Team 1
TOOL06A
To the Information Network team:
I am writing to report on the work being done to document and restrict packet flows to only the expected level and type of traffic. The objective of this was to ensure that the company network is not being used for illegal or unprofessional purposes.
In order to achieve this objective, the firewall team has documented the construction of their ACL list in order to control which networks get what traffic, and will only allow what is necessary to do their work through the firewall.
Please find attached a screenshot of the ACL list used to create the firewall and packet filtering.
If you have any questions or need further information, please do not hesitate to reach out.
Best regards,
Group 1

Internal DNS-Out-Bound Internal (eth1/2) any any Internal (eth1/2) any Internal (eth1/2) any Internal (eth1/2) any Internal (eth1/2) any Internal (eth1/3) any Internal (e	RULE Name	Source Zone	Source Address	Destination Zone	Destination Address	Service(s)	Action
Internal-ONS-In-Bound	ICMP-Ping	Internet (eth1/3)	any	any	any	ICMP (Ping)	Allow
Web-Browsing4Internal Internal (eth1/2) any Internal (eth1/3) any Internal (eth1/3)	Internal-DNS-Out-Bound	Internal (eth1/2)	any	any	any	DNS (UDP)	Allow
Web-Browsing4User	Internal-DNS-In-Bound	any	any	Internal (eth1/2)	any	DNS (UDP)	Allow
Web-Browsing4User User (eth1/4) any Internet (eth1/3) any set (80, 443)* Allow Web-Browsing4WindowsMachine Internet (eth1/13) any Internet (eth1/3) any web-browsing Allow WFD-Browsing4WindowsMachine Internet (eth1/3) Internet (eth1/3) any web-browsing Allow MTP2Internet Internal (eth1/2) any User (eth1/4) any NTP Allow MTP2Internet Internal (eth1/2) any Internet (eth1/3) any NTP Allow NTP2User Internal (eth1/2) any Internet (eth1/3) any NTP Allow Internal(eth1/2) any Internal (eth1/2) any NTP Allow NTP2User Internal (eth1/2) any Internal (eth1/2) any NTP Allow Internal(eth1/2) any Internal (eth1/2) any NTP Allow User(2NTP Public (eth1/1) any Internal (eth1/2) any NTP Allow User(2NTP <td>Web-Browsing4Internal</td> <td>Internal (eth1/2)</td> <td>any</td> <td>Internet (eth1/3)</td> <td>any</td> <td></td> <td>Allow</td>	Web-Browsing4Internal	Internal (eth1/2)	any	Internet (eth1/3)	any		Allow
Web-Browsing4Public Public (eth1/1) any Internet (eth1/3) any sst (80, 443) Allow Web-Browsing4WindowsMachine Internet (eth1/3) Windows 10 IP Internet (eth1/3) any web-browsing st (80, 443) Allow NTP2Internet Internal (eth1/2) any User (eth1/4) any NTP Allow NTP2Internet Internal (eth1/2) any Internet (eth1/3) any NTP Allow NTP2User Internal (eth1/2) any User (eth1/4) any NTP Allow NTP2User Internal (eth1/2) any User (eth1/4) any NTP Allow NTP2User Internal (eth1/2) any User (eth1/4) any NTP Allow Internal (eth1/2) any User (eth1/4) any NTP Allow Internal (eth1/2) any Internal (eth1/2) any NTP Allow Internal (eth1/2) any Internal (eth1/2) any NTP Allow User-CNTS-CHAIL (Ash)	Web-Browsing4User	User (eth1/4)	any	Internet (eth1/3)	any		Allow
Internet (eth 1/3) Mindows 10 P User (eth 1/4) Mindows 10 P Mindo	Web-Browsing4Public	Public (eth1/1)	any	Internet (eth1/3)	any		Allow
NTP2Public Internal (eth1/2) any Public (eth1/1) any NTP Allow NTP2Internet Internal (eth1/2) any Internet (eth1/3) any NTP Allow NTP Allow NTP2User Internal (eth1/2) any Internet (eth1/3) any NTP Allow NTP Allow NTP NTP Allow NTP N	Web-Browsing4WindowsMachine	Internet (eth1/3)	Windows 10 IP	Internet (eth1/3)	any	ssl (80, 443)	Allow
Internal (eth1/2) any Internal (eth1/3) any NTP Allow	NTP2Internal	Internal (eth1/2)	any	User (eth1/4)	any	NTP	Allow
Internal (eth1/2) any User (eth1/4) any NTP Allow	NTP2Public	Internal (eth1/2)	any	Public (eth1/1)	any	NTP	Allow
Internal (eth1/2) any Internal (eth1/2) any Internal (eth1/2) any Internal (eth1/2) any NTP Allow	NTP2Internet	Internal (eth1/2)	any	Internet (eth1/3)	any	NTP	Allow
Public (eth 1/1) any Internal (eth 1/2) any NTP Allow	NTP2User	Internal (eth1/2)	any	User (eth1/4)	any	NTP	Allow
Internet Internet	Internal2NTP	Internal (eth1/2)	any	Internal (eth1/2)	any	NTP	Allow
User (eth 1/4) any Internal (eth 1/2) any NTP Allow	Public2NTP	Public (eth1/1)	any	Internal (eth1/2)	any	NTP	Allow
Docker (Talk to Abdul WildCard) -	Internet2NTP	Internet (eth1/3)	Windows 10 IP	Internal (eth1/2)	any	NTP	Allow
Company Comp	User2NTP	User (eth1/4)	any	Internal (eth1/2)	any	NTP	Allow
SSHP	Docker (Talk to Abdul WildCard)						
User (eth	Remote Desktop RDP (Talk to Abd						
User-DNS-In-Bound any any User (eth1/4) any DNS (UDP) Allow	SSH?						
Internal - Zone - Transfer - User Internal (eth 1/2) any User (eth 1/4) any DNS (TCP) Allow	User-DNS-Out-Bound	User (eth1/4)	any	any	any	DNS (UDP)	Allow
User (eth1/4) User (eth1/4) any Internal (eth1/2) any Internal (eth1/2) any Internal (eth1/2) Internal (eth1/3) Internal (eth1/2) Internal (eth1/3) Internal (eth1/2) Internal (eth1/3) Internal (eth1/2) Internal (eth1/3) Internal (eth1	User-DNS-In-Bound	any	any	User (eth1/4)	any	DNS (UDP)	Allow
Kerberos2Windows10 User (eth1/4) any Internet (eth1/3) Windows 10 IP TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow Windows10_2Kerberos Internet (eth1/3) Windows 10 IP User (eth1/4) any TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow Kerberos4Windows2016 User (eth1/4) any Internal (eth1/2) any TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow Windows2016_2Kerberos Internal (eth1/2) any User (eth1/4) any TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow User-POP3-Out-Bound User (eth1/4) any Internet (eth1/3) any POP3 TCP 110 Allow User-POP3-In-Bound Internet (eth1/3) any User (eth1/4) any POP3 TCP 110 Allow Public-SMTP-Out-Bound Public (eth1/1) any Internet (eth1/3) any SMTP Allow Public (sMTP-In-Bound Internet (eth1/2) any Public (eth1/1) any SMTP Allow Naima SIEM SPLUNK-WEB Internal (eth1/2) any Int	Internal-Zone-Transfer-User	Internal (eth1/2)	any	User (eth1/4)	any	DNS (TCP)	Allow
Windows10_2Kerberos Internet (eth1/3) Windows 10 IP User (eth1/4) any TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow Kerberos4Windows2016 User (eth1/4) any Internal (eth1/2) any TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow Windows2016_2Kerberos Internal (eth1/2) any User (eth1/4) any TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow User-POP3-Out-Bound User (eth1/4) any Internet (eth1/3) any POP3 TCP 110 Allow User-POP3-In-Bound Internet (eth1/1) any Internet (eth1/3) any POP3 TCP 110 Allow Public-SMTP-Out-Bound Public (eth1/1) any Internet (eth1/3) any SMTP Allow Public-SMTP-In-Bound Internet (eth1/2) any Public (eth1/1) any SMTP Allow Naima SIEM SPLUNK-WEB Internal (eth1/2) any Internal (eth1/2) any Splunk-Web(TCP/8000) Allow Splunk ForwardInternal Internal (eth1/2) any Internal (eth1/2) any	User-Zone-Transfer-Internal	User (eth1/4)	any	Internal (eth1/2)	any	DNS (TCP)	Allow
Kerberos4Windows2016 User (eth1/4) any Internal (eth1/2) any TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow Windows2016_2Kerberos Internal (eth1/2) any User (eth1/4) any TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow User-POP3-Out-Bound User (eth1/4) any Internet (eth1/3) any POP3 TCP 110 Allow Public-SMTP-Out-Bound Public (eth1/1) any Internet (eth1/3) any POP3 TCP 110 Allow Public-SMTP-Out-Bound Public (eth1/1) any Internet (eth1/3) any SMTP Allow Naima SIEM SPLUNK-WEB Internal (eth1/2) any Public (eth1/1) any Splunk-Web(TCP/8000) Allow Splunk TorwardInternal Internal (eth1/2) any Internal (eth1/2) any Splunk (TCP 9997) Allow SplunkForwardPublic Public (eth1/1) any Internal (eth1/2) any Splunk (TCP 9997) Allow	Kerberos2Windows10	User (eth1/4)	any	Internet (eth1/3)	Windows 10 IP	TCP port 88, UDP port 88, TCP port 750, and UDP port 750	Allow
Windows2016_2Kerberos Internal (eth1/2) any User (eth1/4) any TCP port 88, UDP port 88, TCP port 750, and UDP port 750 Allow	Windows10_2Kerberos	Internet (eth1/3)	Windows 10 IP	User (eth1/4)	any	TCP port 88, UDP port 88, TCP port 750, and UDP port 750	Allow
User-POP3-Out-Bound User (eth1/4) any Internet (eth1/3) any POP3 TCP 110 Allow User-POP3-In-Bound Internet (eth1/3) any User (eth1/4) any POP3 TCP 110 Allow Public-SMTP-Out-Bound Public (eth1/1) any Internet (eth1/3) any SMTP Allow Public-SMTP-In-Bound Internet (eth1/3) any Public (eth1/1) any SMTP Allow Naima SIEM SPLUNK-WEB Internal (eth1/2) any Internal (eth1/2) any Splunk-Web(TCP/8000) Allow Splunk Ternal (eth1/2) any Internal (eth1/2) any Splunk-Managment (TCP/8089) Allow SplunkForwardPublic Public (eth1/1) any Internal (eth1/2) any Splunk (TCP 9997) Allow	Kerberos4Windows2016	User (eth1/4)	any	Internal (eth1/2)	any	TCP port 88, UDP port 88, TCP port 750, and UDP port 750	Allow
User-POP3-In-Bound Internet (eth1/3) any User (eth1/4) any POP3 TCP 110 Allow	Windows2016_2Kerberos	Internal (eth1/2)	any	User (eth1/4)	any	TCP port 88, UDP port 88, TCP port 750, and UDP port 750	Allow
Public-SMTP-Out-Bound Public (eth1/1) any Internet (eth1/3) any SMTP Allow Public-SMTP-In-Bound Internet (eth1/3) any Public (eth1/1) any SMTP Allow Naima SIEM SPLUNK-WEB Internal (eth1/2) any Internal (eth1/2) any Splunk-Web(TCP/8000) Allow Splunk managment Internal (eth1/2) any Internal (eth1/2) any Splunk-Managment(TCP/8089) Allow SplunkForwardInternal Internal (eth1/2) any Splunk (TCP 9997) Allow SplunkForwardPublic Public (eth1/1) any Internal (eth1/2) any Splunk (TCP 9997) Allow	User-POP3-Out-Bound	User (eth1/4)	any	Internet (eth1/3)	any	POP3 TCP 110	Allow
Public-SMTP-In-Bound Internet (eth1/3) any Public (eth1/1) any SMTP Allow Naima SIEM SPLUNK-WEB Internal (eth1/2) any Internal (eth1/2) any Splunk-Web(TCP/8000) Allow Splunk managment Internal (eth1/2) any Internal (eth1/2) any Splunk-Managment(TCP/8089) Allow SplunkForwardInternal Internal (eth1/2) any Internal (eth1/2) any Splunk (TCP 9997) Allow SplunkForwardPublic Public (eth1/1) any Internal (eth1/2) any Splunk (TCP 9997) Allow	User-POP3-In-Bound	Internet (eth1/3)	any	User (eth1/4)	any	POP3 TCP 110	Allow
Public-SMTP-In-Bound Internet (eth1/3) any Public (eth1/1) any SMTP Allow Naima SIEM SPLUNK-WEB Internal (eth1/2) any Internal (eth1/2) any Splunk-Web(TCP/8000) Allow Splunk managment Internal (eth1/2) any Internal (eth1/2) any Splunk-Managment(TCP/8089) Allow SplunkForwardInternal Internal (eth1/2) any Internal (eth1/2) any Splunk (TCP 9997) Allow SplunkForwardPublic Public (eth1/1) any Internal (eth1/2) any Splunk (TCP 9997) Allow	Public-SMTP-Out-Bound	Public (eth1/1)	any	Internet (eth1/3)	any	SMTP	Allow
Naima SIEM SPLUNK-WEB Internal (eth1/2) any Internal (eth1/2) any Splunk-Web(TCP/8000) Allow Splunk managment Internal (eth1/2) any Internal (eth1/2) any Splunk-Managment(TCP/8089) Allow SplunkForwardInternal Internal (eth1/2) any Internal (eth1/2) any Splunk (TCP 9997) Allow SplunkForwardPublic Public (eth1/1) any Internal (eth1/2) any Splunk (TCP 9997) Allow	Public-SMTP-In-Bound		-		-	SMTP	Allow
Splunk managment Internal (eth1/2) any Internal (eth1/2) any Splunk-Managment(TCP/8089) Allow SplunkForwardInternal Internal (eth1/2) any Internal (eth1/2) any Splunk (TCP 9997) Allow SplunkForwardPublic Public (eth1/1) any Internal (eth1/2) any Splunk (TCP 9997) Allow	Naima SIEM SPLUNK-WEB	Internal (eth1/2)	any		any	Splunk-Web(TCP/8000)	Allow
SplunkForwardInternal Internal (eth1/2) any Internal (eth1/2) any Splunk (TCP 9997) Allow SplunkForwardPublic Public (eth1/1) any Internal (eth1/2) any Splunk (TCP 9997) Allow	Splunk managment		- ,		-		Allow
SplunkForwardPublic Public (eth1/1) any Internal (eth1/2) any Splunk (TCP 9997) Allow	SplunkForwardInternal			,	-	-	Allow
	SplunkForwardPublic			,	-		
	SplunkForwardInternet		-	,	-		Allow

SplunkForwardUser	User (eth1/4)	any	Internal (eth1/2)	any	Splunk (TCP 9997)	Allow
Public-ECOMM-Out-Bound	Public (eth1/1)	any	Internet (eth1/3)	any	http, https, dns,	Allow
Public-ECOMM-In-Bound	Internet (eth1/3)	any	Public (eth1/1)	any	http, https, dns,	Allow
Public-WEB-Out-Bound (Might be	Public (eth1/1)	any	Internet (eth1/3)	any	http, https, dns,	Allow
Public-WEB-In-Bound (Might be re	Internet (eth1/3)	any	Public (eth1/1)	any	http, https, dns,	Allow
Deny	any	any	any	any	any	DROP