SIGPwny

FA2024 Week 05 • 2024-10-03

Firewalls, Net Inspection, Traffic Monitoring

Sagnik Chakraborty, Michael Khalaf

Table of Contents

Firewalls

- Systems for us to monitor and control inbound and outbound traffic based on a set of predefined rules (ACLs)
- One of the most important tools in a security engineer's arsenal
- Basically a must-have in today's landscape

Types of firewalls

- **Network Firewalls:** filtering traffic based on transport layer; these will look at ingress/egress traffic through specific addresses and protocols like TCP/UDP
- **Web App Firewalls (WAFs):** web applications by filtering and monitoring HTTP traffic, maintaining web access policies (CORS)
- **NGFW**: Next-Gen Firewalls that provide a higher level of application/service awareness, implement features of NFs and WAFs, and provide smart features like DPI, EDR, allowing for a finer grained level of control

Net Firewalls

- Net firewalls will allow for rules at the packet level and can evaluate source and destination IP addresses, port numbers, and protocol types (e.g., TCP, UDP)
- They can come in **stateful** or **stateless** configurations
  - **Stateful** firewalls (e.g. session-based) can monitor the state of active connections and make decisions based on a state machine operating on this connection
  - **Stateless** firewalls will make decisions based on the packet itself and decide to drop or accept it

Configuring Net firewalls

What if I wanted to enable authenticated connections over ssh but drop any other connection?

```
$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
$ sudo iptables -A INPUT -j DROP
```

IP bans?

```
$ sudo iptables -A INPUT -s <BLOCKED IP> -j DROP
```

WAFs

- Will look at Layer 7 (HTTP/HTTPS) traffic to protect web applications from common web exploits
- Good to have to mitigate most common web vulnerabilities (CSRF, SQL injection attempts, XSS)
- You can deploy them either as a reverse proxy listener over HTTP(S)
  - for HTTPS listening, you'd set up your listener and upstreams and then add your server TLS authentication

NGFWs

- The latest and greatest kinds of firewalls will employ traditional firewall functionalities by incorporating application awareness and control, as well as threat intelligence
- They can inspect packets up to and including Layer 7, allowing for WAF capabilities
- Usually they include cool tools to help manage traffic at a higher level, such as EDR tools, DPI, and context-based policies (user identity, application, threat intelligence)

Linux Firewall Configuration

Firewalld Configurations (Linux)

Start & Enable firewalld

```
sudo systemctl start firewalld
sudo systemctl enable firewalld
```

Check Status:

```
sudo firewall-cmd --state
```

Allow A Service (HTTP as an example)

```
sudo firewall-cmd --add-service=http --permanent
```

Deny Specific IP Addresses

```
sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="192.168.1.10" reject'
```

Reload firewalld (manual)

```
sudo firewall-cmd --reload
```

Why Firewalld?

`firewalld` stands out from other Linux firewall configurations due to its dynamic management capabilities, allowing real-time adjustments without restarting the firewall. It employs a zone-based approach, making it easier to apply different rules for various network interfaces. This system enables users to define rules based on trust levels, enhancing flexibility. Additionally, `firewalld` supports rich rules for advanced configurations, accommodating complex security requirements efficiently.

Windows Firewall Configuration

Defender: Domestic Configurations

Enable & Disable Firewall Session:

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
```

Allow App Through: (AAT):

```
New-NetFirewallRule -DisplayName "MyApp" -Direction Inbound -Program
"C:\Path\To\MyApp.exe" -Action Allow
```

Block Incoming IP Traffic Via Address (IPv4):

```
New-NetFirewallRule -DisplayName "Block IP" -Direction Inbound -Action
Block -RemoteAddress 192.168.1.10
```

Advanced Defender Configurations (Extended)

Create Rule for Specific Ports & Protocols:

```
New-NetFirewallRule -DisplayName "Allow HTTP" -Direction Inbound -Protocol
TCP -LocalPort 80 -Action Allow
```

Log Firewall Events:

```
Set-NetFirewallProfile -Profile Domain -LogAllowed True -LogBlocked True
```

Export Firewall Rules:

```
Export-NetFirewallRule -File "C:\FirewallRules.wfw"
```

NetSH advfirewall configurations

Show Firewall Configuration:

```
netsh advfirewall show allprofiles
```

Enable Firewall for Profiles (ex: all profiles)

```
netsh advfirewall set allprofiles state on
```

Inbound Port Traffic Rules

```
netsh advfirewall firewall add rule name="Allow Port 443"
dir=in action=allow protocol=TCP localport=443
```

NetSH Advanced Configurations

Block Specific IP Address:

```
netsh advfirewall firewall add rule name="Block Specific IP"
dir=in action=block remoteip=192.168.1.10
```

Logging Enablement (allprofiles)

```
netsh advfirewall set allprofiles logging
filename="C:\FirewallLog.log" maxfilesize=4096
```

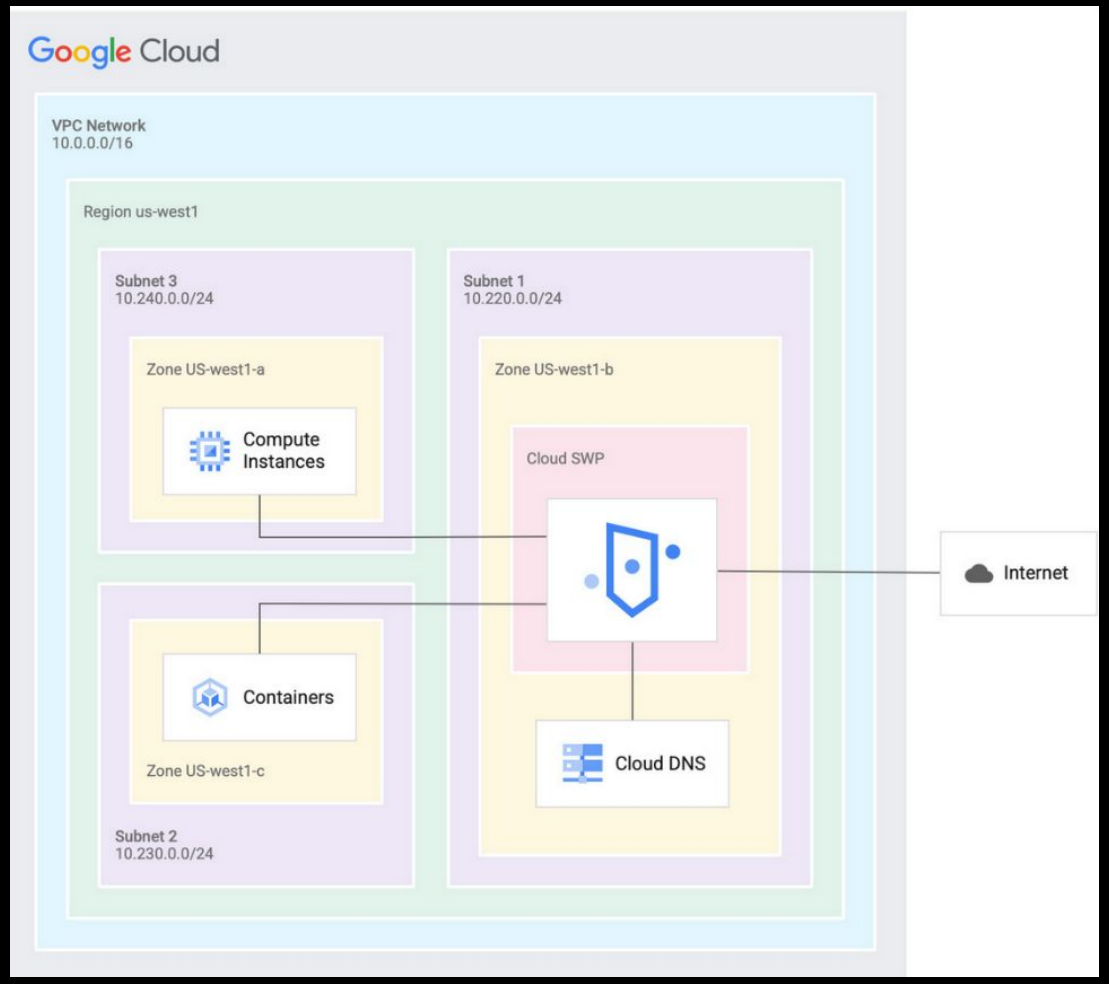
Restore Default Settings

```
netsh advfirewall reset
```

Defense Strategies

Prevent them from getting in, and if they do, give em hell

Egress Filtering



- If an attacker already has a hold on the system, most likely (read: absolutely) they will exfiltrate data back to their C2
- Implementing egress filtering rules are very important for recognizing and breaking these transmissions
- E.g. pass outbound traffic through a dedicated proxy

Egress Tactics: DNS Sinkholing

- **DNS-sinkholing**: redirect or block malicious traffic by manipulating DNS responses for known malicious domains:

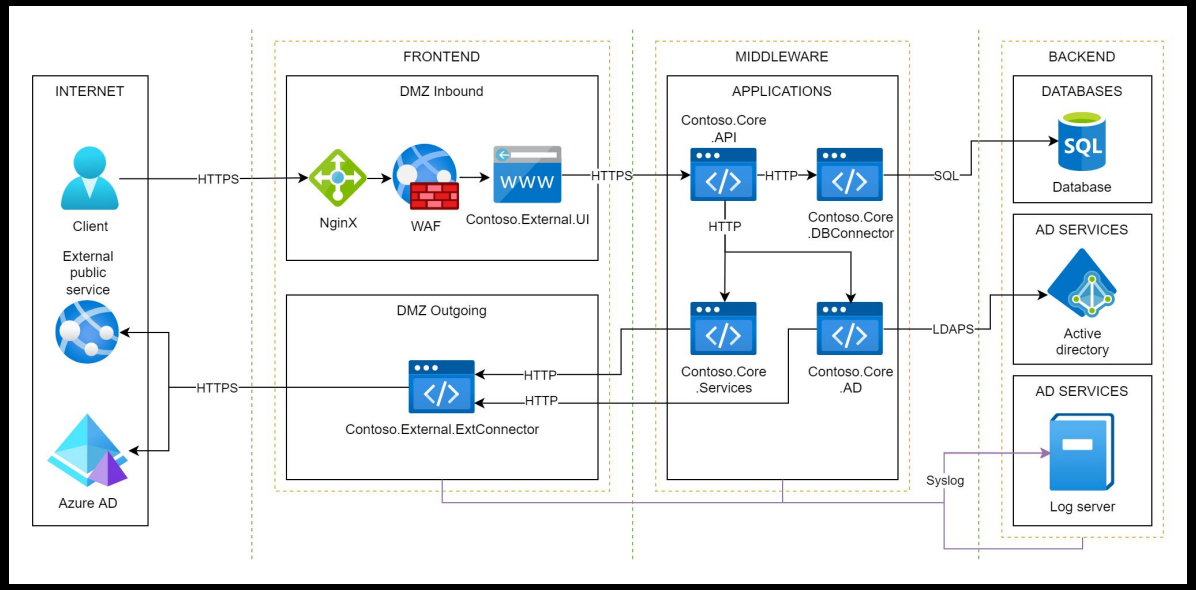
- instead of allowing the system to connect to a malicious domain or IP, you configure your DNS server to return a non-routable IP address or redirect it to a **sinkhole server** that logs the request or nullifies the connection

DNS Sinkholing

- Usually, your DNS server has a list of known malicious domains (usually based on threat intelligence or blocklists). Instead of resolving the domain to its real IP address, the DNS server responds with a non-routable or sinkhole IP where the egress traffic behavior can then be analyzed/flagged

Segmentation

- Dividing a larger network into smaller, distinct subnetworks or segments
- Configuring ACLs for segment-to-segment communication is a good tool for preventing lateral movement



Segmentation

- **Configure Ingress/Egress rules**: specify which services/ports enter or leave a segment (e.g. only LDAPS is configured within a given segment running a service providing dedicated core AD services)
- **Specify User and Device-level access**: Because net segments offer a level of granular control over a regular network setup, it's a lot easier to configure access control on the individual level, and thus control an attacker's degrees of freedom

Micro-Segmentation

- Applying segmentation at the individual workload, application, or even process-based level.
- This is commonly employed within virtualized environments where having a level of process isolation is necessary

- This allows us to provide **identity-based** rulesets rather than relying solely on the IPs or the network boundaries

Micro-seg services

- **Illumio:** Provides micro-segmentation based on the identity and context of workloads, with adaptive security policies that apply across data centers and cloud environments.
- **VMWare NSX**: Provides micro-segmentation capabilities in virtualized environments, allowing for the isolation of virtual workloads with firewall rules.
- **Guardicore**: Offers software-defined segmentation and security across hybrid cloud environments, with detailed visibility into process-level traffic.

Zero-trust Policy

- This is the principle that **no traffic should be trusted by default**, even (perhaps especially) within the network

- Every workload communication is verified and restricted based on strict policy enforcement, ensuring that only legitimate and authorized connections are allowed.

Tieback: Competition Defense Strategies

1. Goal is to stall the red team by purposely organizing things not as they would expect but rather how we'd plan.
2. Give them a bone to fetch, feel more confident by exploring a sliver of genuine or dummy data.
3. Buys the defense team time to further navigate a defense landscape.
4. Segmentation is obviously best practice in order to conduct damage control and containment of a breach.

Next Meetings

`2024-10-08` • **Next Tuesday**

- Windows Privilege Escalation with Ronan

`2024-10-10` • **Next Thursday**

- Docker & Containerization with Sagnik