Contents

[04 PROTECT CHALLENGE 2](#_Toc11162955)

[05 VULNERABILITY ANALYSIS 3](#_Toc11162956)

[06 DETECT CHALLENGE 4](#_Toc11162957)

[07 NOTIFICATION AND ESCALATION 5](#_Toc11162958)

[08 RESPOND CHALLENGE 6](#_Toc11162959)

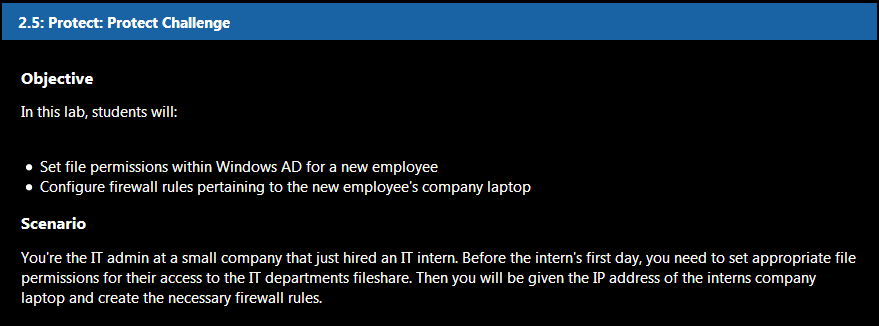
[09 RE-IMAGING 7](#_Toc11162960)

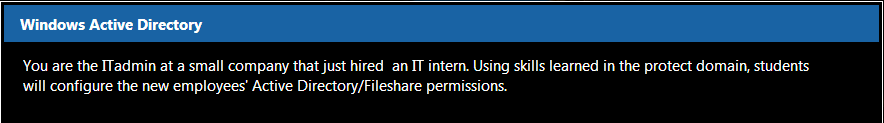
[10 RESTORE POINTS AND PASSWORD RECOVERY 8](#_Toc11162961)

[Appendix 9](#_Toc11162962)

# 04 PROTECT CHALLENGE

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |





## Windows Active Directory

### Login to Windows

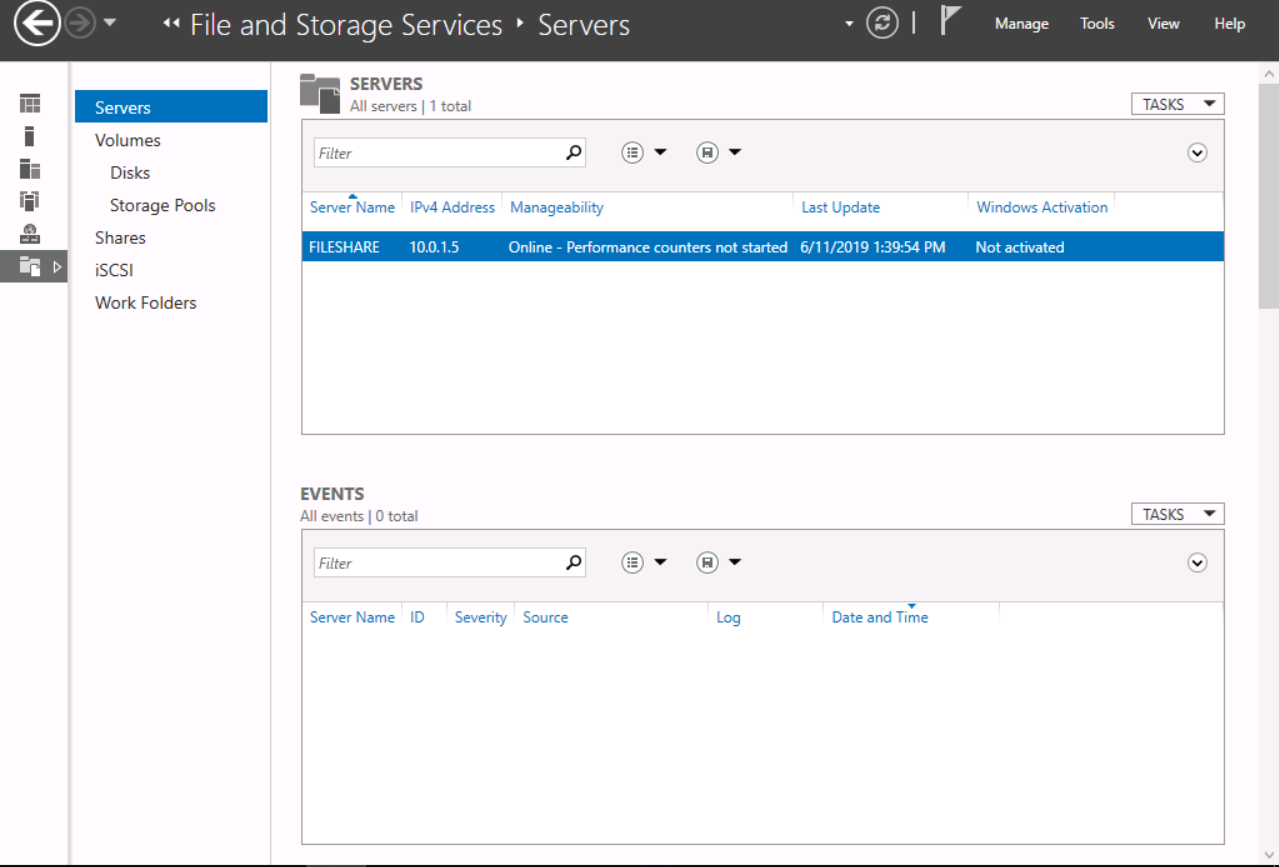
Log in to the Windows Server. User: **itadmin** Password: **IamanIT!**

### Server Manager

Open **Server Manager** (If it doesn't open upon login). Click on **File and Storage Services**.

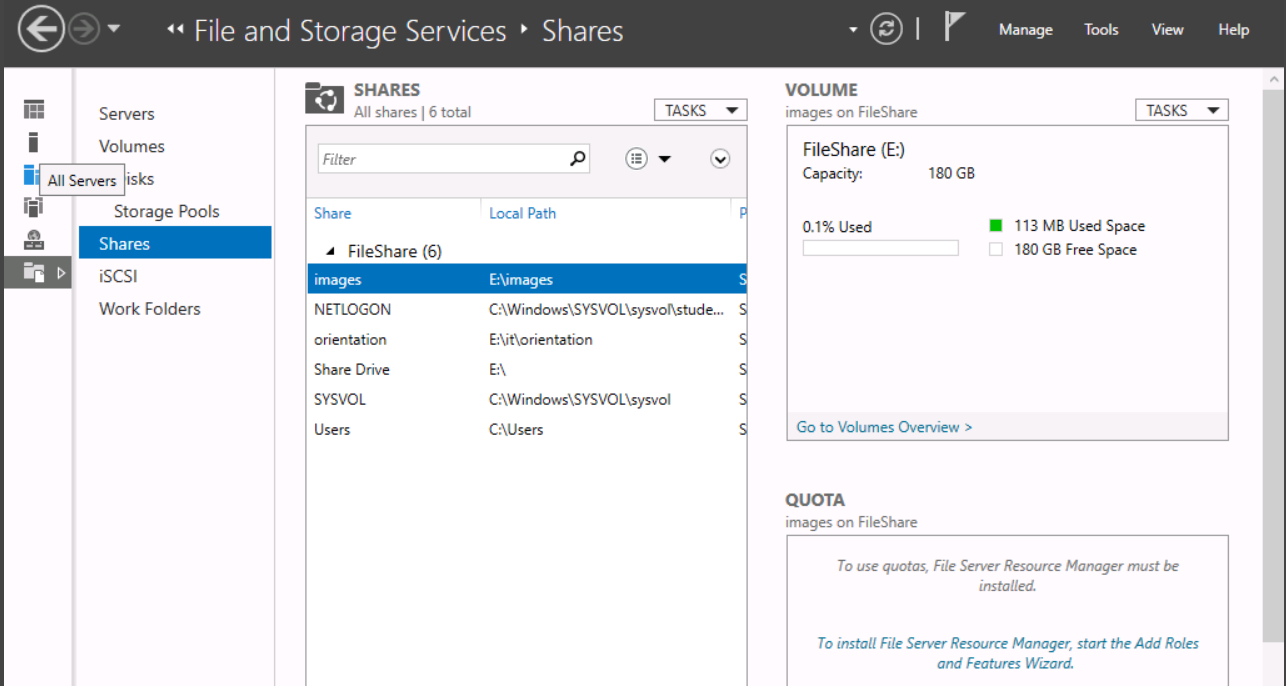
|  |  |
| --- | --- |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |



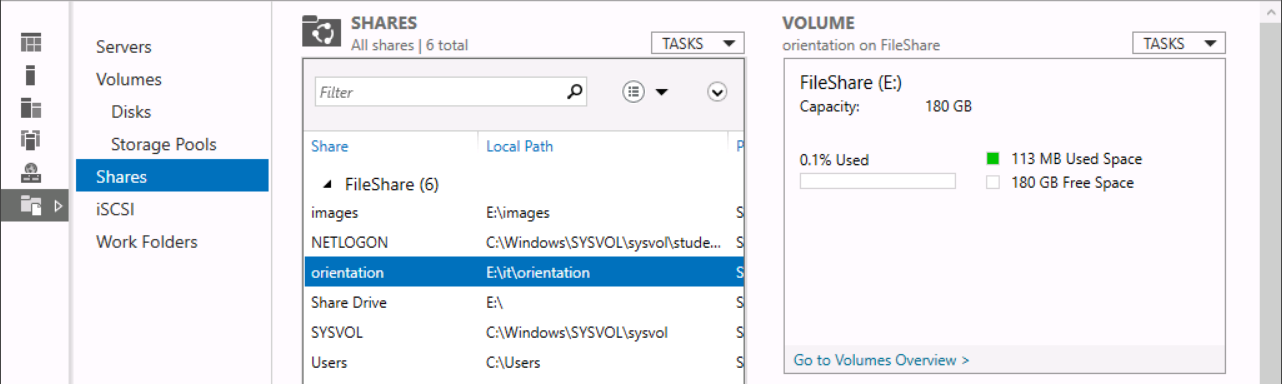
### Orientation Fileshare

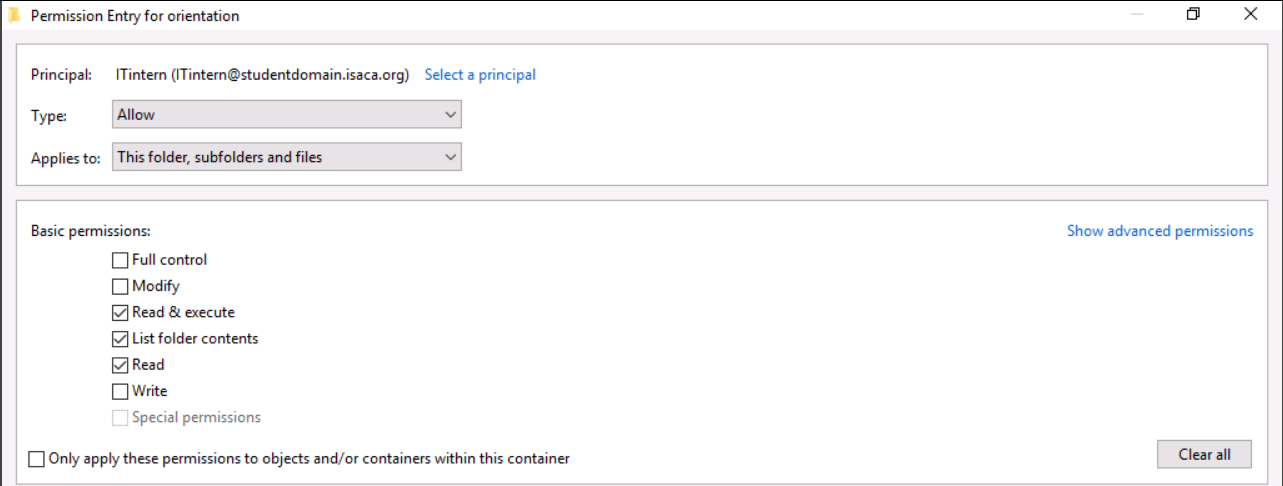
In preparation for their newest team member, the IT team shared an Orientation folder which will contain important documents for their intern's first week. Click **Shares**.

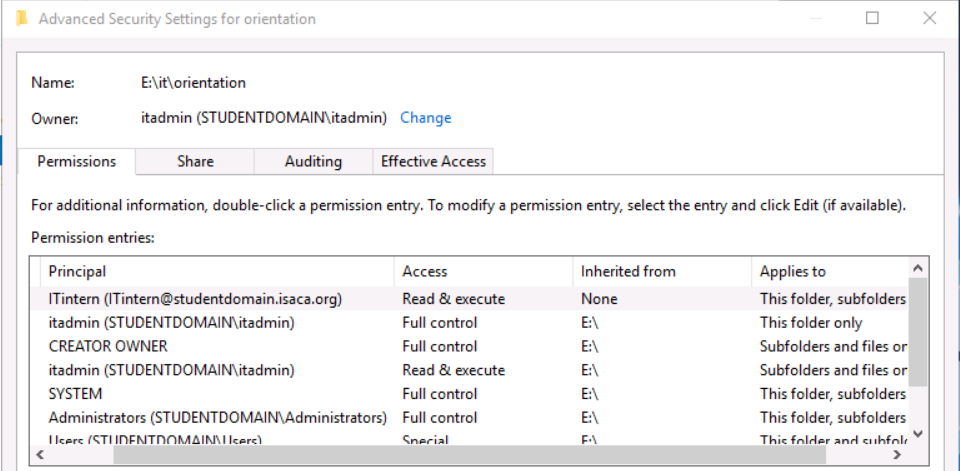


### Configuring Permissions I

For the **E: --> IT --> Orientation** fileshare, give **ITintern Read** and **Execute** permissions. Give **ITadmin full control**.

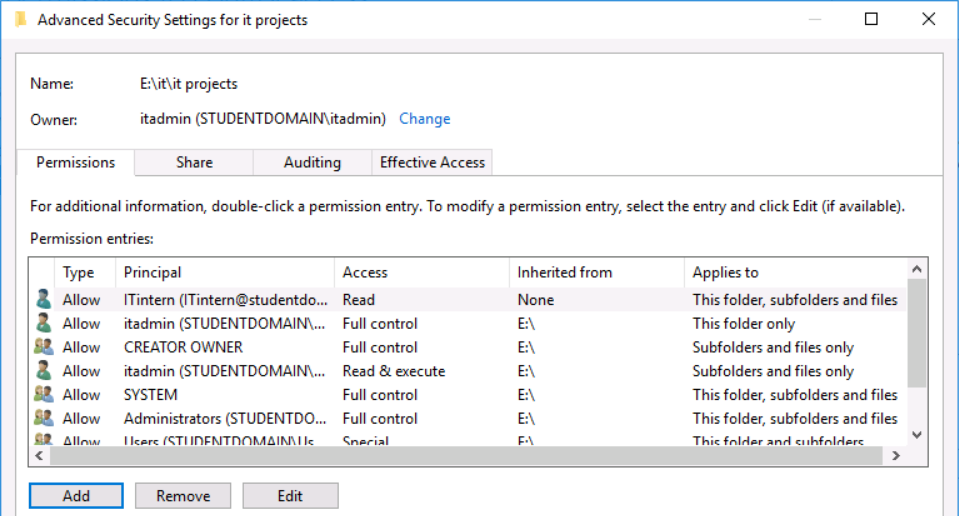




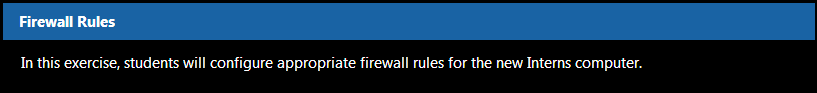


### Configuring Permissions II

Create a share for the **IT projects folder** within the **IT directory**. Give **ITintern** **read-only** permissions.



## Firewall Rules

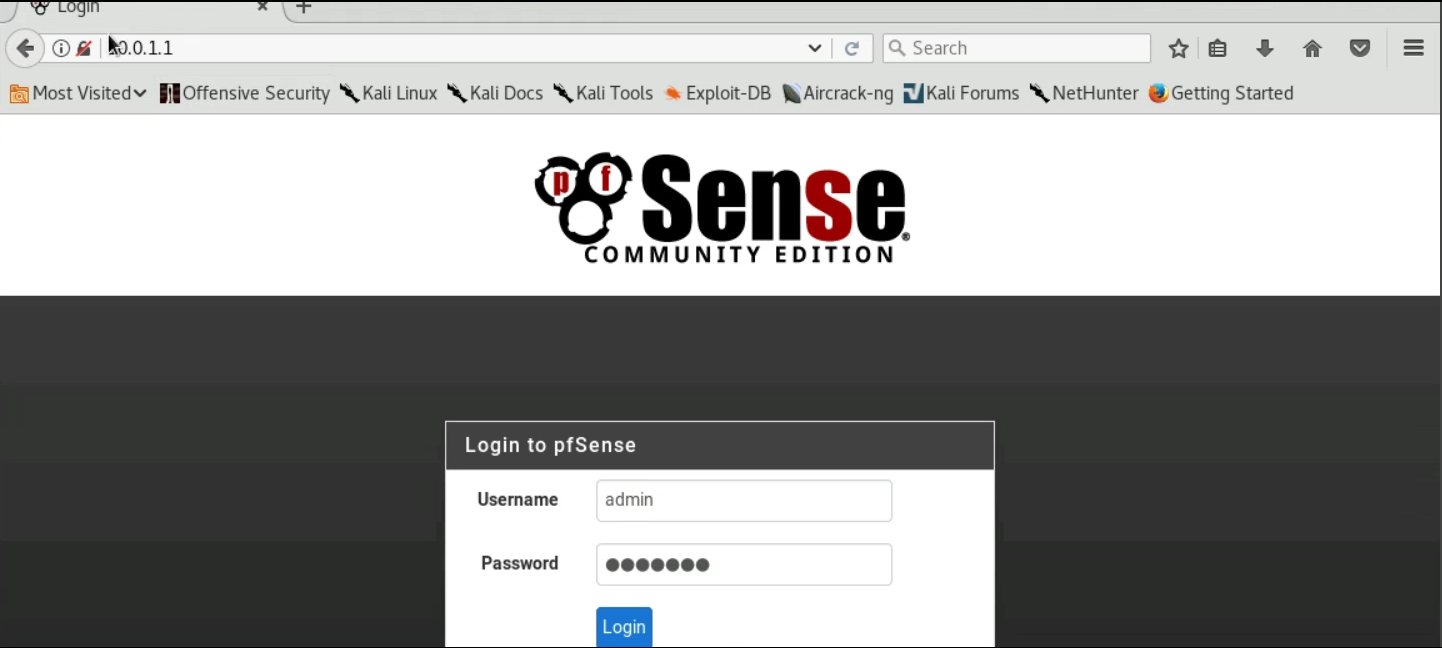


### Login to Kali

Login to Kali with username **root** and password **isaca**., Then, open a browser and navigate to **http://10.0.1.1**

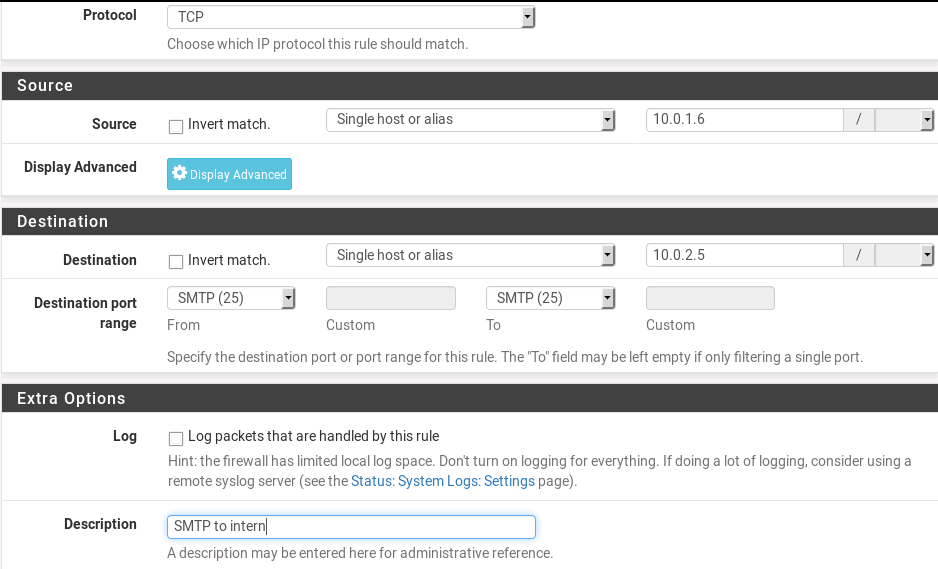
### Login to Pfsense

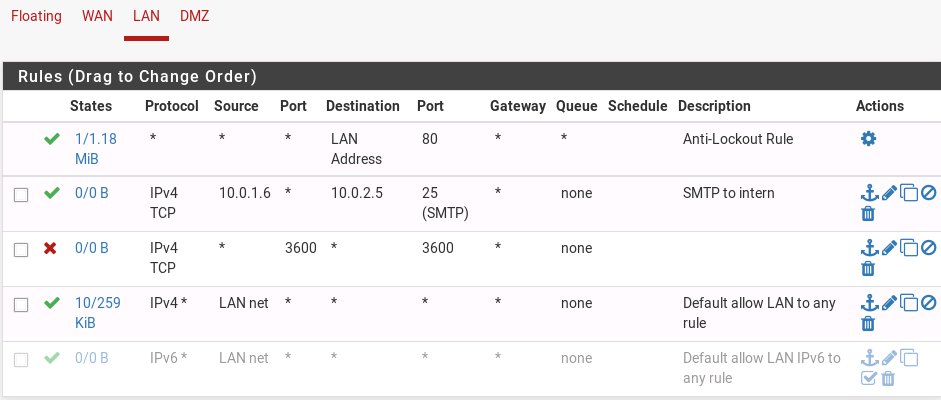
Login to Pfsense with username **admin**, and password **pfsense**



### Mail Server Rule

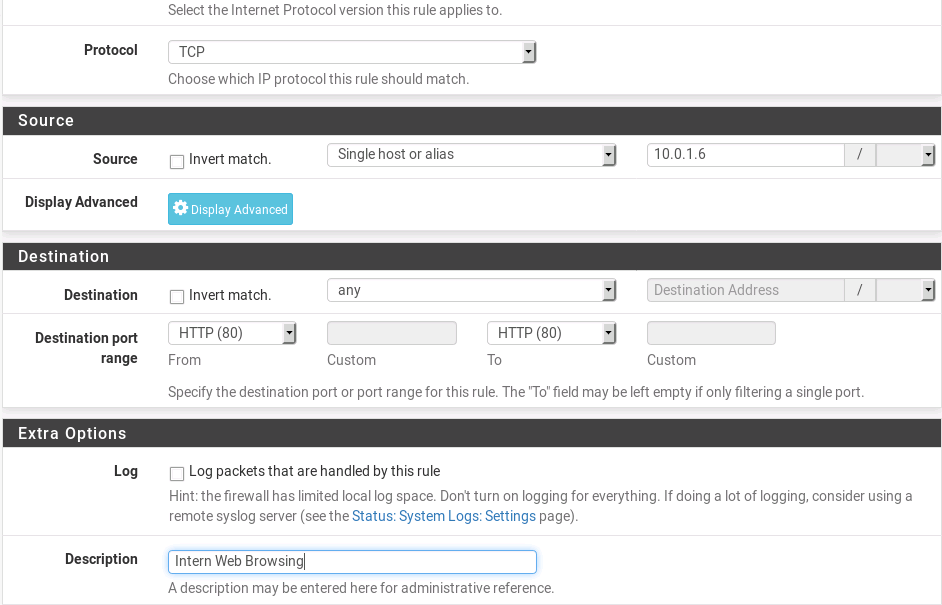
Click **Firewall --> Rules**. Then create a LAN rule allowing the Interns computer to receive mail from our mail server. The mail server is on the **DMZ** with an IP of **10.0.2.5** and uses **SMTP (port 25)** to relay emails. The Intern's new computer has a static IP address of **10.0.1.6** and is on the **LAN**. Set the description as "**SMTP to Intern**".

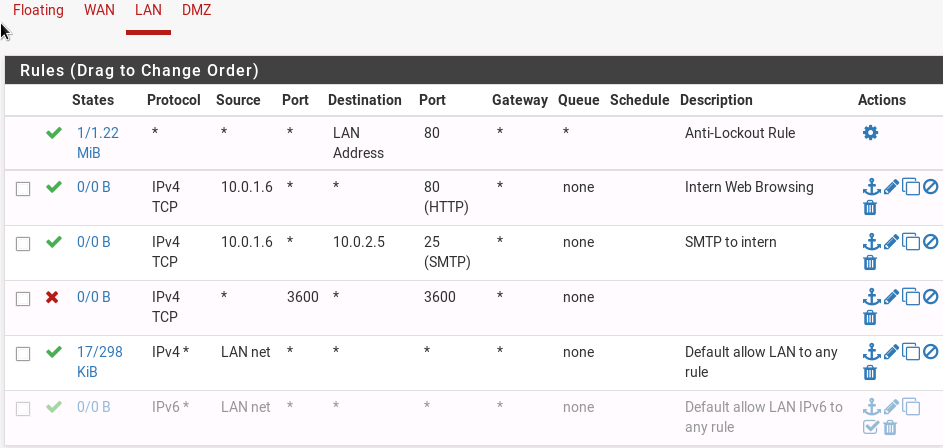




### Web Browsing Rule

Create another LAN rule, this time allowing the intern to browse the web using **HTTPS**. Set the description as "**Intern Web Browsing**".





### Download Configuration

Download your firewall configuration by clicking **Diagnostics --> Backup & Restore**. Then click "**Download configuration as XML**", and rename the file "**InternRules.xml**" and save it to your Desktop.

# 05 VULNERABILITY ANALYSIS

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# 06 DETECT CHALLENGE

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# 07 NOTIFICATION AND ESCALATION

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# 08 RESPOND CHALLENGE

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# 09 RE-IMAGING

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# 10 RESTORE POINTS AND PASSWORD RECOVERY

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# Appendix