



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Firewall Configuration and Optimization

By

Abdullah Azhar Cassim

Supervisor: Odayne Haughton

Project submitted as part of the requirements for the
award of *BSc (Hons) Computing (Computer Networks
and Cybersecurity)*

April 2024

DECLARATION

I Abdullah Azhar Cassim declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

FORM OF CONSENT

I Abdullah Azhar Cassim hereby consent that my Project, submitted in candidature for the BSc (Hons) Computing (Computer Networks and Cybersecurity) degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

ABSTRACT

The main focus of this study is on testing the Cisco ASA 5505 firewall in a lab that was set up to simulate a real network. The main goal is to test the firewall's security features, performance, and dependability to make sure it works for small and medium-sized businesses. Setting up the firewall in a controlled lab environment, adjusting its settings, and running different tests on it, such as checking its security features in different situations, are all part of the project. The results are meant to give a full picture of the firewall's abilities and come up with the best ways to set it up and keep it running in a real-world setting.

Acknowledgements

I want to express my deepest gratitude to several people and organisations whose help was essential in completing this project. I want to start by thanking my supervisor, Odayne Haughton, for all the help, support, and advice he gave me during the research process. His advice and comments during my viva were very important in deciding the direction and steps of this project. I also want to thank all of the instructors at Trinity Saint David's School of Applied Computing for providing the resources and space I needed for my research possible. In addition, I want to thank my peers for their helpful criticism and moral support, which pushed me to overcome problems and aim for excellence. And I'm very thankful for all the help, advice, and support I got along the way.

Contents

ABSTRACT.....	3
Acknowledgements.....	4
Chapter 1. Introduction Aims and Objectives.....	8
1.1 Introduction.....	8
1.2 Aims.....	9
1.3 Objectives	10
Chapter 2. Literature Review	12
2.1 Introduction to literature review.	12
2.2 Research on Cisco ASA 5505.....	13
2.3 Study-1.....	13
2.4 Study-2.....	14
2.5 Research on Cisco ASA 5505 Cont'd.	16
Chapter 3. Research Methodology.....	18
3.1 Methods of Testing	20
3.2 Statistical Analysis Methods.....	20
3.3 Positivist research philosophy.....	21
3.4 Hypothesis.....	22
4. Design	23
4.1 Topology	23
4.2 Requirements	27
Chapter 5. Implementation.....	29
5.1 Basic configurations.....	29
5.2 Network Scan/ Vulnerability Scan.....	30
5.2.1 Nessus	31
5.2.2 Nmap.....	34
5.2.3 Scan's conclusion.....	39
5.3 Additional configurations	39
5.4 DoS Attack (BlackNurse Attack).....	42
5.4.1 The Attack.....	42
5.4.2 The results.....	43
Chapter 6. Conclusions and recommendations.....	46
6.1 Conclusion	46

6.2 Further Avenues for research?	47
Chapter 7. Reflection	48
Bibliography	49
Appendix.....	52
Basic Firewall Configuration on ASA 5505:.....	52
Router 1 Configuration:	56
Router 2 Configuration:	62
Router 3 Configuration:	68
Final ASA configuration:.....	73

Figure 1: Topology design	23
Figure 2:IP addressing	24
Figure 3: End Devices in the Topology	25
Figure 4: Network devices after wiring	26
Figure 5: Network devices before connecting	26
Figure 6: Updating firewall ASDM/ASA images using TFTP server	29
Figure 7: First Nessus host discovery scan (PC-C to firewall outside interface)	31
Figure 8:overview of the scan.....	32
Figure 9: vulnerabilities detected.....	33
Figure 10: ping test from PC-C's Kali virtual machine	34
Figure 11: vulners scan	34
Figure 12: vuln scan.....	34
Figure 13: port scan	35
Figure 14: UDP scans	36
Figure 15: port scan from inside network.....	37
Figure 16: -script vuln scan.....	38
Figure 17: DMZ configured.....	39
Figure 18: DMZ on the ASDM.....	40
Figure 19:NAT configuration	40
Figure 20: ASDM shows the ACL's configured	41
Figure 21: Inspection Policy	41
Figure 22: Hping3 command on PC-C kali from external network.....	42
Figure 23: ASDM POV after the attack.....	43
Figure 24: CPU utilization graph.....	44
Figure 25: Syslog Messages during the attack.....	44
Figure 26: Other ASDM graph stats during the attack	45
Figure 27: Hosts could access webui set up on edge router during attack	46

Chapter 1. Introduction Aims and Objectives

1.1 Introduction

What is Cybersecurity? Well, in networking it refers to the techniques, tools, standards, and regulations designed to protect networked infrastructure and devices against harm, misuse, and unauthorised access. Cybersecurity covers a broad spectrum of methods intended to safeguard data integrity, confidentiality, and availability during network transfers. Cybersecurity is now a major concern due to the growing reliance on networked devices for both personal and professional activity. Threats related to cybersecurity have become more complicated as a result of hackers continuously identifying and taking advantage of vulnerabilities in the increasingly complex systems these days. Defenders now face serious obstacles as a result, and they must work extremely hard to detect and counter these threats.

One of the key parts of cybersecurity in networking is the use of firewalls. Secure internal networks and untrusted external networks, like the internet, are separated by firewalls. They help in preventing unwanted access to or from a network by keeping an eye on and managing incoming and outgoing network traffic according to the established security policies. A study conducted by the KTH Royal Institute of Technology delves into the role of firewalls in network security, firewalls function on different layers of the network protocol stack to filter traffic. Firewall can be a hardware, software, or a combination of both. By enforcing restrictions on network traffic, firewalls safeguard computer networks against malware and attacks [1, 2, 3]

Cybersecurity research also shows how important it is to have security training, encryption, and authentication procedures. Data sent over networks is safer when it is encrypted and turned into a coded file that can only be read by someone with the right decryption key. Authentication procedures make sure that only people who are allowed to can access network resources. Security training gives people the knowledge and skills to spot and stop possible security threats. [4]

To put it simply, cybersecurity in networking is a complex field that focuses on using different technologies and methods to protect network infrastructure and data. Firewalls, encryption, authentication mechanisms, and ongoing security training are vital components that enhance a strong cybersecurity stance. Continuous research and development in cybersecurity methods and technologies is critical for protecting networked systems against increasing cyber threats. Over the years, various types of firewalls have been developed, each with specific functions and capabilities suited to different network environments and security needs,

Packet filtering firewalls: The most basic kind of firewalls, packet filtering firewalls regulate connectivity to networks by examining incoming and outgoing packets and, depending on the source and destination IP addresses, protocols, and port numbers, allowing or blocking them. These firewalls don't look at a packet's payload; they work at the network level. Their simplicity also means that, although they're quick and have low overhead, they offer very basic protection and are vulnerable to IP spoofing.

Stateful inspection firewalls: Also known as dynamic packet filtering firewalls and like packet filtering firewalls, they check the header data but also monitor the status of network connections (TCP streams). These firewalls can decide more intelligently, depending on the circumstances of the session, whether packets to allow or deny by keeping a status table updated. Because they identify patterns of authorised traffic, they provide greater security than static packet filtering.

Proxy firewalls: Operating at the application layer, proxy firewalls, sometimes known as application-level gateways, serve as a middleman between end users and the services they utilise. They stop direct links between networks inside and outside. Proxy firewalls can provide comprehensive auditing and logging as well as restrict particular programmes or services by examining the traffic's content. Nevertheless, because of the depth of inspection and processing needed, they might cause substantial network delay.

Web application firewalls: Specialized firewalls called web application firewalls guard against application-layer assaults such cross-site scripting (XSS), cross-site request forgery (CSRF), and SQL injection. High protection from web-based assaults is offered by WAFs, which can be tailored to the particular applications they safeguard and analyse HTTP requests in particular. [5]

Cloud Firewalls (FWaaS): Cloud-based firewalls, sometimes known as Firewall as a Service (FWaaS), offer network protection as a scalable and adaptable service housed in the cloud. Organisations needing remote access solutions or those with cloud-based infrastructure may find these firewalls very helpful. They are easy to expand with the requirements of the company and provide centralised management.

Next-Generation Firewalls (NGFW): A Next-Generation Firewall (NGFW) is an advanced network security system that incorporates features to go beyond the capabilities of conventional firewalls to offer stronger defence against more complex cyber threats. NGFWs are intended to solve the shortcomings of conventional firewalls, which mostly concentrate on extra functionality including application awareness, SSL/SSH inspection, deep packet inspection (DPI), and intrusion prevention systems (IPS). Modern threats including sophisticated malware and application-layer attacks are intended to be blocked by NGFWs. They offer network traffic visibility and finer security controls.

1.2 Aims

This project's main aim is to assess the capabilities of the Cisco ASA 5505 Firewall in a lab setting that mimics real-life scenarios. Assessing its security features, performance, and dependability is part of this to make sure it satisfies organisational security needs. The project seeks to create a set of best practices for the deployment and upkeep of the firewall in a production environment as well as a thorough knowledge of its efficiency in operation.

The general research question I'm attempting to address is: "How effective is the Cisco ASA 5505 firewall in terms of security features, performance, and dependability when subjected to real-life network scenarios?"

This question raises a number of important points:

Security Features: Evaluating the firewall's ability to keep threats, attacks, and unwanted access off a network. This involves assessing its capacity to manage and filter traffic for the prevention of malicious activity, as well as its capacity to manage and prevent intrusions and different security methods.

Performance: is the assessment of the firewall's effect on network performance. This involves timing, throughput, and the handling of simultaneous connections. It also involves understanding how various security policies or settings impact the network's responsiveness and speed.

Dependability: is figuring out how reliable the firewall is in multiple operational environments. This covers its ability to keep network integrity and availability without regular downtimes or interruptions, its durability against different network threats, and its stability over long periods of time.

By tackling these problems, the research project aims to provide a comprehensive evaluation of the Cisco ASA 5505's suitability for small- to medium-sized corporate environments, considering its security features as well as its impact on overall network performance and dependability.

1.3 Objectives

Setup and Configuration:

- In a controlled lab setting that replicates a small to medium-sized business network, install the Cisco ASA 5505 firewall.
- To include the firewall into the lab network, configure interfaces, hostnames, and IP addresses.
- Use NAT rules, and access control lists (ACLs) among other security policies and rules according to the requirements of the simulated environment.

Security Features Evaluation:

- To find possible firewall setup flaws, use vulnerability scans with programmes like Nessus or OpenVAS.
- Testing the intrusion prevention capabilities of the firewall, simulate attack scenarios including SQL injections, cross-site scripting (XSS), and Denial of Service (DoS) attacks.
- Test the firewall's content filtering capabilities by creating rules to prohibit particular kinds of traffic and then trying to get around them.

Evaluating Performance

- Ascertain performance and latency in both normal and stressful (high traffic load) situations.
- Examine how well the firewall handles several connections at once to determine its capacity and management of several data streams.
- To find out if the hardware resources of the firewall are sufficient for anticipated loads, examine CPU and memory utilization in various test scenarios.

Dependability Assessment

- Monitor the firewall's stability over an extended period under normal and peak loads.
- Test failover and redundancy mechanisms if applicable, to evaluate the firewall's reliability in scenarios of component failure.
- To evaluate general reliability, note and examine any downtime or performance degradation.

Documentation and Reporting

- Record every setup and testing setting and modification done.
- Record in great detail every test result, including any security flaws, performance statistics, and stressed-out system behavior.
- Write an extensive report that summarizes the results, discusses the firewall's performance, and makes suggestions for future enhancements or changes.

Review and Adjustments

- Find any places that need work by going over the test results and starting configurations.
- To guarantee best performance and security, make the necessary firewall configuration changes depending on test results and retest as needed.
- Put any modifications and final configurations into the project documentation.

Through methodically addressing these goals, my project seeks to assess the capabilities of the Cisco ASA 5505 firewall in detail and ascertain if it is appropriate for safeguarding a network environment typical of small to medium-sized businesses.

Chapter 2. Literature Review

2.1 Introduction to literature review.

Next-Generation Firewalls (NGFWs) represent a major turning point in the history of network security as the industry reacts to the changing nature of cyberthreats and the growing complexity of internet traffic. With an emphasis on their effects on the firewall market and the larger network security ecosystem, this follows the evolution of NGFWs from their invention to their present position as a mainstay of contemporary cybersecurity strategy.

Early in the 1980s, the idea of a firewall emerged as a way to manage network access. Firewalls were first only basic network-layer packet filters that looked at packet headers to decide whether to allow or prohibit traffic according to port numbers, source and destination IP addresses. But when internet use increased and the range of apps grew, these conventional firewalls proved insufficient. They were unable to enforce rules based on apps or users and to defend against application-layer assaults because they could not examine the payload of packets or comprehend the context of the traffic.

An important development came with the early 1990s advent of stateful inspection firewalls. By monitoring the status of active connections, these firewalls helped them to decide more wisely whether packets to admit or reject. Stateful inspection firewalls could not, however, identify or regulate programmes operating over standard ports or thoroughly examine the traffic's content, which became more and more crucial as web applications multiplied.

A new breed of firewalls that appeared in the middle of the 2000s and were intended to solve the shortcomings of conventional and stateful firewalls was dubbed the "Next-Generation Firewall." NGFWs could examine, identify, and control applications independent of the port or protocol utilised by combining the features of their predecessors with deep packet inspection (DPI), application awareness, and user identity information. Moving from port-based to application-based policies was a paradigm change in network security.

NGFWs brought in a number of important functions that distinguished them from previous firewall technologies:

Application Awareness and Control: NGFWs' ability to recognise and manage applications enables businesses to impose security rules at the application level.

Integrated Intrusion Prevention Systems (IPS): Have the ability to look for known weaknesses in traffic in order to identify and stop assaults.

Advanced Threat Protection: To fend off complex attacks, including zero-day threats, NGFWs provide sophisticated capabilities like sandboxing and threat intelligence integration.

User Identity Awareness: They give more precise access control by enforcing policies based on user identity rather than just IP addresses.

With the release of NGFWs, the firewall industry was greatly affected and new benchmarks for network security solutions were established. As it became clearer and clearer that traditional, stateful firewalls were insufficient to fend against contemporary attacks, NGFWs spread quickly throughout a number of industries. This change also encouraged firewall manufacturers to innovate; several of the more established firewall companies now include NGFW features in their product lines.

NGFWs brought new difficulties, such as higher resource needs and complexity, which could affect network performance, even with their benefits. Moreover, NGFWs have to be updated all the time to offer efficient defence against the ever changing cyber threats. One encouraging path for the future development of NGFWs is the combination of machine learning and artificial intelligence for automated threat identification and response. [6] [7]

2.2 Research on Cisco ASA 5505.

There have been many reviews, discussions, and studies of the Cisco ASA 5505 firewall on a variety of sites, such as technical blogs, user forums, and some academic and professional publications.

People have talked about their experiences with the Cisco ASA 5505's performance and setup on sites like the Cisco Community and Reddit. Many users have said that it works well and is reliable for small businesses. However, they have also said that it doesn't have as much speed or as many advanced security features like IPS and deep packet inspection as newer models or next-generation firewalls. Cisco's own paperwork gives a full rundown of the ASA 5505 and all of its features as a firewall that can work for small businesses and branch offices. It talks about how the firewall can provide fast firewall services, SSL and IPsec VPN, and a lot of networking options in a flexible, simple-to-control device. Cisco's own paperwork gives a full rundown of the ASA 5505 and all of its features as a firewall that can work for small businesses and branch offices. It talks about how the firewall can provide fast firewall services, SSL and IPsec VPN, and a lot of networking options in a flexible, simple-to-control device.

ResearchGate published an article comparing the Cisco ASA and Fortinet FortiGate and talking about what firewalls can do in general to protect networks. This study isn't just about the ASA 5505, but it does show how Cisco firewalls stack up against other big brands when it comes to security, pointing out the pros and cons of each, this will be talked about more below. Another study published by ResearchGate looked at how well and how efficiently different firewall technologies, such as the Cisco ASA series, worked. The study looked at a lot of different firewall technologies, but it focused on how well hardware and software firewalls work compared to each other. It also talked about the ASA series' network security features.

2.3 Study-1.

Using a Cisco Adaptive Security Appliance (ASA) 5505 as a testing firewall, the research paper written by Luleå University of Technology students in Sweden offered thorough insights into the planning and execution of an online pedagogical Information Security (InfoSec) laboratory. The Cisco ASA 5505 was used in a pilot test for the online InfoSec lab's "Firewall Configuration and

Testing" feature. The firewall's main job was to keep students in a safe space where they could do hands-on activities related to server security design. In particular, it was meant to protect against Denial of Service (DoS) attacks. Setting up and testing network traffic rules on the ASA 5505 is important for learning about and using security measures in a real-life network setting.

The study showed a few important results from using the Cisco ASA 5505:

Hands-on Learning: The firewall made it possible to use what they had learned in the classroom in real life, which is very important for information security students. By setting up and trying the firewall, students could see right away how different security settings affected the system.

Technical Skill Development: The exercise helped in enhancing the technical skills of the students, particularly in configuring and managing firewalls to defend against network attack

Understanding of Real-World Applications: Using a real firewall like the Cisco ASA 5505 helped students understand the difficulties and complexities of managing safety in the real world.

The use of Cisco ASA 5505 in this study is in line with what other studies have found about how important it is for cybersecurity education to include real-world practice. As an example, research has shown that using real network security devices like firewalls in simulation-based learning makes students much smarter and better at protecting networks. Additionally, the study backs up the idea that good cybersecurity education should include both theoretical information and practical skills that can be used right away in the workplace. Several studies have used this method, where live firewalls and other network security tools are an important part of the learning process and help bridge the gap between theory and practice. [8]

2.4 Study-2.

Two top Next Generation Firewalls (NGFWs)—Cisco's Adaptive Security Appliance (ASA) and Fortinet's FortiGate—are thoroughly compared in the research paper "Comparison between Cisco ASA and Fortinet FortiGate" that was published in the Journal of Electrical and Computer Engineering in May 2019. The research concentrates on several aspects including the performance, throughput, security features, setup, and management capabilities of rival firewall solutions. [9]

Key Findings

Performance & Throughput: As compared to Cisco ASA's maximum of 320Gbps, Fortinet FortiGate has a wider throughput range of 17Gbps to 1Tbps, according to the study. This implies that FortiGate might be better able to manage bigger traffic volumes.

Security Features: Both firewalls have strong security features, such as web blocking, advanced threat protection, and intrusion prevention. But FortiGate is known for being very good at handling encrypted data, which is becoming more and more important as the number of encrypted apps and services grows.

Configuration & Management: Fortinet FortiGate has a management console that is easier for people to use, making it easier for them to explore and set up than Cisco ASA's interface, which is said to be less intuitive.

Integration and Modularity: Cisco ASA gives better security features and modularity when combined with other Cisco services, such as Firepower. This is helpful for environments with a lot of moving parts. FortiGate works well on its own, but it also works well with the rest of the Fortinet environment, which is called Fortinet Security Fabric.

Cost-Effectiveness: Fortinet FortiGate is praised for being cheaper than Cisco ASA, offering less expensive features that are just as good or better.

How does it fit in with other field studies?

The results of this study agree with those of other studies that have been done on checking firewalls and network security. As an example, other sources also stress how important it is to be able to handle high throughput and encrypted information when judging the performance of a firewall. Additional critiques and comparisons also highlight how important it is to have easy-to-use configuration tools and low costs.

Throughput and Performance: Other research and user reviews on platforms like G2 and Spiceworks show that FortiGate usually has higher throughput and better encryption handling than Cisco ASA. [10] [11]

Security and Integration: When testing firewalls, research on thematic analysis and document analysis shows that being able to integrate with larger security environments and keep security features up to date are very important. In these areas, both Cisco and Fortinet do well, but they do so in different ways. [12] [13]

User Interface and Management: Many people have said that the Cisco ASA's user interface is hard to use, which is in line with what this study found. People often say that FortiGate's user interface is simple and easy to use, which helps cut down on setup mistakes and improve security management. [14]

Costs: A common theme in many studies and user reviews is that FortiGate is cheaper than Cisco ASA. This makes it a great choice for businesses that need to stick to a tight budget. [11]

A summary of the study, Cisco ASA and Fortinet FortiGate are side by side compared in every way, showing their pros and cons. The results are in line with larger trends in firewall testing, which stress speed, security, ease of use, and cost-effectiveness as important things to consider when choosing a firewall solution. This study adds important information to the ongoing process of improving and developing firewall technologies in the area of cybersecurity.

2.5 Research on Cisco ASA 5505 Cont'd.

Significant research has been conducted on the Cisco ASA 5505 firewall, particularly focusing on its capabilities to handle and mitigate DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks.

One of the studies from the University of Windsor looked at how well the Cisco ASA 5505 stopped DDoS attacks. For the study, they set up a testbed with two Windows 10 PCs, one to act as the attacker and the other as the target. VirtualBox was used on the attacker's computer to run the attack in a virtual world. The study's goal was to find out how well the ASA 5505 can handle both DoS and DDoS attacks and what its penetration level is. The results showed that the ASA 5505 could handle some kinds of attacks, but it wasn't very good at stopping more complex or high-volume DDoS attacks. This is in line with what people have said about its general flaws on Reddit and Cisco Community. [15]

People on Reddit talked about how the Cisco ASA 5505 isn't perfect at stopping DDoS attacks. The general opinion was that the ASA 5505 can protect against smaller attacks with tools like SYN cookies and rate limiting, but it has trouble with DDoS attacks that are too big for it to handle. This is especially true for attacks that use up all available bandwidth, where the sheer amount of information can overwhelm the firewall. [16]

Similarly, People in the Cisco Community talked about how well the ASA 5505 worked during DDoS attacks. It was noticed that the ASA 5505 does not have built-in DDoS protection mechanisms. For full protection against all types of DDoS attacks, it might be necessary to use additional solutions from Arbour or Radware. In this case, the ASA 5505 shows that it can't handle complex DDoS attacks with a lot of data or attacks at the application layer. There is information in Cisco's own documents about how the ASA 5505 can find threats. The document talks about different threat detection features that can be turned on for the ASA. These include basic and advanced threat detection settings that help find and stop possible attacks. However, these features aren't always useful, and when there are a lot of threats, they can really slow down the firewall. [17]

There is no clear information in the available literatures about which key researchers have tried the Cisco ASA 5505 model. But many articles do talk about different parts of testing and study that have to do with the Cisco ASA 5505 firewall:

Cisco Documentation and Guides:

The ASA 5505 can be set up and tested with the help of Cisco's own technical materials and guides. These papers are usually made by Cisco's own group of network security experts and engineers. These papers are the result of teamwork within Cisco, even if the names of the authors aren't always given.

Community Discussions and User Feedback:

Discussions on sites like Reddit are where IT experts and network managers share their thoughts and experiences with Cisco ASA firewalls, such as the ASA 5505 model. These contributors

aren't exactly researchers in the traditional academic sense, but their real-world tests of the firewall's performance and dependability are still very useful. Blog posts and security studies by organisations such as NCC Group and Rapid7 look closely at and fix problems with the Cisco ASA firmware, including finding possible security holes and slowdowns. Even though these sites don't talk about the ASA 5505 by name, the researchers who worked on them, like Aaron Adams, Cedric Halbronn, and the team at Exodus Intelligence, do a lot to help us understand and improve the security features of Cisco ASA devices. [18] [19]

Academic and Professional Publications:

A study published on ResearchGate says that a Cisco ASA 5505 was used for testing and setting up firewalls. David Hucaby is the researcher being talked about here. He is famous for his work on Cisco products. Hucaby has written a number of books and papers about Cisco networking equipment. These often include performance reviews and tips on how to set up the equipment. [20]

Chapter 3. Research Methodology

A structured study methodology will be used to make sure the results are valid, can be repeated, and can be applied to real-life situations. Here is a full plan how I will organise this research:

Defining Objectives: To begin, state the testing's goals clearly. Evaluations of the firewall's performance under various traffic loads, reliability over time, and capacity to prevent illegal access could be among the objectives.

Literature review: Reading existing research on firewall testing methods, previous tests on the Cisco ASA 5505, and any related case studies should be done in detail. In order to understand what the firewall can do and what problems or weaknesses it usually has, this information is required, something that was done in the last chapter

Develop some hypothesis: Come up with hypotheses about how the Cisco ASA 5505 will work in different situations based on the literature study. Examples of hypotheses could be about the firewall's throughput when it's under a lot of stress or how well it stops certain types of cyberattacks, as stated in the project plan.

Design and Implementation: Make sure that the lab setting is very similar to the network where the firewall would normally be used in the real world. This includes the right computers, network devices, Arranging the network so that it has different segments depicting different organisational units, each with a different amount of security.

Testing Scenarios: (Performance Testing) Check the memory, CPU, and speed usage both when things are normal and when there is a lot of traffic. (Security Testing) Check how the router handles different types of attacks, such as Distributed Denial of Service (DDoS) attacks, SQL injection, and cross-site scripting. For vulnerability testing, using tools like Metasploit, Nmap and Wireshark to capture and analyse packets. (Usability Testing) Access Cisco's Adaptive Security Device Manager(ASDM) to evaluate the ease of configuration and management of the firewall.

Data Collection: Generate traffic with automated tools like HPING3, then log security and performance information. I will record and examine packets with programmes like Wireshark. Conducting the Experiment: Carry out the tests as per the prepared scenarios. For consistency, making sure to record every setup and modification done during the testing.

Analysing the data: Check the theories by analysing the gathered data. Check if the performance as it is and whether it matches the anticipated results using statistical techniques.

Reporting Results: Lastly when the firewall testing is reported, the results are put together in a way that describes the approach that was used, shows the data that was received, and talks about the results. There would be clear pictures in the assessment, like graphs and tables, that show how the firewall worked in different test situations. It would also explain what the findings meant and say if the firewall met the performance and security standards set out in the hypotheses. Furthermore, the report would include suggestions for improving firewall settings or new areas for study based on any strange or unexpected results seen during the tests.

There are several advantages to using a structured research methodology for testing

Systematic Approach: This method presents a structured way of testing, which helps to cover all important aspects of firewall security and performance. by using this technique I can make sure I don't miss any important points by following a structured method.

Reproducibility: The tests are easier to repeat because the conditions, configurations, and methods were carefully written down. This is very important for making sure the results are correct and for letting me repeat the study to confirm the results or do more research.

Controlled environment: Testing in a lab setting lets me change variables and separate out factors that could influence how well the firewall works. This control me get a good idea of what the firewall can and can't do without any outside meddling.

Objective Evaluation: An objective evaluation of the firewall is possible with the help of hypotheses and situations that have already been thought out. This method keeps biases to a minimum, which could happen if the testing wasn't organised.

Quantifiable data: The method emphasises gathering data that can be measured, which makes exact and statistical analysis easier. This method is based on data, which helps us come to stronger conclusions and make smarter choices about how to use the firewall in real life.

Basis for Improvement: This study's results can give us useful information that can help make the configuration and control of the firewall better. Improvements that improve efficiency and security can be made based on the data analysis's suggestions.

The goals of the study should be in line with the evaluation criteria. Some common factors for testing firewalls are:

Performance Metrics: Throughput, latency, CPU and memory usage under various traffic loads

Security Effectiveness: How well it stops known dangers, how well it stops new or "zero-day" attacks, and how well it can handle different kinds of attacks (like DDoS and intrusion attempts).

Reliability and Stability: Uptime, the ability to fail over, and how the system reacts to changes in setup or unstable networks.

Usability and Manageability: How easy it is to set up, how easy it is to use the management interface, and how good the logging and reporting tools are.

3.1 Methods of Testing

Performance testing:

Traffic Simulation: To make both normal and high-stress traffic situations, use tools like Hping3 and Wireshark.

Benchmarking: Set industry standards or look at older models to compare the performance measures (such as throughput and latency).

Security Testing:

Penetration Testing: Use tools like Metasploit to make fake attacks and check how well the firewall can find and stop them.

Vulnerability Scanning: To find holes in the firewall setup, use tools like Nessus.

Reliability and Stability Testing:

Log Analysis: Look through the logs for any security events or strange behaviour.

Stress Testing: Run the firewall continuously under heavy load and keep an eye out for errors or performance issues.

3.2 Statistical Analysis Methods

Descriptive Statistics: Measures like mean, median, standard deviation, and variance can be used to sum up performance data.

Reliability Analysis: Determine the coefficients of reliability to evaluate the firewall's stability over time under different settings.

Data Visualization: Use graphs and charts to better understand complicated data sets by graphically illustrating patterns and comparisons.

By using these evaluation criteria, testing methods, and statistical analysis approaches, the research will provide thorough insights into the performance, security, and usability of the Cisco ASA 5505 firewall. The evaluation is ensured to be comprehensive, objective, and to yield useful conclusions by this methodical approach.

3.3 Positivist research philosophy

There are several good reasons to adopt a Positivist study philosophy:

Objective and Quantifiable Data: Positivism emphasises the need to gather and study objective, measurable data. This fits well with the project's need to find out how well the firewall works, how secure it is, and how reliable it is by looking at real-world data like throughput rates, latency, and the number of tries to get in that were successfully blocked.

Replicability and Generalizability: Positivism promotes a structured and standardised method that makes it possible to repeat the study under similar conditions. This makes sure that the results are reliable. This is very important for making sure that the firewall works well and has good security in different situations, and the results can be used in similar network settings.

Testing Hypotheses: Positivism encourages coming up with hypotheses based on theories or facts that already exist. These hypotheses are then put to the test by doing rigorous experiments. Hypotheses about the firewall's abilities can be made and tried in a controlled setting as part of this project. This gives us a methodical way to figure out how well it works.

Use of Technology and Instruments: Positivism doesn't get in the way of using technological tools and instruments to gather and analyse data, which is important for a project that needs to do a technical review of a firewall. You can use tools like traffic generators, penetration testing software, and performance tracking apps to get real-world information about how well and safely the firewall works.

Focus on Cause and effect: The positivist method tries to find links between causes and effects, which is useful for figuring out how various configurations or security threats affect the firewall's safety and performance. The project can find specific factors that affect how well the firewall works by separating variables and running controlled tests.

Makes Comparison and Benchmarking Easier: The positivist method produces quantitative data that makes it easier to compare with industry benchmarks or older models of firewalls. This information can help you figure out how the Cisco ASA 5505 stacks up against other products on the market and find ways to make it better.

In conclusion, a positivist research theory is a good fit for this project because it prioritises objective data collection, hypothesis testing, and the use of technology. These are all important for getting a full picture of how effectively and securely the Cisco ASA 5505 firewall works

3.4 Hypothesis

For this project, which will test a Cisco ASA 5505 firewall, the experimental hypotheses will be based on three key areas.

Performance: In the first hypothesis, we will look at how well the firewall works generally, including its throughput and latency when it is working normally. To do this, we will need to test the firewall's highest throughput without losing many packets and its latency when different types of traffic are going through it.

Performance During a Denial of Service (DoS) Attack: The second theory will test how well the firewall works during a Denial of Service (DoS) attack. This will test the firewall's specific ability to keep working and handle data well during different types of DoS attacks, like SYN or UDP floods.

How Well Different ACLs and policies work: The third hypothesis will look at how well various Access Control Lists (ACLs) and firewall rules handle and protect network traffic. This is done by setting up the firewall with different security policies and rules to see how well it can stop people who aren't supposed to be there from getting in while still letting valid traffic through based on the rules that were set.

These theories are meant to thoroughly test the Cisco ASA 5505's abilities to handle normal traffic as well as attack situations, as well as its adaptability in enforcing complicated security rules and laws. The results will show how well the firewall works in different operating settings and how reliable it is at keeping network resources safe.

Chapter 4. Design

4.1 Topology

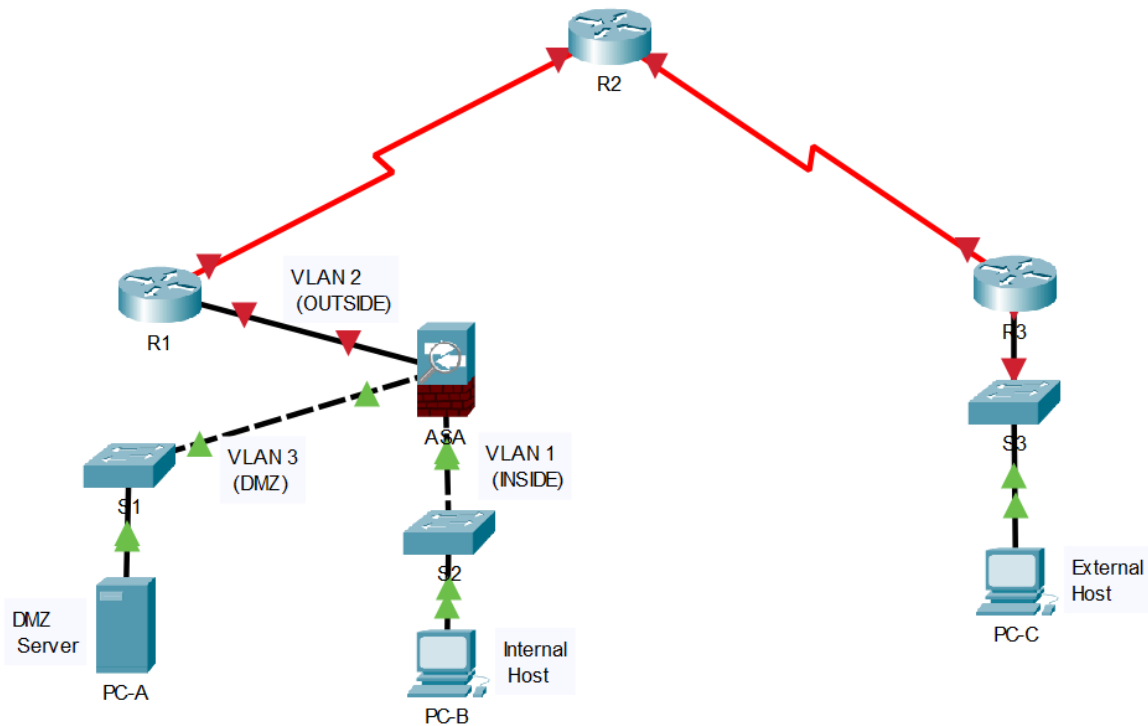


Figure 1: Topology design

This network topology is perfect for a small business because it has a Cisco ASA 5505 to handle and protect network traffic well. A Demilitarised Zone (DMZ) is an important part of this configuration for keeping the internal network safe from threats from the outside while having services that people can access, like web servers. Using Static NAT (Network Address Translation) makes it easier for these services to connect to the internet using controlled IP addresses, which makes security better. Access Control Lists (ACLs) are also used to finely control the data coming into and going out of the network, making sure that only people who are allowed to can get in. This setup not only keeps private company information safe, but it also offers strong, expandable network management tools that can change as the business does. This makes it the best choice for small companies that want to keep their network safe and running smoothly.

IP Addressing Table for the proposed Topology:

Device	Interface	Ip	Subnet	Default gateway	Loopback Address
Router 1	G0/0/0	209.165.200.225	255.255.255.248	n/a	n/a
	S0/1/0	10.1.1.1	255.255.255.252	n/a	
Router 2	S0/1/0	10.1.1.2	255.255.255.252	n/a	172.30.1.1 255.255.255.0
	S0/1/1	10.2.2.2	255.255.255.252	n/a	
Router 3	G0/0/1	172.16.3.1	255.255.255.0	n/a	n/a
	S0/1/1	10.2.2.1	255.255.255.252	n/a	
ASA 5505	Vlan 1 (e0/1)	192.168.1.1	255.255.255.0	n/a	n/a
	Vlan 2 (e0/2)	209.165.200.226	255.255.255.248	n/a	
	Vlan3(e0/3)	192.168.2.1	255.255.255.0	n/a	
PC-A	Eth0	192.168.2.3	255.255.255.0	192.168.2.1	n/a
PC-B	Eth0	192.168.1.3	255.255.255.0	192.168.1.1	n/a
	VM-Windows7	192.168.1.4	255.255.255.0	192.168.1.1	
	VM-Kali	192.168.1.5	255.255.255.0	192.168.1.1	
PC-C	Eth0	172.16.3.3	255.255.255.0	172.16.3.1	n/a
	VM-Kali	172.16.3.4	255.255.255.0	172.16.3.1	

Figure 2:IP addressing

Note: Switches had basic default configurations.

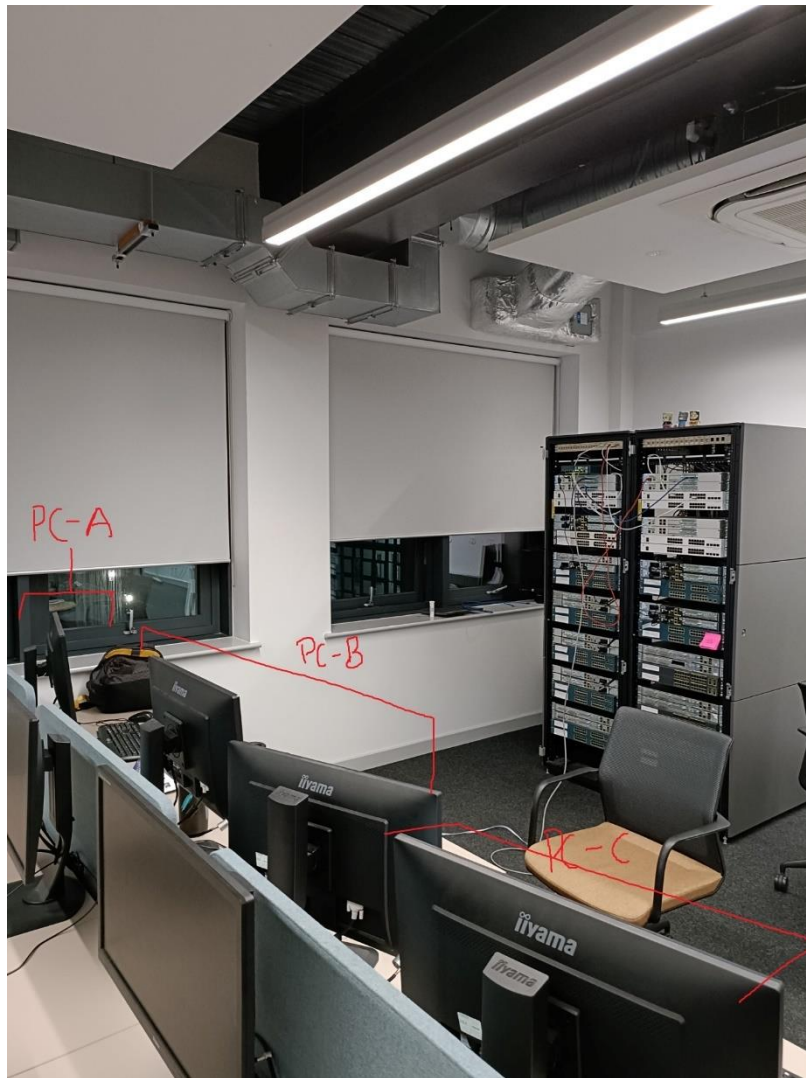


Figure 3: End Devices in the Topology

Note: PC-B has two virtual machines running (Windows 7/ kali linux), and PC-C has just one (Kali linux) running.

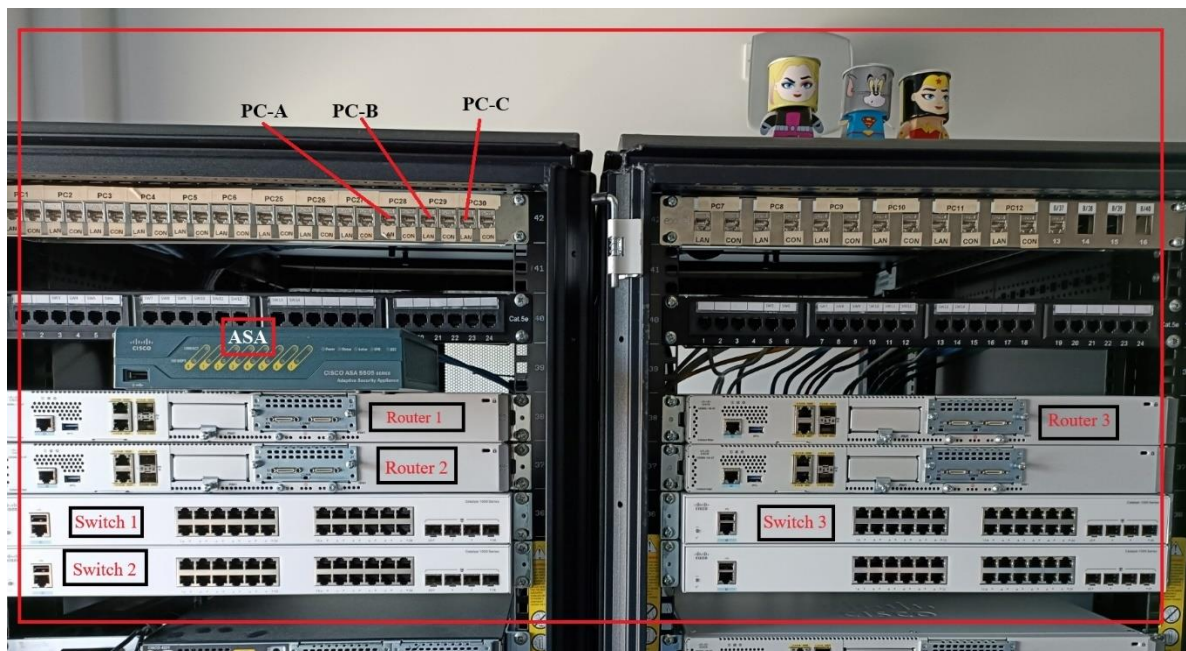


Figure 5: Network devices before connecting

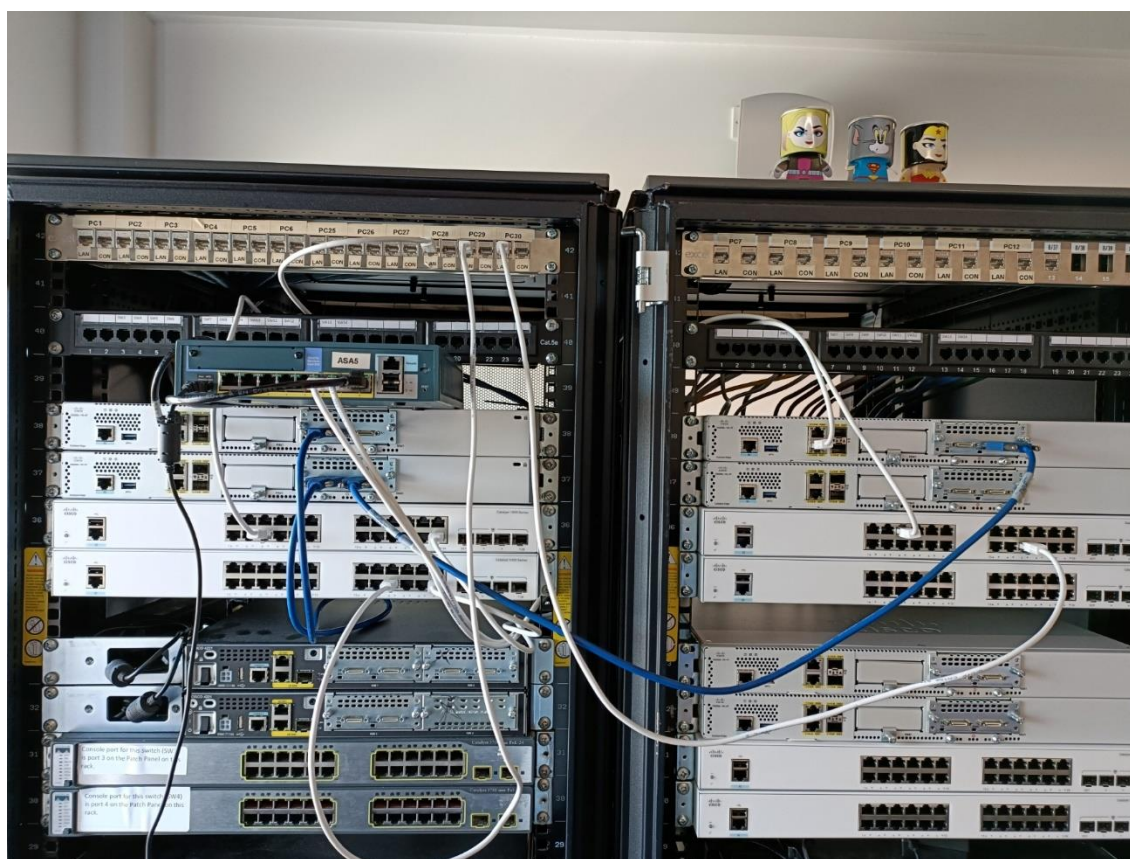


Figure 4: Network devices after wiring

The topology is designed to make basic device settings, security levels, routing, NAT, DHCP, AAA, and access control policies among other configurations and tests easier. It enables modelling of actual network situations in which the ASA firewall controls and filters traffic between several network zones, therefore acting as an essential part of network security.

Network Segmentation

Inside Network: This section is linked to the ASA's inside interface and has internal devices that need safe access to resources outside the company.

Outside Network: The ASA interface that links to R1, signifying the connectivity to the outside internet.

DMZ, or "Demilitarised Zone," is a separate network segment that is connected to an ASA's dedicated DMZ interface. It is used to host public services that need to be available from the internet but not from the internal network.

4.2 Requirements

HARDWARE:

Routers (R1, R2, R3):

These routers simulate the internet and internal networks. R1 acts as the Customer Premises Equipment (CPE) managed by the ISP, connecting the internal network to the internet. R2 represents an intermediate internet router, and R3 simulates another ISP that connects a remote administrator for network management.

Cisco ASA 5505:

The ASA serves as the edge security device, positioned between the internal network and the ISP. It is responsible for firewall functionalities, NAT, and DHCP services, providing a security barrier against external threats while managing internal traffic.

Switches (S1, S2, S3):

These switches are used to connect the internal devices, including PCs and the ASA, facilitating internal communications and connectivity to the ASA for protected internet access.

PCs (PC-A, PC-B, PC-C):

These PCs represent end-user devices within the network, used to test connectivity, access control policies, and the overall impact of ASA configurations on client access.

SOFTWARE AND TOOLS

Cisco Adaptive Security Device Manager (ASDM): GUI-based control and setting up of the ASA firewall. This tool is very important for making it easier to handle advanced settings like firewall policies, NAT rules, and more.

Terminal emulator software, like PuTTY, lets you access the ASA and other network devices' command line interface's to set them up and control them.

Virtual Machines: a kali Linux machine to run tools like Nmap and Hping3 so we can experiment with the behaviour of the firewall under different traffic simulations both in and outside the network.

Traffic simulation tools: Tools like Hping3 and Wireshark to manipulate packets and analyse them

Chapter 5. Implementation

5.1 Basic configurations

Along with connecting the devices, the first step of the project is to set up the topology and other network devices, such as switches and routers. The main job here is to set up the basic running configuration for each of these devices and save them on the start-up config. This is an essential step as it makes sure that any original settings are saved and can be used again later. As part of the configurations, hostnames, interface settings, and other basic network commands that are needed for the network to work are set. Before setting up the ASA device, this step lays the groundwork for the network.

The next step was to connect to the ASA and use the CLI Setup mode to set up the ASA 5505's basic settings. At first, the console port is used to connect to the ASA and a terminal emulation program was used on the computer, PuTTY was used in this scenario. To see the hardware, software, and current configuration settings, different "show" commands were used. Finding out the ASA version, connections, and licence information is part of this. I saw that the firewall needed to be updated because it was using old software. To do this, I set up a TFTP server on PC-B (the admin PC) and then used the firewall's command line to update the Adaptive Security Device Manager(ASDM) and the ASA boot up image

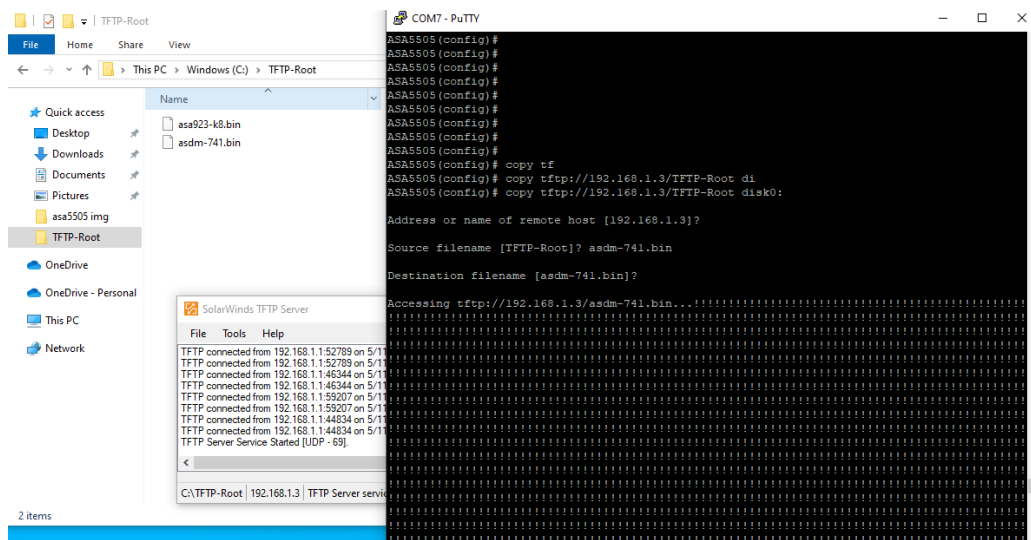


Figure 6: Updating firewall ASDM/ASA images using TFTP server

with a focus on improving the basic settings and using the CLI to set the amount of interface security. As part of this, I set up configurations like the hostname and domain name and make the device even safer by creating login and allow passwords. The time and date are set, and the appropriate security levels are applied to both the inside and outside interfaces, outside interfaces were given a security level of 0 which means its not safe and blocks almost all packets from passing unless a policy or ACL deems it to, inside interfaces were given a value of 100

indicating its a trusted port, therefore users from inside can ping outside but not the other way around . To make sure the ASA works and can talk to other devices as planned, connectivity tests are run.

The ASA also has SSH and HTTPS access set up to allow secure management of the device remotely. This is an important part because it not only makes sure that the ASA is working with the default settings, but it also secures the interfaces to protect against unauthorized access. For now the only places where SSH and HTTPS were set up were on the inside interfaces. Later tests and scans will show why this is important.

The firewall's configurations will be attached on the Appendices.

5.2 Network Scan/ Vulnerability Scan

Now all of the network devices in the topology are set up in their basic configurations. We can now move on to the tests. First, a network scan was carried out. Two main tools were used to scan. Both Nessus and Nmap were used.

Nmap: The word "Nmap" stands for "Network Mapper." It is a free and open-source tool for scanning networks and checking their security. To find hosts and services on a computer network, it sends packets to specific hosts and looks at the replies. In this case, finding the firewalls, open ports, operating system, and software versions on device. This helps with managing networks and evaluating security. [21]

Nessus: Tenable, Inc. created Nessus, a tool for full vulnerability scanning. It is made to find security holes in devices, apps, operating systems, and cloud services, among other IT assets. Nessus looks for problems like bugs in software, missing patches, malware, and incorrect settings. This helps us and businesses find and fix weak spots before hackers can take advantage of them. [22]

5.2.1 Nessus

5.2.1.1 Outside Network Scan

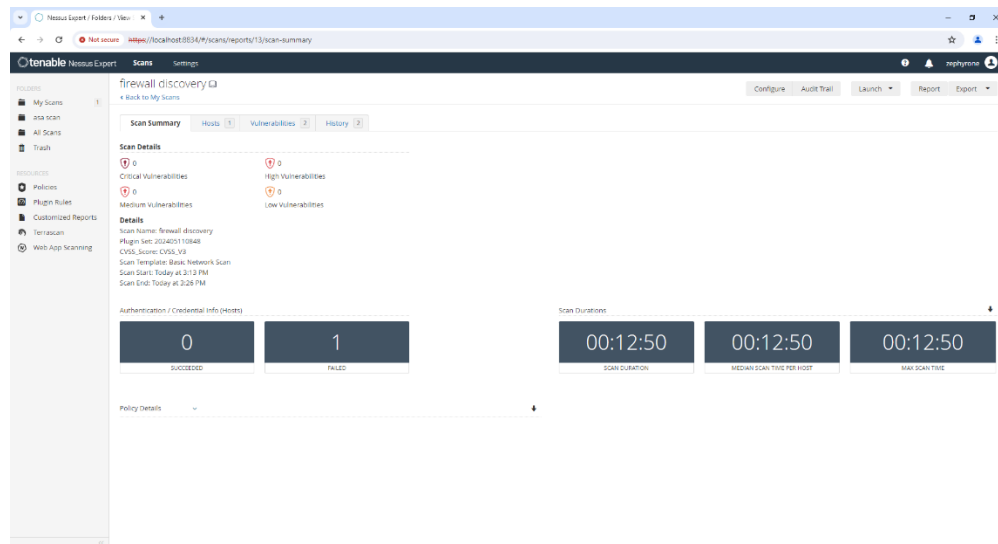


Figure 7: First Nessus host discovery scan (PC-C to firewall outside interface)

The image above shows a Nessus vulnerability scan report which was conducted on the Cisco ASA 5505 firewall. The scan was initiated from an external network to assess the security posture of the firewall's outside interface. The scan summary indicates that there are no critical, high, or medium vulnerabilities found. The risk level is typically determined by the severity of the vulnerabilities found during the scan. Since the scan summary shows zero critical, high, and medium vulnerabilities, we can infer that the risk level for this particular scan is low.

The absence of critical, high, or medium vulnerabilities in the report suggests that the firewall may be effectively protecting the network from certain threats. However, the report indicates that the scan was able to proceed and gather information about the firewall, which means that the scan was not entirely blocked.

5.2.1.2 Inside Network Scan

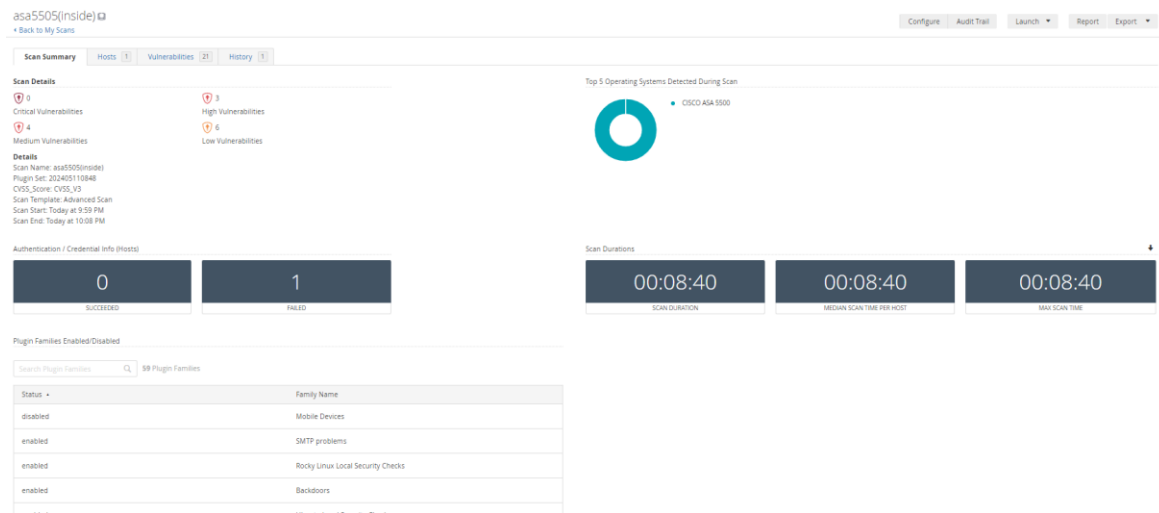


Figure 8:overview of the scan

The scan has identified various levels of vulnerabilities: no critical vulnerabilities, 4 medium vulnerabilities, 6 low vulnerabilities, and a total of 21 vulnerabilities detected.

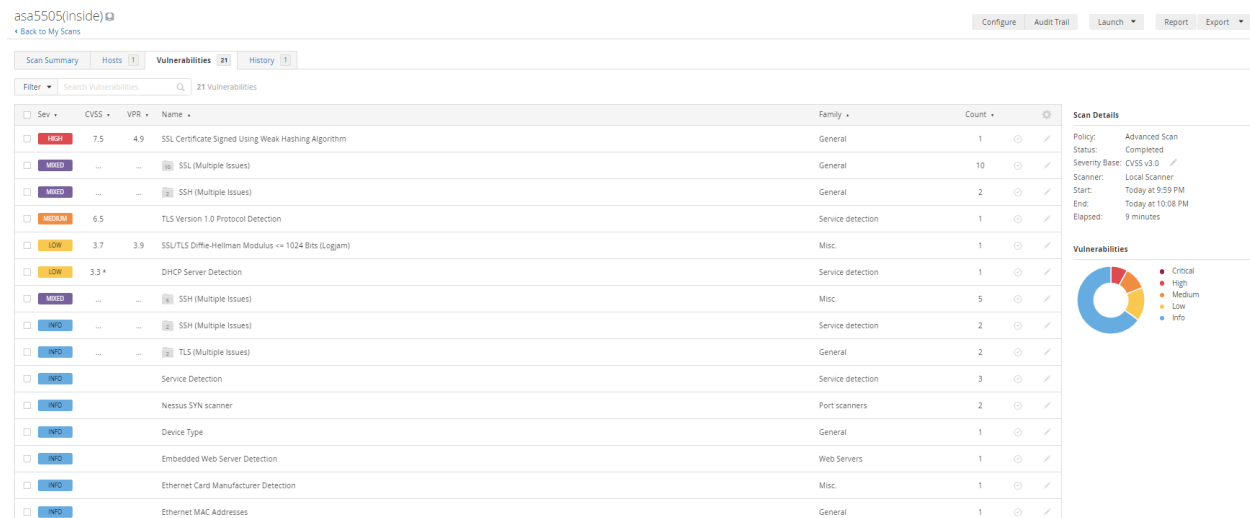


Figure 9: vulnerabilities detected

The vulnerabilities tab of the Nessus scan report shows that the ASA 5505 firewall has a number of security problems that need to be fixed. One high severity vulnerability, four medium severity vulnerabilities, and six low severity flaws have been found.

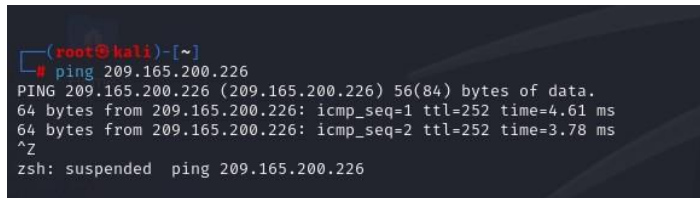
The high-severity vulnerability is related to an SSL certificate with a weak hashing method, which could lead to spoofing attacks or the theft of private information. Some problems with medium severity are weaknesses in the SSL/TLS protocols and possible faults in the Diffie-Hellman key exchange system that could be used to read encrypted messages.

Most of the low-severity vulnerabilities have to do with service detection, like finding a DHCP server, and other problems that might not be a direct threat but still need to be fixed to make the firewall safer generally.

5.2.2 Nmap

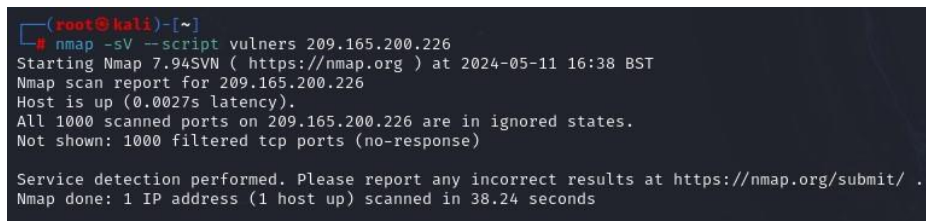
5.2.2.1 Outside Network Scans

The images provided below show a set of commands run from the Kali Linux terminal from PC-C's Virtual machine from the external network of the topology to locate and check for vulnerabilities on the asa 5505's outside interface that uses the IP address 209.165.200.226.



```
(root@kali)-[~]
# ping 209.165.200.226
PING 209.165.200.226 (209.165.200.226) 56(84) bytes of data.
64 bytes from 209.165.200.226: icmp_seq=1 ttl=252 time=4.61 ms
64 bytes from 209.165.200.226: icmp_seq=2 ttl=252 time=3.78 ms
^Z
zsh: suspended ping 209.165.200.226
```

Figure 10: ping test from PC-C's Kali virtual machine

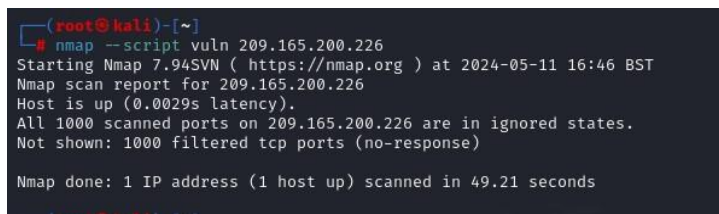


```
(root@kali)-[~]
# nmap -sV --script vulners 209.165.200.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 16:38 BST
Nmap scan report for 209.165.200.226
Host is up (0.0027s latency).
All 1000 scanned ports on 209.165.200.226 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.24 seconds
```

Figure 11: vulners scan

"nmap -sV --script vulners 209.165.200.226" was the first Nmap command I used. The -sV flag is used for service version detection, which attempts to determine the version of the services running on open ports. When the command is run with the "--script vulners" option, a script from the Nmap Scripting Engine (NSE) is run to check the services found for known vulnerabilities. The script looks at the Vulners database, which has a huge list of known vulnerabilities. But the results show that all 1000 scanned TCP ports are in an ignored state. This means that no open ports were found, so no information about service versions or security vulnerabilities could be found.



```
(root@kali)-[~]
# nmap --script vuln 209.165.200.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 16:46 BST
Nmap scan report for 209.165.200.226
Host is up (0.0029s latency).
All 1000 scanned ports on 209.165.200.226 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 49.21 seconds
```

Figure 12: vuln scan

I then used "nmap --script vuln 209.165.200.226" as my second Nmap command. This command uses the "--script vuln" option to run a set of NSE scripts that are specifically designed to detect

known vulnerabilities. As with the previous scan, the results indicate that all 1000 scanned ports are in an ignored state, suggesting that no vulnerabilities were found during this scan.

```
(root@kali)~# nmap -p- -A 209.165.200.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 16:51 BST
Nmap scan report for 209.165.200.226
Host is up (0.012s latency).
All 65535 scanned ports on 209.165.200.226 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
Network Distance: 4 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 0.49 ms 172.16.3.1
2 3.09 ms 10.2.2.2
3 9.53 ms 10.1.1.1
4 28.92 ms 209.165.200.226

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1364.81 seconds
```

Figure 13: port scan

By running "nmap -p- -A 209.165.200.226" on Nmap. The -p option tells Nmap to look at all 65535 TCP ports, and the -A option lets it find the operating system, find the version, look at scripts, and traceroute.

As shown by the "Host is up", the output shows that the host is up. The scan does not give specific information about the operating system, though, because "Too many fingerprints match this host to give specific OS details." In this case, it seems like the firewall might be hiding the OS fingerprint in some way, or the scan results aren't clear enough to correctly identify the OS. It also shows that all 65535 TCP ports that were scanned are in "ignored states," which means that none of them sent an answer. This usually means that the firewall is stopping the probes, which keeps Nmap from finding out whether the ports are open, closed, or filtered.

The output also has a traceroute to the target IP address that shows the route packets take to get to the host. The traceroute shows four hops, each with its own IP address and round-trip time (RTT).

```
(root@kali)-[~]
# nmap -sU -p50-59 209.165.200.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 17:28 BST
Nmap scan report for 209.165.200.226
Host is up (0.0027s latency).

PORT      STATE      SERVICE
50/udp    open|filtered re-mail-ck
51/udp    open|filtered la-maint
52/udp    open|filtered xns-time
53/udp    open|filtered domain
54/udp    open|filtered xns-ch
55/udp    open|filtered isi-gl
56/udp    open|filtered xns-auth
57/udp    open|filtered priv-term
58/udp    open|filtered xns-mail
59/udp    open|filtered priv-file

Nmap done: 1 IP address (1 host up) scanned in 17.98 seconds

(root@kali)-[~]
# nmap -sV -sU -p50-59 209.165.200.226
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 17:30 BST
Nmap scan report for 209.165.200.226
Host is up (0.0027s latency).

PORT      STATE      SERVICE      VERSION
50/udp    open|filtered re-mail-ck
51/udp    open|filtered la-maint
52/udp    open|filtered xns-time
53/udp    open|filtered domain
54/udp    open|filtered xns-ch
55/udp    open|filtered isi-gl
56/udp    open|filtered xns-auth
57/udp    open|filtered priv-term
58/udp    open|filtered xns-mail
59/udp    open|filtered priv-file

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.82 seconds
```

Figure 14: UDP scans

The picture shows the outcomes of UDP scans done on the firewall's external port. The scans show that a number of UDP ports are in a "open|filtered" state. This means that these ports did not respond, so it is not clear whether they are open or blocked by a firewall. As you can see, the ports on the list are for services like xns-time, domain, xns-ch, isi-gl, xns-auth, priv-term, xns-mail, and priv-file. The "open|filtered" state means that the ASA 5505 firewall is set to not react to the kinds of probes sent by the Nmap scan. This is a common security measure to keep hackers from finding out about the network.

In conclusion, the scans done from the outside network indicate that the ASA 5505 firewall is operational and responding to pings; nevertheless, the ignored status of all scanned ports indicates that the Nmap vulnerability scans did not find any open ports or recognised vulnerabilities. The absence of details regarding the port states in the Nmap scan reports suggests that the firewall is doing a good job by ignoring the scans.

5.2.2.2 Inside Network Scans

```
(root@kali)~[~]
# nmap -p- -A 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 17:16 BST
Nmap scan report for 192.168.1.1
Host is up (0.00057s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Cisco SSH 1.25 (protocol 1.99)
|_sshv1: Server supports SSHv1
|_ssh-hostkey:
|_ 2048 aa:9e:f0:a4:3c:52:38:64:ce:e5:bb:ec:28:7c:da:ba (RSA1)
|_ 2048 13:9f:dc:43:ca:49:db:b0:51:ad:62:9c:1a:20:16:66 (RSA)
443/tcp   open  ssl/http Cisco ASA 5510 firewall http config
|_http-title: Cisco ASDM 7.4(1)
|_Requested resource was /admin/public/index.html
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=ASA Temporary Self Signed Certificate
|_Not valid before: 2024-05-11T12:25:25
|_Not valid after: 2034-05-09T12:25:25
MAC Address: 3C:08:F6:AB:14:66 (Cisco Systems)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: firewall
Running (JUST GUESSING): Cisco ASA 8.X (96%), Juniper embedded (87%)
OS CPE: cpe:/a:cisco:adaptive_security_appliance_software:8.4 cpe:/h:juniper:
```

Figure 15: port scan from inside network

In the above image, the "-p" option tells nmap to look at all 65535 TCP ports, and the "-A" option lets it look for OSs, versions, scripts, and traceroutes. It looks like two ports are open:

Port 22/tcp is open for SSH (Secure Shell)

Port 443/tcp is open for SSL/HTTPS which is used for secure web-based management of the firewall via the Cisco ASDM (Adaptive Security Device Manager).

The scan does not reveal any specific security configurations or vulnerabilities, but it does tell us useful things about the firewall's services and how it's set up in general. The open ports show that the firewall is set up for remote management, which should be secured appropriately to prevent unauthorized access

```

(root@kali)~# nmap -script vuln 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 20:09 BST
Nmap scan report for 192.168.1.1
Host is up (0.00048s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp    open  https
| ssl-dh-params:
| VULNERABLE:
| Diffie-Hellman Key Exchange Insufficient Group Strength
| State: VULNERABLE
| Transport Layer Security (TLS) services that use Diffie-Hellman groups
| of insufficient strength, especially those using one of a few commonly
| shared groups, may be susceptible to passive eavesdropping attacks.
| Check results:
| WEAK DH GROUP 1
|   Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: RFC2409/Oakley Group 2
|   Modulus Length: 1024
|   Generator Length: 8
|   Public Key Length: 1024
| References:
|   https://weakdh.org
|_ http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|   http://ha.ckers.org/slowloris/
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
MAC Address: 3C:08:F6:AB:14:66 (Cisco Systems)

Nmap done: 1 IP address (1 host up) scanned in 544.99 seconds

```

Figure 16: -script vuln scan

The -script vuln option in Nmap is being used to look for known vulnerabilities on the target IP address 192.168.1.1. The results of the scan show the following:

Status of the host: The host is up, meaning the firewall is online and responding to network requests.

Open Ports: Two ports are open, SSH and SSL/HTTPS which we gathered from Figure 14

Potential Vulnerabilities: The scan has identified potential vulnerabilities, including issues with SSL/TLS and SSH services. For example, the scan points out a "Diffie-Hellman Key Exchange Insufficient Group Strength" vulnerability, which could make encrypted communications susceptible to eavesdropping if not properly configured.

5.2.3 Scan's conclusion

According to scans done on the firewall's external interface, the system is up and running and actively answering network requests. It seems, nevertheless, that the firewall is successfully hiding information about its services. Strict safety protocols are in place to prevent unauthorised access or reconnaissance, as seen by the scans' inability to identify any open ports or the particular operating system.

In conclusion, the ASA 5505 firewall's inside interface seems to be more vulnerable than its outside interface because of the many vulnerabilities that have been found. One of the most serious problems is with using an SSL certificate with a weak hashing method. It means that attacks could happen on the internal network that take advantage of these weaknesses. This could put the data's privacy and security at risk. The found flaws, like problems with SSL/TLS protocols and the Diffie-Hellman key exchange system, suggest that the firewall's internal defences may not be as strong as thought. These vulnerabilities need to be fixed right away to make the inside interface more secure.

5.3 Additional configurations

Next, we'll look at more advanced configurations for the internal network, such as routing, address translation, and inspection rules. Setting up a static default route is the main thing that needs to be done here so that the ASA can route data to unknown destinations through a gateway. This is crucial for the ASA to effectively handle traffic that is not destined for known internal networks.

Finally, i focus on configuring the DMZ (Demilitarized Zone) on a Cisco ASA device, along with setting up Static Network Address Translation (NAT) and Access Control Lists (ACLs).

Demilitarised Zones (DMZs) are an important part of network design because they separate an organization's trusted internal network from untrusted external networks like the internet. Hosting public-facing services like web, email, and DNS servers that need to be available from the external network is its main goal. These services are kept separate from the internal network to reduce the risk of direct attacks. [23]

Setting up a DMZ in the topology we use means setting up specific interfaces on the firewall (Ethernet0/0 on the ASA5505) that establish and enforce the boundaries between the internal network, the DMZ, and the outside network. This setup makes sure that anyone from the outside can't get into the DMZ and use its services without breaking the security of the private network.

```
ASA5505(config-if)# show switch vlan
```

VLAN	Name	Status	Ports
1	inside	up	Et0/1, Et0/3, Et0/4, Et0/5 Et0/6, Et0/7
2	outside	up	Et0/0
3	dmz	up	Et0/2

```
ASA5505(config-if)#
```

Figure 17: DMZ configured

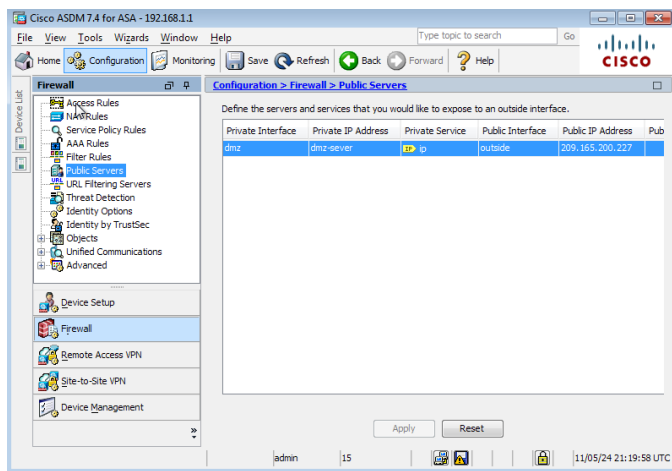


Figure 18: DMZ on the ASDM

Network Address Translation (NAT) is set up. Before sending data to the internet, NAT is needed to change the private IP addresses of devices on an internal network to public IP addresses. This keeps public IP addresses safe and also makes things safer by keeping internal IP addresses from getting seen by networks outside the network. Also, the inspection policy are set. These policies tell the ASA what kinds of traffic are allowed through the firewall. This way, it can make sure that only legitimate traffic gets through and that any unwanted or harmful traffic is stopped.

```
ASA5505(config)# object network INSIDE-NET
ASA5505(config)# object network INSIDE-NET
ASA5505(config)# object network INSIDE-NET
ASA5505(config-network-object)# subnet 192.168.1.0 255.255.255.0
ASA5505(config-network-object)# nat (insi
ASA5505(config-network-object)# nat (inside,out
ASA5505(config-network-object)# nat (inside,outside) dyn
ASA5505(config-network-object)# nat (inside,outside) dynamic in
ASA5505(config-network-object)# nat (inside,outside) dynamic interface
ASA5505(config-network-object)# end
ASA5505# sh run obje
ASA5505# sh run object
object network INSIDE-NET
subnet 192.168.1.0 255.255.255.0
```

Figure 19: NAT configuration

Setting up security rules and Access Control Lists (ACLs) is the next step. ACLs are very important for controlling the data that comes into and goes out of a network. making and using ACLs that say based on IP addresses, protocols, and ports what kinds of links are allowed and which are not. Also defined and implemented are security policies, which include settings that tell the ASA how to handle different types of data and threats. For the organization's security standards to be followed and the network to be safe from attacks and unauthorised entry, these rules are necessary.

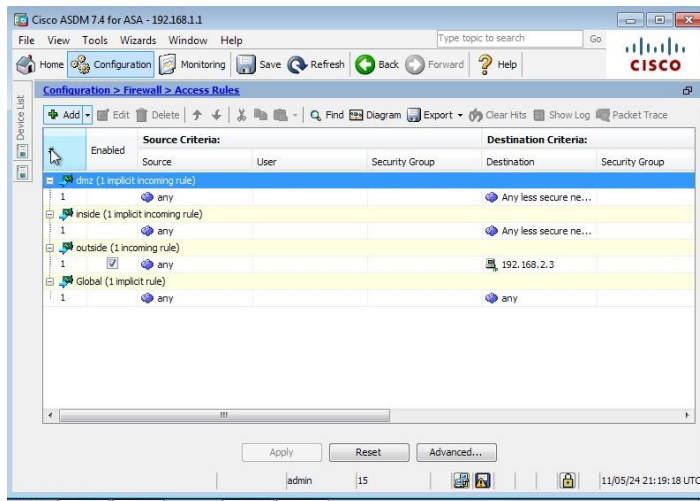


Figure 20: ASDM shows the ACL's configured

```

ASA5505# conf t
ASA5505(config)#
ASA5505(config)# pol
ASA5505(config)# policy-map
ASA5505(config)# policy-map glo
ASA5505(config)# policy-map glob
ASA5505(config)# policy-map global_
ASA5505(config)# policy-map global_
ASA5505(config)# policy-map global_polic
ASA5505(config)# policy-map global_policy
ASA5505(config-pmap)# class
ASA5505(config-pmap)# class insp
ASA5505(config-pmap)# class inspec
ASA5505(config-pmap)# class inspectio
ASA5505(config-pmap)# class inspection
ASA5505(config-pmap)# class inspection_default
ASA5505(config-pmap-c)# inspe
ASA5505(config-pmap-c)# inspect icm
ASA5505(config-pmap-c)# inspect icmp
ASA5505(config-pmap-c)#

```

Figure 21: Inspection Policy

The commands that I gave in the above picture make a policy map called "global_policy." This is a list of rules that tell the firewall how to handle traffic. There is a mention to a class map called "inspection_default" in this policy map. This class map usually has a list of traffic types that the firewall should check out.

"inspect icmp" is the last command. It adds Internet Control Message Protocol (ICMP) inspection to the usual inspection class. Devices on a network use ICMP to send error messages and operational information. It is also often used for diagnostic reasons, like the "ping" command to check connectivity. The firewall can let ICMP packets (like ping responses) go back to the sender by inspecting ICMP data.

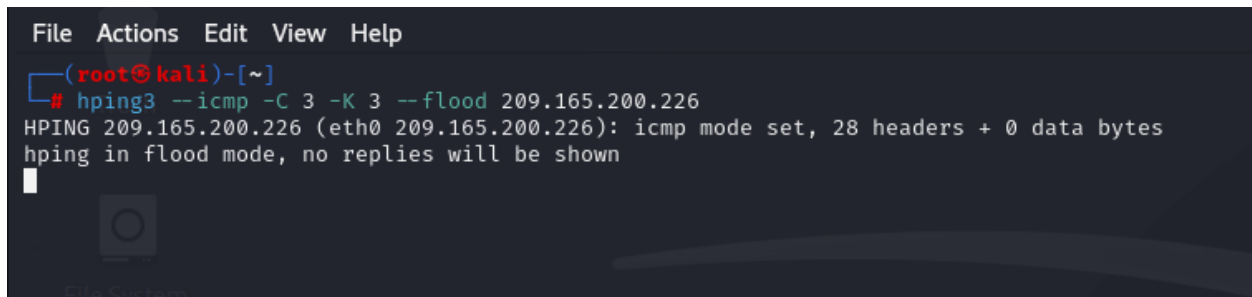
5.4 DoS Attack (BlackNurse Attack)

Overloading a computer or network with too much data is what a Denial-of-Service (DoS) attack does. The goal is to shut it down so that its intended users can't use it. The BlackNurse attack is a certain kind of DoS attack that uses a low-volume ICMP (Internet Control Message Protocol) flood. It uses ICMP Type 3 Code 3 packets, which are usually used to show that a target port can't be reached. Even though BlackNurse only needs about 15 to 18 Mbps of bandwidth, it can successfully overload the CPUs of targeted firewalls, causing major problems even when there isn't much traffic. This kind of attack is known for how well it can disrupt network systems with not very many resources. [24]

Why I chose BlackNurse Dos attack?

It works especially well against an ASA 5505 firewall because it uses low-volume ICMP Type 3 Code 3 packets to make the firewall's CPU work hard, which can cause problems even with 15–18 Mbps of bandwidth. BlackNurse is not like other high-volume DDoS attacks because it doesn't flood the network with data. Instead, it uses the processing of specific ICMP packets to stop operations with very few resources. [25]

5.4.1 The Attack

A terminal window with a dark background and light-colored text. The window has a menu bar at the top with 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(root@kali)-[~]'. The command entered is '# hping3 --icmp -c 3 -K 3 --flood 209.165.200.226'. The output shows 'HPING 209.165.200.226 (eth0 209.165.200.226): icmp mode set, 28 headers + 0 data bytes' and 'hping in flood mode, no replies will be shown'. A cursor is visible on the line following the output.

```
File Actions Edit View Help
(root@kali)-[~]
# hping3 --icmp -c 3 -K 3 --flood 209.165.200.226
HPING 209.165.200.226 (eth0 209.165.200.226): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Figure 22: Hping3 command on PC-C kali from external network

"hping3 --icmp -c 3 -K 3 --flood 209.165.200.226" is the command that is shown in figure 22. Its purpose is to send a lot of ICMP packets to the given IP address, which is the firewall's outside interface. "--icmp" means to use ICMP packets, "-c 3" means to send three packets, "-K 3" makes each packet 3 bytes long, which is used in a blacknurse attack, and "--flood" sends the packets as quickly as possible without waiting for answers.

This command is meant to flood the target with so many ICMP packets that it can't handle them. If the firewall isn't set up to handle this kind of attack correctly, it could result in a denial-of-service (DoS) condition. Firewalls, like the Cisco ASA 5505, are made with ways to find and stop flooding threats, such as ICMP floods. Depending on how it is set up, the firewall may either rate-limit ICMP messages, block them completely, or wait until a certain amount of them are sent before taking action to stop the attack from affecting the availability of the network.

In reality, how the firewall responds to this command would rely on its security policies and the defences it has in place. It could record the attack, get rid of the extra ICMP packets, or

temporarily block the source IP address. As long as the firewall is set up correctly, it should be able to handle the flood without stopping valid traffic or services.

5.4.2 The results

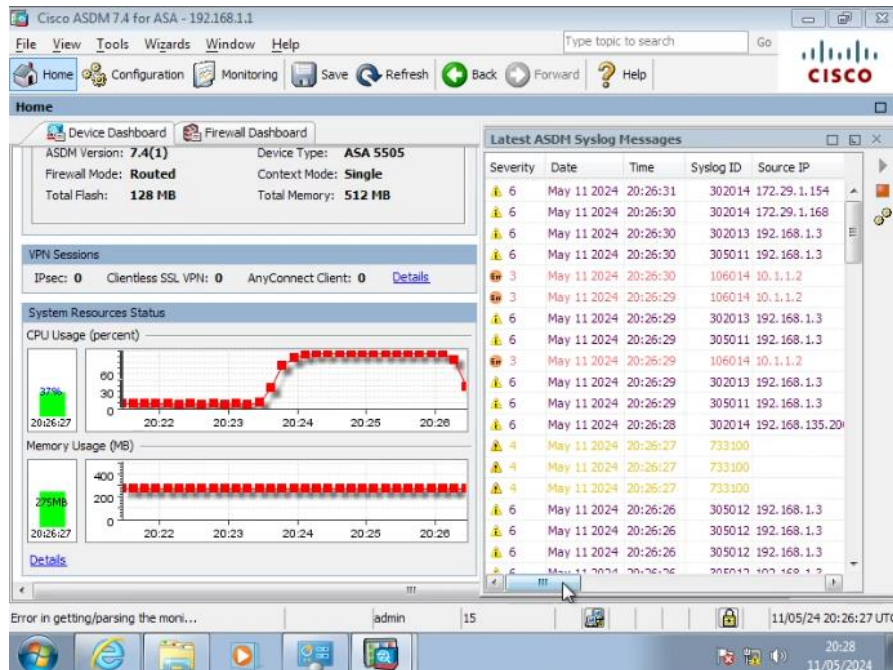


Figure 23: ASDM POV after the attack

The firewall's reaction to the BlackNurse icmp flood attack is shown graphically in the screenshot taken from the Cisco ASDM during that attack. A large increase in the firewall's CPU usage can be seen on the figure below, it indicates the attack was placing a high processing demand on the device. This high CPU usage is a typical symptom of such an attack, as the appliance works to handle the influx of ICMP packet

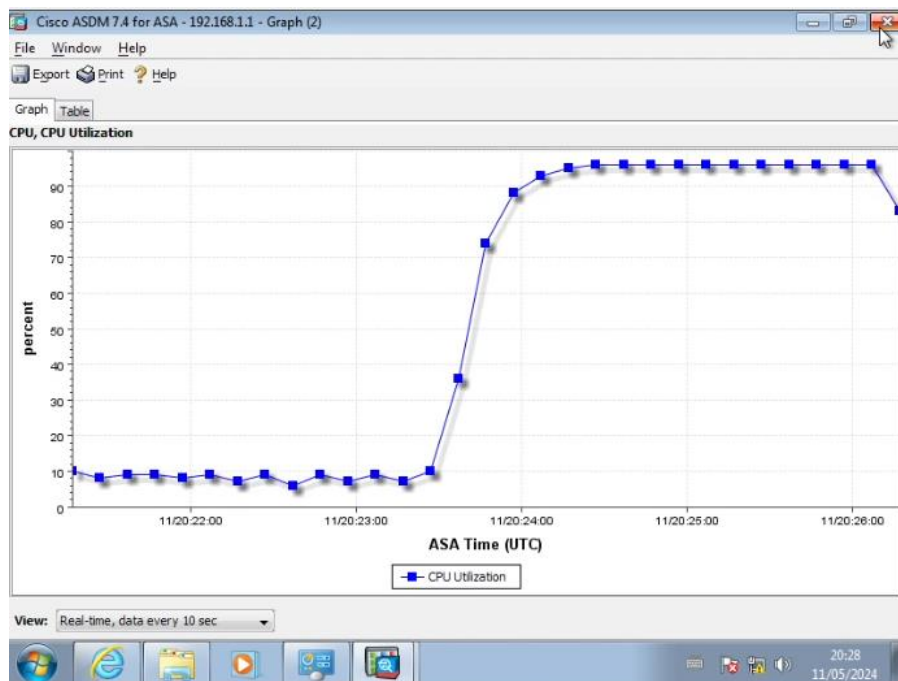


Figure 24: CPU utilization graph

The Syslog messages show that the firewall is picking up and reacting to the ICMP traffic. There are many entries that show ICMP connection attempts were denied. So, it looks like the firewall's security features are actively stopping the attack by blocking the bad traffic.

The table shows the following columns: Severity, Date, Time, Syslog ID, Source IP, Source, Destination IP, and Destination Description. The entries are all from May 11, 2024, at 20:24:09, showing denied ICMP traffic from 172.16.3.4 to 172.16.3.4.

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destination Description
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic
3	May 11 2024	20:24:09	313001	172.16.3.4			Denied ICMP type=3, code=3 from 172.16.3.4 on i
4	May 11 2024	20:24:09	313005				No matching connection for ICMP error message: ic

Figure 25: Syslog Messages during the attack

The syslog messages that were recorded during the ICMP flood attack show how the firewall dealt with the large amount of ICMP data. The messages are part of the firewall's logging system. They keep track of events that have to do with security and are used for tracking and fixing problems.

Because there are multiple "Denied ICMP" entries in the Figure, we can see that the firewall is always blocking ICMP data. There is a severity level, a syslog ID, an IP address for the source, and a description that usually has the ICMP type and code. Syslog severity levels used by the Cisco ASA 5505 firewall run from 0 (emergencies) to 7 (debugging). Levels of severity facilitate classification of the kind and significance of recorded data. Informational messages are handled at severity level 6, for example, and error messages at level 3.

The "Denied ICMP" messages mean that the firewall's access control lists (ACLs) are set up to block ICMP data. This is something that was configured in the previous section; it's a standard way to protect against network scanning and denial-of-service attacks. The messages often include an ICMP type and code that relate to a specific reason for the denial, like "port unreachable" or "communication administratively prohibited."

The firewall is constantly looking for and blocking the unwanted ICMP packets during the attack. This keeps them from getting to the internal network. Maintaining network functionality and keeping it safe from possible threats depend on this behaviour. The firewall's ability to handle and record this kind of event shows how strong its security is and how it protects the network from bad things.

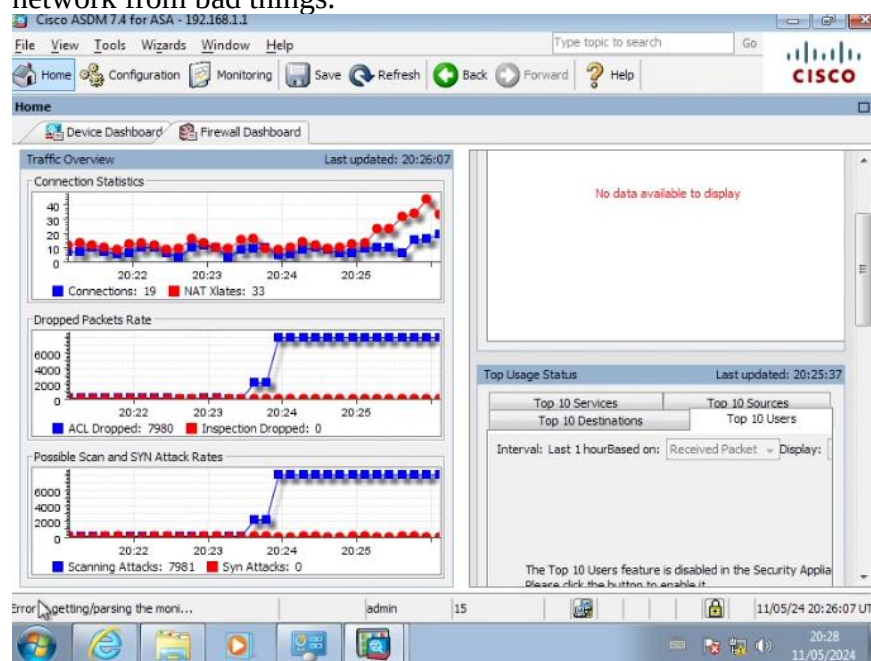


Figure 26: Other ASDM graph stats during the attack

Changing numbers of connections in the "Connection Statistics" graph could be due to the ICMP flood attack. A high number of dropped packets in the "Dropped Packets Rate" graph is another sign that the firewall is blocking the attack traffic. It's possible that the activity in the "Possible Scan and SYN Attack Rates" graph is linked to the ICMP flood or other scanning attempts.

Chapter 6. Conclusions and recommendations

6.1 Conclusion

The purpose of testing on the ASA 5505 firewall was to see how well it could defend against DDoS attacks and find and stop attempts to break in. Within my project proposal, I first suggested that the "firewall's performance would degrade under increasing attack traffic" and that "its intrusion detection capabilities would improve with the complexity of the attack."

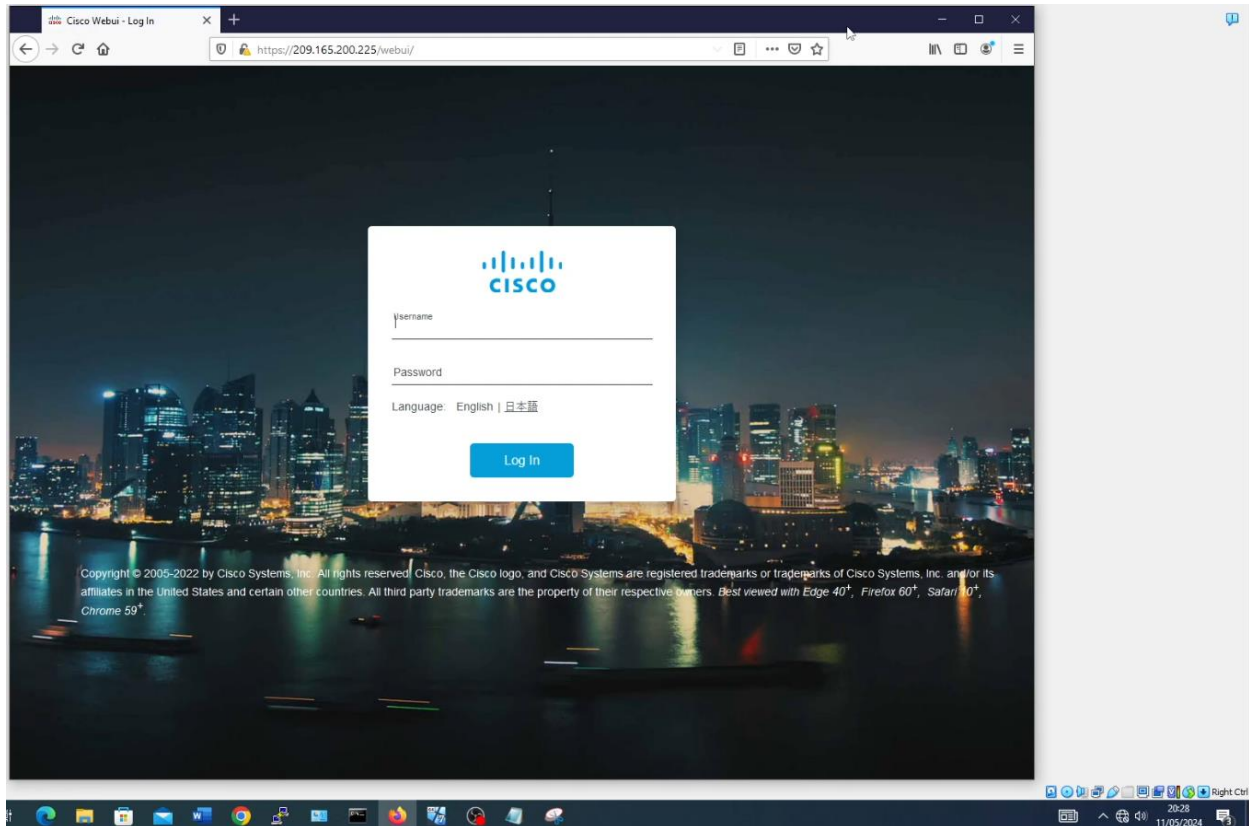


Figure 27: Hosts could access webui set up on edge router during attack

Based on the information gathered, it's clear that the firewall's CPU usage went up a lot during the ICMP flood attack. This means that the firewall was under a lot of stress. The syslog messages showed that the firewall was actively blocking ICMP traffic, which means it saw the threat and took action. But the fact that the host from the internal network kept working shows that the firewall was still able to keep the internal network safe, even though it was busy.

The key takeaways from this project are:

1. The firewall was capable of maintaining internal network operations during the DDoS attack, indicating a level of resilience.
2. The firewall's CPU was heavily utilized during the attack, which could be a concern for sustained attacks over a longer period.

3. The firewall's intrusion detection and prevention mechanisms were functional, as evidenced by the denied ICMP traffic, but the testing did not conclusively demonstrate an increase in detection capability with the complexity of the attack.

If I were doing the experiment again, I would have taken the following things into account for better outcomes:

1. Putting in place extra firewall policies and rules to optimise the reaction to different attack paths.
2. Performing a wider variety of attack simulations to evaluate the firewall's resistance to various DDoS assaults and infiltration techniques.
3. Increasing the monitoring configuration to record more precise performance data may yield more in-depth understanding of how the firewall behaves in an attack scenario.
4. Long-term testing to determine how long the firewall will last and how much performance will drop over time.

Overall, the tests were helpful because they showed what the firewall could do and where speed and security policy configuration could be improved.

6.2 Further Avenues for research?

The project on setting up and testing the Cisco ASA 5505 firewall in a simulated network environment offers a number of areas that could be studied further in the future. The thorough testing and review of the firewall's performance, security features, and dependability in different situations has shown areas that need more research. In the future, researchers might work on making the firewall better able to deal with more complex cyber threats, like advanced persistent threats (APTs), zero-day attacks and other firewall attacks, which were not fully explored in this project. Also, looking into adding next-generation firewall features like application-aware security policies and better intrusion prevention systems could help us learn more about how to make network security tools better. Another possible area of study is comparing the Cisco ASA 5505 to newer firewall technologies to see how firewall solutions have changed over time and how well they work in changing network environments. This would help us learn how security devices in corporate networks work and how to update them.

Chapter 7. Reflection

As I worked on my project, I learned a lot of things that were not related to the technical side of network security. Planning and getting ready meticulously was one of the most important things I learned. I learned how important it is to pay attention to details and be thorough by setting up a simulated network environment and making sure the firewall's settings were correct. I had underestimated how long it would take to do everything, nevertheless the challenges taught me how valuable and important it is to plan and prepare.

This project had a big effect on my growth as a person as well. It forced me to leave my comfort zone, especially when it came to problem-solving and critical thought. Having to deal with and get past problems, like getting unexpected results during testing made me stronger and more flexible. I'm more sure of my skills to deal with difficult issues and adjust to new situations because of these experiences.

Reflecting on the project, I think there were some ways I could have done things better. For example, a more thorough review of the firewall's abilities could have been achieved by making a more detailed plan to complete this report and including a wider range of attack simulations. I could have learned more about how the firewall worked in different situations by improving my monitoring setup to collect more specific performance data. I would have learned how to analyse things better and the project would have been better if these changes had been made.

Also, this project showed how important "soft" skills are, like being able to organise your time well, and work alone. Keeping the project's scope under control within the time limit needed careful planning and setting of tasks in order of importance. Dealing with and getting past setbacks like loss of a family member, taught me how important it is to keep going and be flexible. These skills helped me do well on the project and will help me in everything I do from now on. To be fair, the project taught me a lot of things that weren't just technical. And it changed me as a person and as someone who wants to learn. Along with a solid foundation in network security, it taught me a variety of soft skills that are important for success in any area.

Bibliography

- [1] J. BONNEVIER and S. HEIMLÉN, "The Role of Firewalls in Network Security," *KTH ROYAL INSTITUTE OF TECHNOLOGY*, p. 74, 2018.
- [2] C. Collier, "Firewalls: How They Relate to Cybersecurity," *CyberMaxx*, 2022.
- [3] A. S. Wazan, "Cybersecurity in networking: adaptations, investigation, attacks, and countermeasures," *Springer Link*, vol. 78, pp. 133-134, 2023.
- [4] A. M. Ghouri, "EXPLORING THE ROLE OF CYBER SECURITY MEASURES (ENCRYPTION, FIREWALLS, AND AUTHENTICATION PROTOCOLS) IN PREVENTING CYBER-ATTACKS ON E-COMMERCE PLATFORMS," *International Journal of eBusiness and eGovernment Studies*, vol. 15, no. 1, pp. 444-469, 2023.
- [5] V. Redya, D. K. S. Chatrapati and D. V. N. Kamalesh, "Paper on Types of Firewall and Design Principles," *International Journal of Science and Research (IJSR)*, vol. 6, no. 391, p. 8, 2015.
- [6] R. Ferguson, "ComputerWeekly.com," Tech Target, 11 07 2012. [Online]. Available: <https://www.computerweekly.com/news/2240159432/The-history-of-the-Next-Generation-Firewall>.
- [7] Paloalto. Networks, "The History of Firewalls | Who Invented the Firewall?," Palo alto networks. [Online].
- [8] S. Iqbal, D. Thapa, A. I. Awad and T. Päivärinta, "Conceptual Model of Online Pedagogical Information Security Laboratory:," *Hawaii International Conference on System Sciences*, p. 10, 2015.
- [9] M. Faizan, S. S. Hegde and N. V. Yaligar, "Comparison between Cisco ASA and Fortinet FortiGate," *Journal of Electrical and Computer Engineering*, vol. 21, no. 34-36, p. 3, 2019.
- [1] Spiceworks, "Fortigate equivalent to a Cisco firepower 1120 ASA.," Spiceworks, 11 2022.
- 0] [Online]. Available: <https://community.spiceworks.com/t/fortigate-equivalent-to-a-cisco-firepower-1120-asa/940076>.
- [1] G2, "Compare Cisco ASA 5500-X Series and FortiGate NGFW," G2, [Online]. Available: <https://www.g2.com/compare/cisco-asa-5500-x-series-vs-fortigate-ngfw>.
- [1] G. Bowen, "Document Analysis as a Qualitative Research Method," *Research Gate*, vol. 9, 2] no. 2, p. 40, 2009.
- [1] V. Braun and V. Clarke, "Thematic analysis.," *Research Gate*, vol. 2, pp. 57-71, 2012. 3]
- [1] Robcheney1, "FortiGate vs Cisco firewalls in our latest Firewall Roundup!," Corporate 4] Armor, 27 12 2021. [Online]. Available: <https://www.corporatearmor.com/newsroom/cisco/fortigate-vs-cisco-firewalls-in-our-latest-firewall-roundup/>.
- [1] M. Patel, "Demilitariz Demilitarized Zone: An Ex one: An Exceptional La ceptional Layer 5] of Network Security t er of Network Security to," *University of Windsor*, p. 62, 2020.
- [1] nightwaif, "Reddit," Reddit, 2017. [Online]. Available:
- 6] https://www.reddit.com/r/AskNetsec/comments/681123/ways_to_protect_against_ddos_attacks_with_cisco/?rdt=58793.

- [1] Cisco, "Cisco," Cisco, 20 06 2023. [Online]. Available:
7] <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113685-asa-threat-detection.html>.
- [1] W. Webb, "A Short Approach: The Cisco ASA 5505 as a Stepping Stone Into Embedded
8] Reverse Engineering," Rapid7, 14 06 2016. [Online]. Available:
<https://www.rapid7.com/blog/post/2016/06/14/asa-hack/>.
- [1] M. Lewis, "Cisco ASA series part three: Debugging Cisco ASA firmware," NCC group, 2
9] 10 2017. [Online]. Available: <https://research.nccgroup.com/2017/10/02/cisco-asa-series-part-three-debugging-cisco-asa-firmware/>.
- [2] D. Hucaby, Cisco ASA, PIX, and FWSM Firewall Handbook, Indianapolis, IN 46240 USA
0] : Cisco Press , 2007.
- [2] Lyon, Gordon "Fyodor";, "The Official Nmap Project Guide to Network Discovery and
1] Security Scanning," nmap, [Online]. Available: <https://nmap.org/book/toc.html>.
- [2] Awati, Rahul;, "What is Nessus?," TechTarget, 06 2023. [Online]. Available:
2] <https://www.techtarget.com/searchnetworking/definition/Nessus>.
- [2] Hiter, Shelby;, "What Is a DMZ Network? Definition, Architecture & Benefits," eSecurity
3] Planet, 07 04 2023. [Online]. Available: <https://www.esecurityplanet.com/networks/dmz-network/>.
- [2] J. Ullrich, "ICMP Unreachable DoS Attacks (aka "Black Nurse")," 10 11 2016. [Online].
4] Available:
<https://isc.sans.edu/diary/ICMP%2BUnreachable%2BDoS%2BAttacks%2Baka%2BBlack%2BNurse/21699>.
- [2] E. Hjelmvik, "BlackNurse Denial of Service Attack," 10 11 2016. [Online]. Available:
5] <https://www.netresec.com/?page=Blog&month=2016-11&post=BlackNurse-Denial-of-Service-Attack>.

Appendix

Basic Firewall Configuration on ASA 5505:

```
ASA5505(config)# sh run
: Saved
:
: Serial Number: JMX181940WM
: Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz
:
ASA Version 9.2(4)
!
hostname ASA5505
domain-name cisco.com
enable password PmNe1e0C3tJdCLe8 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdL.2KYOU encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
```

```
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address 209.165.200.226 255.255.255.248
!
boot system disk0:/asa923-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name cisco.com
pager lines 24
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-741.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.1.0 255.255.255.0 inside
ssh timeout 10
ssh key-exchange group dh-group1-sha1
console timeout 0
```

```
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password eY/fQXw7Ure8Qrz7 encrypted privilege 15
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
```

Cryptochecksum:8cf5932caa539e015e95ae6d6ac79191
: end
ASA5505(config)#

Router 1 Configuration:

R1#sh run

Building configuration...

Current configuration : 6343 bytes

!

! Last configuration change at 17:23:01 UTC Sat May 11 2024 by admin

!

version 17.6

service timestamps debug datetime msec

service timestamps log datetime msec

! Call-home is enabled by Smart-Licensing.

service call-home

platform qfp utilization monitor load 80

platform punt-keepalive disable-kernel-core

!

hostname R1

!

boot-start-marker

boot-end-marker

!

!

security passwords min-length 10

enable secret 9

\$9\$m3fsxtSDOcFOhU\$G9MYVcflA7z0LutqVAkjKqyWjndoWW4MYIQhvK1WZMA

!

no aaa new-model

!

!

!

!

!

!

!

ip domain name cisco.com

!

!

!

login on-success log

!

!

!

!

!

!

!

subscriber templating
multilink bundle-name authenticated

!
!
!

crypto pki trustpoint TP-self-signed-3032915588
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3032915588
revocation-check none
rsa-keypair TP-self-signed-3032915588

!

crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl

!

!

crypto pki certificate chain TP-self-signed-3032915588

certificate self-signed 01

30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 33303332 39313535 3838301E 170D3234 30353131 31303035
32315A17 0D333430 35313131 30303532 315A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 30333239
31353538 38308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 0100B350 92D4E2B2 46ABB2B2 5CB027D7 A14DFCAB 8DE96DB8 2C75DF0E
4064147C 4EFE7C6A 8504D252 D23A0D0E 23593A8F 8D1E6CBB 115803F2 560D9B3E
0732540E A32E0AB5 C0D63C3E 9BD81905 E83F39D6 98F34BEC 87B5463A C38DB63A
9CBFA286 3038A807 5BD35250 EAB7213D D0DD43F5 A48BFE7A 47F13100 333BD17B
E11263C1 405C85D9 B0625FFC 549CD97E D5F0CDAF EC5E524F F5131563 D8219963
1C4BD16E 12FBA097 1266509E BFD88736 A22FC12F B4C4788A A0F5245E B79CAD81
2E375983 13F55390 88498FE0 DD05EBE9 28050200 BF5CCE36 F63D4D71 936794C8
7016F162 DDA90352 3F3366B9 9CA5F97A 74DD360E F5E76B1E 724D4C27 521B8B39
E6AE4DBD 49890203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603 551D2304 18301680 14E85811 0B77AFD4 E3C52379 95809BBA D79DA47A
5E301D06 03551D0E 04160414 E858110B 77AFD4E3 C5237995 809BBAD7 9DA47A5E
300D0609 2A864886 F70D0101 05050003 82010100 88909A2C 7E3C40C9 1A4AB78C
601D0FA9 53ADB7A5 61DB300F 3DD1DAFC 502C4310 3CB5417A 57EE5BBD D4768910
C03690FB C04067A7 509ADFA9 B1510562 CE8D3E0E DC5CD6B2 C454FD71 6BA9ECF3
90B02DF8 5C3ABCF0 9D4E98AE ED963400 7E3A66F0 553F48F6 5822DCBC 948650AE
B03D4969 8FCD57A7 1D9B0280 81124783 AB86A277 FC8D44A3 4062AD63 743018C5
1DCC019E F0CA6C42 971403EB D028BF60 0A867E66 6827870B E6D967FB 9D37E101
88BDA32E 087CBFBC 932B6300 8F2D3477 C651BD64 0EBF6448 2E5CA0C3 98D7158D
409A1DEB 8D15277B 6AD05FD7 0F9C441D 238D6838 EA0B02D3 A88495F6 3C79C43B
0E69CA8A D880441F 6965AD57 28A0F3B0 4FF384A7

quit

crypto pki certificate chain SLA-TrustPoint

certificate ca 01

30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1

6C9E3D8B

D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD

230E3AFB

418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28

quit

!

!

license udi pid C8200L-1N-4T sn FGL2725L1T6

memory free low-watermark processor 67482

!

diagnostic bootup level minimal

!

spanning-tree extend system-id

!

username admin secret 9

\$9\$/DHSs7xMXC0W9k\$W1K/vjG1TfVqxDpgiDf9FN1A.vNgC3sT2CryExYL59U

!

redundancy

mode none

!

!

```
!  
!  
!  
!  
!  
!  
interface GigabitEthernet0/0/0  
  ip address 209.165.200.225 255.255.255.248  
  negotiation auto  
!  
interface GigabitEthernet0/0/1  
  no ip address  
  shutdown  
  negotiation auto  
!  
interface GigabitEthernet0/0/2  
  no ip address  
  shutdown  
  negotiation auto  
!  
interface GigabitEthernet0/0/3  
  no ip address  
  shutdown  
  negotiation auto  
!  
interface Serial0/1/0  
  ip address 10.1.1.1 255.255.255.252  
!  
interface Serial0/1/1  
  no ip address  
  shutdown  
!  
ip http server  
ip http authentication local  
ip http secure-server  
ip forward-protocol nd  
ip route 0.0.0.0 0.0.0.0 Serial0/1/0  
ip route 0.0.0.0 0.0.0.0 10.2.2.2  
!  
!  
!  
!  
!  
!  
control-plane  
!
```

```
!  
line con 0  
  exec-timeout 5 0  
  logging synchronous  
  login local  
  stopbits 1  
line aux 0  
line vty 0 4  
  exec-timeout 5 0  
  login local  
  transport input ssh  
line vty 5 14  
  login  
  transport input ssh  
!  
call-home  
  ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com  
  ! the email address configured in Cisco Smart License Portal will be used as contact email  
  address to send SCH notifications.  
  contact-email-addr sch-smart-licensing@cisco.com  
  profile "CiscoTAC-1"  
  active  
  destination transport-method http  
!  
!  
!  
!  
!  
!  
end
```

```
R1# sh ip pro  
R1# sh ip protocols ?  
  multicast Multicast global information  
  summary Short form answer  
  topology Display protocols for a topology instance  
  vrf Display protocols for a VPN Routing/Forwarding instance  
  | Output modifiers  
  <cr> <cr>
```

```
R1# sh ip protocols  
*** IP Routing is NSF aware ***
```

```
Routing Protocol is "application"  
  Sending updates every 0 seconds  
  Invalid after 0 seconds, hold down 0, flushed after 0
```

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Maximum path: 32

Routing for Networks:

Routing Information Sources:

Gateway Distance Last Update

Distance: (default is 4)

R1# sh ip int br

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	209.165.200.225	YES	manual	up	up
GigabitEthernet0/0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0/3	unassigned	YES	unset	administratively down	down
Serial0/1/0	10.1.1.1	YES	manual	up	up
Serial0/1/1	unassigned	YES	unset	administratively down	down

R1#sh vlan br

VLAN Name	Status	Ports
1 default	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

R1#

Router 2 Configuration:

R2#sh run

Building configuration...

Current configuration : 6136 bytes

!

! Last configuration change at 19:57:42 UTC Sat May 11 2024

!

version 17.6

service timestamps debug datetime msec

service timestamps log datetime msec

! Call-home is enabled by Smart-Licensing.

service call-home

platform qfp utilization monitor load 80

platform punt-keepalive disable-kernel-core

!

hostname R2

!

boot-start-marker

boot-end-marker

!

!

!

no aaa new-model

!

!

!

!

!

!

!

!

!

!

!

login on-success log

!

!

!

!

!

!

!

subscriber templating

multilink bundle-name authenticated

!

!

!
crypto pki trustpoint TP-self-signed-786720880
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-786720880
revocation-check none
rsakeypair TP-self-signed-786720880

!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl

!
crypto pki certificate chain TP-self-signed-786720880
certificate self-signed 01

3082032E 30820216 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 37383637 32303838 30301E17 0D323430 35313131 30303430
385A170D 33343035 31313130 30343038 5A303031 2E302C06 03550403 1325494F
532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3738 36373230
38383030 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02
82010100 AB7A5393 BD760022 663ED222 06C6FAC9 BAF455F7 C6F9B91E 796D4E14
F5E0CA9A CE54E97B A4925396 B0DFD3D6 3AC0D1E1 230E1FC6 35329E3D EC245586
AD319697 98506575 2D0C37EE 5A6EDE92 3CEE4564 0B4BA4F3 84997606 D308330E
A839A1C0 BCC16D9E FB045024 B7C8042A 46497D1C A5831BC4 6329490D 3F054458
CE5E664F B8C4086B AC0747D2 B4EB7B09 117C84EB 3E783B97 84566A71 DE85F02F
852A6954 1BAF4960 652E027A F19EF230 490DC786 B6AE40AB D118E1FF 282714F9
2F344470 00DBA85B 8BD5ED78 843FFC67 1822B312 2E37FFE8 00CF68E0 3FBFA76F
CFA52380 C7C59319 0D30059E 0E2B53EA 0E9ED6CE 3182DE4A 430E6593 C2163AD9
EEAFA39D 02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
0603551D 23041830 16801459 76FBA43D 68B57E3C 5E0ED510 565643BB F6E1BD30
1D060355 1D0E0416 04145976 FBA43D68 B57E3C5E 0ED51056 5643BBF6 E1BD300D
06092A86 4886F70D 01010505 00038201 0100A627 87BE2BEB 000EA87C 91C3DF6F
7B8EED7E 6D91EE25 EA648253 30F70B10 DA09CD8D 2A4F9A8B AA3B07A5
EDF3DA6E

3107A3E6 EF880DFA 2AC8AB6D 2E1B7946 3CB74B73 D42F2B7D A786397B FB9B39B3
5DA2AA20 6ED40F0F 23F4ED72 27705C2C 488FE636 FDB18BA7 58486675 36C90D14
87952AB9 C54CCDDA F8D1DD01 342F2A05 6E66E959 892A6216 4EB4AC82 0CBFAE32
D2C20DCA A5F86693 726E66DB E336EA52 4B0FB05C 1DB591FF 3CE3B3E1 31A9A827
45DE2B44 10575750 B6A8FA3C A507D1EB 3DE92EA2 D2529734 9918C27E 73856629
13681A8A 0AEB662F BA489740 17A38335 99351AA5 04196D79 8B2F3E38 4CFCECC7
E76100B8 C51C81CD EE91CD07 84D91768 FC5A

quit

crypto pki certificate chain SLA-TrustPoint
certificate ca 01

30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363

6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1
6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD
230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
!
!
license udi pid C8200L-1N-4T sn FGL2725L1SA
memory free low-watermark processor 67482
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
redundancy
mode none
!
!
!
!
!
!
!

```
!  
interface Loopback0  
 ip address 172.30.1.1 255.255.255.0  
!  
interface GigabitEthernet0/0/0  
 no ip address  
 shutdown  
 negotiation auto  
!  
interface GigabitEthernet0/0/1  
 no ip address  
 shutdown  
 negotiation auto  
!  
interface GigabitEthernet0/0/2  
 no ip address  
 shutdown  
 negotiation auto  
!  
interface GigabitEthernet0/0/3  
 no ip address  
 shutdown  
 negotiation auto  
!  
interface Serial0/1/0  
 ip address 10.1.1.2 255.255.255.252  
!  
interface Serial0/1/1  
 ip address 10.2.2.2 255.255.255.252  
 clock rate threshold 64000  
!  
ip http server  
ip http authentication local  
ip http secure-server  
ip forward-protocol nd  
ip route 172.16.3.0 255.255.255.0 Serial0/1/1  
ip route 209.165.200.224 255.255.255.248 Serial0/1/0  
!  
!  
!  
!  
!  
!  
control-plane  
!  
!
```

```

line con 0
  stopbits 1
line aux 0
line vty 0 4
  login
  transport input ssh
line vty 5 14
  login
  transport input ssh
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
!
!
!
!
!
!
end

```

R2# show ip in

R2# show ip interface br

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0/3	unassigned	YES	unset	administratively down	down
Serial0/1/0	10.1.1.2	YES	manual	up	up
Serial0/1/1	10.2.2.2	YES	manual	up	up
Loopback0	172.30.1.1	YES	manual	up	up

R2#sh ip proto

R2#sh ip protocols

*** IP Routing is NSF aware ***

Routing Protocol is "application"

Sending updates every 0 seconds

Invalid after 0 seconds, hold down 0, flushed after 0

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Maximum path: 32

Routing for Networks:

Routing Information Sources:

Gateway Distance Last Update

Distance: (default is 4)

R2#

Router 3 Configuration:

```
R3#sh run
```

```
Building configuration...
```

```
Current configuration : 5955 bytes
```

```
!
```

```
! Last configuration change at 11:15:45 UTC Sat May 11 2024
```

```
!
```

```
version 17.6
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
! Call-home is enabled by Smart-Licensing.
```

```
service call-home
```

```
platform qfp utilization monitor load 80
```

```
platform punt-keepalive disable-kernel-core
```

```
!
```

```
hostname R3
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
!
```

```
!
```

```
no aaa new-model
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
login on-success log
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
subscriber templating
```

```
multilink bundle-name authenticated
```

```
!
```

!
!
crypto pki trustpoint TP-self-signed-1344490233
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1344490233
revocation-check none
rsakeypair TP-self-signed-1344490233

!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl

!
!
crypto pki certificate chain TP-self-signed-1344490233

certificate self-signed 01
30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 31333434 34393032 3333301E 170D3234 30353131 31303035
32325A17 0D333430 35313131 30303532 325A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 33343434
39303233 33308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 0100A6C1 CEA6A521 D5E1BA1C 708FF293 494571B1 C71C9B8B 29BB9C9D
C79457E9 EB4BD92B 38C966DE AD5083B3 AAE62424 7A1F0FF6 2A7FA4A8 0DCF5C41
01E33C72 1CDEE214 AC901267 AEE89F39 65CB0E21 AD88C170 8598340D 7F10526E
928F722C 5DE0A257 133D4381 C0F679E4 355F4CA1 50946AE2 E68BF089 8BBB7CD2
75EC663F E47A1607 388ACEA3 1DC896C1 A666C57C 53E63485 63CB56F0 D22D6682
62A8F628 2BFE3697 2284D90D 5FE0B134 BFBBF5C5 38554F00 D29E340F FE70130E
8BA4C7A3 94B7757B B7FF6D10 67067386 5750434B C18483B4 650B95C3 72B51FAF
B9563A97 42D5FDC8 72341648 17428D01 1A852BAE E6C1240F 38EF6039 AE50E9A5
6511E5AD D1970203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603 551D2304 18301680 1426384A E44A5D24 E19DDE48 4F6D4723 B576BAB0
C5301D06 03551D0E 04160414 26384AE4 4A5D24E1 9DDE484F 6D4723B5 76BAB0C5
300D0609 2A864886 F70D0101 05050003 82010100 1163E4A2 C5B7057B 12D39DA1
D3735EF3 224DA376 F70E33BA 54DF60C5 1958AE48 D3B7E92D 6F2713C8 85754093
417F5017 5F76CD3A 6022F7F4 1683F01D 8445337A 78CBE483 AC501C52 7FCA7B2C
2B14AB7B BE561AB6 DBA1C486 28E57AA2 A3622953 C5FA6618 CE4153A6 4B051C4C
C4CC4A18 F47515E2 BC9BA002 1F66F83E 5290D665 981A31B7 E9E37C0A 9E3A8138
6D833E31 AE0A2CA8 2E6401C8 96B5FF2B 6998CDA3 B54BEB32 BC045FB7 2C05BA19
454F15AC 44204798 24AA9D8E F1FDDA45 C293CCA9 A0D309D8 5E4D8515 F6B541AE
8C9174CC 53D84950 31452014 6EE63747 0053B4AD 8C3A4E67 ADF5CEE9 91AC8BC3
71307104 E0561AE1 4EA2FE0F 43983208 A9847177

quit

crypto pki certificate chain SLA-TrustPoint
certificate ca 01

30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363

6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1
6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD
230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
!
!
license udi pid C8200L-1N-4T sn FGL2725L1NM
memory free low-watermark processor 67482
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
redundancy
mode none
!
!
!
!
!
!
!

```
!  
interface GigabitEthernet0/0/0  
  no ip address  
  negotiation auto  
!  
interface GigabitEthernet0/0/1  
  ip address 172.16.3.1 255.255.255.0  
  negotiation auto  
!  
interface GigabitEthernet0/0/2  
  no ip address  
  negotiation auto  
!  
interface GigabitEthernet0/0/3  
  no ip address  
  negotiation auto  
!  
interface Serial0/1/0  
  no ip address  
!  
interface Serial0/1/1  
  ip address 10.2.2.1 255.255.255.252  
!  
ip http server  
ip http authentication local  
ip http secure-server  
ip forward-protocol nd  
ip route 0.0.0.0 0.0.0.0 Serial0/1/1  
!  
!  
!  
!  
!  
!  
control-plane  
!  
!  
line con 0  
  stopbits 1  
line aux 0  
line vty 0 4  
  login  
  transport input ssh  
line vty 5 14  
  login  
  transport input ssh
```

```

!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
!
!
!
!
!
!
end

```

```

R3#
R3#sh ip int br

```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	unassigned	YES	unset	down	down
GigabitEthernet0/0/1	172.16.3.1	YES	manual	up	up
GigabitEthernet0/0/2	unassigned	YES	unset	down	down
GigabitEthernet0/0/3	unassigned	YES	unset	down	down
Serial0/1/0	unassigned	YES	unset	down	down
Serial0/1/1	10.2.2.1	YES	manual	up	up

```

R3#sh ip pro
R3#sh ip protocols
*** IP Routing is NSF aware ***

```

```

Routing Protocol is "application"
Sending updates every 0 seconds
Invalid after 0 seconds, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Maximum path: 32
Routing for Networks:
Routing Information Sources:
Gateway Distance Last Update
Distance: (default is 4)

```

```

R3#

```

Final ASA configuration:

```
ASA5505(config)# sh run
: Saved
:
: Serial Number: JMX181940WM
: Hardware:  ASA5505, 512 MB RAM, CPU Geode 500 MHz
:
ASA Version 9.2(4)
!
hostname ASA5505
domain-name cisco.com
enable password PmNe1e0C3tJdCLe8 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
  switchport access vlan 3
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
```

```
!  
interface Vlan2  
  nameif outside  
  security-level 0  
  ip address 209.165.200.226 255.255.255.248  
!  
interface Vlan3  
  no forward interface Vlan1  
  nameif dmz  
  security-level 70  
  ip address 192.168.2.1 255.255.255.0  
!  
boot system disk0:/asa923-k8.bin  
ftp mode passive  
dns server-group DefaultDNS  
  domain-name cisco.com  
object network INSIDE-NET  
  subnet 192.168.1.0 255.255.255.0  
object network dmz-sever  
  host 192.168.2.3  
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3  
pager lines 24  
logging enable  
logging asdm informational  
mtu inside 1500  
mtu outside 1500  
mtu dmz 1500  
icmp unreachable rate-limit 1 burst-size 1  
asdm image disk0:/asdm-741.bin  
no asdm history enable  
arp timeout 14400  
no arp permit-nonconnected  
!  
object network INSIDE-NET  
  nat (inside,outside) dynamic interface  
object network dmz-sever  
  nat (dmz,outside) static 209.165.200.227  
access-group OUTSIDE-DMZ in interface outside  
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1  
timeout xlate 3:00:00  
timeout pat-xlate 0:00:30  
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02  
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00  
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00  
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute  
timeout tcp-proxy-reassembly 0:01:00
```

```
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.1.0 255.255.255.0 inside
ssh 172.16.3.3 255.255.255.255 outside
ssh timeout 10
ssh key-exchange group dh-group1-sha1
console timeout 0

dhcpd dns 209.165.201.2
dhcpd option 3 ip 192.168.1.1
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics host
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password eY/fQXw7Ure8Qrz7 encrypted privilege 15
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
```

```

inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
class class-default
  user-statistics accounting
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:f8c3e4754e0d4ecb0f09e2aae2575c4d
: end

```

ASA5505(config)# sh switch vlan

VLAN Name	Status	Ports
1 inside	up	Et0/1, Et0/3, Et0/4, Et0/5 Et0/6, Et0/7
2 outside	up	Et0/0
3 dmz	up	Et0/2

ASA5505(config)#

