Results of BGP adjacency

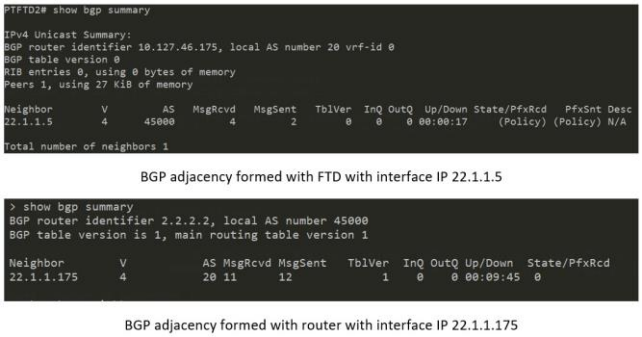

Fig.17. Establishment of BGP adjacency

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.