanWizard, external API function calls (unsecure connection)
HTTPS (443)	Web administration, ScanWizard, external API function calls (secure connection)
FTP (21)	Internal FTP Server. (external access needed only for support issues)
SSH (22)	Secure shell (external access needed only for support issues)
NetBIOS	SMB (137-139,445)/Access to local share and other internal SMB features
Database (3306)	Internal MySQL database (external access needed only for support issues)
Graphics (6000):	X Windows graphics system
Internal communication (1234-1240)	Internal interprocess communication system

- After modifying the values, click on the **APPLY** button to transfer the modified settings.

NOTE!	**If port 80 is blocked for the localhost, the touchscreen interface and its applications (ScanWizard Touch, Application selection screen) will be blocked immediately. A black touchscreen display will appear. This happens as soon as the incoming or outgoing connection is blocked for 127.0.0.1.**

2. Firewall: Outgoing Connections

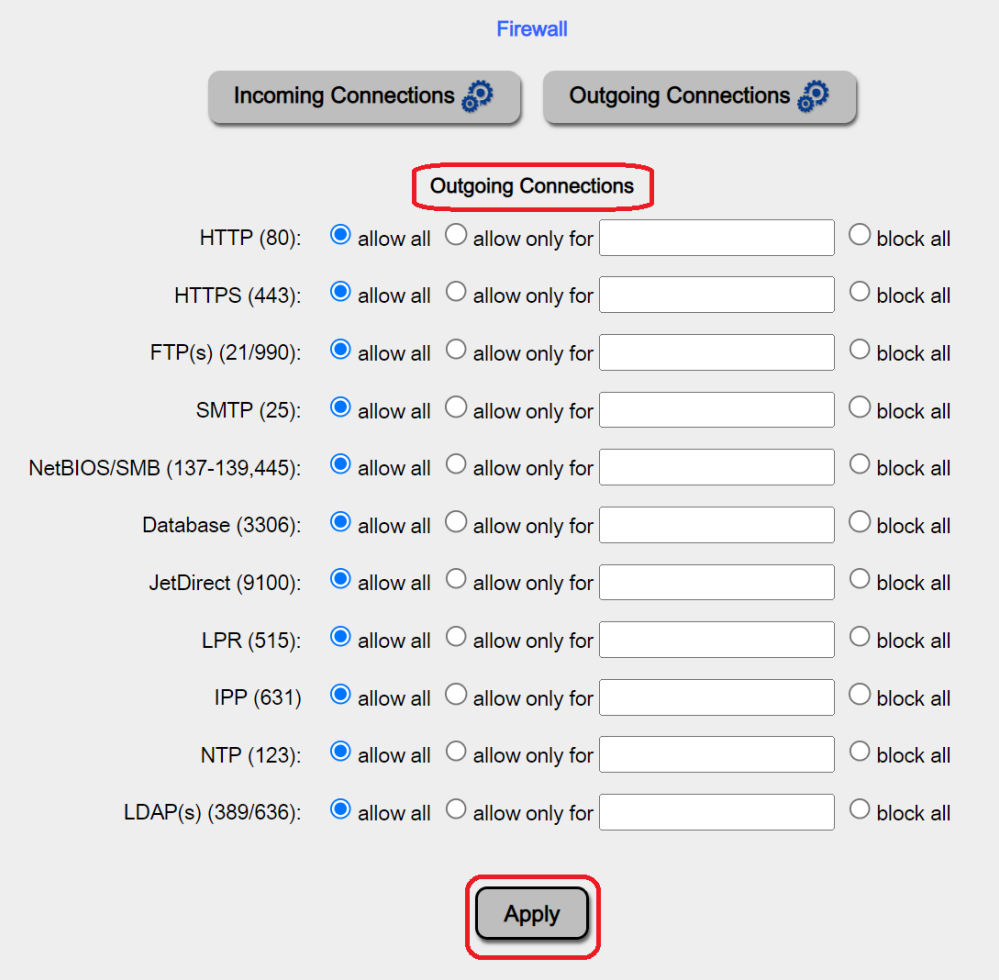

Figure 4: Firewall: Outgoing Connections

Protocol (Port): Service	Description, Meaning
HTTP (80)	Cloud export, billing server access
HTTPS (443)	Cloud export, billing server access
FTP(s) (21/990)	FTP export
SMTP (25)	Mail export
NetBIOS/SMB (137-139,445)	Export to SMB network shares and printing to SMB network printer queues
Database (3306)	MySQL Export
JetDirect (9100)	Printing to network printers with JetDirect interface
LPR (515):	Printing to network printers with LPR/LPD interface
IPP (631)	Internet Printing CUPS server
NTP (123)	Requests to an external time server
LDAP (389/636)	LDAP / Actvice Directory search requests

- After modifying the values, click on the **APPLY** button to transfer the modified settings.

NOTE!	**If port 80 is blocked for the localhost, the touchscreen interface and its applications (ScanWizard Touch, Application selection screen) will be blocked immediately. A black touchscreen display will appear. This happens as soon as the incoming or outgoing connection is blocked for 127.0.0.1.**

12. IT-Security of Scan2Net® Scanners

Please find below the links to our information document and video to this:

White Paper: Network Security of Scan2Net Scanners

https://www.imageaccess.de/_WhitePapers/PDF/WhitePaper_Security.pdf

Explanation Video: IT-Security of Scan2Net® Scanners

https://www.imageaccess.de/?page=ScannersWT36-600ProductVideos&lang=en#

13. Scan2Net Linux Upgrade

With S2N firmware version 7.30 and above you can update the Scan2net Debian based Linux system (internal web server, e.g.) with the latest available Debian security updates in four steps.

NOTE!	**Scan2Net Linux Upgrade always updates the installed services and programs with all currently available security updates and their associated patch levels.**

Step 1: Preparations: System Restore Point

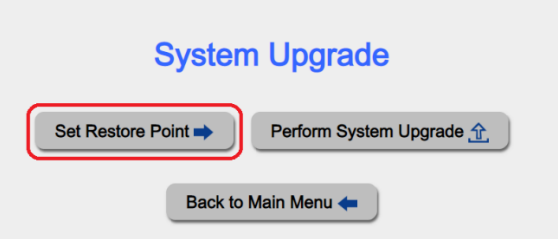

Figure 5: System Upgrade: Set a Restore Point first!

- In web browser / Scanner-IP / Setup Device / Poweruser / Updates & Uploads / Linux Upgrade / System Restore Point.
- Set first a System Restore Point to be able to start the scanner with the latest successful running system.

Step 2: Connect the scanner to the internet

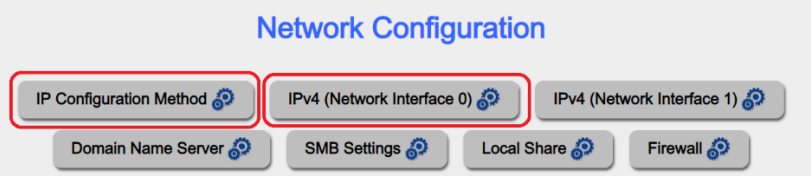

Figure 6: Network Setup

- In web browser / Scanner-IP / Setup Device / Poweruser / Base Settings / Linux Upgrade / Network Configuration: You may need to change the actual network setup.

NOTE!	**It is not possible to specify a proxy in the settings interface to receive the updates. The scanner therefore requires direct Internet access without an intermediate proxy server.**

Step 3: Perform Linux Upgrade

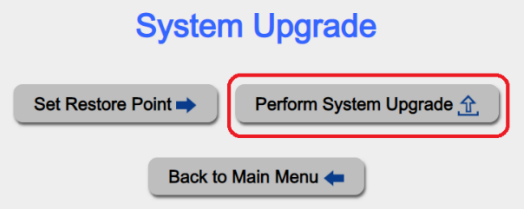

Figure 7: Perform Debian Linux Upgrade

- In web browser / Scanner-IP / Setup Device / Poweruser / Updates & Uploads / Linux Upgrade /
- Click on Perform Linux Upgrade to start the Linux upgrade
- **Wait until the Linux upgrade finish with a scanner restart!**

NOTE!	**Generally, the pentest tools used do not check the patch levels of the installed and updated software versions with which a previously reported vulnerability has already been closed. Therefore, please perform the update first and then check the installed versions for their respective patch levels!**

Step 4: Reset the scanners network setup to the requirements for the scanning process.

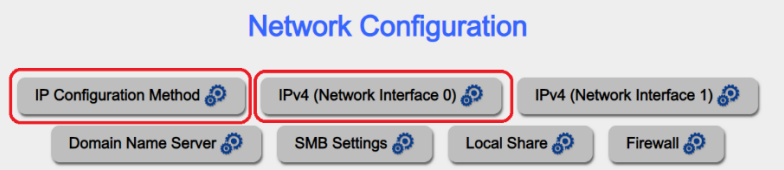

Figure 8: Network Setup

- In web browser / Scanner-IP / Setup Device / Poweruser / Base Settings / Linux Upgrade / Network Configuration: You may need to reset the network setup back to the requirements for the scanning process.

14. Trouble Shooting

If the scanner

- does not restart by itself after the Linux update,
- does not complete the reboot after the Linux update is finished,
- or does not work properly after a reboot,
- you can load the previously set restore point.

15. Restore System

- For the Scan2Net system recovery, please follow the instructions in the scanner setup instructions manual.

16. Certificates

If you want to install a client certificate on the scanner, this must be done as follows.

- A zip archive must be created with the client certificate (CRT format) and the appropriate KEY file without password protection.
- This archive must be uploaded in the S2N web interface as power user in the respective menu.
- Connect your Scan2Net scanner via web browser.
- In Scan2Net / Setup Device / Poweruser (LG: Poweruser / PW: Poweruser) / Base Settings / Certificates upload your client certificate (CRT format) and the appropriate KEY file without password protection.

Figure 9: Upload own Client Certificate to the sanner

17. Root Certificates

In Scan2Net / Setup Device / Poweruser (LG: Poweruser / PW: Poweruser) / Base Settings / Certificates / Root CA certificates

- upload your own Root Ca certificates or
- update the installed Root Certificates.

18. Own trusted Root CA certificate (PEM)

In Scan2Net / Setup Device / Poweruser (LG: Poweruser / PW: Poweruser) / Base Settings / Certificates / Own trusted Root CA certificate (PEM)

- add your own trusted Root CA certificate (PEM)

19. Validate Certificates

A certificate authority (CA) validates certificates for secure network connections (e.g. HTTPS), which claim to be certified from this CA online.

- Select Yes to activate the certificate validation. This only works if the scanner is connected to internet or a responsible local network CA.
- If certificate validation is set to Yes and no connection to the CA is possible, some secure network connections might fail.
- No disables the certificate validation.

20. Isolate Scanner Network from Intranet

Another way of making sure only one user can work with the scanner, is a private network. Connect the scanner to a second network port and establish a point-to-point connection with the scanner. The disadvantage of this configuration is, that the scanner can only transfer data to the local computer and not directly to a resource in the Intranet.

21. Further Information

For more information see our Internet Security Video found on our YouTube channel.

End of Document