Firewalls

Security in Computer Networks

R. Venkateswaran

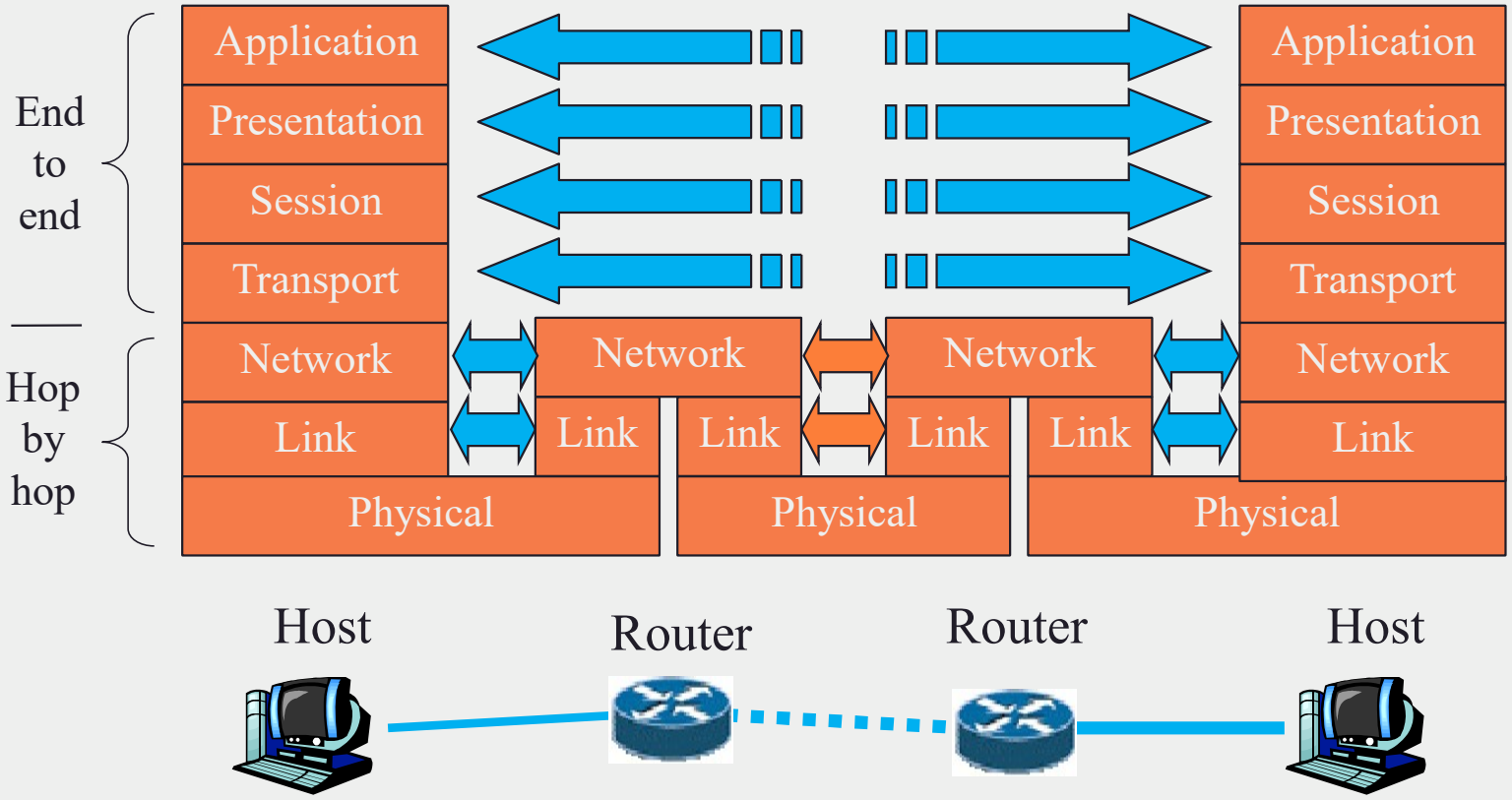
Acknowledgment

The material used in this slide deck contains lots of borrowed text and figures from various sources found on the Internet.

My humble THANKS to respective Authors

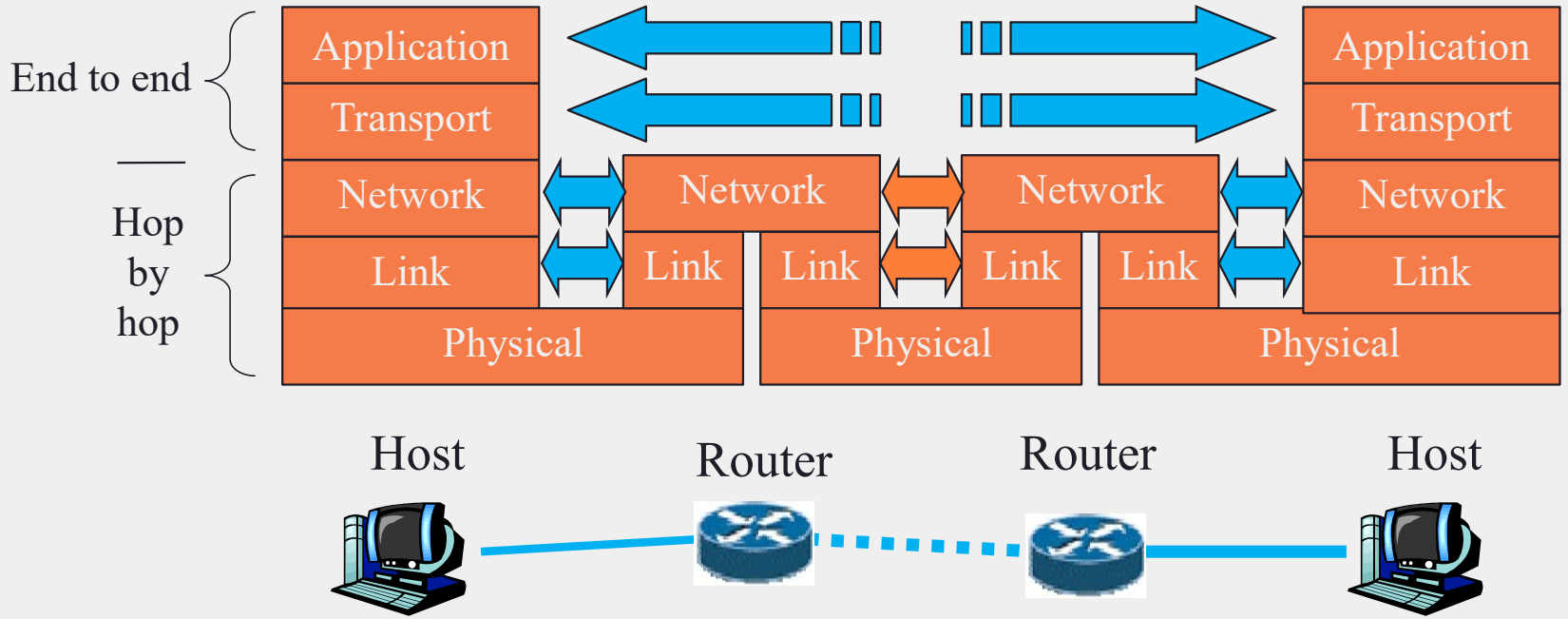
© 2025 R Venkateswaran

OSI 7 Layer



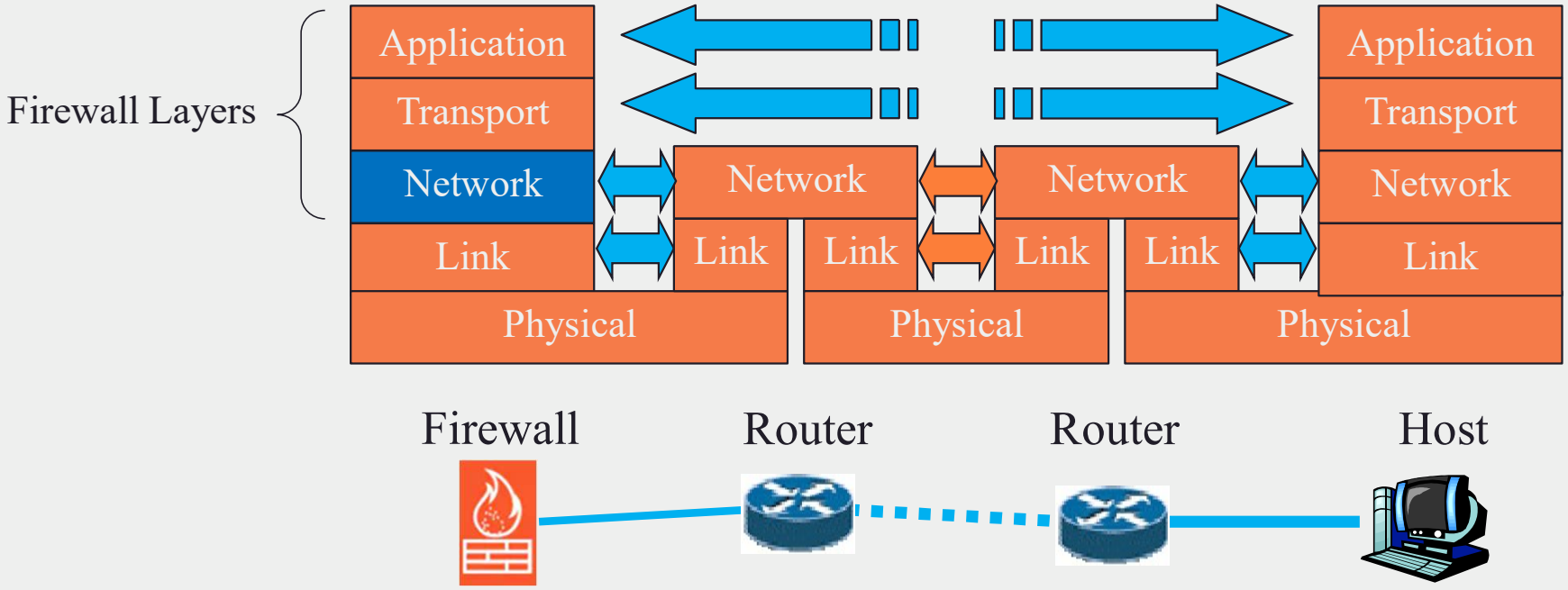
© 2025 R Venkateswaran

TCP/IP Layers



© 2025 R Venkateswaran

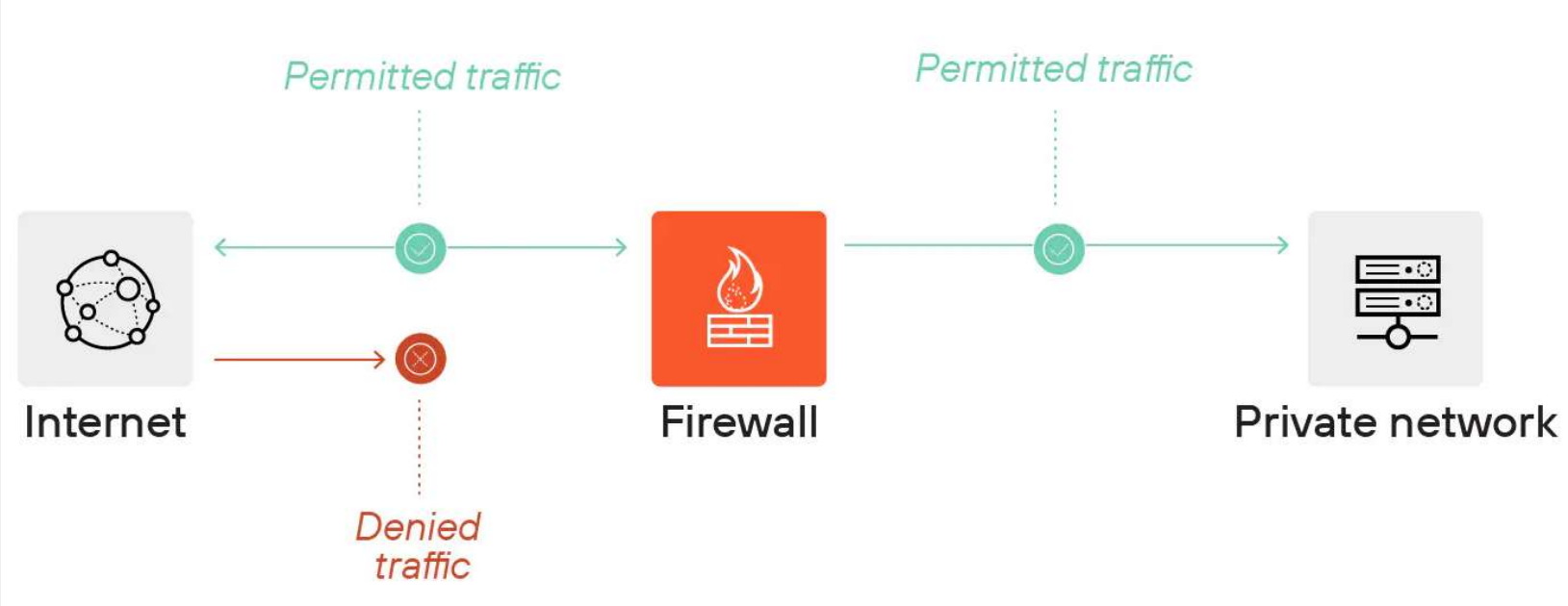
Firewall Layers



© 2025 R Venkateswaran

What is a Firewall?

- **Barrier** between private and external networks
- **Checks** and **filters** data based on ***set security rules***



© 2025 R Venkateswaran

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall

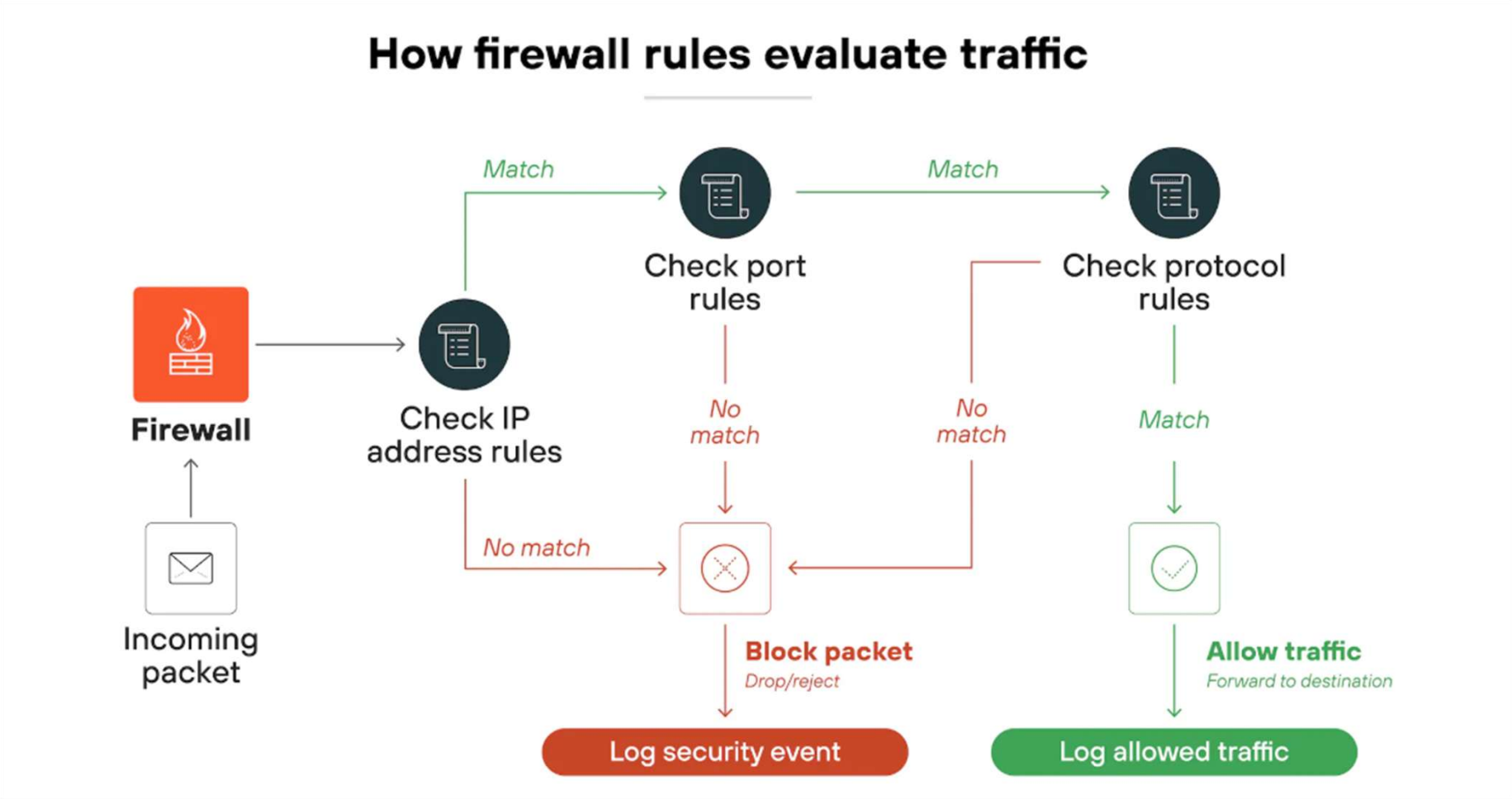
Different types of firewall

- Packet Filter (Layer 3/4)
  - Allows/Denies based on IP Packet header information
  - Can use Source/Dest IP Address, Protocol or Source/Dest Port No. (Transport Layer Header)
  - Each packet is evaluated independently to take the decision

© 2025 R Venkateswaran

Source: https://www.zenarmor.com/docs/network-security-tutorials/best-open-source-firewalls

Packet Filter – Stateless Firewall



© 2025 R Venkateswaran

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall

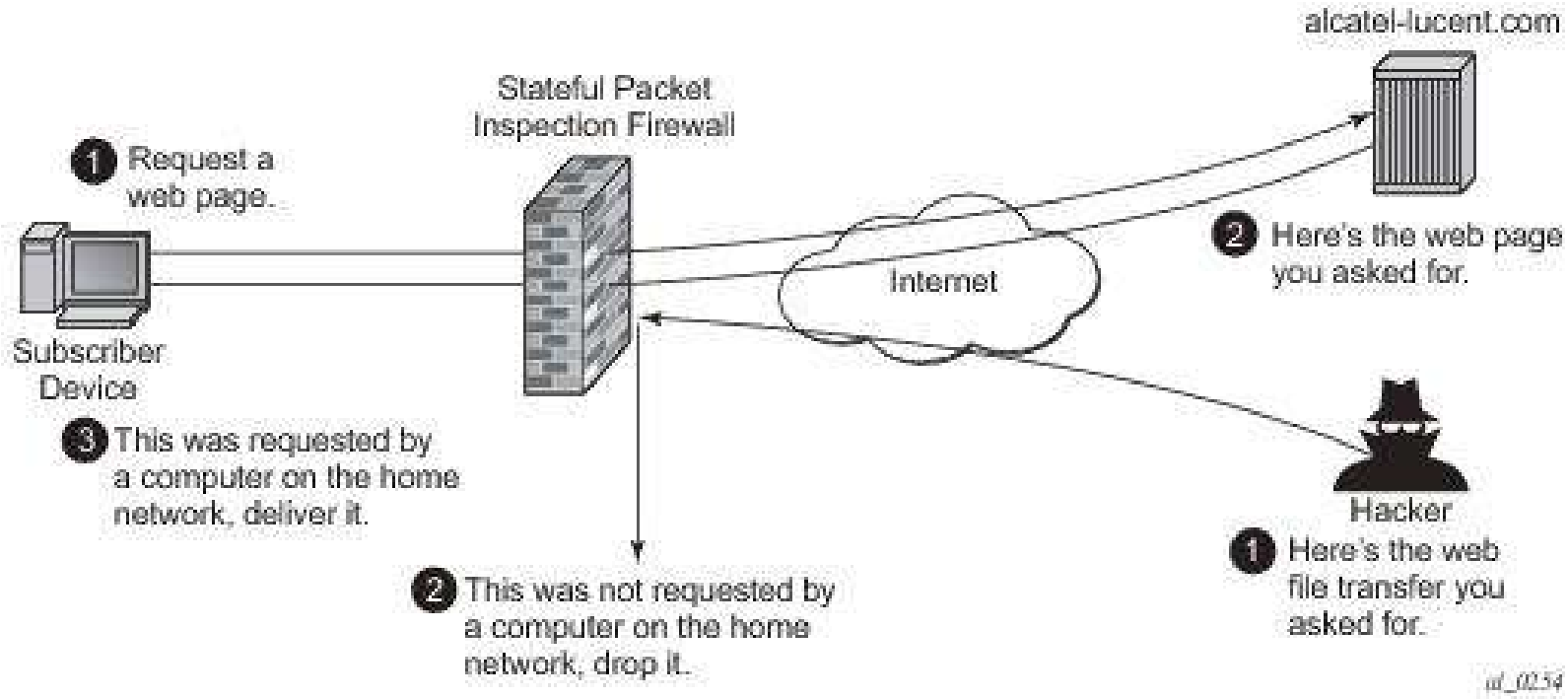
Different types of firewall

- Packet Filter (Layer 3/4)
  - Allows/Denies based on IP Packet header information
  - Can use Source/Dest IP Address, Protocol or Source/Dest Port No. (Transport Layer Header)
  - Each packet is evaluated independently to take the decision
- Stateful Packet Filter
  - All properties of Packet Filter apply
  - Further maintains state and keeps track of specific communications (remembers IP Addr/Port numbers)

© 2025 R Venkateswaran

Source: https://www.zenarmor.com/docs/network-security-tutorials/best-open-source-firewalls

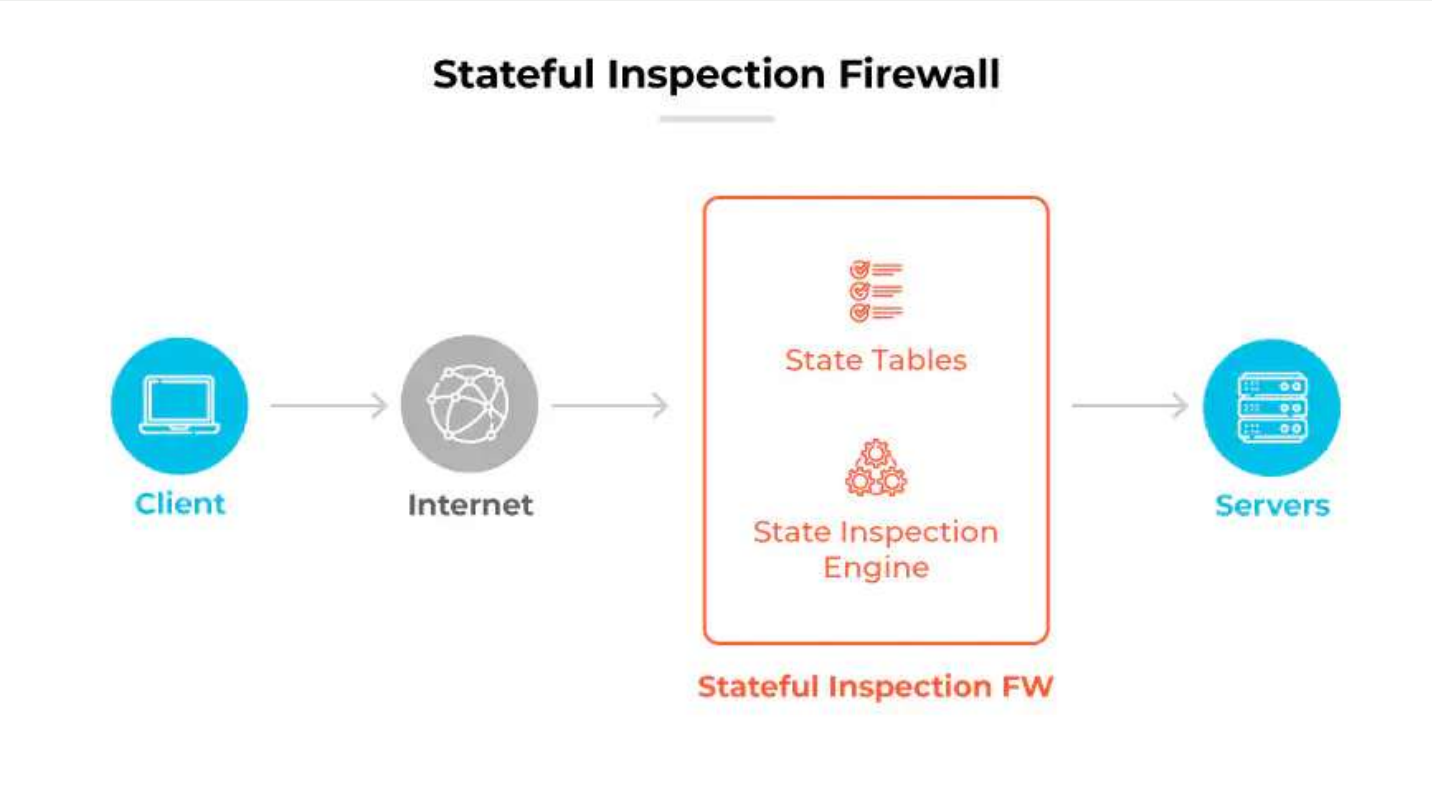
Stateful Packet Filter



© 2025 R Venkateswaran

Source: https://documentation.nokia.com/html/0_add-h-f/93-0267-HTML/7X50_Advanced_Configuration_Guide/AA-FW.html

Stateful Firewall



© 2025 R Venkateswaran

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-a-stateful-firewall

Stateful vs Stateless Firewalls

Stateful vs. Stateless Firewalls	
Stateful Firewalls	**Stateless Firewalls**
• Track ongoing connections	• Inspect packets individually
• Understand traffic context	• Rely on set rules
• Remember previous interactions	• No memory of past traffic
• Detect patterns for security	• Block by basic criteria
• Manage complex traffic types	• Simple, uniform filtering
• Ideal for dynamic networks	• Suitable for basic needs
• Provide detailed access control	• Offer general access control

© 2025 R Venkateswaran

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-a-stateful-firewall

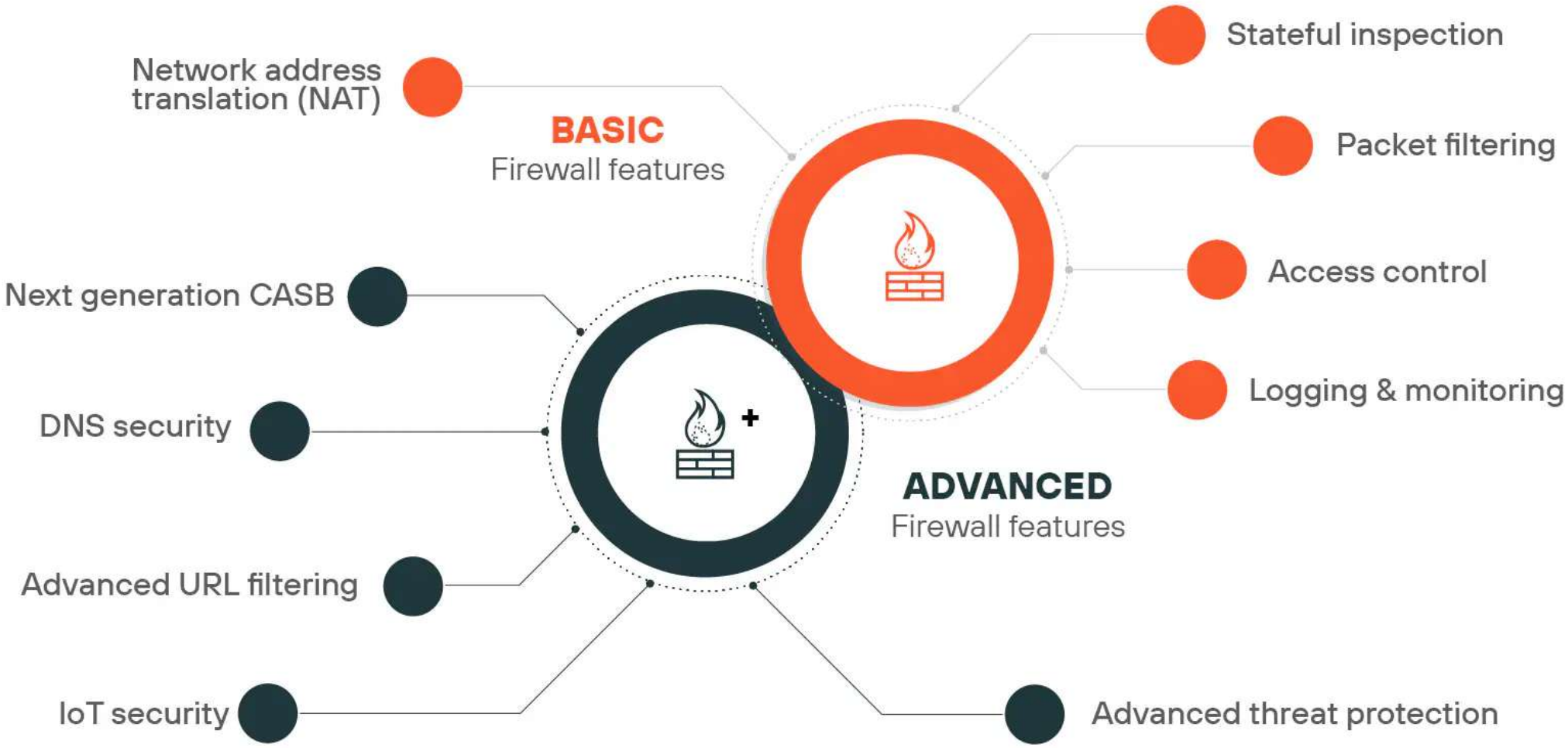
Different types of firewall

- Packet Filter (Layer 3/4)
  - Allows/Denies based on IP Packet header information
  - Can use Source/Dest IP Address, Protocol or Source/Dest Port No. (Transport Layer Header)
  - Each packet is evaluated independently to take the decision
- Stateful Packet Filter
  - All properties of Packet Filter apply
  - Further maintains state and keeps track of specific communications (remembers IP Addr/Port numbers)
- Layer 7 / Application Layer Firewall
  - All properties of Stateful Packet filter apply
  - Web/content filtering
  - Application awareness and control to see and block malicious applications
  - Integrated intrusion detection and prevention

© 2025 R Venkateswaran

Source: https://www.zenarmor.com/docs/network-security-tutorials/best-open-source-firewalls

Firewall features



© 2025 R Venkateswaran

Firewall features		
Category	**Feature**	**Description**
Basic	Packet filtering	Evaluates packets based on criteria like IP address or port to allow or block traffic.
	Stateful inspection	Tracks the state of active connections to allow only legitimate traffic.
	Network Address Translation (NAT)	Modifies packet IP addresses to conserve addresses and hide internal network structure.
	Logging and monitoring	Records network activity for analysis and response to potential threats.
	Access control	Applies rules to regulate which users or systems can access network resources.
Advanced	Advanced threat prevention	Uses deep learning to detect zero-day attacks and automate protection workflows.
	Advanced URL filtering	Uses real-time deep learning to stop known and unknown web threats.
	DNS security	Applies ML and analytics to block advanced DNS-based attacks and reduce tool sprawl.
	IoT security	Segments and protects IoT devices using Zero Trust and contextual machine learning.
	Next-generation CASB	Secures SaaS apps in real time with deeper visibility and modern data protection.

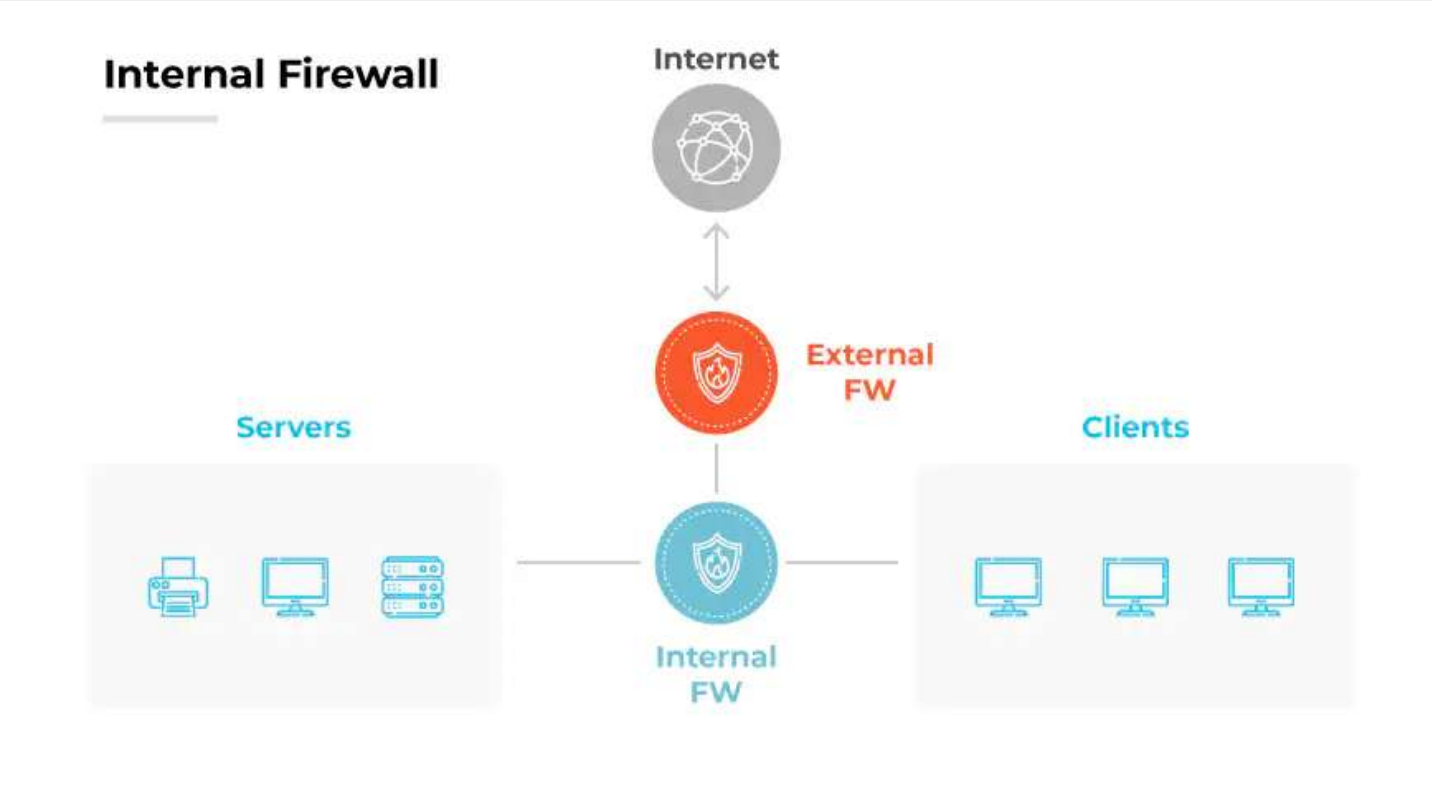
Source: https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall

Firewall benefits		
Category	**Benefit**	**Description**
Basic	Monitoring and filtering network traffic	Inspects data packets and blocks harmful patterns using stateful inspection.
	Preventing virus infiltration	Blocks known virus patterns and supports antivirus tools. NGFWs improve detection of advanced threats.
	Blocking unauthorized access	Applies access controls to limit interactions to trusted sources only.
	Upholding data privacy	Prevents sensitive data exposure by monitoring inbound and outbound traffic.
	Supporting regulatory compliance	Logs and controls access to sensitive data to support audit readiness and compliance.
Advanced	Enhanced user identity protection	Applies security policies based on user identity for more precise access control.
	Control over application use	Identifies and restricts app usage to approved applications only.
	Encrypted traffic security without privacy compromise	Inspects encrypted traffic for threats while preserving user privacy.
	Advanced threat protection	Protects against known and emerging threats across multiple attack vectors.
	Automated threat intelligence sharing	Detects and responds to threats using shared global intelligence feeds.
	Zero Trust principles	Applies continuous authentication and verification to reduce implicit trust.

Source: https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall

Firewall Deployments

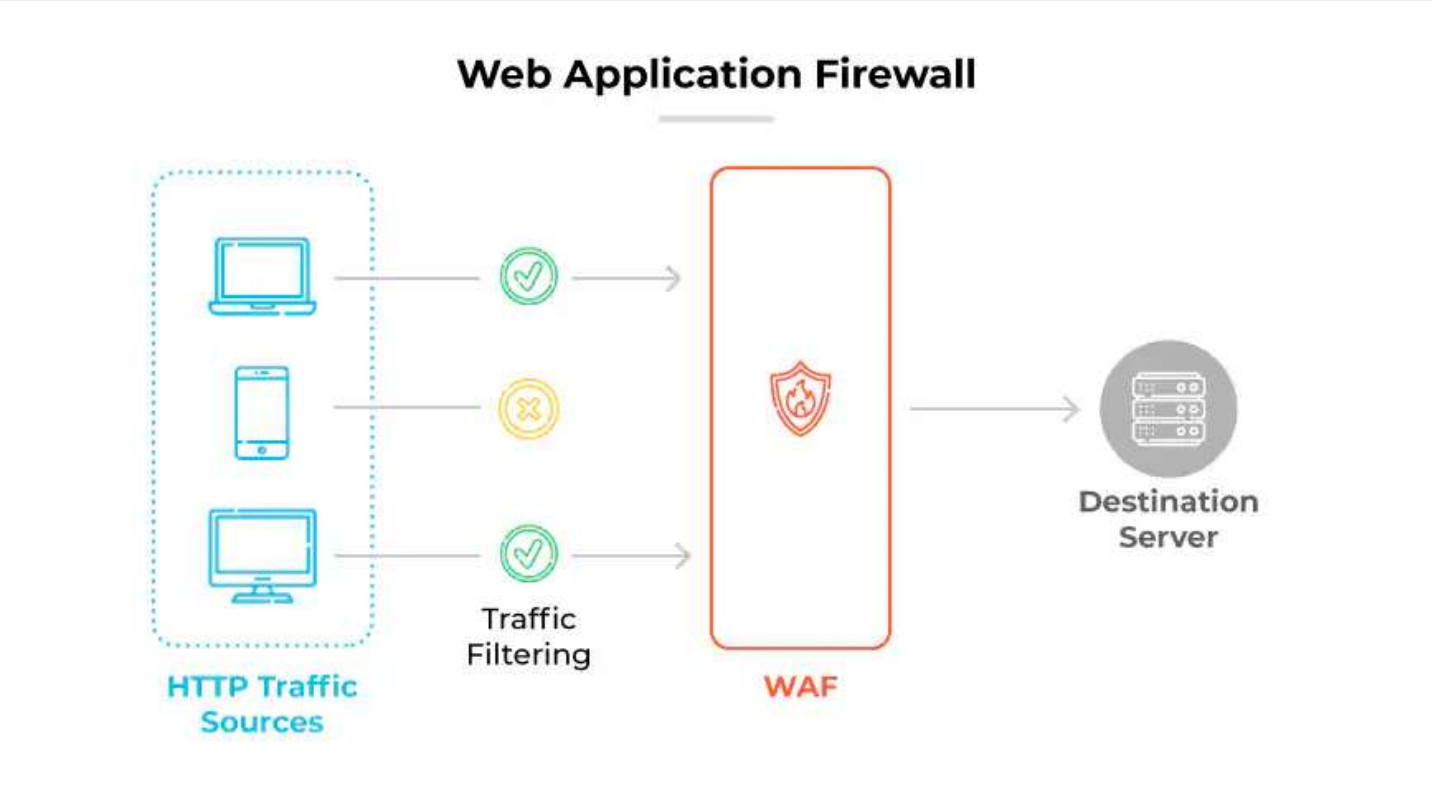
External (North-South) and Internal (East-West) Firewall



© 2025 R Venkateswaran

Source: https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls

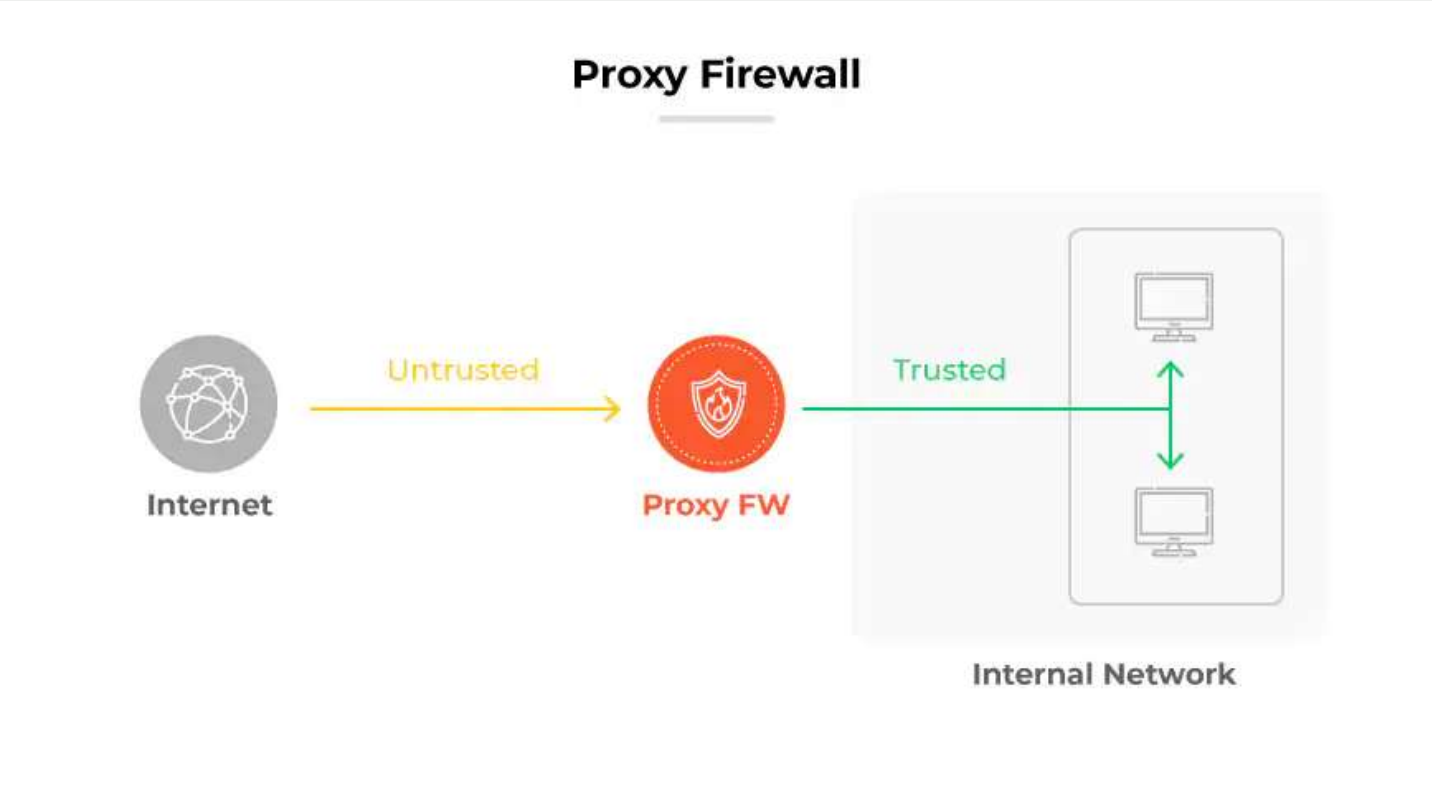
Web Application Firewall – prevents internal content from leaving the Enterprise



© 2025 R Venkateswaran

Source: https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls

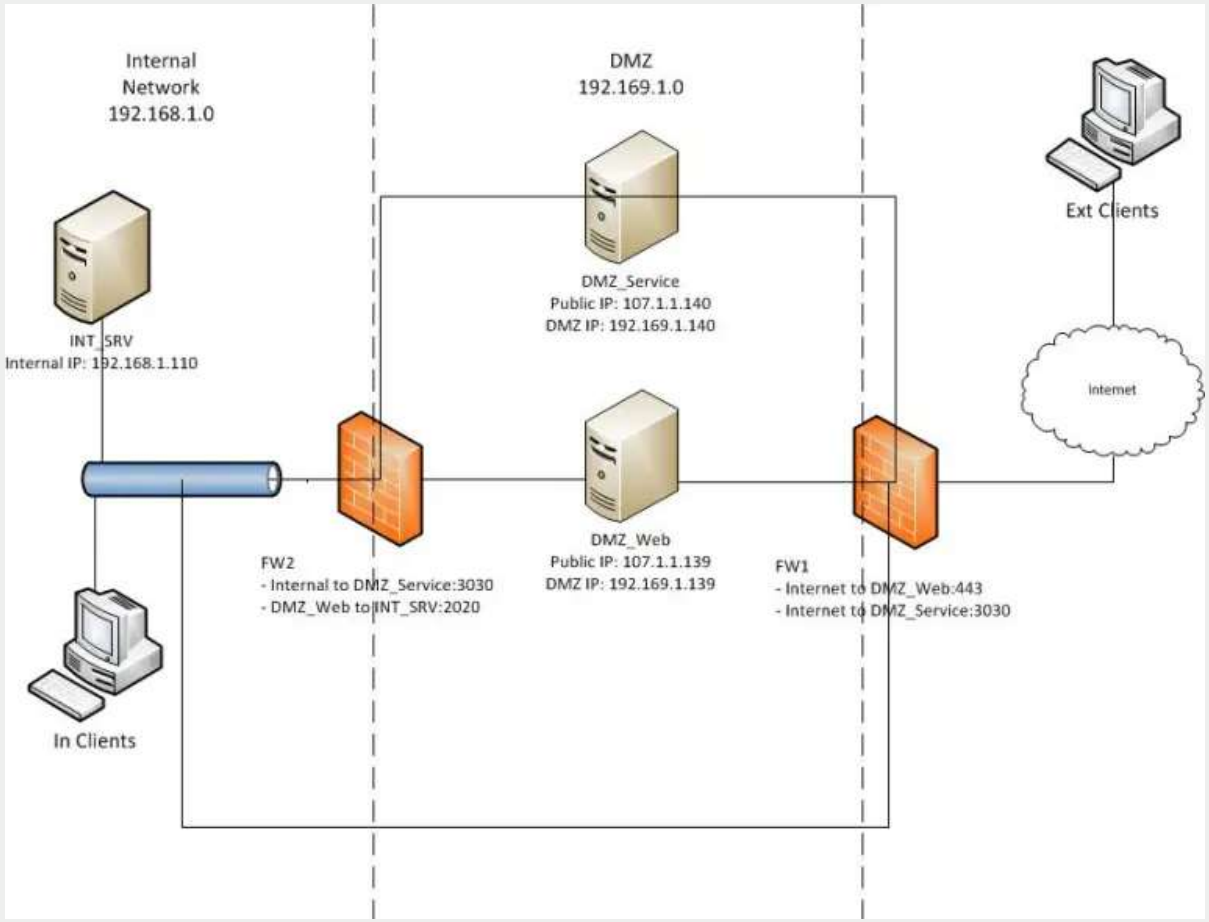
Proxy Firewall



© 2025 R Venkateswaran

Source: https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls

Demilitarized Zone (DMZ) setup in Enterprises



© 2025 R Venkateswaran

Source: https://tolumichael.com/dual-firewall-vs-single-firewall-dmz/

Questions and Discussions

Email: venkateswaranr.comp@coeptech.ac.in