

Firewall Configuration Quick-Start Checklist

This checklist is designed to assist network administrators in the beginning stages of their firewall hardware configuration process. This is not an exhaustive list of all possible options, services, & considerations and as such should not be utilized as a finalized text for network security documentation. The purpose of this checklist is to help in gathering the necessary preliminary data that will be required while configuring your network.

If you have any questions about something you find in this checklist, **contact our Firewalls.com Professional Services Support team at 317-225-4117 for personalized assistance.**



Company Name:

Friendly Site Name:

Firewall Serial Number:

Firewall Secured with Rack Mount

Yes

No

Employee Completing Configuration:

Firewall Brand & Model:

Security Services Expiration Date:

Firewall has POE

Yes

No

Pre-Configuration

The specific goals of your firewall configuration will be highly shaped by the applications actually being utilized on your network and the users that access them. Therefore, the wisest first step in any configuration process should be to audit all of the variable details that the real-world usage of your network dictate. Use the space provided below to record relevant information about your applications and users, as these details will be referenced throughout the checklist.

Internally-Hosted Network Applications

Application Name	Users/Groups/Zones That Require Access	Internally Hosted?	
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>
		Yes <input type="checkbox"/>	No <input type="checkbox"/>

Pre-Configuration

Active User Groups & Zones

Group/Zone	Number of Users	Restricted Applications	Special Notes

Section 1 – WAN Settings

WAN Connection Type:

Dynamic (DHCP)

ISP Provider: _____

Download Bandwidth Speed: _____

Backup WAN Connection

Yes

No

Static IP

ISP Provider: _____

Download Bandwidth Speed: _____

WAN Public IP Address: _____

WAN Subnet Mask: _____

WAN Gateway: _____

WAN DNS Server 1: _____

WAN DNS Server 2: _____

Backup WAN Connection

Yes

No

Section 2 – LAN Settings

LAN IP Address: _____

Subnet Mask: _____

Internal DNS Server IP Address: _____

DHCP Enabled on Firewall LAN

Yes

No

List any additional Networks, VLANs, or Static Routes:

Section 3 – Wireless Networks

Corporate Network SSID: _____

Pre-Shared Key: _____

Wireless Network Bridged to the Internal Network

Yes

No

Include a Guest Network

Yes

No

Section 4 – Firewall Rules & Policies

Outbound Policies

LAN > WAN Allow All Outbound

Yes

No

Block Custom TCP/UDP Ports Outbound

Yes

No

Additional Ports Opened Outbound: _____

Inbound Policies

Port Forwards for VOIP

Yes

No

Port Forwards for Email:

Yes

No

Additional Port Forwards for Internal Hosting Services: _____

Section 5 – Security Settings

Inspection Mode (Circle One)

Flow Based

Proxy Based

GeoIP Blocking

Enable:

Yes

No

GeoIP Blocking Exclusions: _____

Content Filtering Service

Enable:

Yes

No

Content Filtering by Categories

Allow: _____

Monitor: _____

Block: _____

Additional Websites or Categories to Allow/Monitor/Block: _____

Access Control Lists

Enable:

Yes

No

Resources & Network Functions

Allow: _____

Prioritize: _____

Block: _____

Additional Security Services

Gateway AntiVirus:

Yes

No

Anti-Spyware:

Yes

No

Intrusion Prevention System:

Yes

No

Section 6 – Advanced Features & Options

Active Directory Integration:

Yes

No

Enable Single Sign On:

Yes

No

Enable MAC-IP Trusted Pairing:

Yes

No

Enable DPI/SSL:

Yes

No

Email SMTP:

Yes

No

High Availability:

Yes

No

VOIP Configuration:

Yes

No

Enable SMAC Filtering:

Yes

No

Create Local Backup:

Yes

No

Enable Advanced Threat Protection:

Yes

No

Disable HTTP Management Access:

Yes

No

Default Admin Credentials Changed:

Yes

No

Additional Cloud Security & AWS Requirements: _____

Additional Regulatory Compliance Requirements: _____

Section 7 – Firewall Rule Documentation

Best practices dictate that admins maintain dynamic documentation for all of the rules active on a network firewall. The next two pages of this document will help outline the types of rules and their functions implemented during this configuration.

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Firewall Rule Name: _____
Date Added: _____
Expiration (If Applicable): _____
Rule Created By: _____
Purpose of Rule: _____
Services & Applications Affected: _____
Users, Groups, & Devices Affected: _____

Section 8: Physical Security

While all previous sections of this document covered the virtual attack vectors of a network firewall, it is also critically important that physical security of the appliance be considered and documented. Who has access to your server rack, what times and days of the week your appliances are accessible, and procedures for physical access can play as important a role in network security as any service subscription or configuration setting.

Friendly Name of Firewall Location: _____

Who Has Access to Server Rack Housing This Firewall: _____

Which Days of the Week & Times Is Server Rack Accessible: _____

Who to Contact in Case of Natural Disaster or Emergency Loss: _____

Section 9: Additional Notes

Have questions about any of the Professional Service options offered by Firewalls.com? Give us a call at 866-403-5305 or email sales@firewalls.com for information about configuration services, next-gen firewall products, network security bundles, Security-As-A-Service, & more. Our Professional Services team is 100% local, performing all work out of our Indianapolis-based Security Operations Center.

Managed Security Service

Configuration Services

Premium Support

Custom Security Solutions