Internal Machines: (eth1/2) 172.20.240.254/24

Docker:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task | Application | Service | Source Interface | Source IP | Destination Interface | Destination IP | Action |
|  |  |  |  |  |  |  |  |

**Debian 8.5 DNS/NTP:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task | Application | Service | Source Interface | Source IP | Destination Interface | Destination IP | Action |
| DNS | Dns  Dns-over-https  Dns-over-tls  Dnscrypt – (for privacy and security)  Tcp-over-dns  Paloalto-dns-security  Ms-win-dns | Service-https  Service-http | Any | Any | Public  Internal  External  User  trusted | Any | Allow  +  Restrictions to be enabled via web interface |
| NTP | Ntp | Application Default | Any  For Now | Any  For Now | Multicast | 172.16 - 172.31  Ful Range | Allow  +  Restrictions |

Where do we get the time from?

**Public Machines: (eth1/1) 172.20.241.254/24**

Splunk 8.1.1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task | Application | Service | Source Interface | Source IP | Destination Interface | Destination IP | Action |

**CentOS 7 E-comm**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task | Application | Service | Source Interface | Source IP | Destination Interface | Destination IP | Action |
| E-Commerce | Any  (For Now) | Service-https | any | any | any | any | Allow  +  Restrictions + Full Logging |
| URL Categories Allowed are: Online Store and Backup, Business and E-Economy, Content delivery Networks, Government, recreation and hobbies, reference and research, search engine, shopping, social Networking, Web Advertisements, Web-Based Email, Web-hosting, streaming media, Entertainments and Arts, Home and Garden | | | | | | | |

**Fedora 21 WebMail/WebApps – GUI ?**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task | Application | Service | Source Interface | Source IP | Destination Interface | Destination IP | Action |
| WebMail | Smtp  nfs  Gmail  Outlook-web-online  Yahoo mail  Rpc  Rpc-over-http  activesync | Service-https | Public | 172.20.241.40 | Any | 172.16. – 172.31  Any | Allow  + Restrictions |
| Imap  Pop3  Nfs  Rpc  Rpc-over-http  activesync | Service-https | Any | Any | Public | 172.20.241.40 | Allow  +Monitoring and Vulnerability Restrictions |
| WebApps | Web-browsing | Service-http  Service-https | Any | 172.16-172.31  Internal  User  Public | External  Internal  Public  User  Trusted | 172.16. – 172.31 | Allow  But  With Strict Restrictions |

**User Based Machines: (eth1/4) 172.20.242.254/24**

**Ubuntu 14 Web [Not sure what is required]**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task | Application | Service | Source Interface | Source IP | Destination Interface | Destination IP | Action |
| Web | Web-browsing | Service-https  Service-http | Any | 172.16-172.31  Internal  User  Public | External  Internal  Public  User  Trusted | 172.16. – 172.31 | Allow  But  With Strict Restrictions |

**2012 AD/DNS/DHCP**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task | Application | Service | Source Interface | Source IP | Destination Interface | Destination IP | Action |
| AD | Active-directory  Active-directory-base  Ms-directory-service-setup  Ad-selfservice | Service-https | User  **Public** [Must]  Internal | Any | User  Public  Internal  trusted | Public  Internal  User and  172.16. – 172.31  Address Range | Allow |
| DNS | Dns  Dns-over-https  Dns-over-tls  Dnscrypt – (for privacy and security)  Tcp-over-dns  Paloalto-dns-security  Ms-win-dns | Service-https  Service-http | Any | Any | Public  Internal  External  User  trusted | Any | Allow  +  Restrictions to be enabled via web interface |
| DHCP | Dhcp  Dhcpv6  addp | Service-https  Service-http | Internal  Public  Trusted  User  [External] | Any | Internal  User  Public  [External] | 172.16 – 172.31. Full range  +  External if necessary | Allow  +  Restrictions |

**Ubuntu Workstation**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task | Application | Service | Source Interface | Source IP | Destination Interface | Destination IP | Action |
|  |  |  |  |  |  |  |  |

**External Machines:**

Windows 10

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Task | Application | Service | Source Interface | Source IP | Destination Interface | Destination IP | Action |

Last Rule:

Set rulebase security rules Default0 to any from any source any destination any category any application any service any action allow

>configure

#set rulebase security rules <rule name> from <source zone> to <destination zone> source <any/IP> category any application <any/application> service <any/application default/service name> destination <any/IP> action allow/deny

#exit

>commit

# set rulebase security rules <name> from <source zone> to <destination zone> destination <ip> application <application> service <any/application-default/service name> action <allow/deny> (press enter)



Internal Systems: (eth1/2) 172.20.240.254/24

Docker/Remote

Debian 8.5 DNS/NTP

User: (eth1/4) 172.20.242.254/24

Ubuntu 14 Web

2012 AD/DNS/DHCP

Ubuntu Workstation

Public Facing: (eth1/1) 172.20.241.254/24

Splunk 8.1.1

CentOS 7 E-comm

Fedora 21 WebMail/WebApps

Out: (eth1/3)

Windows 10

Management: 172.20.242.150

Set rulebase security rules Default0 to any from any source any destination any category any application any service any action allow

About HTTP?

Plan of Action:

1. Change the Password – set passwd
   1. **Set password** in CLI or in the **GUI it is in Administrators > Admin**
   2. **configure** – for going into configuration mode
      1. If step, **set mgt-config users admin password**
      2. If step, **set mgt-config users administrator password**
   3. **commit**

These process will commit the password to the new configuration file, which will be used to load the passwords into the active user database upon reboot. If the commit is not committed prior to reboot, the new password will be set to the old one.

1. System Version: command > “debug swm info”
2. Update the system – Also look for time period.
3. If User Account creation is necessary, then
   1. set mgt-config users <username> password [or] set mgt-config users <username> permissions role-based superuser
   2. enter a strong password and commit
4. Update the system – Something greater than 8.1.17
   1. GUI – Device>Dynamic Updates
   2. request system software download version 8.x.x
   3. request system software install version 8.x.x
   4. request restart system
5. For Network Interfaces: in configuration mode “show network interface”
6. Set rules as below:

9. To see the current configuration: use ‘show’ command in configure mode.
10. Disable Services like telnet, snmp, smb,
    1. set deviceconfig system service disable-telnet yes
    2. set deviceconfig system service disable-snmp yes
    3. perform a commit
11. To view the current security policies:
    1. show running security-policy
    2. For set format output:
       1. set cli config-output-format set
       2. configure
       3. edit rule base security
       4. show
12. To find a particular rule:
    1. show rulebase security rules <rulename>
13. To delete a particular rule:
    1. delete rulebase security rules <rulename>
14. For Viewing Jobs: show jobs all [or] show jobs id <Job\_ID>
15. Deny all Rule

Security Policy rule

DNS and NTP -Debain



Services:

HTTP

HTTPS

SMTP

POP3

SSH

DNS



Text

Description automatically generated

Resources:

Update Pan OS:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CloaCAC>

Application center:

<https://applipedia.paloaltonetworks.com>

Hung or Pending Job:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhFCAS>

Restarting the Management Server:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhFCAS>

View Create and Delete Policies:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClaCCAS>

Internal Systems: (eth1/2) 172.20.240.254/24

Docker/Remote

Debian 8.5 DNS/NTP

User: (eth1/4) 172.20.242.254/24

Ubuntu 14 Web

2012 AD/DNS/DHCP

Ubuntu Workstation

Public Facing: (eth1/1) 172.20.241.254/24

Splunk 8.1.1

CentOS 7 E-comm

Fedora 21 WebMail/WebApps

* Set rulebase security rules Fed1 to External from Public source 172.20.241.40 destination any category web-based-email application smtp service service-https action allow
* Set rulebase security rules Fed1 to External from Public source 172.20.241.40 destination any category web-based-email application smtp service service-https action allow

Out: (eth1/3)

Windows 10

Management: 172.20.242.150

Set rulebase security rules Default0 to any from any source any destination any category any application any service any action allow