DUY TAN UNIVERSITY

INTERNATIONAL SCHOOL

~🕮~

GROUP PROJECT

NETWORK SECURITY

Topic:

Introduction To Palo-Alto Firewall

Teacher : Msc. Dang Ngoc Lam

Class : CMU-CS 427 BIS

No	Name	ID	Grades
1	Lưu Đức Khánh	27211135267	
2	Bùi Hữu Khánh	27211142437	
3	Huỳnh Nguyễn Minh Phú	27211121671	
4	Phạm Hồng Sơn	27211138616	
5	Trần Thị Anh Vân	27201448217	

Danang, May 2024

CONTENT

1. Introduction to Palo-Alto firewall 1
    1.1. Overview 1
    1.2. Architecture 2
    1.3. Advantage and disadvantage of Palo-Alto Firewall 4
2. Features 5
3. Policy 7
    3.1. Policy rules 7
    3.2. Security Profile 7
        A. URL Filtering Basic 9
        B. URL Filtering Features 10
    3.3. NAT 10
4. Routing and Default Routing 12
    4.1. Routing 12
    4.2. Default Routing 12
5. IDS and IPS 13
    5.1. IDS (Intrusion Detection System) 13
    5.2. IPS (Intrusion Prevention System) 13
    5.3. IPS and IDS in Palo Alto Firewall 13
6. Log 14
    6.1. Log types 14
    6.2. Log Actions 16
7. Demo Palo Alto Firewall 18
    Topology 18
    Virtual Routers Configuration 20
    DHCP Relay 21
    Source NAT (NAT PAT) 21
    Destination NAT 25
    After creating the NAT rule, configure the corresponding Security rule, especially for the NAT overload scenario. 25
    Configure APP-ID Features 26
    URL Filtering - Custom URL 27
    External Dynamic Lists 30
    File Blocking 31
    Data Filtering 33
    DoS Protection 36
8. Reference 39

1. Introduction to Palo-Alto firewall

1.1. Overview

Palo Alto Networks next-generation firewalls inspect all traffic (including applications, threats, and content), and send that traffic to the user, regardless of location or device type. The user, application, and content-the elements that run the business - become integral components of the b n enterprise security policy. This allows users to align security with business policies, as well as write rules that are easy to understand and maintain.

As part of Security Operating Platform, the next-generation firewalls provide organization with the ability to:

- Securely enable applications (including software-as-a-service applications), users, and content by classifying all traffic (regardless of port).
- Reduce risk of an attack using a positive enforcement model, by allowing all desired applications and blocking everything else.
- Apply security policies to block known vulnerability exploits, viruses, ransomware, spyware, botnets, and other unknown malware, such as advanced persistent threats.
- Protect the data centers (including virtualized data centers) by segmenting data and applications, as well as enforcing the Zero Trust principle.
- Apply consistent security across on-premises and cloud environments.
- Embrace secure mobile computing by extending the Security Operating Platform to users and devices, no matter where they are located.
- Get centralized visibility and streamline network security, making the data actionable to prevent successful cyber attacks.
- Identify and prevent attempts to steal credentials by stopping the submission of valid corporate credentials to illegitimate websites, and neutralizing an attacker's ability to use stolen credentials for lateral movement or network compromise by enforcing authentication policies at the network layer.

New generation firewall, is a firewall device based on user authentication, application or content based authentication. With this mechanism, administrators can easily identify applications and content within the data stream and the level of threat coming from which user.

1.2. Architecture

Currently, security technology companies have launched new generation firewall products to help us have more options, but among security companies, Palo Alto Networks brings a difference in technology and innovation. The architecture is as follows:

- The Palo Alto Next-Generation Firewall device with its advanced and powerful architecture, combined with high-speed specialized hardware, provides outstanding security features, helping to overcome the disadvantages of the model. traditional firewall security and better meets current security requirements, becoming one of the effective security solutions today. Palo Alto is always highly rated and for four consecutive years (from 2011 to 2017) has been in the leading group of technology trends, according to Gartner's assessment.

- By supporting multiple deployment models on the same device at the same time: Tap Mode (monitoring), Virtual Wire Mode (in-line), L2 Mode, L3 Mode, customers will be very flexible in deployment as well as helps optimize and preserve investment and operating costs of network security solutions.

With single-stage parallel processing architecture – Single-Pass Parallel Processing™ (SP3) Architecture – Supports both hardware and software concurrently: single-stage parallel execution of all App-ID features, User-ID, Content-ID as well as having a dedicated processing chip (FPGA) for each separate task will help ensure high-speed processing performance with the lowest latency. Dedicated processor chips using FPGA technology allow reprogramming without the need to replace hardware, enhancing system stability and providing much faster response times than traditional solutions.

- Just one unified security policy that covers all tasks, helping customers simplify their entire security setup as well as provide proactive security with just a few clicks. Allows newly approved applications to operate in the system and automatically denies and prohibits access to unapproved software. At the same time, it will help customers minimize the risk of errors in security settings and minimize security vulnerabilities that exist in traditional solutions.

- Separating the control plane/data plane on the hardware architecture helps the system have high availability and not be interrupted when the throughput through the data processing block suddenly increases.

- With the ACC (Application Command Center) monitoring interface, network security administrators can monitor all applications running in the system, network security risks with detailed information (e.g. viruses), spyware, application and operating system vulnerabilities, botnets...) detect and prevent attacks accessing the system as well as have immediate access to relevant detailed log sections for

immediate solutions. In-depth information helps create accurate troubleshooting plans.

- WildFire solution helps proactively prevent APT (unknown malware) threats with a fast response time of 30 to 60 minutes to help minimize the risk of zero-day attacks. At the same time, it helps automatically update malware identification samples for Threat Prevention and update malware-sites for URL filtering filter, helping customers have comprehensive and proactive protection against next-generation malware threats. new.

- The ability to classify bandwidth (QoS) for each user and application as well as real-time bandwidth monitoring helps customers proactively reserve bandwidth for priority applications and users/user groups. high, ensuring real-time usability understanding.

- Remote access protection through GlobalProtect supports both IPSec and SSL VPN and is built into the device, helping customers not need to spend extra money on purchasing licenses for SSL VPN users, optimizing and preserving them. investment costs.

- With comprehensive and consistent protection for both physical and virtual environments, and consistent centralized administration and monitoring capabilities for both environments, security administrators can synchronize settings across both environments. two environments and proactively manage security as well as clearly separate responsibilities on the virtualized environment, which is set up and managed by the virtualization server administrator in traditional solutions.

- With the ability to create advanced reports built into the device, customers do not need to spend extra money to buy additional modules or separate software to create advanced reports like with traditional solutions.

- Palo Alto has the ability to control applications, users, and content using three advanced identification technologies: App-ID, User-ID and Content-ID.

Using four different data classification mechanisms, App-ID™ accurately identifies which applications are actually running on the network infrastructure regardless of what service port or protocol the application is running on. any, or whether it is SSL encrypted or not.

- Content-ID is a stream-based scanning engine that helps detect and block threats and limit unauthorized transfers of data files and sensitive content.

- User-ID allows administrators to associate user information with applications, create policies, log data and report. Furthermore, this has helped Palo Alto solve integration and processing challenges that many other NG-Firewalls have not been able to solve.

1.3. Advantage and disadvantage of Palo-Alto Firewall

1.3.1. Disadvantages of Palo Alto Traditional Palo-AltoFirewall

As the main model commonly used globally, however, the traditional firewall security model has some disadvantages as follows:

- It is impossible to read and understand each type of information and analyze its good or bad content. It is only possible to prevent the intrusion of unwanted information sources but must clearly define the address parameters.

- It is impossible to stop an attack if it does not pass through it, such as attacks from within.

- Cannot resist attacks by viruses, malware…

- Only identifies and controls throughput with protocols and service ports, but cannot identify applications, especially web applications that use the same HTTP protocol and service port 80.

With the limitations of the traditional firewall security model, along with the strong and continuous development of attack techniques, there is a need for an upgraded, optimized and smarter security model. to ensure system safety against threats. From there, a new generation firewall solution was born.

The Palo Alto Next-Generation Firewall device with its advanced and powerful architecture, combined with high-speed specialized hardware, provides outstanding security features, helping to overcome the disadvantages of the model. traditional firewall security and better meets current security requirements, becoming one of the effective security solutions today. Palo Alto is always highly rated and for four consecutive years (from 2011 to 2017) has been in the leading group of technology trends, according to Gartner's assessment.

1.3.2. Advantages The Next Generation Palo-Alto Firewall

The new generation Firewall has many features that allow network administrators to have comprehensive control over their network:

- Identify applications in the system that do not depend on ports or network protocols, helping to accurately identify and secure smart applications that can switch ports or network protocols to operate to avoid control. control of security systems.

- Enables policies to be deployed based on user or user group identity rather than just checking the network's IP address.

- Integrated attack prevention technology protects the system in real-time against attacks and malicious software embedded in applications as well as security vulnerabilities of applications or operating systems. operate in the system.

- Friendly interface, making the management of system protection policies simpler, as well as allowing customization of detailed visual reports linking the user to the application and potential threats. – helps administrators gain an overview and help make decisions faster and more timely.

- Simultaneous multi-threaded architecture helps ensure overall system performance in the order of gigabits per second, ensuring minimal latency even with all active features enabled.

2. Features

The Palo Alto Networks next-generation firewalls provide granular control over the traffic allowed to access the network. The primary features and benefits include:

- **Application-based policy enforcement (App-ID)** - Access control according to application type is far more effective when application identification is based on more than just protocol and port number. The App-ID service can block high risk applications, as well as high risk behavior, such as file-sharing, and traffic encrypted with the Secure Sockets Layer (SSL) protocol can be decrypted and inspected.
- **User identification (User-ID)** - The User-ID feature allows administrators to configure and enforce firewall policies based on users and user groups instead of or in addition to network zones and addresses. The firewall can communicate with many directory servers, such as Microsoft Active Directory, eDirectory, SunOne, OpenLDAP, and most other LDAP-based directory servers to provide user and group information to the firewall. This information can be used for secure application enablement that can be defined per user or group. For example, the administrator could allow one organization to use a web-based application but not allow any other organizations in the company to use that same application. Administrators can also configure granular control of certain components of an application based on users and groups (see User Identification).
- **Threat prevention**—Threat prevention services that protect the network from viruses, worms, spyware, and other malicious traffic can be varied by application and traffic source (see Objects > Security Profiles).
- **URL filtering**—Outbound connections can be filtered to prevent access to inappropriate websites (see Objects > Security Profiles > URL Filtering).
- **Traffic visibility**—Extensive reports, logs, and notification mechanisms provide detailed visibility into network application traffic and security events. The Application Command Center (ACC) in the web interface identifies the applications with the most traffic and the highest security risk (see Monitor).
- **Networking versatility and speed**—The Palo Alto Networks firewall can augment or replace the existing firewall and can be installed transparently in any network or

configured to support a switched or routed environment. Mulgigabit speeds and a single-pass architecture provide these services to clients with little or no impact on network latency.

- **GlobalProtect** - The GlobalProtect™ software provides security for client systems, such as laptops that are used in the field, by allowing easy and secure login from anywhere in the world.
- **Fail-safe operation** - High availability (HA) support provides automatic failover in the event of any hardware or software disruption (see Device > Virtual Systems).
- **Malware analysis and reporting** - The WildFire™ cloud-based analysis service provides detailed analysis and reporting on malware that passes through the firewall. Integration with the AutoFocus™ threat intelligence service allows assessing the risk associated with network traffic at organization, industry, and global levels.
- **VM-Series firewall** - A VM-Series firewall provides a virtual instance of PAN-OS poisoned for use in a virtualized data center environment and is ideal for private, public, and hybrid cloud computing environments.

3. Policy

3.1. Policy rules

Policies enable control firewall operation by enforcing rules and automatic actions. The firewall supports the following policy types:

- **Security**: Determine whether to block or allow a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service.

- **Network Address Translation (NAT)**: Translating addresses and ports.

- **Quality of Service (QoS):** Identify traffic requiring QoS treatment (either preferential treatment or bandwidth-limiting) using a defined parameter or multiple parameters and assign it a class.

- **Policy Based Forwarding:** Identify traffic that should use a different egress interface than the one that would normally be used based on the routing table.

- **Decryption**: Identify encrypted traffic that you want to inspect for visibility, control, and granular security.

- **Application Override**: Identify sessions to bypass App-ID layer 7 processing and threat inspection. Traffic that matches an application override policy forces the firewall to handle the session as a stateful inspection firewall at layer 4. Only use Application Override when needed and in the most highly trusted environments where users can apply the principle of least privilege strictly.

- **Authentication**: Identify traffic that requires users to authenticate.

- **DoS Protection**: Identify potential denial-of-service (DoS) attacks and take protective action in response to rule matches.

3.2. Security Profile

3.2.1. Profile overview

Security Policies allow/block traffic, while Security Profiles scan allowed traffic for threats like malware. Security Profiles are applied after the Security Policy allows the traffic.

The firewall provides default Security Profiles, but custom ones can be created. There are best practice recommendations for configuring Security Profiles. Security Profile Groups apply multiple Profiles together in one step.

3.2.2. Profile type

- **Antivirus Profiles**: Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads. Using a stream-based malware prevention engine, which inspects traffic the moment the first packet is received, the Palo Alto

Networks antivirus solution can provide protection for clients without significantly impacting the performance of the firewall. This profile scans for a wide variety of malware in executables, PDF files, HTML and JavaScript viruses, including support for scanning inside compressed files and data encoding schemes. If you have enabled Decryption on the firewall, the profile also enables scanning of decrypted content.

- **Anti-Spyware Profiles**: Anti-Spyware profiles block spyware on compromised hosts from trying to phone-home or beacon out to external command and control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between zones. For example, you might want to have custom Anti-Spyware profiles that minimize inspection between trusted zones, while maximizing inspection on traffic received from an untrusted zone, such as internet-facing zones.

- **Vulnerability Protection Profiles**: Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorized access to systems. While Anti-Spyware profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection profiles protect against threats entering the network

- **URL Filtering Profiles**: The filtering address allows tracking and controlling how users access the web via HTTP and HTTPS. The firewall comes with a default configuration to block websites known as malware website, scam websites and adult content site. You can use the default configuration in the rules of privacy policy, copy it to use as the starting point for the new URL filtration configuration or the new URL will have all the categories placed to allow for permission to Show in online traffic. After that, the new customization has added the URL configuration and the list of specific websites that need to be blocked or allowed, providing more detailed control through the URL category.

- **Data Filtering Profiles**: Data filtering data to prevent sensitive information such as credit cards or social security numbers leaving the network is protected. Data filtration configuration also allows filtering keywords, such as sensitive project names or secret words. It is important to focus records on the desired files to reduce positives.

- **File Blocking Profiles**: The firewall uses file blocking configurations to block the specified files through the specified applications and in the direction of the specified session (sent/outside/both). The application may be placed in a warning or blocking mode when uploading and/or downloading and you may specify which application will follow the file block configuration. It is also possible to configure customized pages that will appear when the user tries to download the specified file type. This allows users to spend some time considering whether they want to download a file.

- **WildFire Analysis Profiles**: Use a WildFire Analysis profile to enable the firewall to forward unknown files or email links for WildFire analysis. Specify files to be forwarded for analysis based on application, file type, and transmission direction (upload or download). Files or email links matched to the profile rule are forwarded to either the WildFire public cloud or the WildFire private cloud (hosted with a WF-500 appliance), depending on the analysis location defined for the rule. If a profile rule is set to forward files to the WildFire public cloud, the firewall also forwards files that match existing antivirus signatures, in addition to unknown files.

- **DoS Protection Profiles**: DoS Protection profiles provide detailed control for Denial of Service (DoS) protection policy rules. DoS policy rules allow you to control the number of sessions between interfaces, zones, addresses, and countries based on aggregate sessions or source and/or destination IP addresses. There are two DoS protection mechanisms that the Palo Alto Networks firewalls support.

- **Zone Protection Profiles**: Zone Protection Profiles provide additional protection between specific network zones to protect the zones against attack. The profile must be applied to the entire zone, so it is important to carefully test the profiles to prevent issues that might arise with the normal traffic traversing the zones. When defining connections per second (cps) thresholds limits for zone protection profiles, the threshold is based on the packets per second that do not match a previously established session.

- **Security Profile Group**: A group of security documents is a collection of security records that are considered a unit and then easily added to the privacy policy rules. Applications are often assigned together to be added to the groups of documents to simplify the creation of security policies. Setting a group of default security documents, new security policies will use the settings determined in the default file group to check and control traffic in accordance with the main rules. Security book. Name a group of default security documents to allow the configuration in that group to be added to new security policies by default. This allows you to automatically include favorite documents in new policy rules without having to add security records every time you create a new rule.

3.2.3. URL Filtering

A. URL Filtering Basic

URL filtering technology protects users from web-based threats by providing granular control over user access and interaction with content on the Internet. Developing a URL filtering policy that limits access to sites based on URL categories, users, and groups.

For granular control over user access to categories, create a URL Filtering profile and define site access for predefined and custom URL categories; then, apply the profile to Security policy rules. Also using URL categories as match criteria in Security policy rules. URL Filtering Use Cases:

- Palo Alto Networks URL Filtering Solution
- URL Filtering Support
- Local Inline Categorization
- How Advanced URL Filtering Works
- URL Filtering Profiles
- URL Categories
- URL Filtering Use Cases

B. URL Filtering Features

After configuring the basic components of the URL filtering deployment, consider configuring the following features:

- Inline Categorization
- SSL/TLS Handshake Inspection
- URL Admin Override
- Credential Phishing Prevention
- URL Filtering Response Pages
- Safe Search Enforcement
- Remote Browser Isolation (RBI) Integration (Prisma Access only)

3.3. NAT

3.3.1. NAT Overview

If Layer 3 interfaces are defined on the firewall, configure a Network Address Translation (NAT) policy to specify whether source or destination IP addresses and ports are converted between public and private addresses and ports. For example, private source addresses can be translated to public addresses on traffic sent from an internal (trusted) zone to a public (untrusted) zone. NAT is also supported on virtual wire interfaces.

NAT rules are based on source and destination zones, source and destination addresses, and application service (such as HTTP). Like security policies, NAT policy rules are compared against incoming traffic in sequence, and the first rule that matches the traffic is applied.

As needed, add static routes to the local router so that traffic to all public addresses is routed to the firewall. May also need to add static routes to the receiving interface on the firewall to route traffic back to the private address.

The following tables describe the NAT and NPTv6 (IPv6-to-IPv6 Network Prefix Translation) settings:

- NAT Policies General Tab
- NAT Original Packet Tab
- NAT Translated Packet Tab
- NAT Active/Active HA Binding Tab

3.3.2. NAT Policy Match

Field	Description
Select Test	Select the policy match test to execute.
From	Enter the zone where the traffic originated.
To	Select the destination zone of the traffic.
Source	Enter the IP address where the traffic originated.
Destination	Enter the destination IP address of the traffic.
Source Port	Enter the specific port the traffic originated from.
Destination Port	Enter the specific destination port for which traffic is intended.
Protocol	Enter the IP protocol used for routing. Can be 0 to 255.
To Interface	Enter the destination interface on the device for which the traffic is intended.
HA Device ID	Enter the ID of the HA device: - 0—Primary HA peer - 1—Secondary HA peer

4. Routing and Default Routing

4.1. Routing

Routing is essential for a firewall that is deployed in layer 3 mode. Palo Alto Firewall supports static as well as dynamic routing such as RIP, OSPF, BGP.

- The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.

- Open Shortest Path First (OSPF) to enable a logical router to determine the most cost efficient links to a traffic destination. OSPF determines routes dynamically by obtaining information from other routers and advertising routes to other routers by way of Link State Advertisements (LSA). The router keeps information about the links between it and the destination to make highly efficient routing decisions. A cost is assigned to each router interface, and the best routes are determined to be those with the lowest cost, when summed over all the encountered outbound interfaces and the interface receiving the LSA.

- Border Gateway Protocol (BGP) is the primary internet routing protocol. BGP determines network reachability based on IP prefixes that are available within autonomous systems (AS), where an AS is a set of IP prefixes that a network provides has designated to be a part of a single routing policy rule.

4.2. Default Routing

Configure a static route for a logical router to configure Layer 3 traffic to take a certain route without participating in IP routing protocols. A default route is a specific static route. If dynamic routing is not used to obtain a default route for the logical router, a static default route must be configured. When the logical router has an incoming packet and finds no match for the packet destination in its route table, the logical router sends the packet to the default route. The default IPv4 route is 0.0.0.0/0; only a IPv4 default route is supported.

By default, static routes have an administrative distance of 10. When the firewall has two or more routes to the same destination, it uses the route with the lowest administrative distance. By increasing the administrative distance of a static route to a value higher than a dynamic route, use the static route as a backup route if the dynamic route is unavailable.

While configuring a static route, specify whether the firewall installs an IPv4 static route in the unicast or multicast route table (RIB), or both tables, or doesn’t install the route at all.

5. IDS and IPS

5.1. IDS (Intrusion Detection System)

- Main function: IDS is responsible for monitoring and analyzing network traffic to detect suspicious activities or potential attacks.

- Action: IDS does not prevent attacks but only records and alerts network administrators about unusual or suspicious events.

- Operational mechanism: IDS works by using signatures to compare with known attack patterns, or by behavioral analysis to identify unusual activities.

5.2. IPS (Intrusion Prevention System)

- Main function: IPS also monitors and analyzes network traffic like IDS, but in addition, it has the ability to prevent attacks when they are detected.

- Active: IPS proactively blocks threats by dropping packets, blocking connections, or hindering malicious actions.

- Operational mechanism: IPS uses both signatures and behavioral analysis to detect attacks, then deploy appropriate prevention measures.

5.3. IPS and IDS in Palo Alto Firewall

- Integration: On Palo Alto's firewall, both IDS and IPS are integrated into the Threat Prevention module. These features not only detect but also prevent threats, providing comprehensive network protection.

- Management and Configuration: Administrators can configure policies and rules to determine how threats are handled. The system can be set up to only warn or to both warn and prevent.

- Updates: Signatures and threat databases are regularly updated by Palo Alto Networks to ensure detection and blocking of the latest threats.

6. Log

6.1. Log types

- **Traffic**: Displays an entry for the start and end of each session. Each entry includes the date and time, source and destination zones, addresses and ports, application name, security rule name applied to the flow, rule action (allow, deny, or drop), ingress and egress interface, number of bytes, and session end reason.

The Type column indicates whether the entry is for the start or end of the session, or whether the session was denied or dropped. A “drop” indicates that the security rule that blocked the traffic specified “any” application, while a “deny” indicates the rule identified a specific application.

If traffic is dropped before the application is identified, such as when a rule drops all traffic for a specific service, the application is shown as “not-applicable”.

- **Threat**: Displays an entry for each security alarm generated by the firewall. Each entry includes the date and time, a threat name or URL, the source and destination zones, addresses, and ports, the application name, security rule name applied to the flow, and the alarm action (allow or block) and severity.

The Type column indicates the type of threat, such as “virus” or “spyware;” the Name column is the threat description or URL; and the Category column is the threat category (such as “keylogger”) or URL category.

- **URL Filtering:** Displays logs for URL filters, which control access to websites and whether users can submit credentials to websites.

Select Objects > Security Profiles > URL Filtering to define URL filtering settings, including which URL categories to block or allow and to which are wanted to grant or disable credential submissions. Can also enable logging of the HTTP header options for the URL.

- **WildFire Submissions:** Displays logs for files and email links that the firewall forwarded for WildFire analysis. The WildFire cloud analyzes the sample and returns analysis results, which include the WildFire verdict assigned to the sample (benign, malware, grayware, or phishing). It is possible to confirm if the firewall allowed or blocked a file based on Security policy rules by viewing the Action column.

- **Data Filtering**: Displays logs for the security policies with cached Data Filtering profiles, to help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall, and File Blocking profiles, that prevent certain file types from being uploaded or downloaded.

- **HIP Match**: Displays all HIP matches that the GlobalProtect™ gateway identifies when comparing the raw HIP data reported by the agent to the defined HIP objects and HIP profiles. Unlike other logs, a HIP match is logged even when it does not match a security policy.

- **GlobalProtect:** Displays GlobalProtect connection logs. Use this information to identify the GlobalProtect users and their client OS version, troubleshoot connection and performance issues, and identify the portal and gateways to which users connect

- **IP-Tag**: Displays information about how and when a tag was applied to a particular IP address. Use this information to determine when and why a particular IP address was placed in an address group and what policy rules impact that address. The log includes Receive Time (the date and time when the first and last packet of the session arrived), Virtual System, Source IP-Address, Tag, Event, Timeout, Source Name, and Source Type.

- **User-ID**: Displays information about IP address-to-username mappings, such as the source of the mapping information, when the User-ID agent performed the mapping, and the remaining time before mappings expire. This information can be used to help troubleshoot User-ID issues.

- **Decryption:** Displays information about decryption sessions and undecrypted sessions for traffic that a No Decryption profile controls, including GlobalProtect sessions.

By default, the logs show information about unsuccessful SSL Decryption handshakes. Enable logging for successful SSL Decryption handshakes in Decryption Policy rules Opons. Logs display a wealth of information that enables identify weak protocols and cipher suites (key exchange, encryption, and authentication algorithms), bypassed decryption activity, decryption failures and their causes (e.g., incomplete certificate chain, client authentication, pinned certificates), session end reasons, and more. For traffic the firewall doesn't decrypt and to which apply a No Decryption profile, the log shows sessions blocked because of server certificate verification issues.

- **GTP**: Displays event-based logs that include information on the wide range of GTP attributes. These include GTP event type, GTP event message type, APN, IMSI, IMEI, End User IP address, in addition to the TCP/IP information that the next-generation firewall identifies such as application, source and destination address and timestamp.

- **Tunnel Inspection**: Displays an entry for the start and end of each inspected tunnel session. The log includes the Receive Time (date and time the first and last packet in the session arrived), Tunnel ID, Monitor Tag, Session ID, Security rule applied to the tunnel traffic, and more.

- **SCTP**: Displays SCTP events and associations based on logs generated by the firewall while it performs stateful inspection, protocol validation, and filtering of SCTP traffic. SCTP logs include information on the wide range of SCTP and its payload protocol attributes, such as SCTP event type, chunk type, SCTP cause code, Diameter Application ID, Diameter Command Code, and chunks. This SCTP information is provided in addition to the general information that the firewall identifies, such as source and destination address, source and destination port, rule, and timestamp.

- **Configuration**: Displays an entry for each configuration change. Each entry includes the date and time, the administrator username, the IP address from where the change was made, the type of client (web interface or CLI), the type of command executed, whether the command succeeded or failed, the configuration path, and the values before and aer the change.

- **System**: Displays an entry for each system event. Each entry includes the date and time, the event severity, and an event description.

- **Alarms**: The alarms log records detailed information on alarms that are generated by the system. The information in this log is also reported in Alarms.

- **Authentication**: Displays information about authentication events that occur when end users try to access network resources for which access is controlled by Authentication policy rules. Use this information to help troubleshoot access issues and to adjust the Authentication policy as needed. In conjunction with correlation objects, Authentication logs can also be used to identify suspicious activity on the network, such as brute force attacks.

- **Unified**: Displays the latest Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering log entries in a single view. The collective log view enables investigating and filtering these different types of logs together (instead of searching each log set separately). Or, choose which log types to display: click the arrow to the left of the filter field and select traffic, threat, url, data, and/or wildfire to display only the selected log types.

The firewall displays all logs so that role-based administration permissions are respected. When viewing Unified logs, only the logs that have permission to see are displayed.

6.2. Log Actions

6.2.1 Filter Logs

Each log page has a filter field at the top of the page. Add artifacts to the field, such as an IP address or a time range, to find matching log entries. The icons to the right of the field enable applying, clearing, creating, saving, and loading filters.

6.2.2. Export Logs

Export all logs matched to the current filter to a CSV-formatted report and continue to the Download file. By default, the report contains up to 2,000 lines of logs. To change the line limit for generated CSV reports, select Device > Setup > Management > Logging and Reporting Settings > Log Export and Reporting and enter a new Max Rows in CSV Export value.

6.2.3. Highlight Policy Actions

Select to highlight log entries that match the action. The filtered logs are highlighted in the following colors:

- Green - Allow.
- Yellow - Continue, or override.
- Red - Deny, drop, drop-icmp, rst-client, reset-server, reset-both, block continue, block-override, block-url, drop-all, sinkhole.

6.2.4. Change Log Display

To customize the log display:

- Change the automatic refresh interval - Select an interval from the interval drop-down (60 seconds, 30 seconds, 10 seconds, or Manual).
- Change the number and order of entries displayed per page - Log entries are retrieved in blocks of 10 pages.
- Use the paging controls at the boom of the page to navigate through the log list.
- To change the number of log entries per page, select the number of rows from the per page drop-down (20, 30, 40, 50, 75, or 100).
- To sort the results in ascending or descending order, use the ASC or DESC drop-down.
- Resolve IP addresses to domain names - Select Resolve Hostname to begin resolving external IP addresses to domain names.
- Change the order in which logs are displayed - Select DESC to display logs in descending order beginning with log entries with the most recent Receive Time. Select ASC to display logs in ascending order beginning with log entries with the oldest Receive Time.

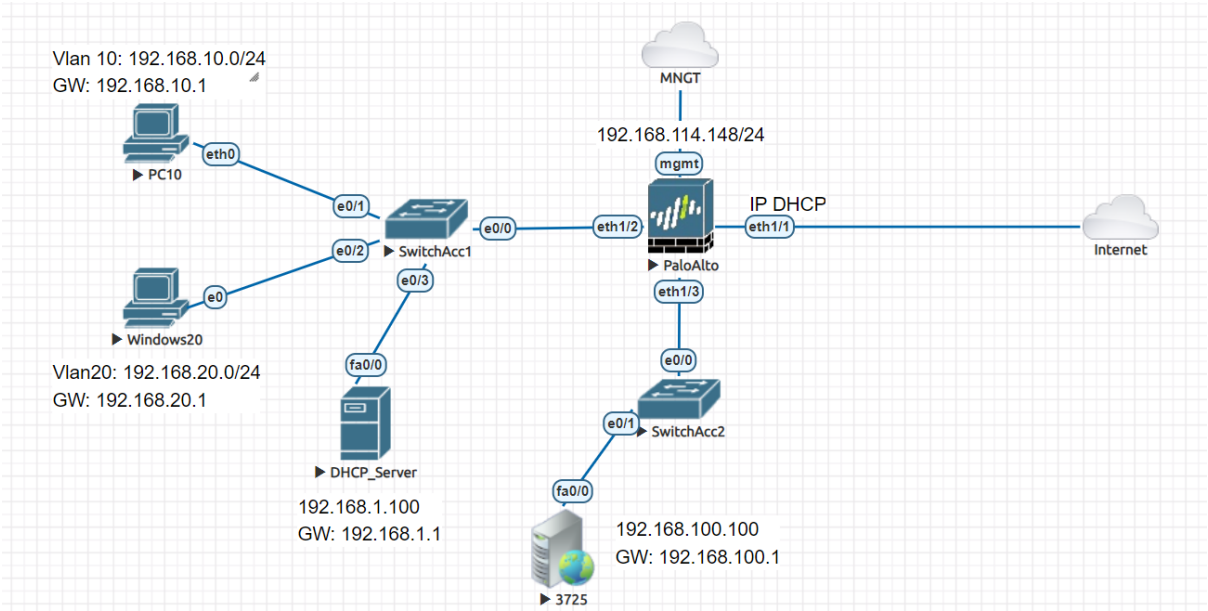
6.2.5. View Details for Individual Log Entry

To view information about individual log entries.

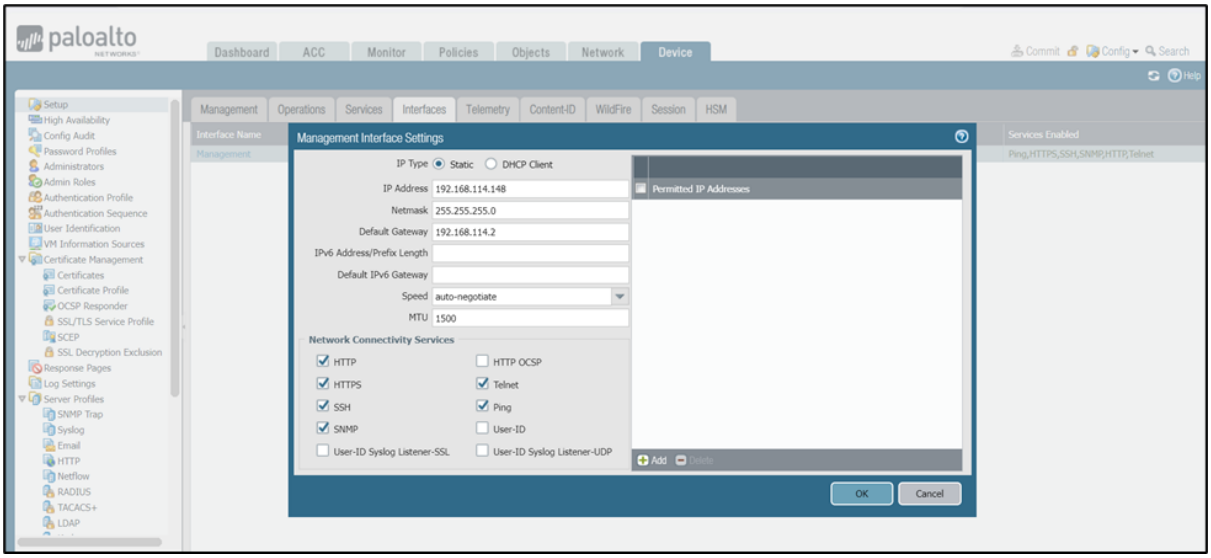
7. Demo Palo Alto Firewall

Deploying Palo Alto 8.0 on EVE-NG.

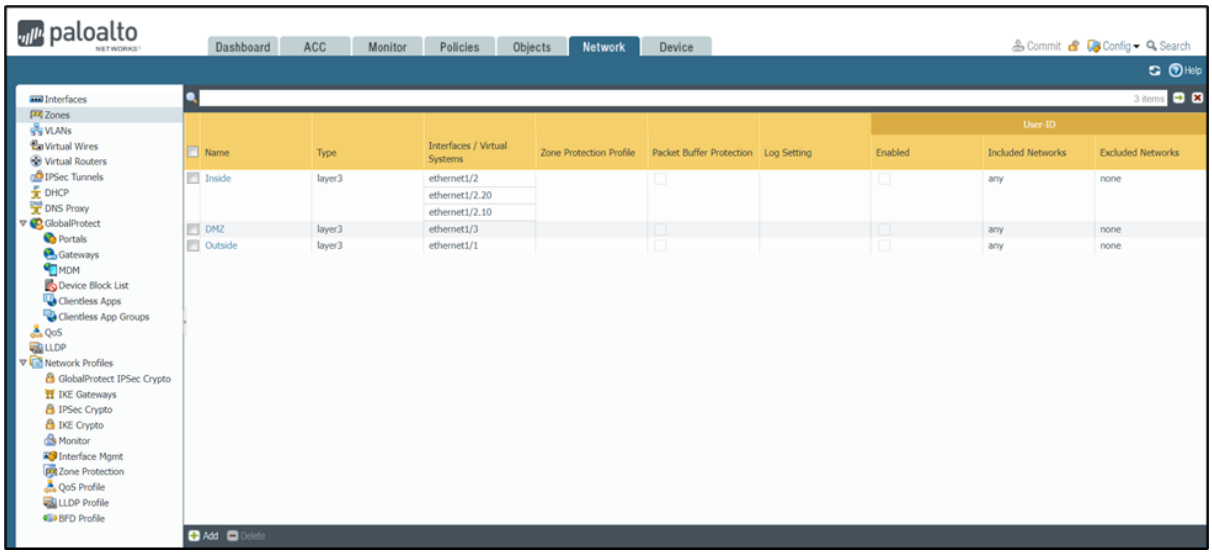
Topology



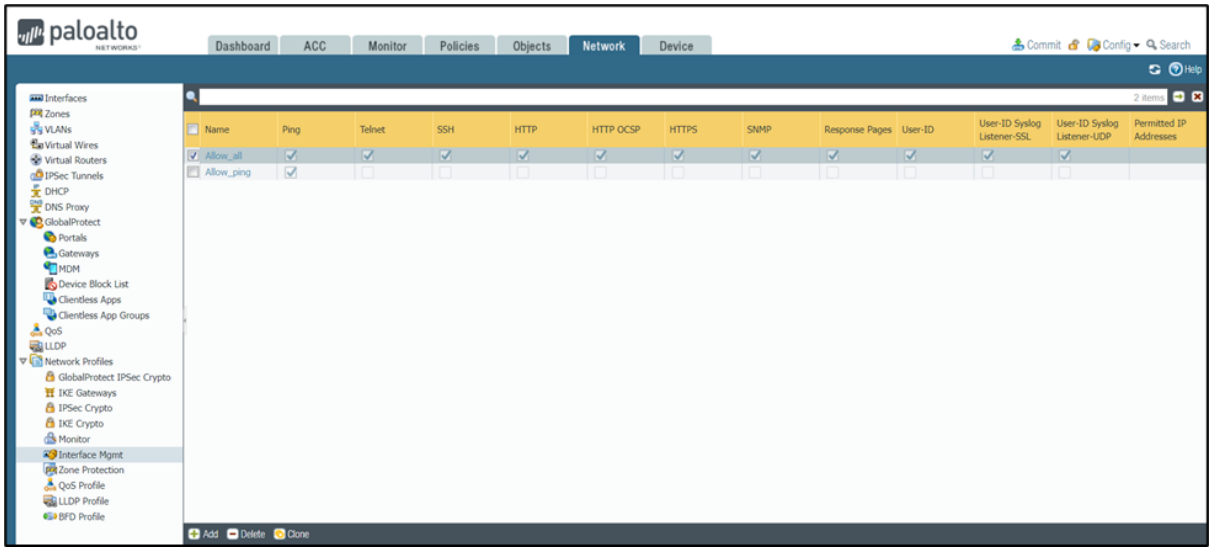
- Configure Ip for Management Interface.



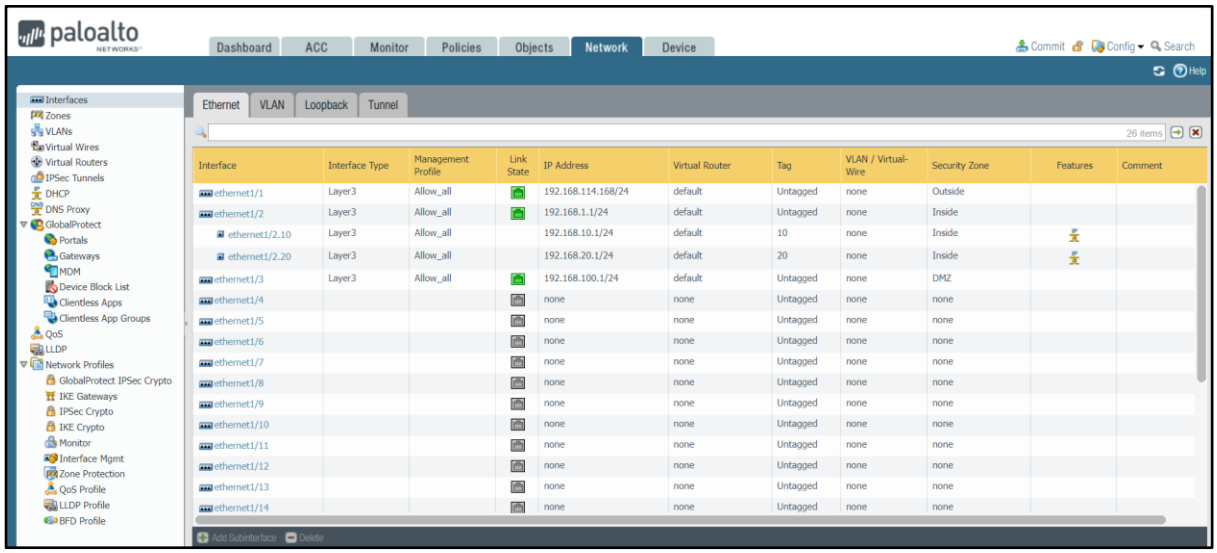
- Create Zones: Inside (Trusted), Outside (Untrusted) and DMZ.



- Create management profiles.

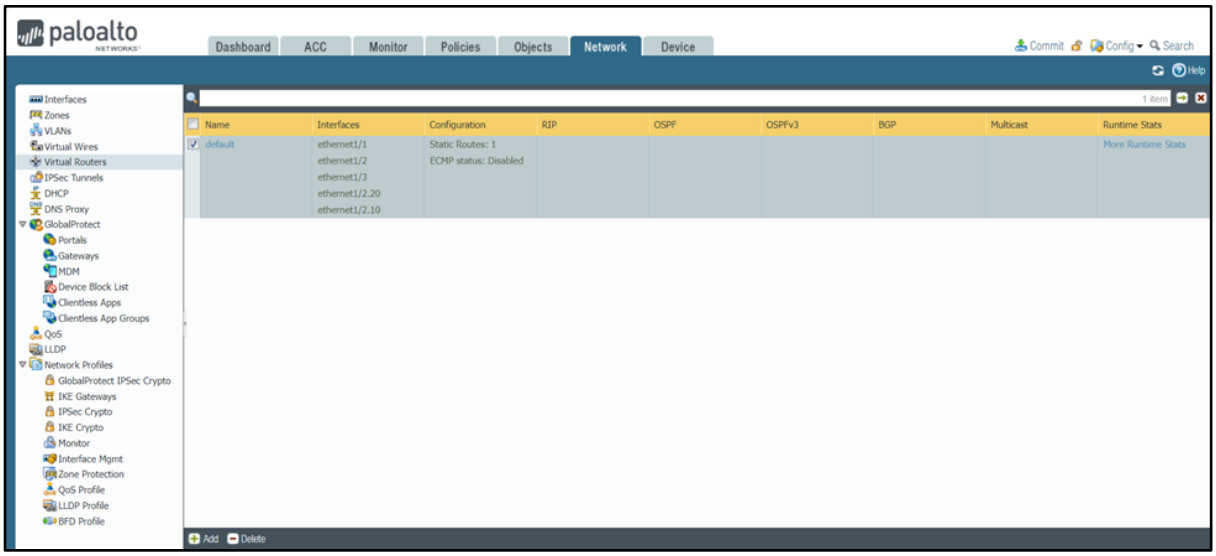


- Configure ip for Interfaces.



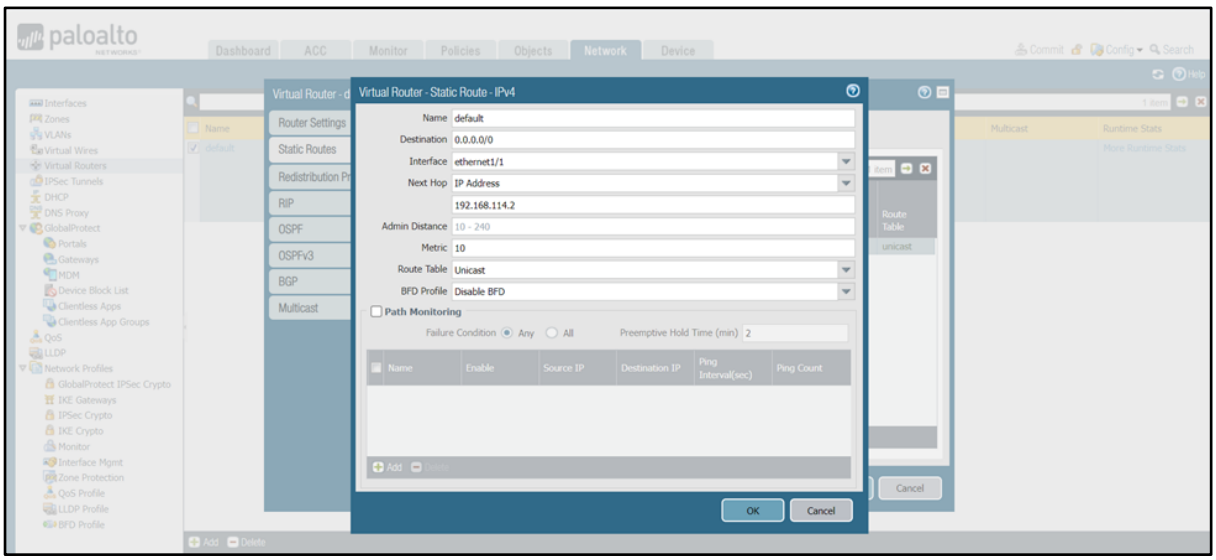
Virtual Routers Configuration

To configure a static route on a PAN VM-series, go to **Network > Virtual Routers > Select** the appropriate **VRF**.



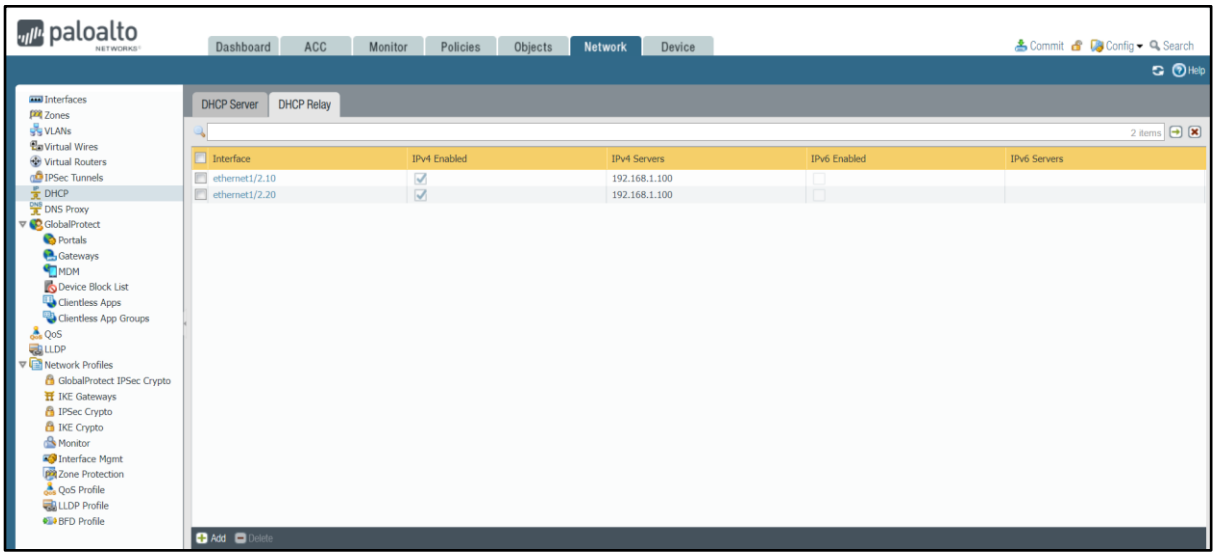
In the **Static Route**, fill in the following information:

- **Name**: The name of the static route.
- **Destination**: Specify the destination address or network to be routed to..
- **Interface**: Select the interface that will be responsible for sending the packets to the route.
- **Next Hop**: Enter the IP address that the packets will be sent to for this route.



DHCP Relay

- Select **Network > DHCP > DHCP Relay**.
- **Add > Choose Interface > Fill** in Ipv4 or IPv6 of DHCP Server.



Source NAT (NAT PAT)

NAT (NAT architecture is handled before Security Rule, so after configuring NAT, additional Security Rule needs to be configured to allow it to operate).

To configure NAT, go to **Policies > NAT > Add**.

In the General tab, configure the following information to define the NAT:

- Name: Enter a name for the NAT rule.
- Group Rules By Tag: This allows administrators to group NAT rules by tags, making it easier to manage and configure them.
- NAT Type: Specify the type of NAT that will operate on the IP address.

In the Original Packet tab, define the traffic that will be subject to NAT:

- Source Zone: Specify the zone from which the traffic originates.
- Destination Zone: Specify the zone to which the traffic is destined.
- Destination Interface: Specify the interface that will handle the destination traffic.
- Service: Specify the service of the traffic that will be matched for NAT.
- Source Address: Specify the source address of the traffic.
- Destination Address: Specify the destination address of the traffic.

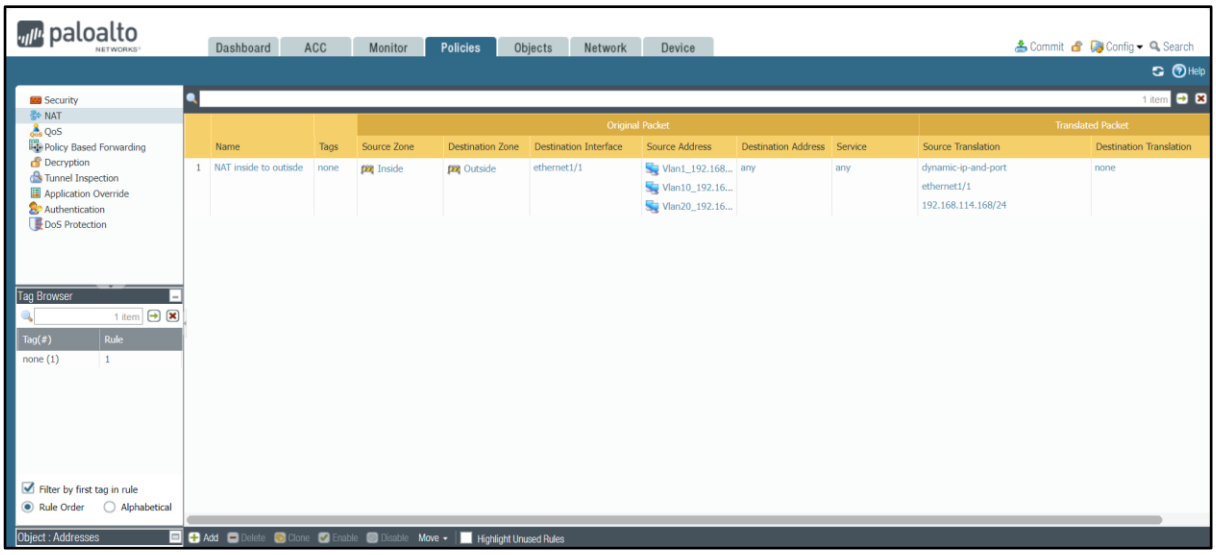
Note: If "any" is selected, it means match all traffic. This configuration is similar to a security rule to determine which traffic will be NAT'ed.

Next, in Translated tab:

- Translate Types: Supports Dynamic IP and Port (Selects an available address from a pool based on a hash of the source IP address), Dynamic

IP (Translates to the next available address in a specified pool, but port numbers remain unchanged), Static IP (The same address is always used for translation, and the port does not change)

- Address Type: Depending on the Translate Type, the available parameters may vary. For NAT overload scenarios, the translation will be based on the IP address of the interface.
- Interface: Select the interface that will be responsible for performing the translation.
- IP Address: Specify the IP address of the interface that will handle the translation.

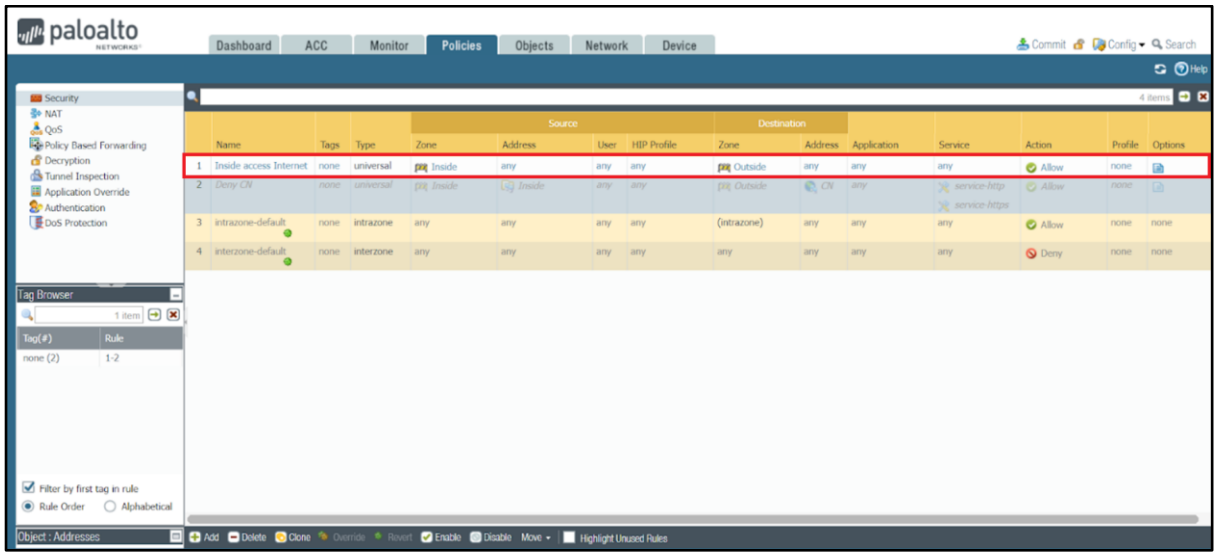


After creating the NAT rule, configure the corresponding Security rule, especially for the NAT overload scenario.

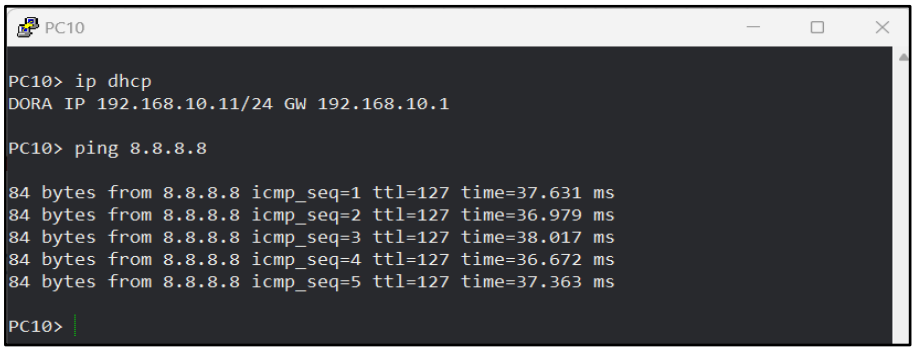
- Source Zone: Specify the zone from which the traffic originates.
- Destination Zone: Specify the zone to which the traffic is destined.
- Source Address: Specify the source address or address group.
- Destination Address: Specify the destination address or address group.
- Service: Specify the service or service group.
- Action: Set the action to "Allow" to permit the traffic.

Notes:

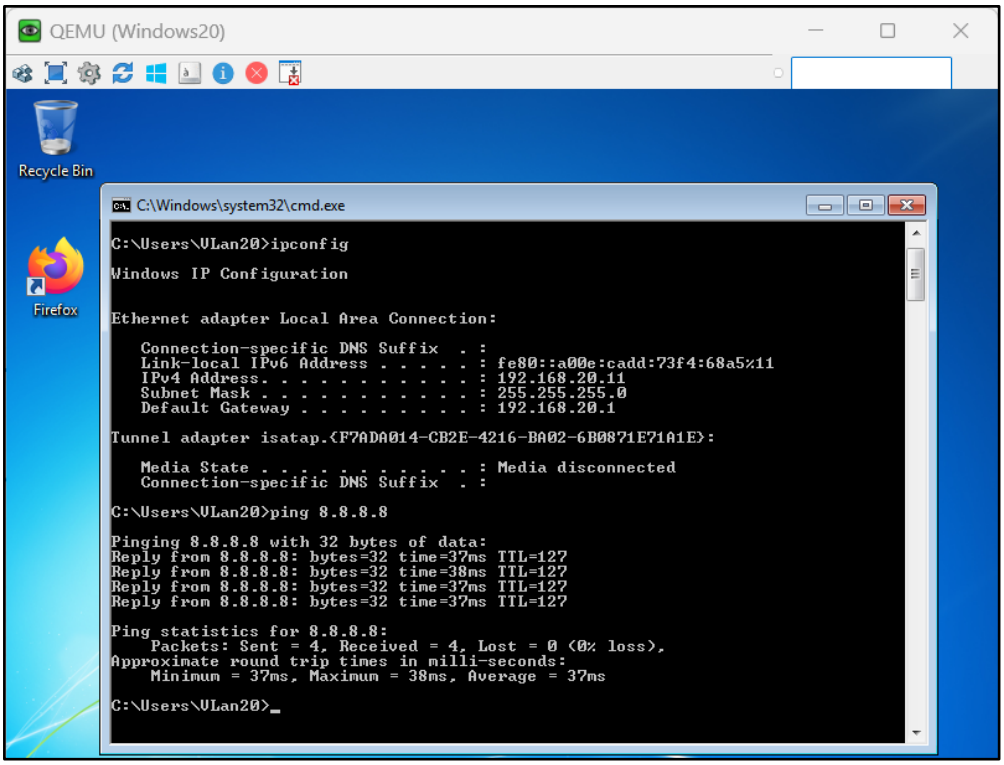
- Inside: Traffic coming from Local Area Network
- Outside: Traffic coming from Wide Area Network.
- DMZ: DMZ zone that contains WebServer, Linux Server, FTP Server.
- Intrazone: Traffic that originates and terminates within the same security zone on the firewall.
- Interzone: Traffic flowing between different security zones.
- Universal: Intrazone & Interzone combined.



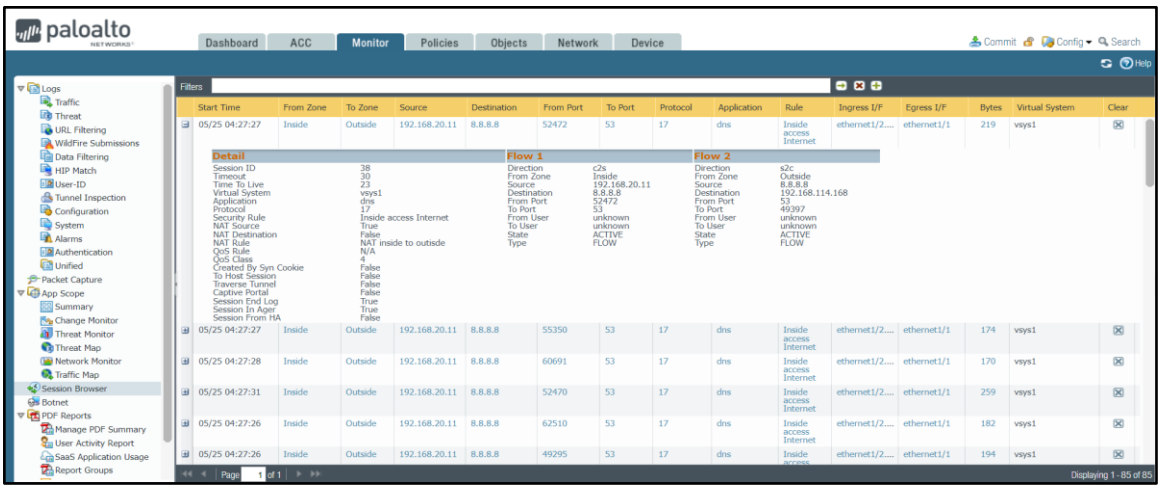
- Request IP DHCP at PC10 and ping to 8.8.8.8 → Successful.



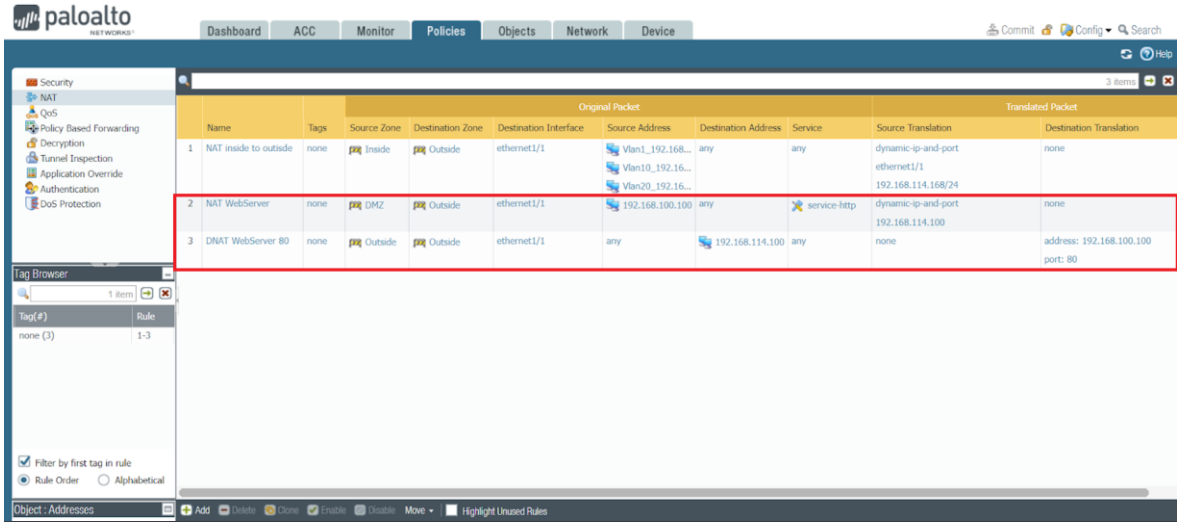
- Request IP DHCP at PC20 and ping to 8.8.8.8 → Successful.



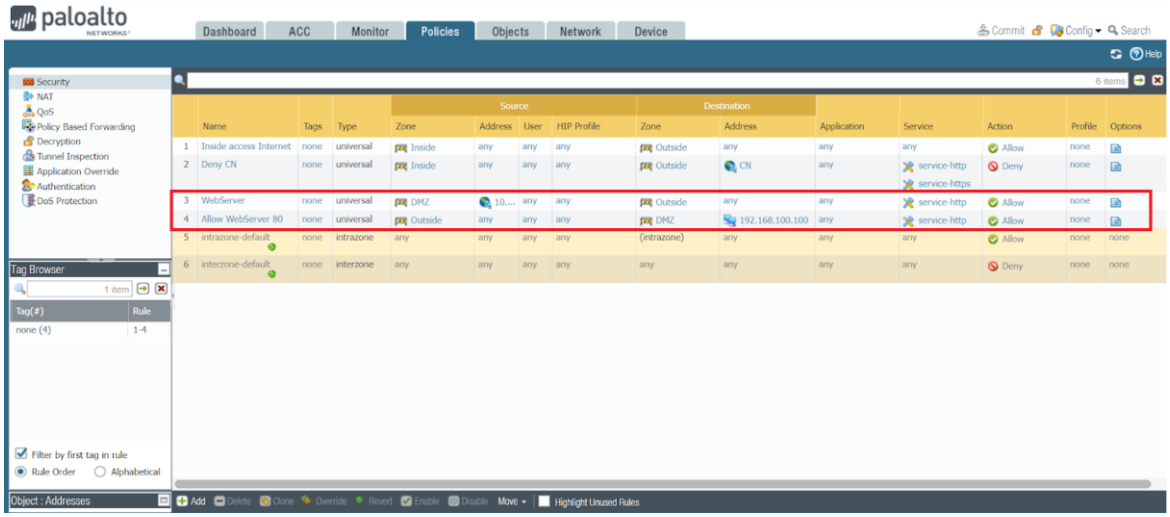
- Check the connected sessions to the internal server in the **Monitor > Session Browser.** → NAT Activated.



Next, to create a static SNAT rule that allows access based on an ip other than the IP on the outside port (can be an alias ip or an ip provided by the network), do the same as above.



- Create Security Policies.



Destination NAT

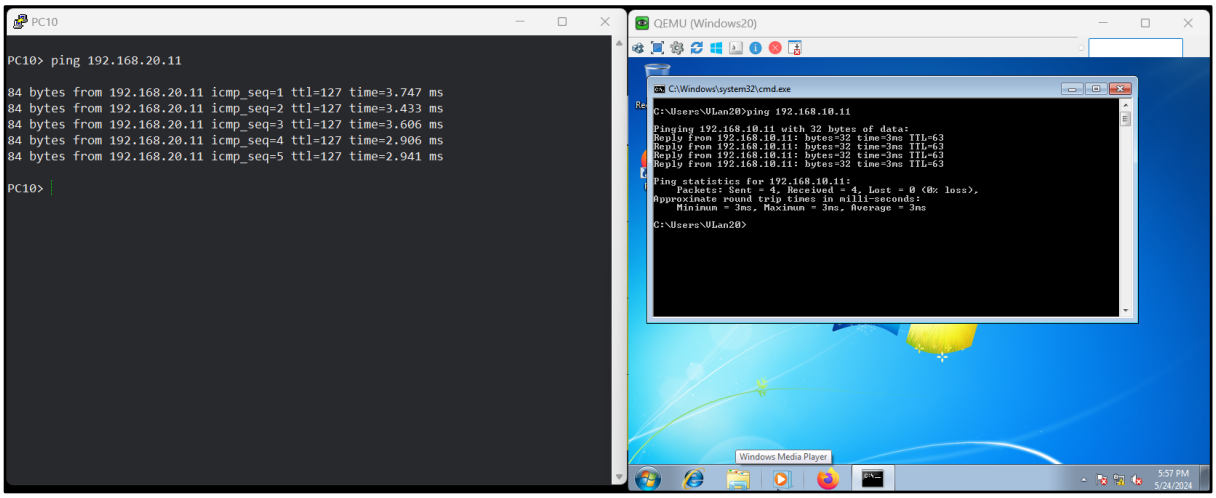
- General Tab (Go to **Policies > NAT > General**).
  Select the General tab to configure a name and description for the NAT.
    + Name: Enter a name to identify the rule.
    + Description: Enter a description for the rule.
    + Tag: Add and specify the tag. A policy tag is a keyword or phrase that allows you to sort or filter policies. This is useful when you have defined many policies and want to view those that are tagged with a particular keyword.
    + NAT Type: Specify the type of translation:
- Original Packet.
    + Source Zone: Outside.
    + Destination Zone: Outside.
    + Destination Interface: ethernet1/1.
    + Service: service-http.
    + Source Address: Any.
    + Destination Address: 192.168.114.100
- Translated Packet.
    + Source Address Translation: None.
    + Destination Address Translation: 192.168.100.100.
    + Translated Port: 80.

After creating the NAT rule, configure the corresponding Security rule, especially for the NAT overload scenario.

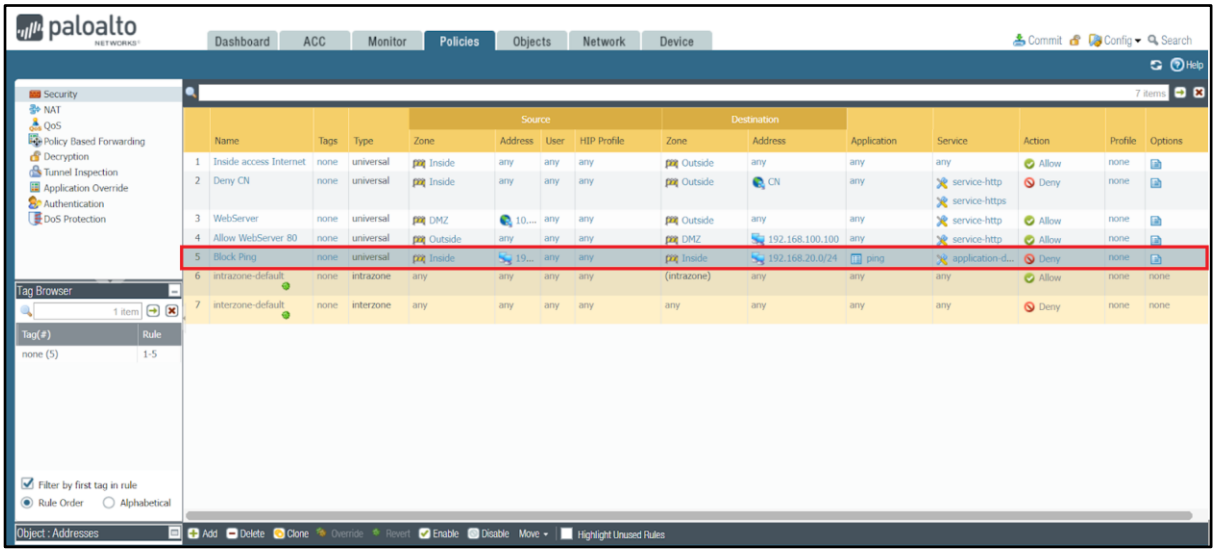
- Source:
    + Source Zone: Outside.
    + Source Address: Any.
- Destination:
    + Destination Zone: DMZ.
    + Destination Address: 192.168.114.100.
- Application: Any.

Configure APP-ID Features

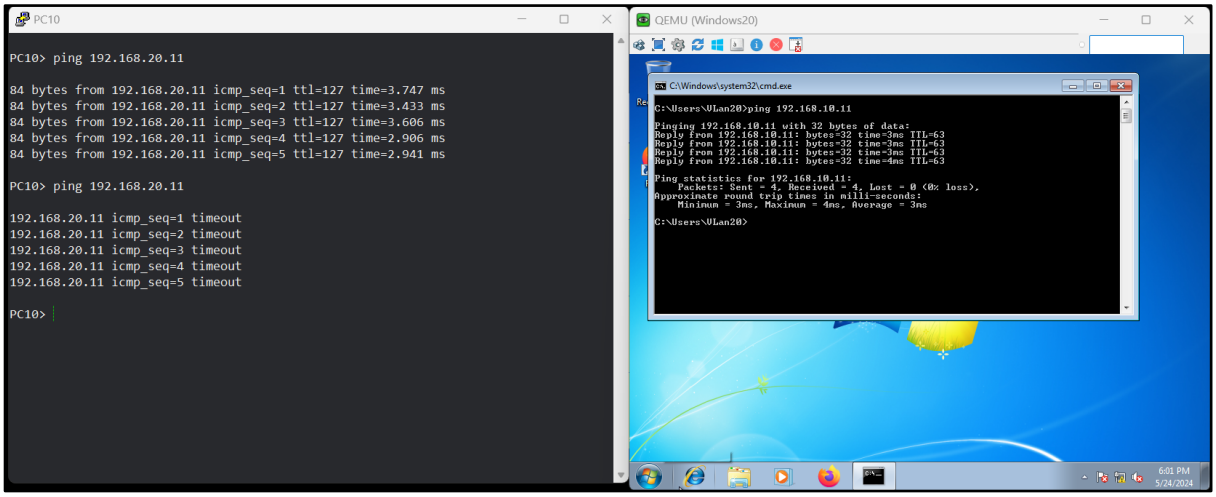
- Try to ping between two VLANs → Successful.



Use APP-ID to block VLAN 10 pinging to VLAN 20 in **Policies > Security**.



- Ping to VLAN 20 on PC VLAN 10 → Failed.



URL Filtering - Custom URL

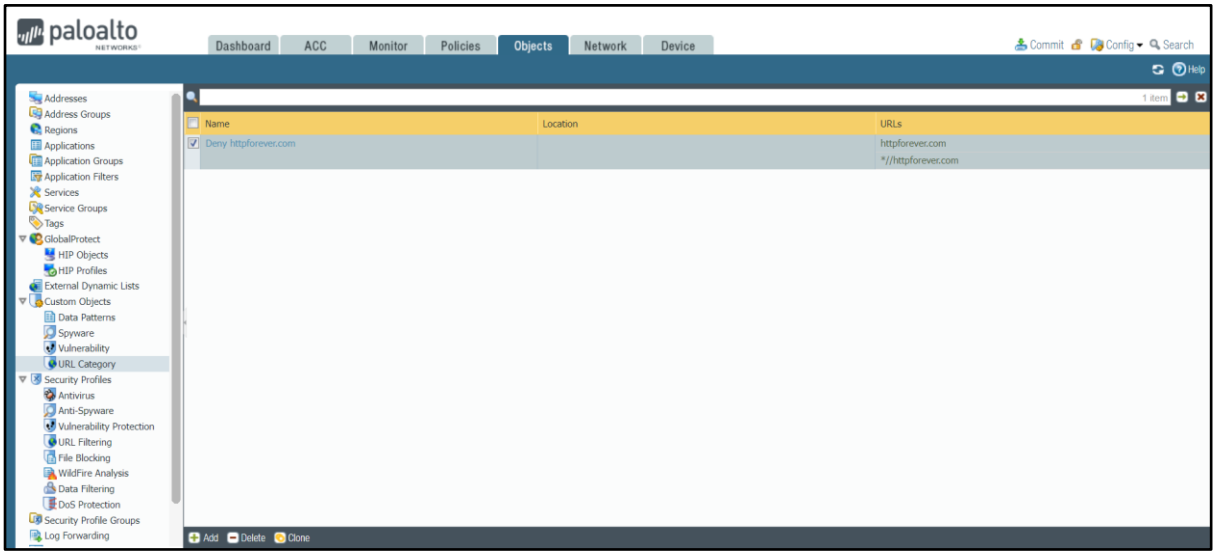
To start configure Custom URL Category, go to **Objects > Custom Objects > URL Category > Select Add**.

Then proceed to fill in the information as follows:

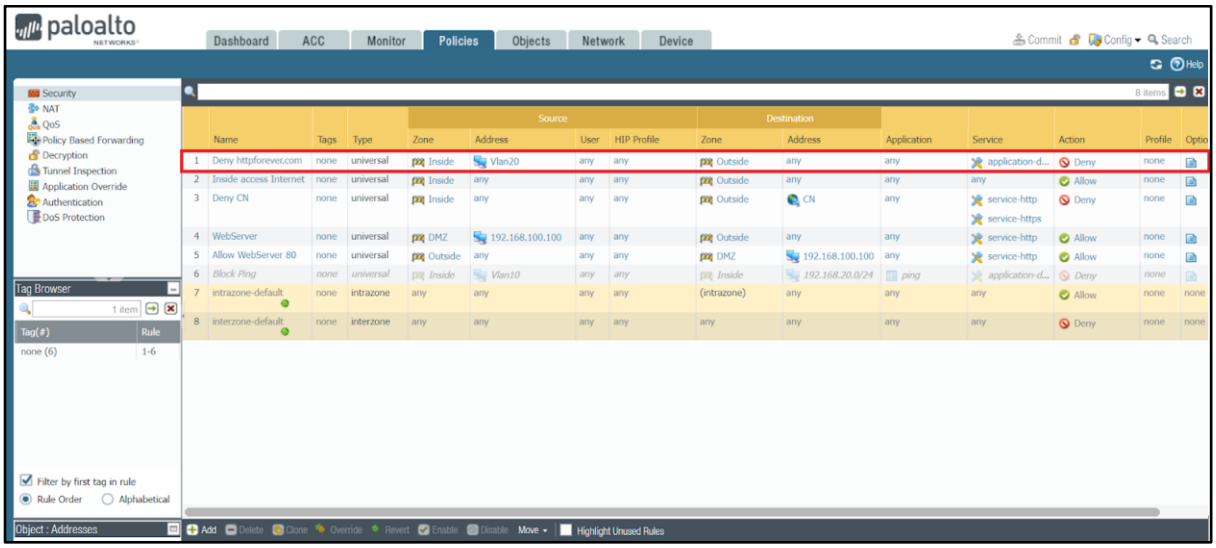
- Name: Name of the Custom Category.
- Type: Select the Category type, there are 2 options:
  + URL List: Allows you to define the appropriate URLs manually.
  + Category Match: Allows select multiple predefined Categories from Palo Alto.
- SITES: Enter the appropriate URLs.
- CATEGORIES: Select the relevant Categories.

Note: When configuring the URLs, you can use special characters to match as desired, such as:

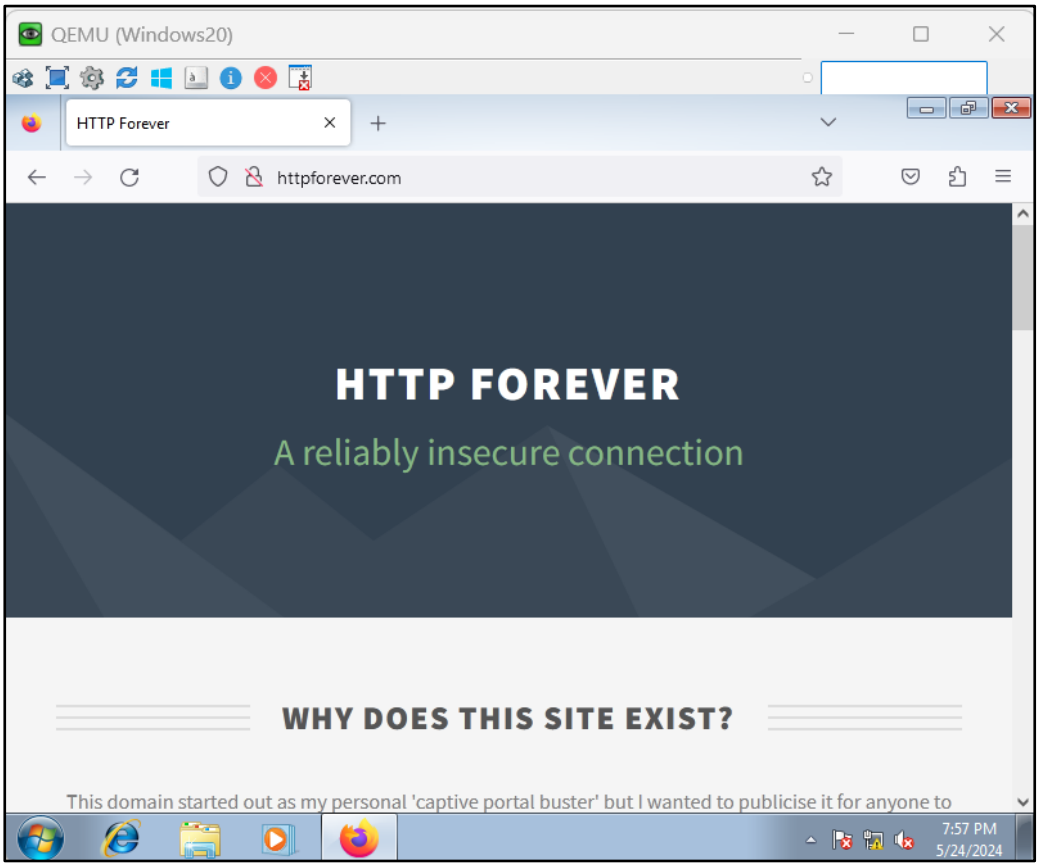
- "/" to match the exact URL.
- "*" to match all characters.



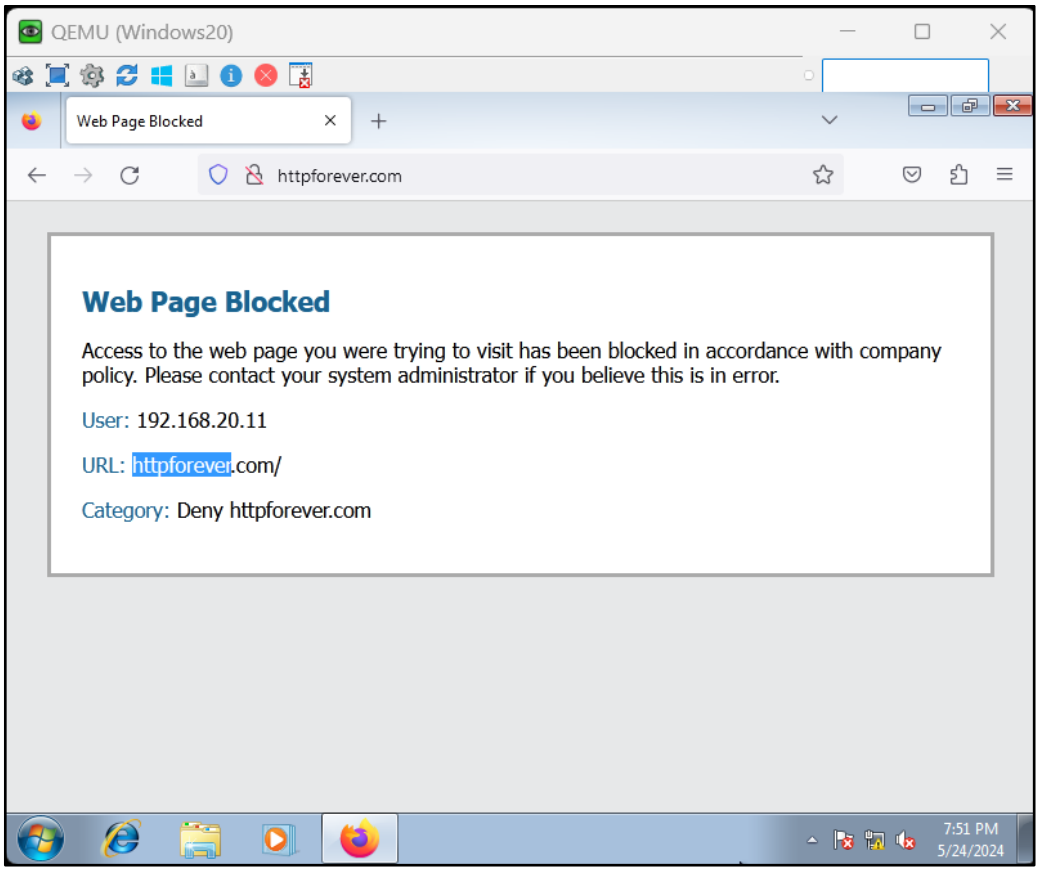
- After the configuration is complete, proceed to apply the Custom URL Category to the Policy to block access to http://httpforever.com from PCs belonging to VLAN 20.


paloalto
NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Config
Search
Help
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
Tag Browser
Tag(#)
Rule
none (6)
1-6
Filter by first tag in rule
Rule Order
Alphabetical
Object : Addresses
Source
Destination
Name
Tags
Type
Zone
Address
User
HIP Profile
Application
Service
Action
Profile
1 Deny httpforever.com none universal Inside Vlan20 any any Outside any any application-d... Deny none
2 Inside access Internet none universal Inside any any any Outside any any any Allow none
3 Deny CN none universal Inside any any any Outside CN any service-http service-https Deny none
4 WebServer none universal DMZ 192.168.100.100 any any Outside any any service-http Allow none
5 Allow WebServer 80 none universal Outside any any any DMZ 192.168.100.100 any service-http Allow none
6 Block Ping none universal Inside Vlan10 any any Inside 192.168.20.0/24 ping application-d... Deny none
7 intrazone-default none intrazone any any any any (intrazone) any any any Allow none none
8 interzone-default none interzone any any any any any any any any Deny none none
Add
Delete
Clone
Override
Revert
Enable
Disable
Move
Highlight Unused Rules

- Before Custom URL Category.



- After Custom URL Category.

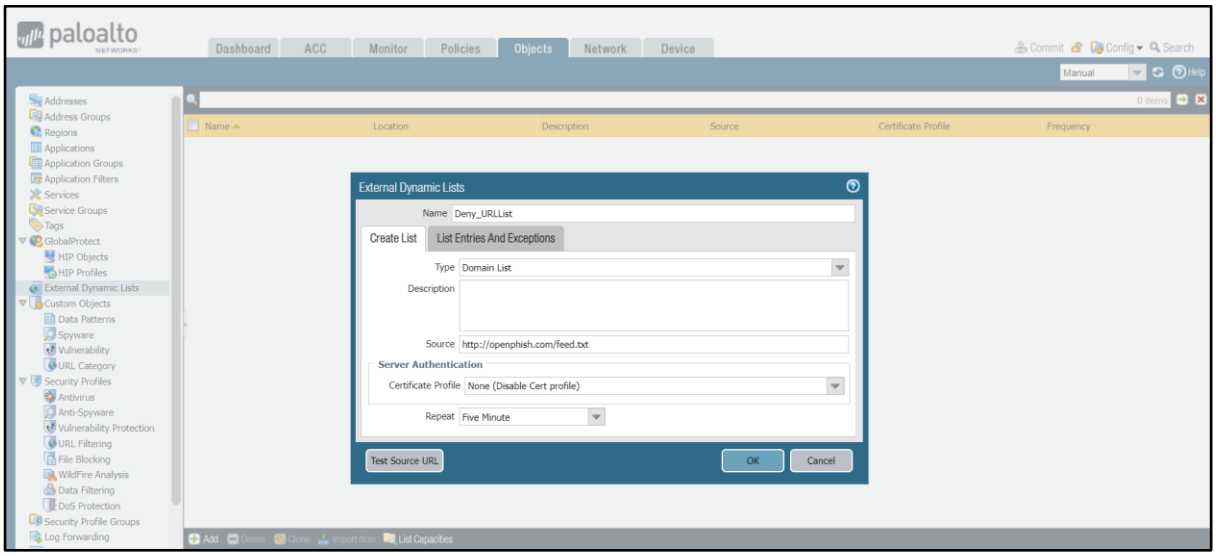


External Dynamic Lists

In case the administrator wants to block multiple URLs based on external sources (such as Threat Intelligence or from Palo Alto's sources), use External Dynamic Lists on Palo Alto by configuring them in **Objects> External Dynamic Lists > select Add**.

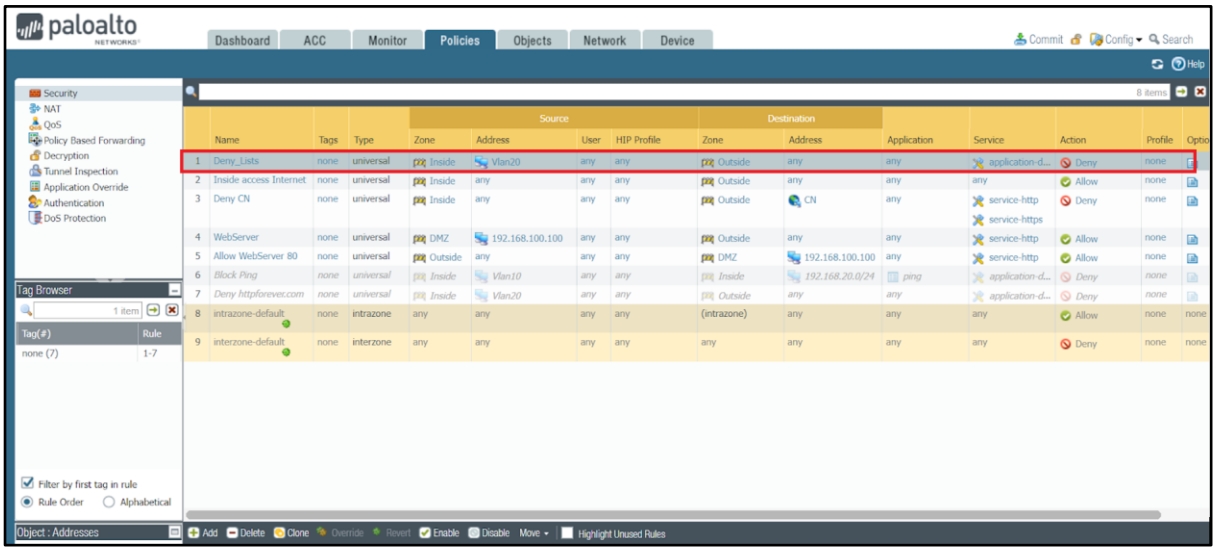
Next, proceed to configure the following information:

- Name: Name of the External Dynamic List (EDL).
- Type: Select URL List to update the URLs from the EDL.
- Source: Source providing the URL list.
- Check for updates: Periodic time to query and update the URL list.
- Test Source URL: Check the connection to the EDL.



If the connection test is successful, the result will look like the image below.

After completing the above step, proceed to apply it to the Policy with the URL Category will be the EDL that was configured, for PCs belonging to the VLAN 20.



File Blocking

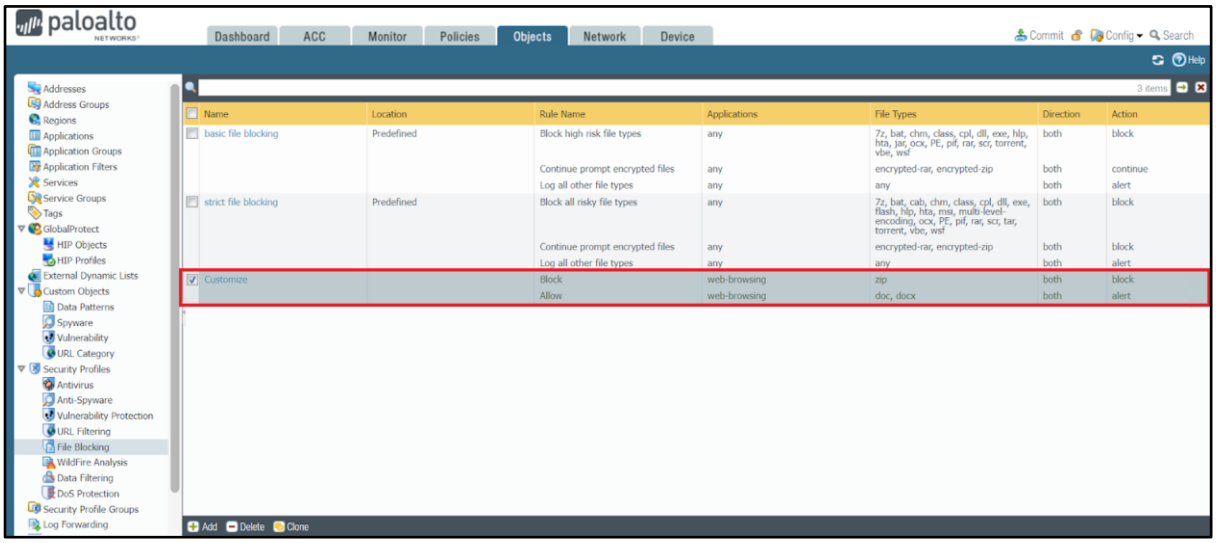
Go to **Objects > Security Profiles > File Blocking > Select Add**.

Next, proceed to configure the following information for the File Blocking Profile:

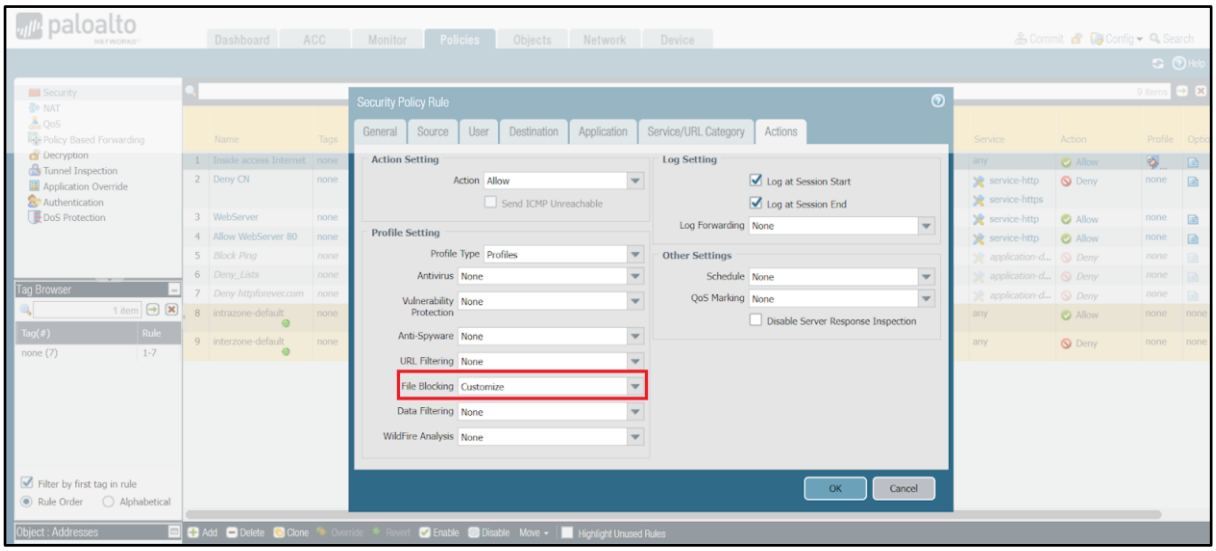
- Name: Name of the File Blocking Profile.
- NAME: Policy name within the File Blocking Profile (the order of matching rules will be from top to bottom).
- APPLICATIONS: App-ID of the traffic belonging to the policy.
- FILE TYPES: Supports selecting different file types at the same time.

- DIRECTION: Direction of traffic operation, with 2 options: download/upload or both (both).
- ACTION: Action when traffic matches the Policy, including:
    + Continue: Displays a portal page warning about the file information matching the policy, and chooses "continue" to allow the file to pass through.
    + Alert: Still allows the file to be executed but logs a warning in the Data Filterings logs.
    + Block: Blocks the file when it matches the policy.

In this demo, it will allow downloading .doc and .docx files with a warning when downloaded through the browser, and block when downloading .zip files through the web browser.

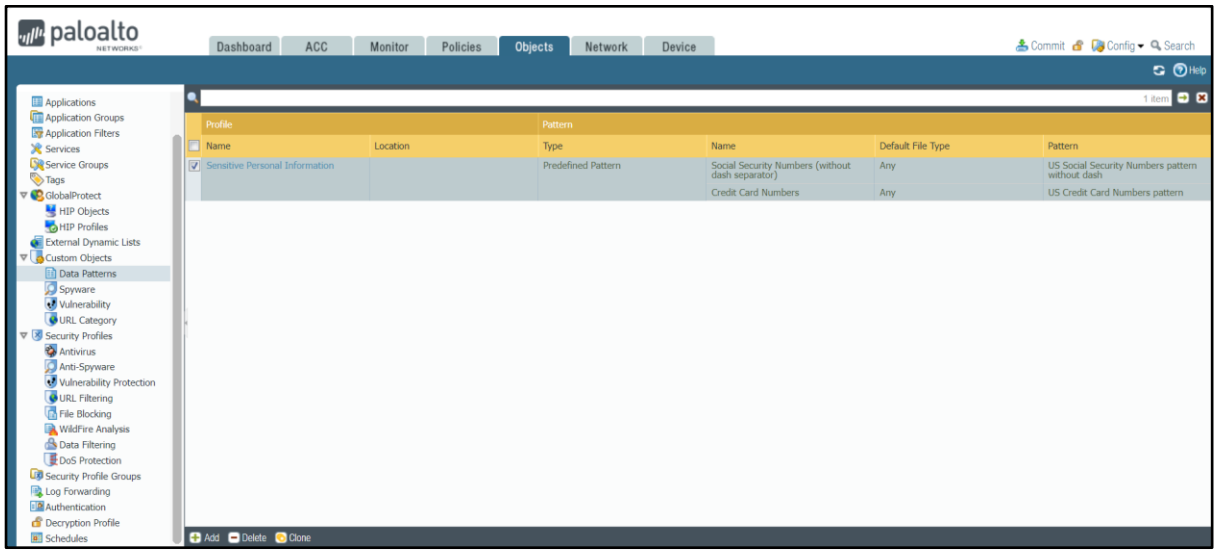


To apply the File Blocking feature, it needs to be applied to the Security Policy. In this demo, it will be applied to the internet traffic.



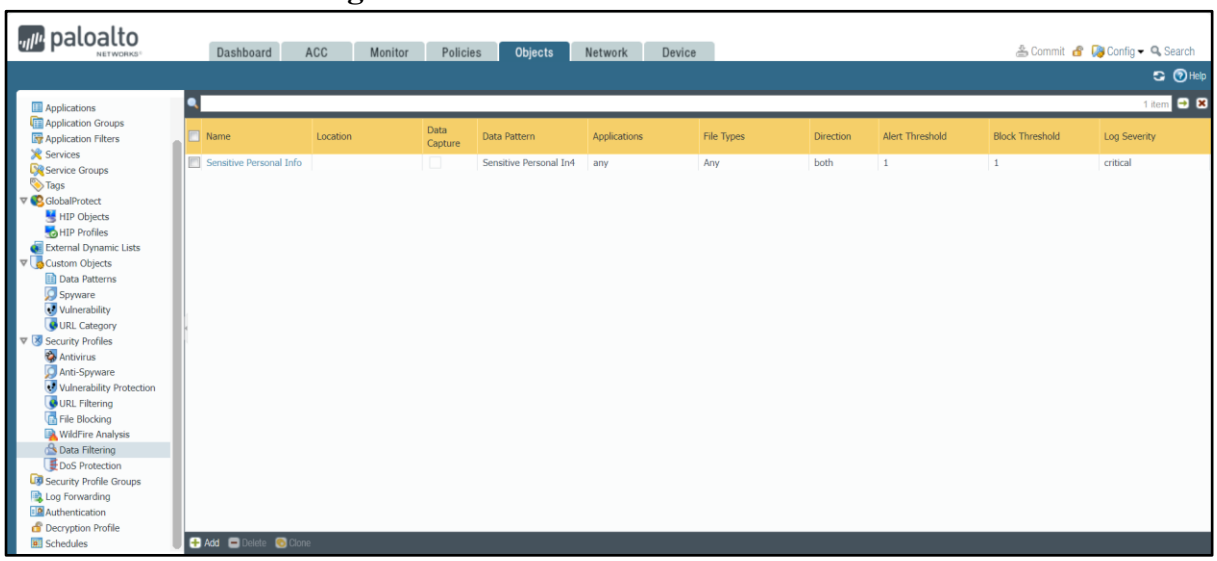
Data Filtering

First, to configure the Data Filtering feature, you need to define data patterns (or Data Pattern) in **Objects > Custom Objects > Data Patterns > select Add**.

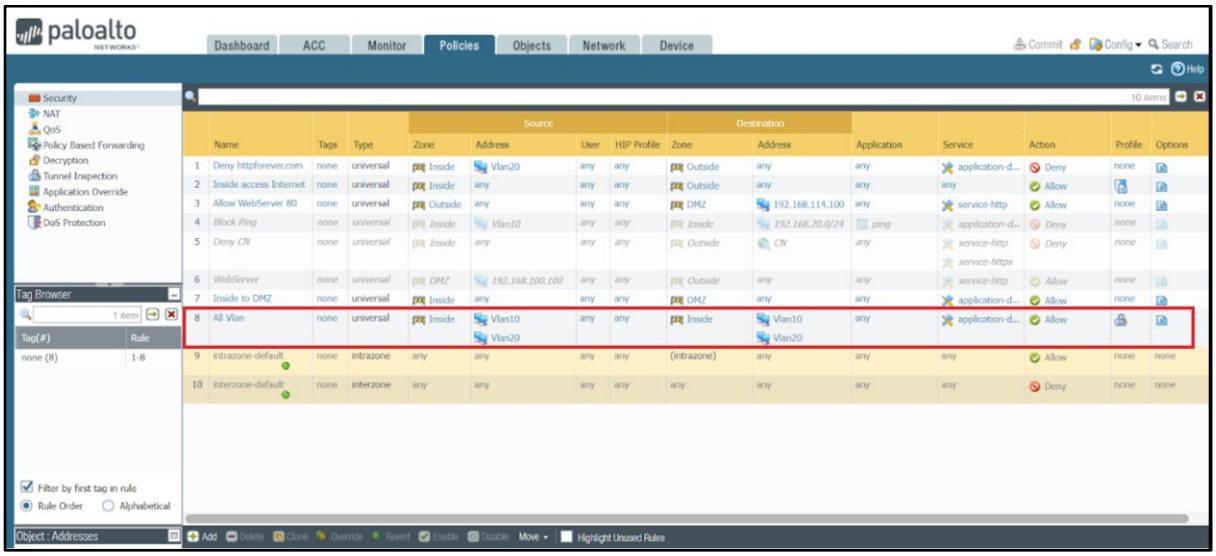


Next, enter a name for the template and select a template type. Here, select the Predefined Pattern template (Use Predefined Pattern to scan files to find CCCD numbers and credit card numbers). Selecting the data type of Credit Card Numbers will help identify bank cards (16-digit credit card numbers), for CCCD numbers, select Social Security Numbers (without dash separator) (9-digit CCCD numbers do not exist dash).

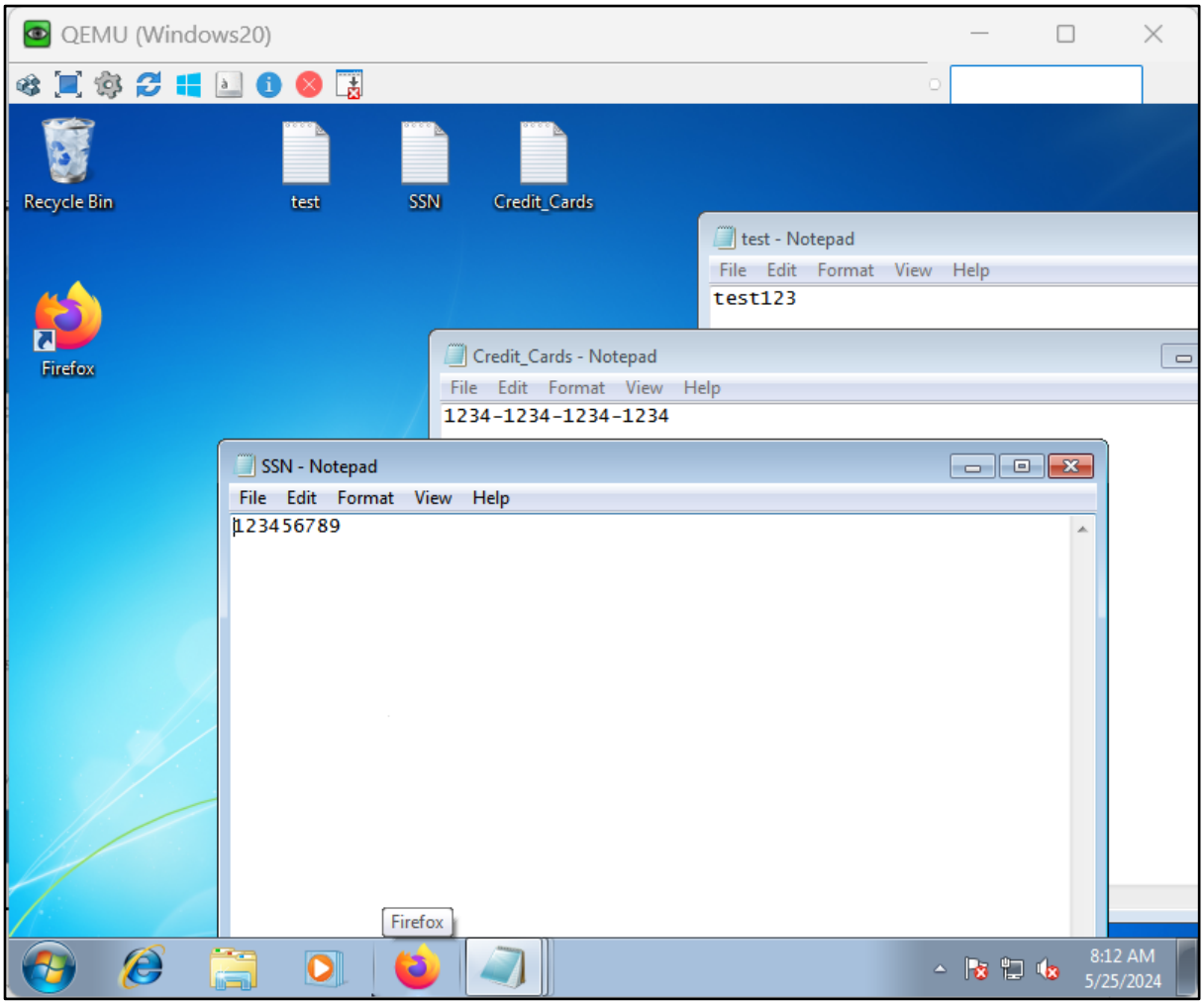
Then proceed to configure Data Filtering Profile in **Objects > Security Profiles > Data Filtering > Select Add.**



Next, for Data Filtering to work, you need to apply the Security Policy. In this lab, you will apply the Policy to allow communication of PCs in the subnet 192.168.10.0/24 and 192.168.20.0/24.


paloalto
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Config
Search
Help
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
Tag Browser
Tag(#)
Rule
none (8)
1-8
Filter by first tag in rule
Rule Order
Alphabetical
Object : Addresses
Source
Destination
Name
Tags
Type
Zone
Address
User
HIP Profile
Application
Service
Action
Profile
Options
1 Deny httpforever.com none universal Inside Vlan20 any any Outside any any application-d... Deny none
2 Inside access Internet none universal Inside any any any Outside any any any Allow
3 Allow WebServer 80 none universal Outside any any any DMZ 192.168.114.100 any service-http Allow none
4 Block Ping none universal Inside Vlan10 any any Inside 192.168.20.0/24 ping application-d... Deny none
5 Deny CN none universal Inside any any any Outside CN any service-http service-https Deny none
6 WebServer none universal DMZ 192.168.100.100 any any Outside any any service-http Allow none
7 Inside to DMZ none universal Inside any any any DMZ any any application-d... Allow none
8 All Vlan none universal Inside Vlan10 Vlan20 any any Inside Vlan10 Vlan20 any application-d... Allow
9 intrazone-default none intrazone any any any any (intrazone) any any any Allow none none
10 interzone-default none interzone any any any any any any any any Deny none none
Add
Delete
Clone
Override
Revert
Enable
Disable
Move
Highlight Unused Rules

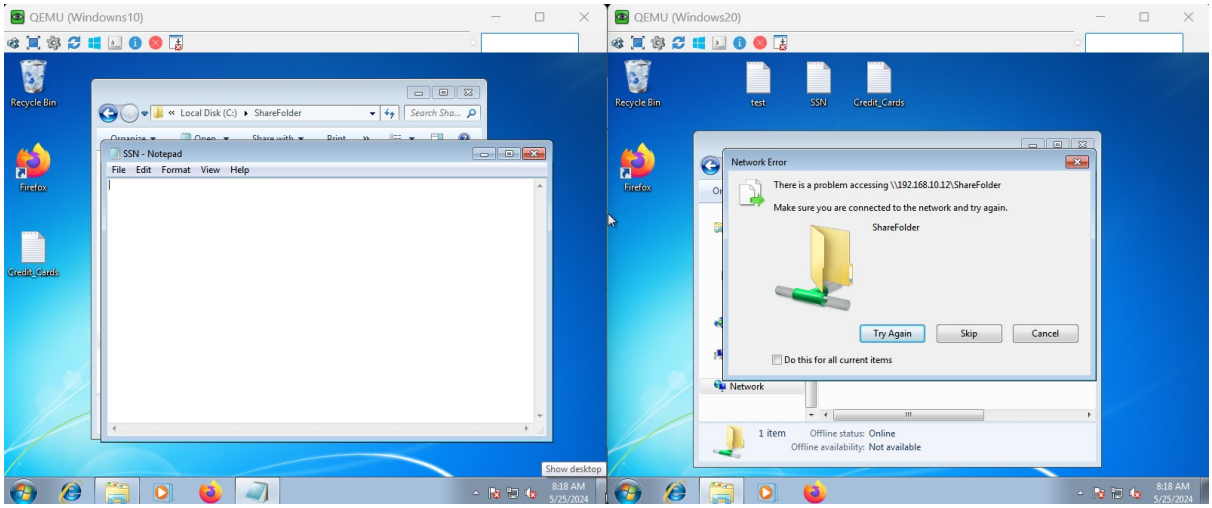
For testing, create 3 files in each PC-Vlan has content like below.



Tiến hành từ PC VLAN 20 truy cập SMB vào PC VLAN 10 để tiến hành download và mở File liên quan đến Credit Card. Lúc này sẽ thấy xuất hiện cảnh báo không thể hoàn thành tác vụ.

From PC VLAN 20, access SMB to PC VLAN 10 to start downloading and Open File about Credit Card. An alert window will inform that the process can’t be

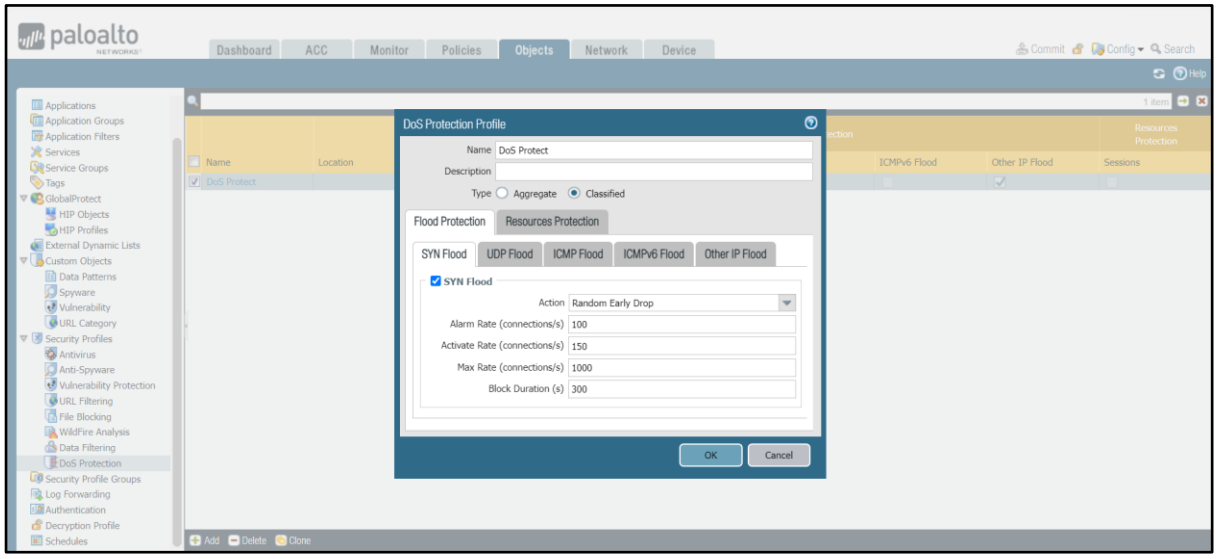
done.



DoS Protection

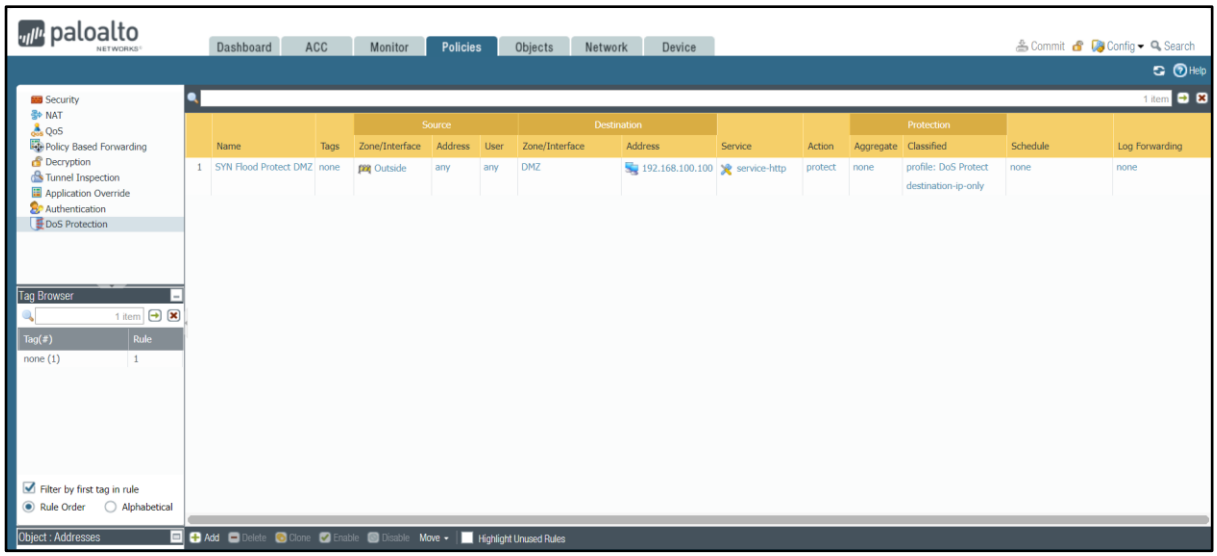
Go to **Objects > Security Profile > DoS Protection** and **Add** a new Object.

- Name: Enter a name.
- Type: Classified (Apply the DoS thresholds configured in the profile to the connections that match the classification criterion (source IP address, destination IP address, or source-and-destination IP address pair).
- **Flood Protection Tab > SYN Flood** tab:
    + Action: Random Early Drop.
    + Alarm Rate: 100 (connection/s)
    + Activate Rate: 150 (connection/s)
    + Max Rate: 1000 (connection/s)
    + Block Duration: 300 (s)

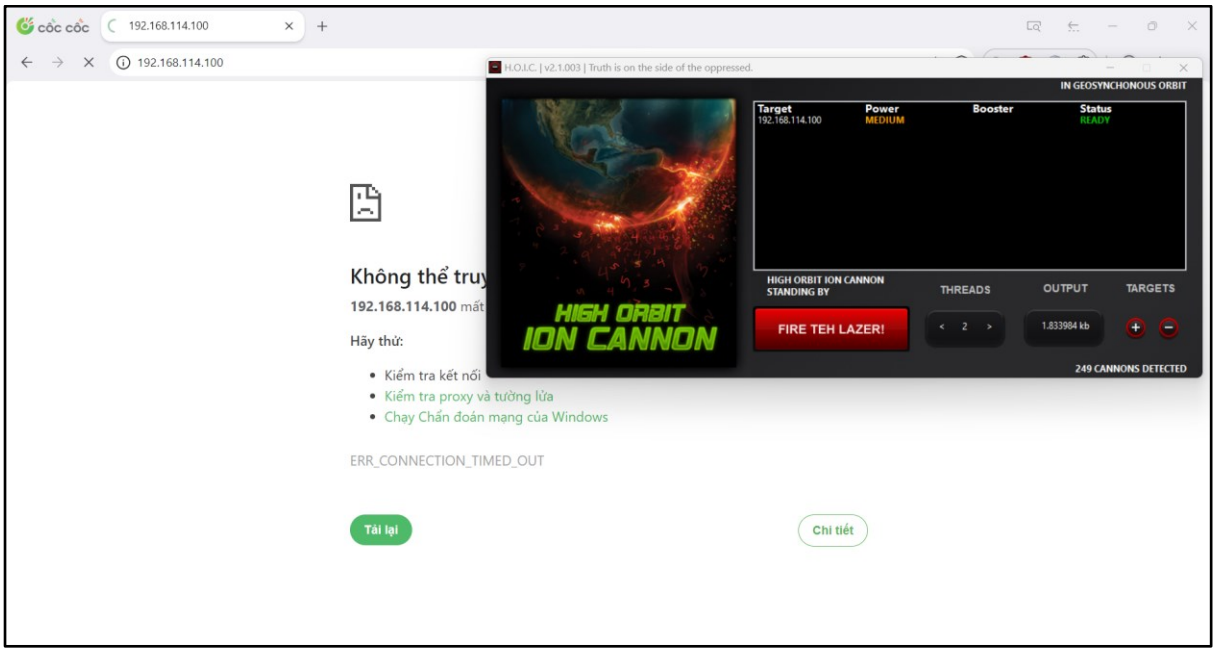


Go to **Policy > DoS Protection** and add a new **Policy DoS Rule**.

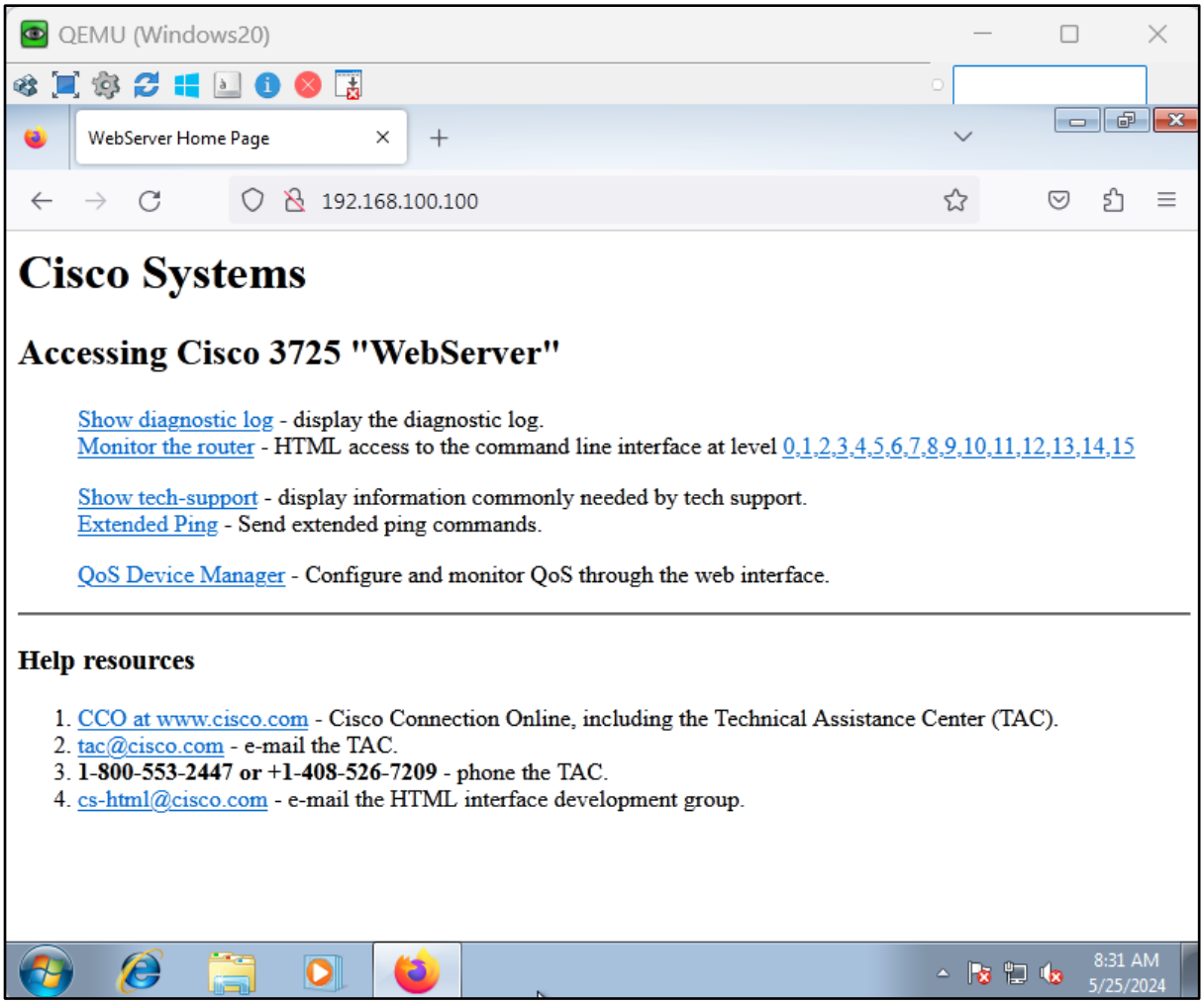
- General tab:
  + Name: create a name for Policy.
- Source tab:
  + Type: Zone.
  + Zone: Outside.
  + Source Address: Any.
- Destination tab:
  + Type: Zone.
  + Zone: DMZ.
  + Destination Address: 192.168.100.100.
- Option/Protection:
  + Service: service-http.
  + Action: Protect.
  + Aggregate: None.
  + Classified Profile: Name of Classified DoS Protection profile.
  + Address: destination-ip-only.



For testing, perform a DOS attack from the Window machine. After a while, Palo Alto will automatically block Windows' IP.



The Virtual Windows still accesses the website, which means the Dos Protection system works smoothly.



8. Reference

1. Palo Alto networks. (n.d.). Paloaltonetworks.com. Retrieved May 15, 2024, from https://docs.paloaltonetworks.com/
2. Leader in cybersecurity protection & software for the modern enterprises. (n.d.). Palo Alto Networks. Retrieved May 15, 2024, from https://www.paloaltonetworks.com/
3. Networks, P. A. (2022). PAN-OS Web Interface Help.
4. Phile. (n.d.-a). Lab Network System Security. Retrieved May 25, 2024, from https://securityzone.vn/f/lab-paloalto-132/
5. BeingProactive. (n.d.).How to connect PALO ALTO Firewall to the Internet | Basic Configuration setup on EVE-NG. https://youtube.com/playlist?list=PLStKtZk4kRRLCGfR2OAJvNuFW4tbtXksy&si=L7g6At4u2DteZt-g