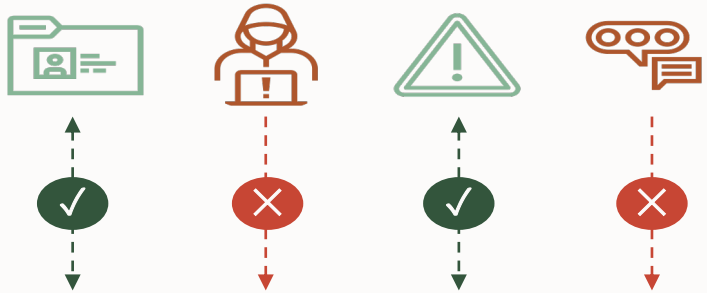
ORACLE

Oracle Cloud Infrastructure (OCI) Network Firewall

OCI Network Firewall features



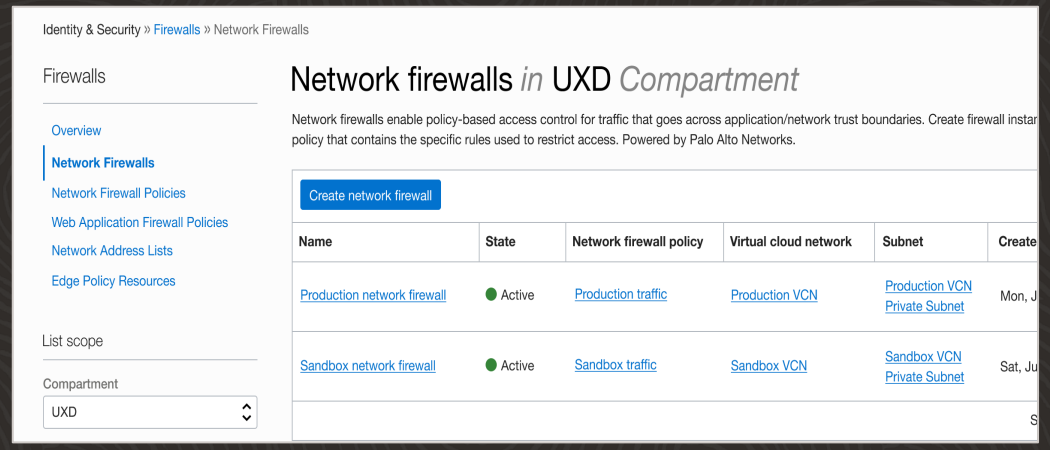
Stateful Rules	Stateful filtering Allow or Deny rules based on 5-tuple information for both IPv4 and IPv6 traffic.
IDS and IPS	Industry-leading signature-based threat detection and prevention (IDS/IPS) engine to automatically stop known malware, spyware, C2 and vulnerability exploits.
URL & FQDN filtering	Control inbound and outbound HTTP/S traffic to a specified list of FQDN including wild cards and custom URLs.
Flexible Policy Enforcement	Secure inbound, outboud and lateral network/application traffic. Can be enforced on OCI gateways as well as intra-vcn subnet traffic.

Customer applications

Oracle Cloud Infrastructure

OCI Network Firewall

OCI Network Firewall is a cloud-native managed firewall service that is built using industry leading **Palo Alto Networks** next-generation firewall technology. It provides advanced threat protection capabilities including custom URL filtering, intrusion prevention and detection (IDS/IPS), and TLS inspection to help prevent malicious traffic and malware propagation.



Customer benefits

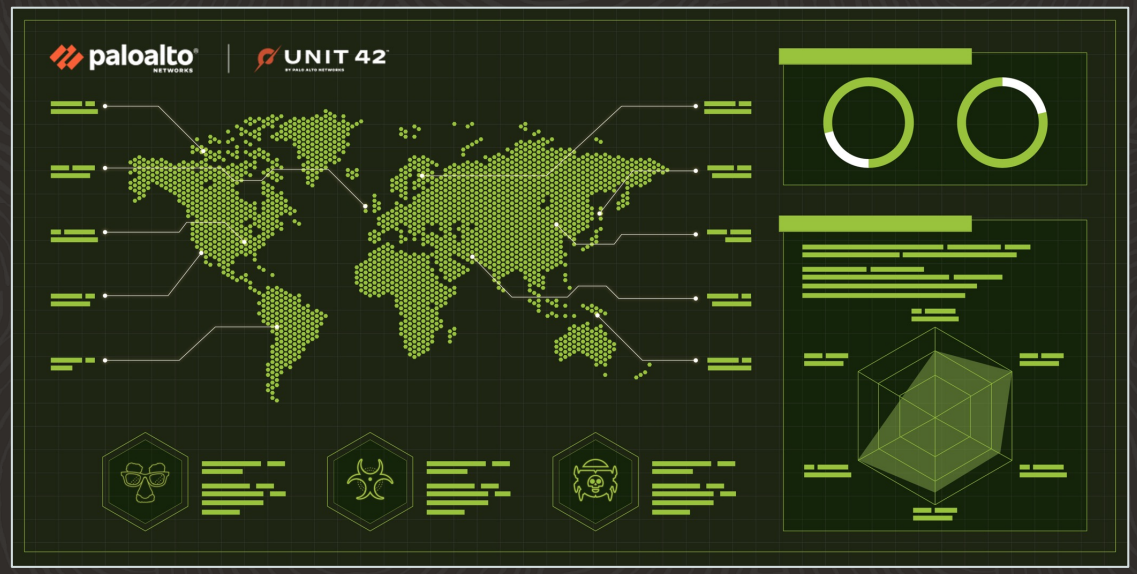
- **Cloud-Native Firewall** - Scalable native service that eliminates the need to manage additional third-party security infrastructure.
- **Deep Integration with OCI** - Natively integrated with OCI platform including logging and metrics services.
- **Layered Defense** - Easily apply deeper security controls and segmentation for encrypted and non-encrypted traffic to customer workloads on OCI.
- **Advanced Threat Protection** – Industry leading threat protection to help monitor and block malware, spyware and vulnerability exploits.
- **Meet Compliance Goals** – Helps meet compliance requirements and stringent security needs of regulated environments.

Intrusion Detection and Prevention and TLS/SSL encrypted traffic inspection

- Integrated IDS and IPS solution built with Palo Alto Networks' threat analysis engine and Unit 42 - security research teams that identify new threat signatures and detection mechanisms.

- Helps detect (IDS) and block (IPS) known exploits, malware, malicious URLs, spyware, command and control (C2) attacks.

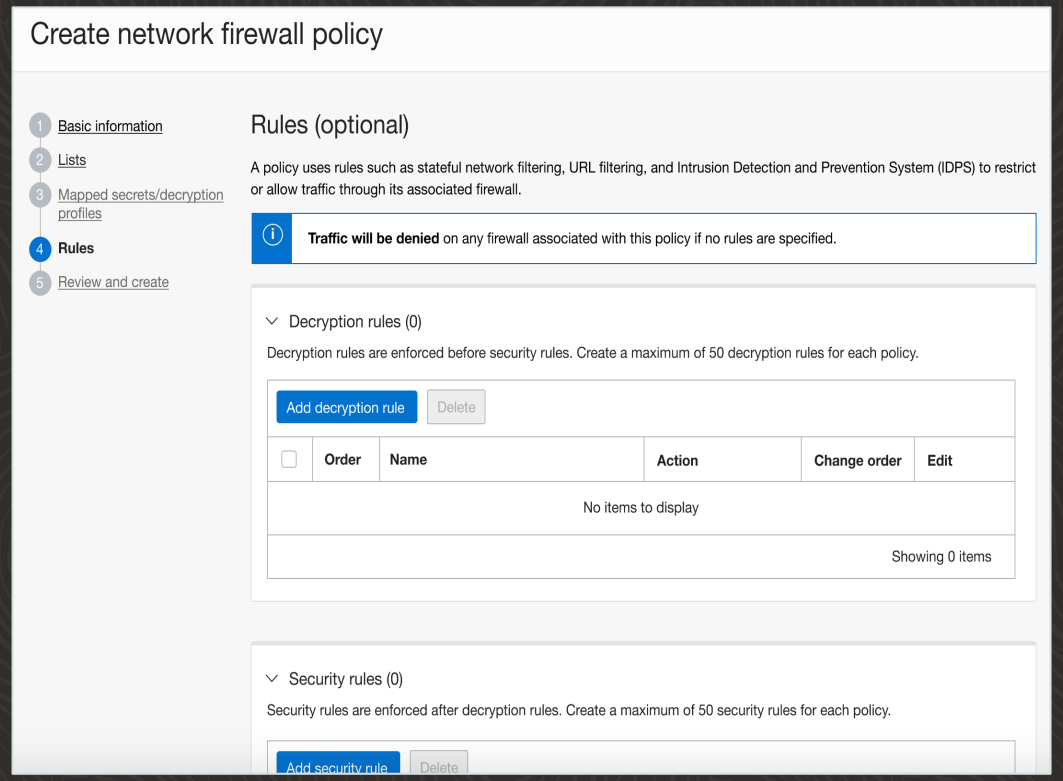
- **Use case:** OCI Network firewall is to be able to apply **Intrusion Detection and Prevention (IDS/IPS) controls to the traffic, including encrypted traffic over SSL/TLS secure channels and to do this, the NGFW must decrypt the SSL/TLS encrypted traffic.**



Stateful Firewall Rules

Enforce *allow* or *deny* stateful filtering rules based on 5-tuple information (source and destination IP address (both IPv4 and IPv6), port, and protocol.

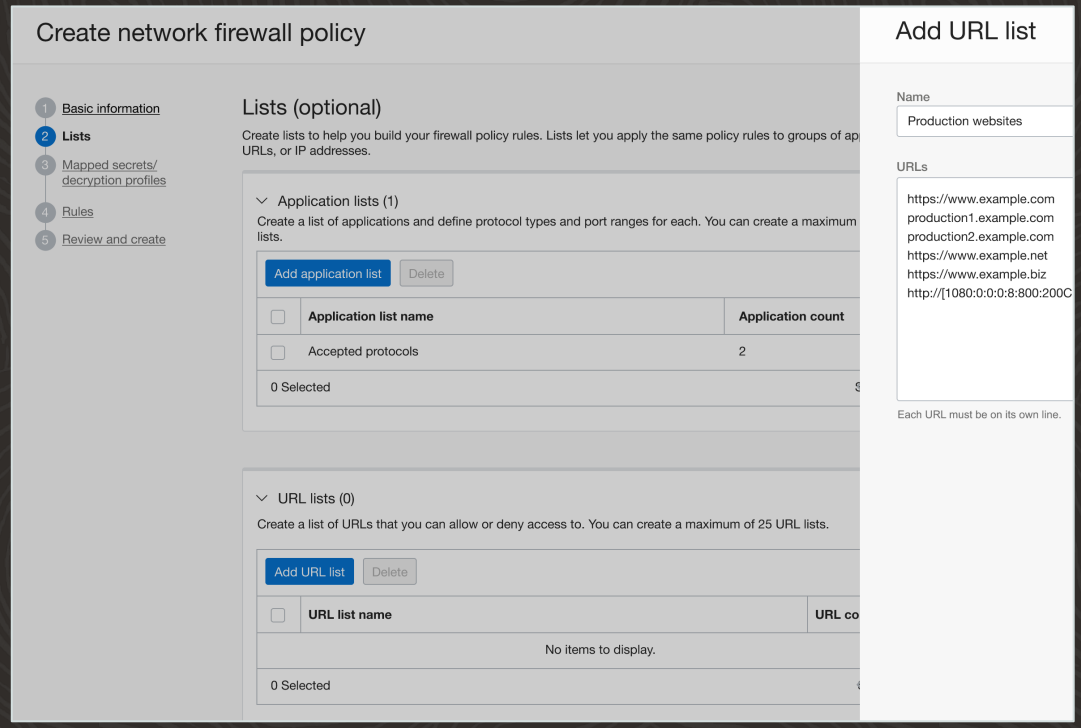
- Rules can be enforced in a customer defined priority order across multiple virtual networks.
- The stateful firewall takes into account the context of traffic flows for more granular policy enforcement.



URL and FQDN Filtering

Use these rules to restrict traffic to a user specified list of fully qualified domain names (FQDN) including wild cards and custom URLs.

- Flexible enforcement for both inbound and outbound traffic
- **SSL Inspection** - allows inspection of HTTPS (TLS 1.2 and 1.3) encrypted traffic. Natively integrated with highly secure OCI Vault.



Difference between Network Security List/groups and OCI Network Firewall features

Network Security lists and groups

Stateful Rules and Stateless Rules for both IPv4 and IPv6 traffic.

CIDR Range or Service (Source IP and Destination IP)

Protocol

Source port

Destination port

>> Access control list on Subnet and NIC level.

>>By default every traffic is denied. Rules need to be created to allow the traffic.

Deny rules can not be created.

OCI Network Firewall

Stateful filtering Allow or Deny rules based on 5-tuple information for both IPv4 and IPv6 traffic.

Signature-based threat detection and prevention (IDS/IPS) engine.

Control inbound and outbound HTTP/S traffic to a specified list of FQDN including wild cards and custom URLs.

Decryption profiles for inbound and outbound HTTPS inspection.

Policies manage traffic for intra VCN and Inter VCN centrally.

OCI Network Firewall and WAF – Better Together

- **OCI Network Firewall** helps secure network and application workloads. It enables policy based visibility and control over applications, users and content including access control, SSL decryption, threat prevention, URL filtering and IDS/IPS capabilities.

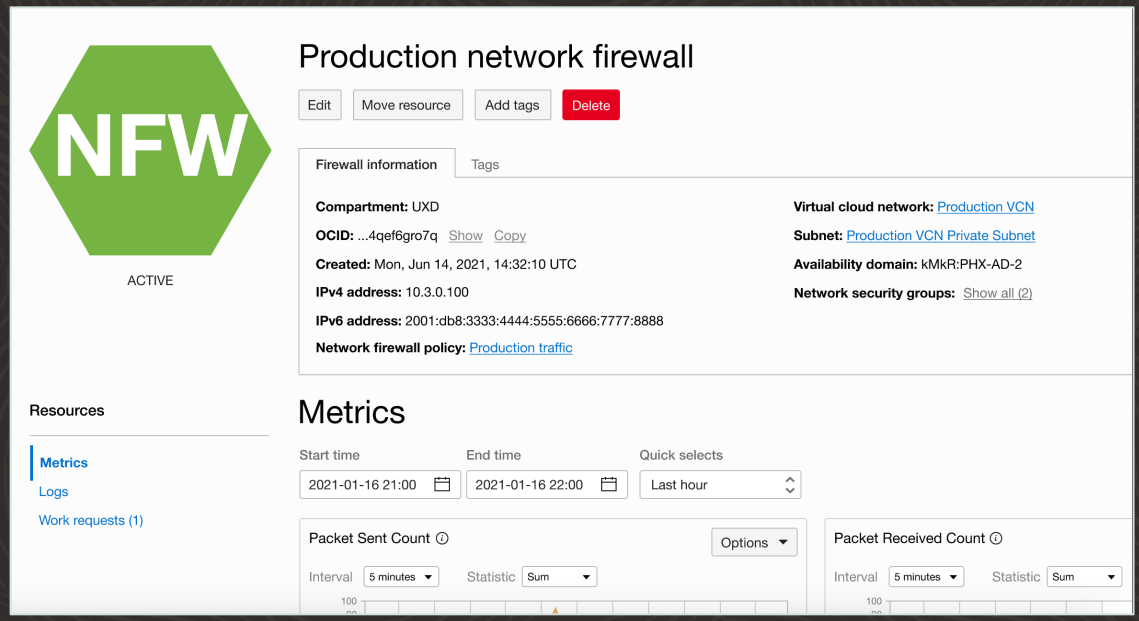
- **OCI WAF** is primarily focused on the security of web applications and operates at the layer 7 (HTTP/S). It helps stop layer 7 attacks whether it's an attempt to exploit vulnerable code-level vulnerabilities such as SQL injection and other OWASP Top 10 vulnerabilities, or a layer 7 DDoS attack.

- **Layered Defense** - In most cases it's important to employ both technologies given the various potential points for intrusion across both networks and web applications.

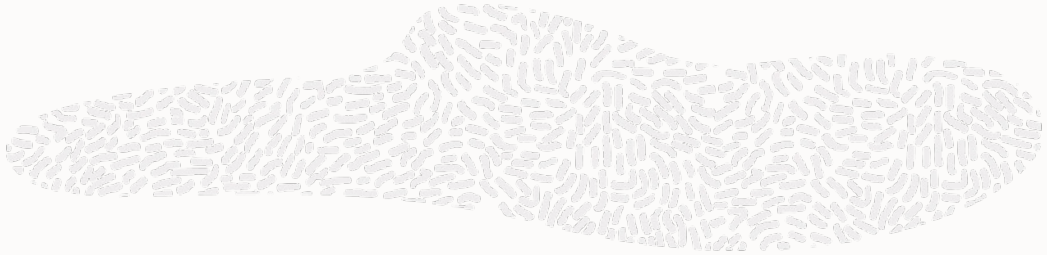
  - For e.g., in 3-tier architecture web-tier can be protected using WAF. But, web tier to app tier and app tier to database tier communications are protected using Network Firewall.

Logging, Monitoring and Analytics

- Network Firewall metrics help monitor the health, capacity, and performance of firewall policies and resources.
- Alarms and Notifications can be configured to notify you when metrics meet alarm-specified triggers.
- Network Firewall logs (integrated with OCI logging) enable you to understand what rules and the countermeasures triggered by requests.
- Logging Analytics provides the *analytics*, making it simpler to explore the data, analyze patterns and out-liners, provide machine learning in the form of clustering and linking, create dashboards, provide topology drill-downs and much more.



OCI Network Firewall – Key Use Cases



- Internet facing applications: Perimeter security
  - Protect against known vulnerabilities, until you have time to patch/update
  - For example: CVE-2017-5638 for Apache Struts
- Outbound: Protect against exfiltration
  - Allow Ubuntu servers to only do apt-get to *.canonical.com for updates
  - Allow only connections to payment gateway to *.amex.com
- East-West between VCNs or subnets: App Segmentation & Zero Trust
  - Block all threats from moving laterally between different trust domains
  - Allow only approved DB admins to only run SQL transactions against MySQL

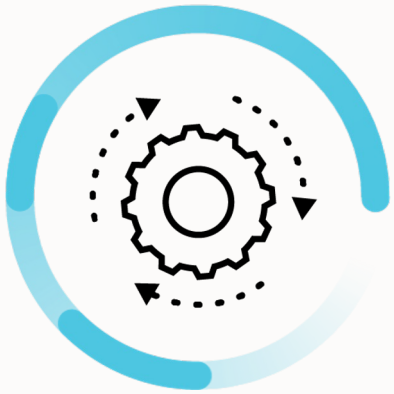
OCI Network Firewall Is...

Best-in-class

Powered by Industry Leading Palo Alto Networks technology, best-in-class network security for all your apps

Cloud-Native

Deep integration with OCI platform and features, cloud-native form factor & deployment models



Automated

Easy integration into DevOps processes for automated deployment and scaling

Easy to Manage

Centralized management and Flexible Policy Enforcement

Thank you