Implementation of Threat policies and Routing process in Firepower Threat Defense

Prajwal S Telkar, Undergraduate Student, Dr. Kiran V, IEEE Senior Member, Associate Professor,
Electronics and Communication Engineering, R V College of Engineering, Bangalore

***Abstract*— Firewall is a guard of the network which inspects the packets based on the rules adopted to be executed in the threat environment. This is used to block flow of undesirable content, forbids unauthorized remote access, and impedes immoral contents, assures security based on protocol and IP address, insulates seamless activity in Enterprise networks, shields conversation and coordination contents and thus this cyber security tool secures the system when administering on internet with humongous amount of malicious data threatening the performance and data of the network structure. Cisco next generation firewalls are equipped to combat the menace and in this project, initially it is focused on the working of the FTD and analyzes the steps carried out in the processes. FMC is the graphical user interface to control FTD which is connected through the management interface. Various policies such as file policy, Prefilter policy, malware policies, provide the firewall to work more efficiently on the firewall. Additionally these firewalls are equipped with routing process to uphold the efficiency of the firewall which behaves as router to establish connection between the network nodes. The routing process is implemented using the firewall which is an IP routing software suite that provides robust facility to adapt the firewall for routing conditions.**

Index Terms— LINA (Linux over ASA), FTD (Firepower Threat Defense), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol)

I. INTRODUCTION

Then weak security practices within a firm might lead to data leakage which might include trade secrets and customers' private details. The basic composition of security system might be arduous to beginners; hence an encyclopedic system is built with many small pieces and hence can expertise in each. Firewalls are once such network security component that has a huge scope for analysis and optimization with new technologies incorporated into the system to make the network system more robust to avoid threats. Adequate network security operations keep information shielded and block vulnerable systems from outside interference. Thus helps a community or organization to be defended and focus on organizational goals.

Alongside of increasing the surveillance of the traffic it is also required to handle the packets with a proper protocol to operate on it. Thus a routing process is implemented to increase the inter operate-ability of the firewall with various protocols made available and thus can choose an efficient routing process to increase the stability of the system. File policy in the firewall is used to detect and stop malware entering into the system. This policy can also be used distinguish and administer based on the file type traffic. File policy is a set of configurations that the system uses to perform malware protection and file control, as part of your overall access control configuration. This assures the access control rule's accustomed in the policy, the files before entering into the system are inspected and based on the decision it allows or blocks the file. The initial phase of access control before the system performs more resource-intensive evaluation is Prefilter policy. The Prefilter policy happens before access control policy. It has two different types named tunnel policy and Prefilter policy. In Prefilter policy we could create a rule with simple IP level, TCP port number, Virtual Local Area Network (VLAN) tagging and match traffic. In tunnel rule which matches encapsulation traffic such as Generic Routing Encapsulation (GRE), IP-in-IP, Internet Protocol version 6 (IPv6)-in-IP, Teredo etc. Access control policy is more on L2 to L7 in Open Systems Interconnection (OSI) model. These threat defense mechanisms protect the network with utmost security. Additionally to these properties, the firewall is also capable of handling routing to form a closed network with the other nodes. This routing process plays a major role in determining the path of the packet within the network. The firewall is capable of supporting various IP routing protocols such as interior gateway protocols like OSPF and exterior gateway protocols like BGP and many such routing protocols are supported. These properties of the firewall are analyzed and implemented with the due modifications to make the system more robust.

II. BACKGROUND

FTD Packet Processing

The decision whether a packet must be forwarded or dropped is decided by the FTD by passing through various parameters as shown in the Figure 1. A packet enters firewall through ingress interface and passes through various steps involved. Once this processes is completed if a packet from the same host with similar properties arrives and if the connection already exists then such packets will not be sent to inspection since it reduces

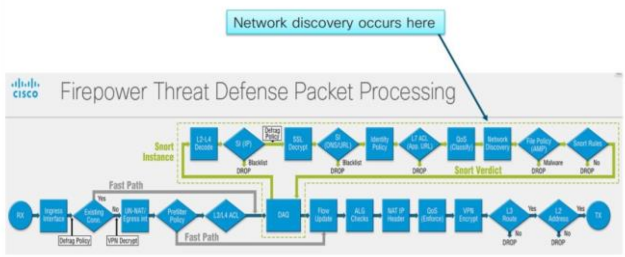


Fig.1. FTD packet process flow

The VPN is decrypted and analyzes whether the packet goes out of egress interface that is whether the packet is coming to FTD or going out of FTD. If a packet arrives with a NATed address, it verifies the UnNATed address to check whether the packet to be allowed. The packet further passes through Prefilter policy which serves as a base policy to check whether the packet must be allowed or if packet required even more complex analysis. This policy will have predefined ACL which verifies if a packet is from an unauthorized source, such packets will be dropped. The packet further processed with L3/L4 ACL's and discard packets if any discrepancy is seen in these layers. Else the packet is allowed for further inspection which passes the packet into Data AcQuisition (DAQ) which determines whether Snort inspection is needed for deeper layer analysis. If no Snort inspection is needed then the packet headers are added, a packet is NATed if it's UnNATed and make the decision whether to forward or drop. This memory is stored in cache and thus can update flow data, update counters, add the header, on egress if it needs to encrypted, leverage L3 route, then leverage Layer 2 (L2) address which is responsible for generating new layer 2 headers which notifies that packet has been inspected and sent by ASA to the next hop. If Snort Inspection (SI), the packet enters SI(IP) which blocks blacklisted IPs, Domain Name System (DNS), and URLs before inspection by advanced features in Access Control Policy (ACP). Traffic blocked here never enters later policies. In SSL policy it decrypts SSL traffic. It has ability to block or decrypt traffic based on criteria. Decrypted traffic can be inspected by later policies. SI(URL, DNS) performs similar to SI(IP). The access control policy is a firewall component which makes decision if traffic should be blocked, allowed or further inspected by file policy and IPS policy. File policy is used for inspecting files for malware. IPS policy inspects IPS Snort rules. Based on the verdict of Snort, ASA decides to drop the packet if blacklisted else allows the packet to pass the firewall.

III. METHODOLOGY

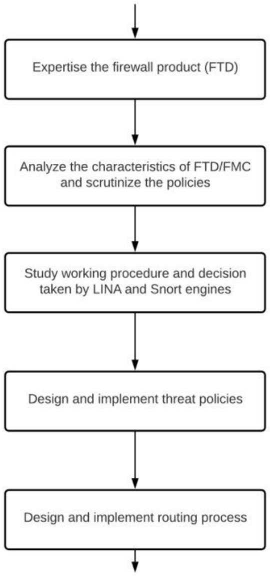

Expertise the firewall product (FTD)
Analyze the characteristics of FTD/FMC and scrutinize the policies
Study working procedure and decision taken by LINA and Snort engines
Design and implement threat policies
Design and implement routing process

Fig.2. Flowchart showing methodology

Network security products that are reliable is a firewall. The firewall designed by Cisco Systems is termed as FTD. To implement the process on such firewall, it is required to expertise in the domain on how a firewall works in the network to protect from the data predators. This can be thoroughly understood by analyzing the characteristics of the firewall by performing various threat defense policies available in the FTD that gives an understanding of the device. While the traffic inspected by the FTD, decision is made through LINA and Snort engine. The process carried by these engines is important to understand what rules and phases a packet is passed through and thus the inspected packet is either dropped or forwarded by the FTD. Various threat policies have been analyzed and the working of the firewall and the phases through which packet passes for inspection is an important aspect to understand. Since an FTD can perform on various tasks, it is required to support various routing protocols on the firewall to have a robust system design for everyday evolving threats. Thus to implement the routing process, an IP routing software package has been used.

IV. DESIGN

Analysis of traffic through FTD

To analyze the properties of FTD, we need to generate traffic through FTD to analyze the processes involved in filtration and phases through which packet goes while passing through firewall. To setup these environment two virtual machines for hosts were deployed in VMware ESXi. Similarly two FTD and a FMC were deployed virtually in the same software. These FTDs were registered on FMC. To register FTD on FMC, on the Command-Line Interface (CLI) of the FTD, we define a manager and registration key which would be verified in FMC by using a command "configure manager add ".

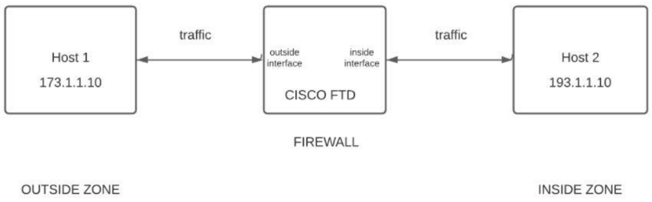


Fig.3. Design to analyze traffic between two hosts through FTD

The configuration of these FTD devices to be done in FMC. This can be done by navigation to Device Management and add device and fill the necessary details of the FTD and register it. This completes the registration of FTD in FMC.

File Policy

Considering the figure 4 an access control policy is defined with two rules such that the files are allowed or blocked considering these. If a file policy is created such that traffic entering into the system matches Rule 1, then such packets are inspected File Policy A, then such packets are blocked and discarded, else it is forwarded to next rule. In rule 2, the entering traffic matches the rule, then such packets are inspected by File Policy B, and these packets are blocked and discarded. If a packet passes all the rules, then such packet is allowed to pass through the firewall. In the file policy design it is discussed on how a file can be blocked when a packet that needs to be sent from inside zone of firewall to the outside zone.

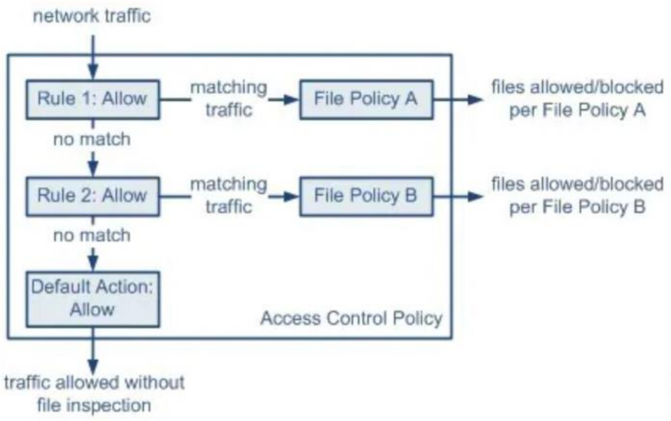


Fig.4. Schematic flow of File Policy operation

Inside zone is configured with network 193.1.1.0/24 and outside zone is configured with network 173.1.1.0/24. A file policy is defined in firewall to test such that any Portable Document Format (PDF) file going out from inside zone to outside zone is blocked.

Prefilter policy

In Prefilter policy three actions can be used named Analyze, Block and Fastpath. If a rule matches based on source or destination IP or port number, if the traffic matches enabled with fastpath mode, then the packet leaves egress interface without any inspection. This helps to reduce latency in a connection. If traffic is traveling from a host to another host, and if these hosts are trusted, then such connection can be enabled with fastpath to avoid latency since the path is already trusted. Analyze mode is used when a new connection is established and this traffic should be inspected, during such situation we can create a rule to analyze the packet which is further sent to access control policy which checks with the rules defined here. Design to analyze Prefilter Policy A Prefilter policy is created and associate with access control policy. In this Prefilter policy we create a rule which allow host from inside to outside and make action as fast path, such that traffic does not goes to Snort engine/Advance inspection and bypass the application level inspection and packet is sent allowed outside. As we know this is used between trusted connections. After fastpath mode is analyzed, Analyze mode is taken to inspect the packet that is passed through the Snort engine and make sure that the packet is inspected by the access rules defined and the traffic is analyzed by the Snort engine. A Prefilter Access control Policy is also designed to test the traffic generated from outside i.e 173.1.1.10 host to 193.1.1.10 host to analyze the how the policy works and also blocked in the same path when the rule is defined in the Blocked mode.

Routing Process

Open Shortest Path First (OSPF)

OSPF is a widely used and supported interior gateway protocol which is used within a single autonomous system. This protocol is a Link-state routing protocol which serves the goal to learn routes between the routers. It learns about every router and subnet within the entire network that results every router has the same information about each other. These router learn about this information is by sending out Link State Advertisement (LSA). This LSA contains information about subnet, router and other network information. Once these essays are flooded OSPF keeps all of this information in a Link State Database (LSDB). The goal here is to have each router same information. Main steps involved in OSPF are: • Become neighbors - Two routers running OSPF on the same link agree to form a neighbor relationship. • Exchange database information- The neighbor routers swap their LSDB information with each other. • Choose the best routes- Each router chooses the best routes to add to its routing table based on the learned LSDB information. The best route is calculated using Shortest Path First (SPF) algorithm.

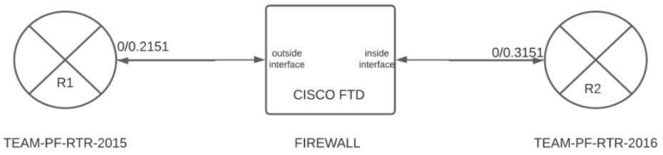


Fig.5. Design to establish OSPF neighbor with FTD

The design is carried out to implement OSPF on Cisco FTD. OSPF is configured on the inside interface of the FTD in Area 0. The router ID is configured with 10.10.10.10. OSPF is also configured on Router 1 (TEAM-PF-RTR-2015), R1 advertises the Loop back network 10.1.1.0/24 in OSPF. FTD is injected with default route towards the inside network.

Border Gateway Protocol (BGP)

BGP is an exterior gateway protocol used to establish connection between the clusters of network nodes. These clusters are known as autonomous systems. Within an autonomous system an interior gateway protocol such as RIP, EIGRP, IGRP, OSPF are used. To connect between two autonomous systems exterior gateway protocol like BGP is used. These Autonomous System (AS) are given a unique number known as Autonomous System Number (ASN). A 2 byte ASN is a 16 bit number and range of values varies from 0 to 65535. The ASN can also be a 4 byte. The only protocol running in internet backbone is BGP. Some features of BGP are it is a standard protocol which is supported by all routers; it is specifically designed for Inter-AS domain routing; it is designed to scale huge inter-network like internet; Classless addressing is supported by BGP and supports Fixed Length Subnet Masks (FLSM), Variable Length Subnet Masks (VLSM), and Classless Inter-Domain Routing (CIDR). The updates are incremental and triggers are supported. BGP is path vector protocol such that it sends the route information along with path in formation. This protocol sends updates to manually defined neighbor as unicast address. Thus in BGP the neighbor is configured manually in router to establish adjacency. This is an application layer protocol that uses TCP for reliability and uses TCP port 179 as a standard port. It also prevents loop that can be formed within the system. A router-id can also be defined to identify BGP peers. This can be set manually, else the IP address of the loopback interface is set as RID, else if a loopback address is not available, then the highest IP address configured on the physical interface is set as the BGP RID.

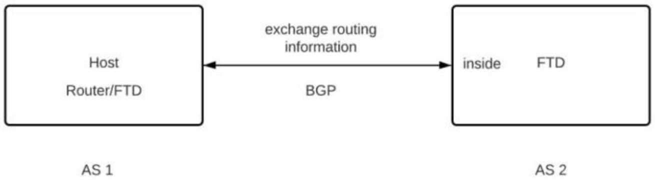


Fig.6. Design to establish BGP neighbor with FTD

This design is incorporated while implementing and testing the FRR BGP routing process setup in FTD and tested using another network node to establish a peering relationship to exchange routing information between the devices. The inside interface is defined GigabitEthernet0/0 with interface IP address 22.1.1.122. Another FTD has been used to establish a peering connection with IP address 10.127.46.175. These devices are defined into separate autonomous systems and the BGP routing process has been enabled in both devices to establish adjacency.

V. IMPLEMENTATION

Implementation to analyze traffic through FTD

Traffic analysis between two hosts

Steps to configure host machines to establish the route between hosts through FTD:
Step 1. Check for the interfaces available on the machine Step 2. $ ifconfig –a Step 3. Assign the interface IP address. Step 4. Add a gateway to pass the traffic and create a static route between the server machines through FTD. Step 5. $ sudo route add –net < IP address > netmask < netmask > gw < gateway > Step 6. The gateway and route added into the route table on machines is verified. Step 7. $ netstat –an Step 8. Create traffic between the machines to analyse the functionality of the FTD.

File Policy

Step 1. Ensure the following licenses are available a) Threat and Malware license b) Adaptive Profiling (enabled by default) c) Access Policy Action (Allow/ Interactive block / Interactive block with reset). Step 2. In FTD choose Device > Device Management to see the available FTD/HA Pair. Step 3. Choose Policies > Access Control > Malware and File section to create a file policy. Step 4. Click on New File Policy > Give a name and description (Name: test policy Description: To block pdf files. Step 5. Click on Add rule > Select application protocol (Any) > Select direction of transfer (Upload) > Select action (Block). Step 6. Select File type categories (PDF files) > File types (*.pdf) > Add > Save. Step 7. If archive files need to be allowed, that can be configured using advanced tab. Step 8. Deploy the configuration on FTD and test the policy.

Prefilter Policy

Step 1. Enter into the FMC > Devices > Device Management to see the available FTD/ HA Pair. Step 2. Choose Policies > Access Control Policy > Check for Prefilter Policy in Base Policy created (Initially default policy is applied). In default prefilter policy, it analyzes all tunnel traffic. Step 3. Choose Policies > Select Prefilter policy > Create a new policy by adding name and description > Add tunnel rule. Step 4. Tunnel rule will inspect the encapsulated traffic which are encapsulated by protocols such as GRE, IP-in-IP, IPv6-in-IP, Teredo port > Add name and description (Name: GRE-test) > Select action (Analyze, block, fastpath). Step 5. Select the option to match tunnels only from source or match tunnels from source to destination based on the requirement. Step 6. Select the interface objects and add to source and destination interface objects and networks accordingly. Step 7. Add tunnel end points by adding source tunnel endpoint (193.1.1.10) and destination tunnel endpoint(173.1.1.10) > Add the rule > Select encapsulation protocol as GRE > Add the rule > Save. Step 8. Once the rule is added to new Prefilter policy, save the configuration and deploy on to FTD to test the policy.

OSPF neighbor

Step 1. On R1 side, enter into config mode and define OSPF process with id in router mode : router ospf 1 . Step 2. Add a network in router 1 which id defined in area 0: network 10.0.0.0 0.255.255.255 area 0 . Step 3. Configure interface (GigabitEthernet0/0.2151) to add security: config > interface gigabitethernet 0/0.2151 > ip ospf authentication message-digest-key 1 md5 cisco123. Step 4. To confirm the configuration on the interface: show running-config interface gigabitethernet 0/0.2151. Step 5. To configure in FTD, go to FMC Devices > Device Management > Select on HA pair > Routing > OSPF > Process 1 > OSPF role: Internal router. Step 6. Referring to Step 5 > Advanced tab > Specify router id > Check on Enable Default Information Originate > Ok. Step 7. Add Area > OSPF process 1 > Area ID – 0 > Add network inside (10.11.11.0/24) > [If authentication enabled > Authentication MD5] > Save. Step 8. In the interface tab > Authentication tab > Add registration key > Save. Step 9. Save the OSPF configuration and deploy it into the FTD. Step 10. To confirm the configuration, in the router check for the neighbor : show ip ospf neighbor. Step 11. To confirm the configuration on FTD, check for the routing information for OSPF protocol on the Inside interface (10.11.11.1). Step 12. To confirm the routing configuration on router which confirms the OSPF protocol configured via 10.11.11.10: show ip route.

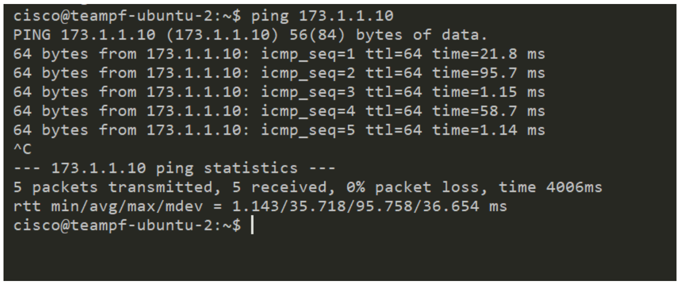
BGP neighbor

This is the implementation method to establish a peer relation between the network devices and this procedure has been followed to establish routing process with a neighbor outside of FTD and exchange routes via LINA data interface

Step 1. In the FTD, enter into LINA CLI (system support diagnostic-cli) > Enter into privileged mode (enable). Step 2. Open the configuration terminal. # configure terminal Step 3. Enter into router configuration mode to configure BGP process and define an autonomous system number. # router bgp < ASN > Step 4. A network local to the autonomous system is specified and added to BGP routing table. # network < network ip > mask < subnet mask > Step 5. Specify a router-id to identify the local device running BGP routing process. # bgp router-id < RID > Step 6. To establish neighbor with the specified AS to add to routing table of the local router. # neighbor < IP address > remote-as < ASN of the neighbor > Step 7. To specify that unicast address has been used to form the peering between the network devices. # address-family ipv4 unicast Step 8. Activate the neighbor IP address to exchange the prefixes for the IPv4 unicast address family with the local router. # neighbor < neighbor IP address > activate Step 9. Repeat the same steps on the remote router in correspondence to establish adja cency. Step 10. Verify the establishment of adjacency between the peers by issuing command. # show bgp neighbors

VI. RESULTS AND DISCUSSION

Results of analysis of traffic through FTD



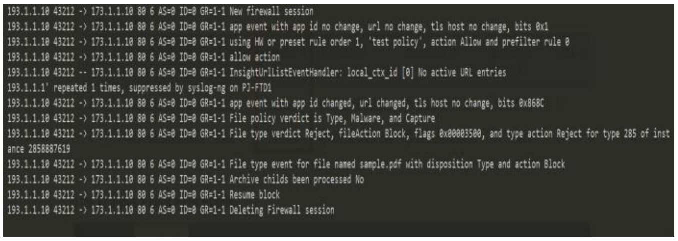
```
cisco@teampf-ubuntu-2:~$ ping 173.1.1.10
PING 173.1.1.10 (173.1.1.10) 56(84) bytes of data.
64 bytes from 173.1.1.10: icmp_seq=1 ttl=64 time=21.8 ms
64 bytes from 173.1.1.10: icmp_seq=2 ttl=64 time=95.7 ms
64 bytes from 173.1.1.10: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 173.1.1.10: icmp_seq=4 ttl=64 time=58.7 ms
64 bytes from 173.1.1.10: icmp_seq=5 ttl=64 time=1.14 ms
^C
--- 173.1.1.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.143/35.718/95.758/36.654 ms
cisco@teampf-ubuntu-2:~$ |
```

Fig.7. Output of end to end traffic analysis

From figure 7, a route between the inside zone host and outside zone host has to be created through FTD. The inside data interface of FTD is configured with 193.1.1.1 and this serves as the gateway for inside host. Similarly the outside data interface of FTD is configured with 173.1.1.1 and this serves as the gateway for outside host. The inside host is configured with 193.1.1.10 and outside host is configured with 173.1.1.10. The packets are analyzed by generating traffic between these hosts by passing though FTD.

Outcomes of File policy

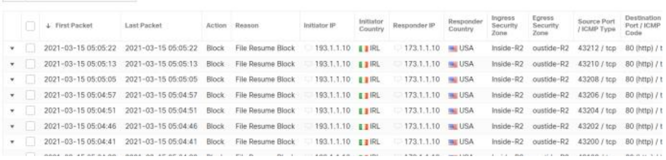
The results for File Policy are analyzed in figure 7. Traffic is generated from inside host to outside host through FTD. Inside host is configured with IP 193.1.1.10 and outside host is configured with IP 173.1.1.10. A new firewall session is opened on source port 43212.



```
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 New firewall session
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 app event with app id no change, url no change, tls host no change, bits 0x1
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 using HW or preset rule order 1, 'test policy', action Allow and prefilter rule 0
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 allow action
193.1.1.10 43212 -- 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 InsightUrlListEventHandler: local_ctx_id [0] No active URL entries
193.1.1.1' repeated 1 times, suppressed by syslog-ng on PJ-FTD1
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 app event with app id changed, url changed, tls host no change, bits 0x868C
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 File policy verdict is Type, Malware, and Capture
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 File type verdict Reject, fileAction Block, flags 0x00003500, and type action Reject for type 285 of inst
ance 2858887619
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 File type event for file named sample.pdf with disposition Type and action Block
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 Archive childs been processed No
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 Resume block
193.1.1.10 43212 -> 173.1.1.10 80 6 AS=0 ID=0 GR=1-1 Deleting Firewall session
```

Fig.8. Output of file policy in FTD CLISH

The phases through which firewall rules are applied can be observed. As discussed in design, a test policy has been created to block PDF files sent from inside host to outside. It can be observed that threat defense license has been applied and a file policy detects that it has file which matches this license. Since a PDF file is sent, a file policy verdict is seen with Reject and file policy action as block. Thus a file policy is successfully deployed and evaluated. This is output is observed in FTD CLISH.

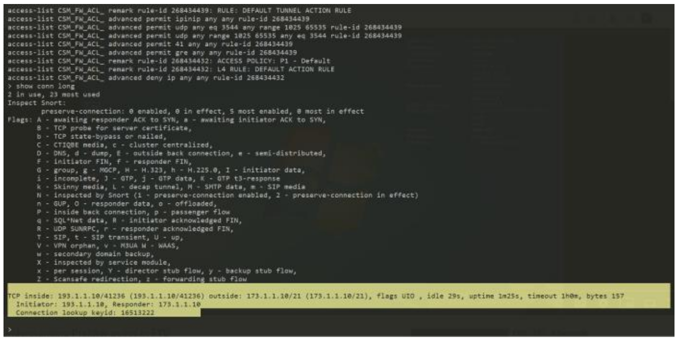


	□	↓ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
▾	□	2021-03-15 05:05:22	2021-03-15 05:05:22	Block	File Resume Block	193.1.1.10	IRL	173.1.1.10	USA	Inside-R2	oustide-R2	43212 / tcp	80 (http) / t
▾	□	2021-03-15 05:05:13	2021-03-15 05:05:13	Block	File Resume Block	193.1.1.10	IRL	173.1.1.10	USA	Inside-R2	oustide-R2	43210 / tcp	80 (http) / t
▾	□	2021-03-15 05:05:05	2021-03-15 05:05:05	Block	File Resume Block	193.1.1.10	IRL	173.1.1.10	USA	Inside-R2	oustide-R2	43208 / tcp	80 (http) / t
▾	□	2021-03-15 05:04:57	2021-03-15 05:04:57	Block	File Resume Block	193.1.1.10	IRL	173.1.1.10	USA	Inside-R2	oustide-R2	43206 / tcp	80 (http) / t
▾	□	2021-03-15 05:04:51	2021-03-15 05:04:51	Block	File Resume Block	193.1.1.10	IRL	173.1.1.10	USA	Inside-R2	oustide-R2	43204 / tcp	80 (http) / t
▾	□	2021-03-15 05:04:46	2021-03-15 05:04:46	Block	File Resume Block	193.1.1.10	IRL	173.1.1.10	USA	Inside-R2	oustide-R2	43202 / tcp	80 (http) / t
▾	□	2021-03-15 05:04:41	2021-03-15 05:04:41	Block	File Resume Block	193.1.1.10	IRL	173.1.1.10	USA	Inside-R2	oustide-R2	43200 / tcp	80 (http) / t

Fig.9. Output of file policy in FMC

A file policy output and sessions was observed in FTD CLISH, and a detailed phase session was analyzed. In this figure 9, it can observe that user interface output on FMC, with packets arriving to FTD from initiator 193.1.1.10 (inside host) to responder 173.1.1.10 (outside host). As discussed, the phases were discussed for 1 packet initiated on source port 43212, here it can be observed how a file is blocked on various packets.

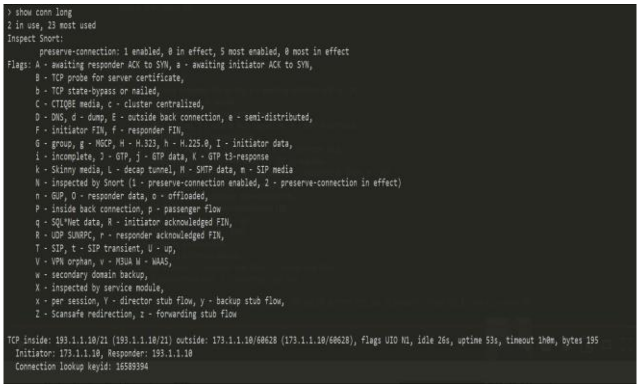
Outcomes of Prefilter Policy



```
access-list CSM_FW_ACL_ remark rule-id 268434439: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 268434439
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 268434439
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 268434439
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 268434439
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 268434439
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: P1 - Default
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268434432
> show conn long
2 in use, 23 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 5 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       B - TCP probe for server certificate,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP inside: 193.1.1.10/41236 (193.1.1.10/41236) outside: 173.1.1.10/21 (173.1.1.10/21), flags UIO , idle 29s, uptime 1m25s, timeout 1h0m, bytes 157
  Initiator: 193.1.1.10, Responder: 173.1.1.10
  Connection lookup keyid: 16513222

>
```

Fig.10. Demonstration of fastpath in Prefilter policy

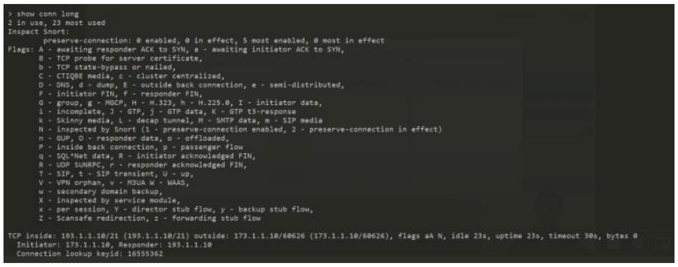
It can be observed from figure 10 that a default tunnel rule has been applied and since the configuration is done for the fastpath, we observe that the packets sent from inside to outside are permitted. This policy is named as P1 policy. In the highlighted part of figure 10 we can observe that 'N' flag is not present which signifies that the traffic is not sent to Snort engine to analyze and thus it is confirmed that fastpath mode is successfully deployed in the firewall.



```
> show conn long
2 in use, 23 most used
Inspect Snort:
        preserve-connection: 1 enabled, 0 in effect, 5 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       B - TCP probe for server certificate,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP inside: 193.1.1.10/21 (193.1.1.10/21) outside: 173.1.1.10/60628 (173.1.1.10/60628), flags UIO N1, idle 26s, uptime 53s, timeout 1h0m, bytes 195
  Initiator: 173.1.1.10, Responder: 193.1.1.10
  Connection lookup keyid: 16589394
```

Fig.11. Demonstration of Snort inspection from outside to inside in Prefilter policy

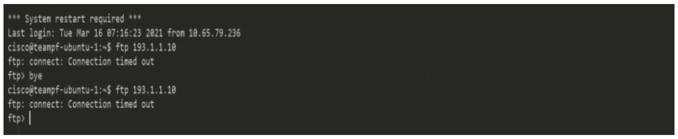
In figure 11 it can be observed that a Prefilter policy is created for packets that are initiated on the outside zone of firewall and is sent through the firewall in Analyze mode such that the packets are sent into the Snort engine and the flag ‘N’ is set which confirms that packets were inspected by snort engine. In also 3rd line of figure 11 we can observe that the firewall indicates Snort has been enabled.



```
> show conn long
2 in use, 23 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 5 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       B - TCP probe for server certificate,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP inside: 193.1.1.10/21 (193.1.1.10/21) outside: 173.1.1.10/60626 (173.1.1.10/60626), flags aA N, idle 23s, uptime 23s, timeout 30s, bytes 0
  Initiator: 173.1.1.10, Responder: 193.1.1.10
  Connection lookup keyid: 16555362
```

Fig.12. Demonstration of fastpath Snort inspection in Prefilter policy

It is observed from figure 12 that a default tunnel rule has been applied and since the configuration is done for the fastpath, we observe that the packets sent from outside to inside are permitted. This policy is named as P1 policy. In the highlighted part of figure 12 we can observe that ‘N’ flag is present which signifies that the traffic is sent to Snort engine to analyze and thus it is confirmed that Analyze mode is successfully deployed in the firewall.

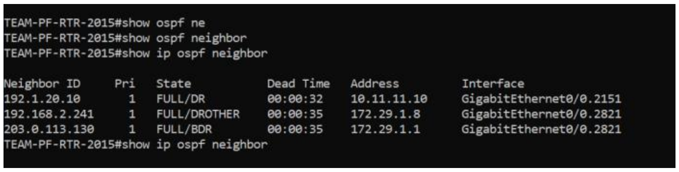


```
*** System restart required ***
Last login: Tue Mar 16 07:16:23 2021 from 10.65.79.236
cisco@teampf-ubuntu-1:~$ ftp 193.1.1.10
ftp: connect: Connection timed out
ftp> bye
cisco@teampf-ubuntu-1:~$ ftp 193.1.1.10
ftp: connect: Connection timed out
ftp> |
```

Fig.13. Demonstration of blocked mode from outside to inside in Prefilter policy

In figure 13, the Prefilter policy is tested with blocked mode. Here the policy is defined to block ftp connection with inside host. As the outside host with IP 173.1.1.10 tries to establish a connection with inside host with IP 193.1.1.10 though firewall, since a Prefilter policy with Blocked mode is configured, it observed that connection could not be established.

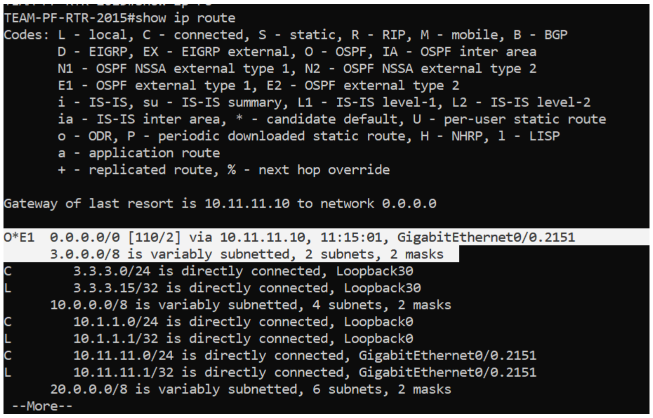
Results of OSPF adjacency



```
TEAM-PF-RTR-2015#show ospf ne
TEAM-PF-RTR-2015#show ospf neighbor
TEAM-PF-RTR-2015#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.1.20.10       1   FULL/DR         00:00:32    10.11.11.10     GigabitEthernet0/0.2151
192.168.2.241     1   FULL/DROTHER    00:00:35    172.29.1.8      GigabitEthernet0/0.2821
203.0.113.130     1   FULL/BDR        00:00:35    172.29.1.1      GigabitEthernet0/0.2821
TEAM-PF-RTR-2015#show ip ospf neighbor
```

Fig.14. Demonstration of OSPF neighbor

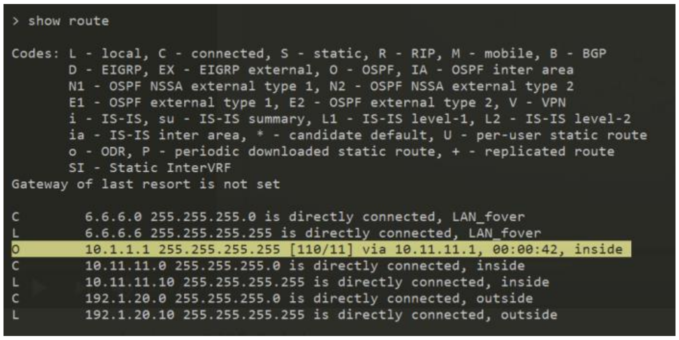
OSPF is a protocol used to establish connection between the routers to exchange route information. An OSPF is configured on routers to establish adjacency between each other through FTD. A router is configured with IP 10.11.11.10 and other router is assigned with IP 192.1.1.10. OSPF is configured on sub-interface GigabitEthernet0/.2151 on one router and on sub-interface GigabitEthernet0/0.3151 on other. Both routers are verified with OSPF neighbor and it can be observed, on router TEAM-PF-RTR-2015, router with Neighbor ID 192.168.2.141 is available. Same can be observed on TEAM-PF-RTR-2016.



```
TEAM-PF-RTR-2015#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.11.11.10 to network 0.0.0.0

O*E1  0.0.0.0/0 [110/2] via 10.11.11.10, 11:15:01, GigabitEthernet0/0.2151
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, Loopback30
L        3.3.3.15/32 is directly connected, Loopback30
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Loopback0
L        10.1.1.1/32 is directly connected, Loopback0
C        10.11.11.0/24 is directly connected, GigabitEthernet0/0.2151
L        10.11.11.1/32 is directly connected, GigabitEthernet0/0.2151
      20.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
 --More--
```

Fig.15. Demonstration of OSPF route on router

To verify OSPF is configured and to evaluate the route through FTD can be observed from figure 15. It is observed that external type OSPF has been configured via 10.11.11.10 on sub-interface 0/0.2151. O*E1 signifies the type of the OSPF configuration available on the router.

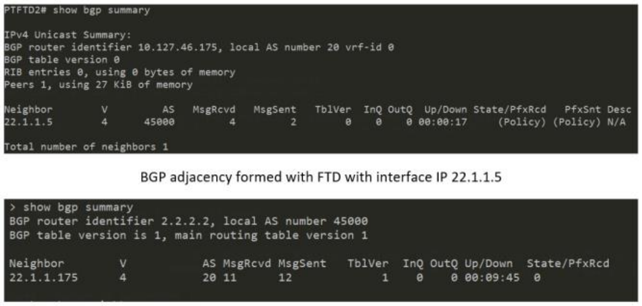


```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        6.6.6.0 255.255.255.0 is directly connected, LAN_fover
L        6.6.6.6 255.255.255.255 is directly connected, LAN_fover
O        10.1.1.1 255.255.255.255 [110/11] via 10.11.11.1, 00:00:42, inside
C        10.11.11.0 255.255.255.0 is directly connected, inside
L        10.11.11.10 255.255.255.255 is directly connected, inside
C        192.1.20.0 255.255.255.0 is directly connected, outside
L        192.1.20.10 255.255.255.255 is directly connected, outside
```

Fig.16. Demonstration of OSPF route on FTD

From figure 16, the OSPF configuration is verified on FTD, such that OSPF is configured on the inside data interface of the FTD with IP 10.1.1.1 and subnet mask of 255.255.255.255. It is also verified this acts as the interface to establish OSPF with the router TEAM-PF-RTR-2015 via 10.11.11.1 which serves as the gateway for the router. Thus OSPF route on FTD is interpreted.

Results of BGP adjacency



```
PTFTD2# show bgp summary

IPv4 Unicast Summary:
BGP router identifier 10.127.46.175, local AS number 20 vrf-id 0
BGP table version 0
RIB entries 0, using 0 bytes of memory
Peers 1, using 27 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down State/PfxRcd   PfxSnt Desc
22.1.1.5        4      45000         4         2        0    0    0 00:00:17     (Policy) (Policy) N/A

Total number of neighbors 1
```

BGP adjacency formed with FTD with interface IP 22.1.1.5

```
> show bgp summary
BGP router identifier 2.2.2.2, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V            AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
22.1.1.175      4            20 11      12             1    0    0 00:09:45  0
```

BGP adjacency formed with router with interface IP 22.1.1.175

Fig.17. Establishment of BGP adjacency

BGP adjacency is formed between a FTD with interface IP 22.1.1.5 and a router with interface IP 22.1.1.175. A router was configured with bgp routing process and similarly the firewall was also configured with bgp and the successful establishment of adjacency is verified.

VII. CONCLUSION

Firewalls are playing a major role in security industry from very long time and have evolved into a strongest gateway to traffic entering the protected area network. These fire walls are now integrated with very advanced technologies which can multi perform tasks. Many tasks such as functioning as encrypted traffic inspection, Intrusion Prevention Systems (IPS), antivirus, Deep Packet Inspection (DPI) and such related high technologies. With such a high advancement in firewalls, Cisco manufactures its commercial grade fire walls and this is termed as Firepower Threat Defense (FTD). This FTD was previously known as Adaptive Security Appliance (ASA), which was capable of handling many tasks. As the years have passed, upgrading in the firewall can be seen such that ASA consisted of the proprietary software Linux over ASA (LINA) and to increase the operate-ability of the firewall, in the Cisco ASA, LINA was added with new software image named Snort which provided even more robustness to the firewall and made it a winner of the market. Nowadays to increase the operate-ability and flexibility of the firewall many process are added on top of the operating system of the firewall. The Cisco firewalls are built with Firepower eXtensible Operating System (FXOS) which is essentially an administrator where ASA runs on top of this. All physical interface operations are done by this. This FTD can be configured graphically too. FTD has an adequate featured management tool where FTD is controlled through this user interface, and this is known as Firepower Management Center (FMC). LINA is the decision maker of FTD which processes the packets for firewall properties. The threat from the outside network can be avoided using various threat policies and this has been implemented, demonstrated and analyzed in this paper. The robust routing software in LINA has been designed to provide routing capabilities for firewall. Thus using these properties of LINA, it was observed that various threats from the external environment can be prevented and the network is made safe from losing vital information. Using this software routing package various routing process such as OSPF and BGP adjacency were formed and verified successfully.

VIII. ACKNOWLEDGEMENT

I am extremely thankful to Mr. Dhinesh Kumar Gollapudi, Engineer Technical Leader, Cisco Systems for constant guidance throughout the project.

REFERENCES

[1] Cisco systems Inc., ”Cisco systems Technology support, IP routing”, Document ID 7039. Cisco Systems Pvt Ltd, 2005.

[2] Cisco Systems Inc., ”Tutorial on NAT feature on ASA 5500 Series”. STG-ASA Team, 2008.

[3] Cisco systems Inc., ”How to setup a Linux environment for compiling and running LINA”. 2008.

[4] Cisco systems Inc., ”ASA Introduction”. Cisco systems, Security Business Group, 2012.

[5] Cisco systems Inc., ”IP Route Infrastructure”. Cisco Systems, Security Business group, 2013.

[6] A. Shaikh, ”Firepower Threat Defense High Availability”. Cisco systems, Technical Services Engineer-Security, 2017.

[7] Cisco systems Inc., ”Securing Networks with Cisco Firepower Next Generation Fire wall (SSNGFW) v1.0”. Cisco systems, Cisco training services, 2016

[8] Cisco systems Inc., ”PIX/ASA High Availability”. Cisco Systems, Security Business Group, 2017.

[9] Cisco systems Inc., ”Routing Module”, EDCS-626509. Cisco Systems, 2017

[10] Cisco Systems Inc., ”Security configuration guide: Unified Threat Defense”. Cisco IOS XE Release 3s, Cisco Systems, 2017.

[11] Cisco Systems Inc., ”Configure Firepower Threat Defense (FTD) Management Interface”, Document ID 212420. Cisco Security Firepower NGFW-Tech notes, 2

[12] J. Wise, ”Cisco Firepower NGIPS Tuning and Best Practices”, 2215. BRKCRT Barcelona, 2019.

[13] Cisco systems Inc., ”Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide”. Cisco Firepower Virtual-Install and Upgrades, 2020

[14] Cisco Systems, “Cisco Firepower Threat Defense Software TCP Flood Denial of Service Vulnerability”, Document ID: 1603297701286110. Cisco Systems, Security Business Group, 2020

[15] Cisco systems Inc., ”Firepower Management Center Configuration Guide, Version 6.7, OSPF for Firepower Threat Defense”. Cisco Firepower Management Center, Configure guides, 2021.