Cyber Hub (/cyber-hub/) / Secure The Network (/cyber-hub/network-security/)

/ What is a Firewall? The Different Types of Firewalls (https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/)

/ 8 Firewall Best Practices for Securing the Network

8 Firewall Best Practices for Securing the Network

Having a firewall security best practice guide for securing the network can communicate to security stakeholders your company's security policy goals, ensure compliance with industry regulations and improve your company's overall security posture.

Below, we dive into some resources and eight firewall security best practices to begin your journey to a better security posture.

NGFW Demo (https://pages.checkpoint.com/next-generation-firewall-demo.html?utm_term=cyber-hub)

Read the Frost & Sullivan Report (https://resources.checkpoint.com/cyber-security-resources/frost-sullivan-check-point-company-of-the-year?utm_term=cyber-hub)

#1. Harden and Properly Configure the Firewall

Most all-in-one firewall solution operating systems are hardened by the vendor (https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80_30_Gaia_Hardening/Content/Topics/Gaia_Hardening.ht
tocpath=______3). If you are deploying a sof [illegible] e OS is first patched and hardened.

In addition to starting with a hardened OS, security admins will want to ensure the firewall is configured securely. Guides are available from vendors and third parties like the Center for Internet Security (CIS), which publishes the CIS Benchmarks Network Devices (https://www.cisecurity.org/cis-benchmarks/). Also, see the SANS Firewall Checklist (https://www.sans.org/media/score/checklists/FirewallChecklist.pdf).

#2. Plan your Firewall Deployment

Firewalls are a vital tool for applying zero trust security (/cyber-hub/network-security/what-is-zero-trust/) principles. They monitor and control inbound and outbound access across network boundaries in a macro-segmented network (/cyber-hub/network-security/what-is-macro-segmentation/). This applies to both layer 3 routed (/cyber-hub/network-security/what-is-osi-model/) firewall deployments (where the firewall acts as a gateway connecting multiple networks) and to layer 2 bridge (/cyber-hub/network-security/what-is-osi-model/) firewall deployments (where the firewall connects and isolates devices within a single network).

When deploying a firewall, the network interfaces of the firewall get connected to these networks or zones. These zones can then be used to simplify the firewall policy. For example, a perimeter firewall will have an external zone connected to the Internet, one or more internal interfaces connected to internal networks, and maybe a DMZ network (/cyber-hub/network-security/what-is-a-dmz-network/) connection. The firewall policy can then be customized as needed to add more granular control.

The firewall will need to be managed. An important question is, "Will the firewall also need a dedicated management interface?" Lights-out Management and serial console access should only be accessible from dedicated, secure networks.

Finally, one firewall is a single point of failure (SPOF). Deploying two or more in a High Availability (HA) cluster ensures security continues if one fails. A better option that continuously uses the resources of each cluster member is a hyperscale network security (/cyber-hub/network-security/what-is-hyperscale/) solution. This also should be considered for networks where the traffic load experiences seasonal peaks.

#3. Secure the Firewall

A firewall is a vital component of an organization's security infrastructure, and it needs to be protected against exploitation. To secure your firewall, take the following steps:

- Disable insecure protocols like telnet and SNMP or use a secure SNMP configuration (https://us-cert.cisa.gov/ncas/alerts/TA17-156A).
- Schedule periodic backups of the configuration and database.
- Enable auditing of system changes and send logs via secure syslog or another method to an external, secured, central SIEM server or firewall management solution for forensics and reporting.
- Add a stealth rule in the firewall policy to hide the firewall from network scans.
- Limit management access to specific hosts.
- Firewalls are not immune to vulnerabilities. Check with the vendor to see if there are any known vulnerabilities and security patches that fix the vulnerability.

#4. Secure User Accounts

Account takeover is a common technique used by cyber threat actors. To secure user accounts on your firewall, do the following:

- Rename or change default accounts and passwords
- Require MFA and/or set a strong password policy (complex passwords with upper and lower case letters, special characters, and numbers, 12 characters or longer, prevent password reuse)
- Use role-based access control (RBAC) for firewall admins. Delegate and limit access to match the user's need for access (i.e., allow only read-only access for auditors and create dedicated access roles and accounts for DevSecOps teams)

#5. Lock Down Zone Access to Approved Traffic

The primary function of a firewall is to enforce and monitor access for network segmentation (/cyber-hub/network-security/what-is-network-segmentation/).

Firewalls can inspect and control north/south traffic across a network boundary. In this macro-segmentation use case, the zones are broad groups like external, internal, DMZ, and guest Wi-Fi. They may also be business groups on separate internal networks like data center, HR, and finance or a production floor in a manufacturing plant that uses Industrial Control Systems (ICS) (/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/).

Firewalls deployed in virtualized private or public clouds can inspect traffic between individual servers or applications that change dynamically as instances are spun up. In this micro-segmentation (/cyber-hub/network-security/what-is-micro-segmentation/) use case, the zones may be defined by applications like web apps or databases. The function of the virtual server may be set by a tag and used in a firewall policy dynamically (/cyber-hub/network-security/what-is-security-management-architecture/how-dynamic-is-your-security-policy/) without human intervention, reducing the chances of manual configuration errors.

In both deployments, macro and micro, firewalls control access by setting a firewall policy rule, which broadly defines access based on traffic source and destination. The service or port used by the application can also be defined. For instance, ports 80 and 443 are default ports for web traffic. On a web server, only access to these ports should be allowed and all other ports blocked. This is a case where whitelisting the allowed traffic is possible.

Egress traffic from an organization to the Internet is more problematic for a whitelisting security policy because it's nearly impossible to say which ports are needed for Internet access. A more common approach for an egress security policy is blacklisting, where known bad traffic is blocked and everything else is allowed via an "accept all" firewall policy rule.

To detect known bad sites, additional security features can be enabled on the next-generation firewall (NGFW) (/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/) in addition to IP and port controls. These include URL filtering and application control. For instance, this can be used to allow access to Facebook but block Facebook games.

#6. Ensure Firewall Policy and Use Complies with Standards

Regulations have specific requirements for firewalls. Any security best practice must comply with these requirements and may require adding additional security controls to any deployed firewall. Example requirements include using virtual private networks (VPNs) to encrypt data in transit, antivirus to prevent known malware, and intrusion detection and prevention systems (IDS/IPS) to detect any network intrusion attempts.

For instance, PCI DSS (https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security) requires firewall zone-based controls between trusted and untrusted zones. This includes using a DMZ and perimeter firewalls between all wireless networks and the cardholder data environments. Some additional PCI DSS requirements include:

- Use anti-spoofing means to detect and block falsified source IP addresses from entering the network. For instance, block inbound traffic on the external interface with a source address of one of the internal networks.
- Not disclose private IP addresses and routing information to unauthorized parties using Network Address Translation (NAT) and removing route advertisements for private networks.
- Every half year, clean up any unnecessary, outdated, or mistaken rules, and ensure that all rule sets allow solely authorized services and ports.
- Encrypt the transmission of cardholder data across open, public networks.

- Install applicable vendor-supplied security patches. Install critical security patches within one month of release. (Given how quickly threat actors take advantage of known vulnerabilities, companies may want to change this to update when a patch is available. An NGFW that automatically updates IPS signatures can protect whole networks from newly announced vulnerabilities.)
- Processes must be in place to limit access based on need to know and according to job responsibilities.
- Track and monitor all access to network resources and cardholder data.
- Using time-synchronization technology, synchronize all critical system clocks and times.
- Regularly test security systems and processes.

#7. Test to Verify the Policy and Identify Risks

With a larger security policy, it can be difficult to visualize how it would process a new connection. Tools exist to perform path analysis and may exist in the security management system to search and find rules.

Also, some security management systems warn when a duplicate object is created or won't install a policy that has a rule that hides another. Regularly test your policy to verify it performs as designed to find unused and duplicate objects.

Firewall policies are typically applied in top-down order and can be optimized by moving top hit rules further up in the inspection order. Regularly inspect the policy to optimize your firewall performance.

Finally, perform regular penetration testing to identify any risks additional security measures that may be needed in addition to the firewall to secure your organization.

#8. Audit Software or Firmware and Logs

Regular audits are essential to ensuring that software and firmware are correct and up-to-date and that logs are correctly configured and operational. Some best practices for these audits include:

- Establish a formal change control plan for modifying the security policy to ensure security isn't compromised.
- Rules with Any set in the source, destination, or port may be holes in the security policy. When possible, change these to add the specific source, destination, or service that is the purpose of the rule.
- Create sections or layers to add a hierarchy to the security policy, making it easier to review.
- Add clean-up rules at the end of the section or layer that match the layer's intent (i.e., allow-all or deny-all).
- Add comments and names to rules to help identify the original purpose of each rule.
- Enable logging to better track network flows and add visibility for forensics investigations and reporting.
- Regularly review audit logs and reports to see who changed the firewall policy.

Recommendations for Check Point Policy Optimization

Check Point provides a number of resources to help with configuring your Check Point NGFW. For a preliminary discussion of the Check Point firewall policy, review this support article on Rulebase Construction and Optimization (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk106597). Also, if you're new to Check Point, check out the CheckMates Community Check Point for Beginners (https://community.checkpoint.com/t5/Check-Point-for-Beginners-2-0/bg-p/check-point-for-beginners-2-0).

For a deeper dive into how to better manage your Check Point solution, take one of our free eLearning courses (/elearning/). You're also welcome to ask for an NGFW or Security Management demo (/demos/#network).

Get Started

Schedule a Security Check Up (https://pages.checkpoint.com/security-checkup.html)

The Check Point Cyber Security Platform (/quantum/unified-cyber-security-platform/)

Check Point Next Generation Firewalls (/quantum/next-generation-firewall/)

Related Topics

Data Center Security Best Practices (/cyber-hub/cyber-security/what-is-data-center/data-center-security-best-practices/)

6 Pillars of Robust Cloud Security (/cyber-hub/cloud-security/what-is-cloud-native-security/)

Consolidated Security Architecture (/cyber-hub/cyber-security/what-is-a-consolidated-security-architecture/)