Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Palo Alto	NIC	172.20.242.150	255.255.255.0 (/24)	N/A
	eth1/1	172.20.241.254	255.255.255.0 (/24)	N/A
	eth1/2	172.20.240.254	255.255.255.0 (/24)	N/A
	eth1/3	172.31.24.2	255.255.255.248 (/29)	172.31.24.1
	eth1/4	172.20.242.254	255.255.255.0 (/24)	N/A
Internal				
Docker/Remote	NIC	172.20.240.10	255.255.255.0 (/24)	172.20.240.254
DNS/NTP	NIC	172.20.240.20	255.255.255.0 (/24)	172.20.240.254
User				
Ubuntu 14 Web	NIC	172.20.242.10	255.255.255.0 (/24)	172.20.242.254
AD/DNS/DHCP	NIC	172.20.242.200	255.255.255.0 (/24)	172.20.242.254
Workstation	NIC	DHCP	DHCP	DHCP
Public				
Splunk	NIC	172.20.241.20	255.255.255.0 (/24)	172.20.241.254
CentOS E-comm	NIC	172.20.241.30	255.255.255.0 (/24)	172.20.241.254
Webmail/Apps	NIC	172.20.241.40	255.255.255.0 (/24)	172.20.241.254
External				
Windows 10	NIC	172.31.23.5	255.255.255.248 (/29)	172.31.23.1

NAT Table

Device	Local IP	Public IP
Internal		
Docker/Remote	172.20.240.10/24	172.25.24.97/24
DNS/NTP	172.20.242.20/24	172.25.24.20/24
User		
Ubuntu 14 Web	172.20.242.10/24	172.25.24.23/24
AD/DNS/DHCP	172.20.242.200/24	172.25.24.27/24
Workstation	DHCP	DHCP
Public		
Splunk	172.20.241.20/24	172.25.24.9/24
CentOS E-comm	172.20.241.30/24	172.25.24.11/24
Webmail/WebApps	172.20.241.40/24	172.25.24.39/24

DHCP Pools

Pool	Network	Start Address	End Address
Local	172.20.242.0/24	Unknown	Unknown

Public	172.25.24.0/24	Unknown	Unknown

Listening Services

Port (TCP)	**Service**	**Version**	**Executable/Note** (if relevant)
Docker/Remote - 172.20.240.10			
135	MSRPC		
2179	VMRDP		C:\Windows\System32\vmms.exe
3389	RDP		
5985	WinRM		
DNS/NTP - 172.20.240.20			
22	SSH	OpenSSH 6.7p1	
53	DNS	BIND 9.9.5	
111	RPC		
Ubuntu 14 Web - 172.20.242.10			
22	SSH	OpenSSH 6.6.1p1	
80	HTTP	Apache httpd 2.4.7	
AD/DNS/DHCP - 172.20.242.200			
88, 464	Kerberos		
135	MSRPC		
389, 3268	LDAP		
445	SMB		SMPv1 Enabled: Eternal Blue
593, 49157	RPC over HTTP	RPC over HTTP 1.0	Note: possible RCE
636, 3269	LDAPS	(TCPwrapped)	
3389	RDP		
5985, 47001	WinRM	HTTPAPI httpd 2.0	
9389	MC-NMF	.NET Framing	
Splunk - 172.20.241.20			
22	SSH	OpenSSH 5.3	Note: possible RCE
8000	HTTP	Splunk httpd	
8089	HTTPS	Splunk httpd	
CentOS E-comm - 172.20.241.30			
22	SSH	OpenSSH 6.6.1	
80	HTTP	Apache httpd 2.4.6	
Webmail/WebApps - 172.20.241.40			
22	SSH	OpenSSH 6.6.1	
25	SMTP	Postfix smtpd	Note: VRFY, ETRN allowed, possible command injection
80	HTTP	Apache httpd 2.4.16 PHP 5.6.15	PHP 5.6 has various RCEs and DoS
110	POP3	Dovecot pop3d	
111	RPC		

143	IMAP	Dovecot	
2049	NFS		
3306	SQL	MariaDB	
9090	HTTP	Cockpit management console	
34980	RPC	nlockmgr	
38732	RPC	status	
Palo Alto – 172.20.242.150			
22	SSH	OpenSSH 7.7	
23	Telnet	Linux telnetd	
80	HTTP		
443	HTTPS		

HTTP and DNS File Locations

Debian: /etc/bind

Ubuntu 14 Web: /var/www/html

CentOS: /var/www/html/prestashop

Fedora: /var/www/html, /usr/share/cockpit