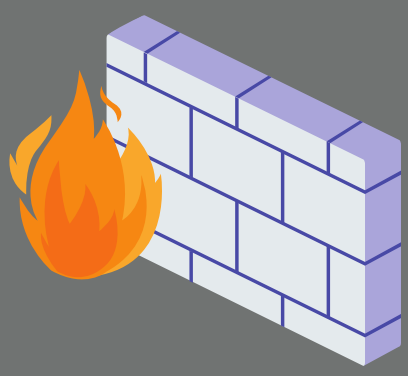


5 CHARACTERISTICS OF A NEXT-GEN FIREWALL

3RT NETWORKS

AS THE RANSOMWARE THREAT RISES, MANY ORGANIZATIONS ARE REVALUATING THEIR CYBERSECURITY TOOLS. FIREWALLS ARE THE FIRST LINE OF ANY ORGANIZATION'S CYBER DEFENSE. FOR THAT REASON, THEY ARE BECOMING THE FOCUS OF THE CYBERSECURITY DISCUSSION.

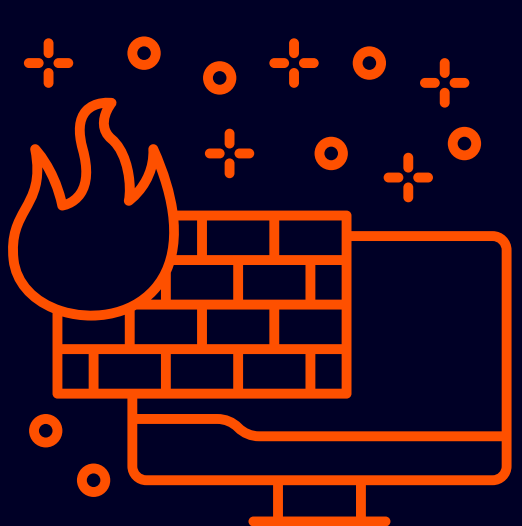
TRADITIONAL FIREWALLS

VS

NEXT-GEN FIREWALLS

A traditional firewall is designed to inspect network traffic. It allows or blocks traffic based on state, port, and protocol, and filters traffic based on administrator-defined rules. For example, a firewall can be programmed to only allow local traffic. It can also be used to block traffic to websites that are known to be threats.

Next-Generation Firewalls (NGFWs) can do everything a traditional firewall can do and more. In addition to basic access control and web-filtering, NGFWs are intelligent enough to block malware and application-layer attacks.



WHY USE A NEXT-GEN FIREWALL

Hackers are getting smarter. The rise of ransomware has put many industries in danger of losing millions of dollars. Even consumers are now affected. Instances like the Colonial pipeline attack left almost 97 million Americans without gas. The threat isn't going to slow down—experts estimate one ransomware attack occurs every 11 seconds.

CHARACTERISTICS TO LOOK FOR IN A NEXT-GEN FIREWALL

Breach Prevention and Identification

The most important function of a firewall is to prevent breaches. However, your defense can never be exactly perfect. That is why a NGFW needs to include advanced security that can detect malware that does slip through the cracks.

This security should include:

- Next-generation IPS
- URL filtering
- Sandboxing and advanced malware protection
- Threat intelligence updates

Network Visibility

If you know a threat has evaded your firewall, but you aren't sure where it is, you will be powerless to isolate it before it can do further damage. That's why NGFWs need to actively monitor your network at all times so it can pinpoint suspicious activity quickly.

Your firewall should give you visibility into:

- Threat activity across users, hosts, networks and endpoints
- When and where a threat originated
- All applications or websites currently being accessed
- Communications between virtual machines and file transfers

Flexible Deployment and Management

As your organization grows, your security solutions need to grow with you. Whether you are a small business or a vast enterprise, your firewall should work for you.

Your Firewall Should:

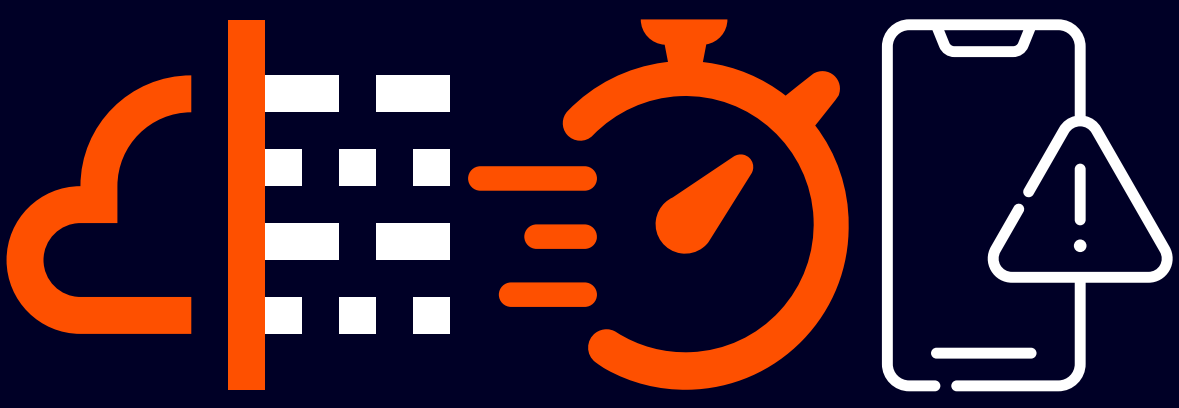
- Include management for every use case
- Deploy on-premise and in the cloud
- Empower you with a wide range of throughput speeds

Fastest Time-to-Detection

On average across all industries, the time between a threat entering a system and IT detecting it is 100 days. The amount of damage and loss that can happen in that time is immense. To avoid this, your NGFW needs to have an excellent time to detection.

Your firewall should be able to:

- Detect threats in seconds
- Detect successful breaches within hours or minutes
- Prioritize alerts so you can respond immediately
- Deploy consistent policies and automatic enforcements

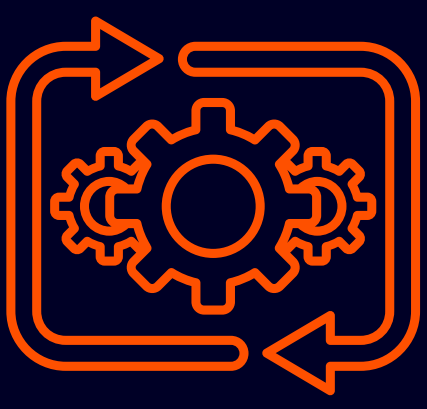


Automation

Your firewall should work in junction with the other devices and systems in your network. By seamlessly integrating with your other tools, it should grow your security posture, not weaken it.

Your firewall should:

- Seamlessly integrate with other security tools
- Automatically share data
- Automate security tasks



FIND THE FIREWALL THAT'S RIGHT FOR YOU

AT 3RT, OUR TECHNOLOGY PROFESSIONALS HAVE IN-DEPTH TECHNICAL KNOWLEDGE BASED ON YEARS OF ONGOING TRAINING, INDUSTRY CERTIFICATION PROGRAMS AND CUSTOMER EXPERIENCES. OUR ENGINEERS CAN HELP YOUR ORGANIZATION CHOOSE THE RIGHT FIREWALL FOR YOUR SPECIFIC SECURITY NEEDS. LEARN MORE ABOUT HOW 3RT CAN HELP.

LEARN MORE

3RT NETWORKS