Five Steps to Firewall Planning and Design

Table of Contents

©2015, Juniper Networks, Inc.

Executive Summary

The guidelines provided in this white paper make up some of the best practices entailed in creating an overall security policy for your organization that underlies deployment of effective firewalls. These guidelines are summarized from a longer document by Juniper Networks, Learn About Firewall Design, which can be found at http://www.juniper.net/techpubs/en_US/learn-about/LA_FIrewallDesign.pdf.

Introduction

Firewall Planning and Design Processes

As many people know, firewall design entails far more than just configuration of the firewall. Processes that comprise an organization's overall security policy inform decisions such as which firewall features are used, where the firewall is enforced, and ultimately, how the firewall is configured.

Firewall technology has evolved from packet filter firewalls to today's next-generation firewalls, and at each stage, new services and solutions have emerged to address the expanding complexity of the cyber landscape—to protect resources and to stop cyberattackers from breaching the firewall for nefarious purposes. Today's sophisticated firewalls incorporate a range of features and services that are the outgrowth of these stages of firewall evolution.

There are five firewall design tasks that apply whether you plan to deploy a single firewall with limited features or multiple full-featured firewalls for the various areas of your environment.

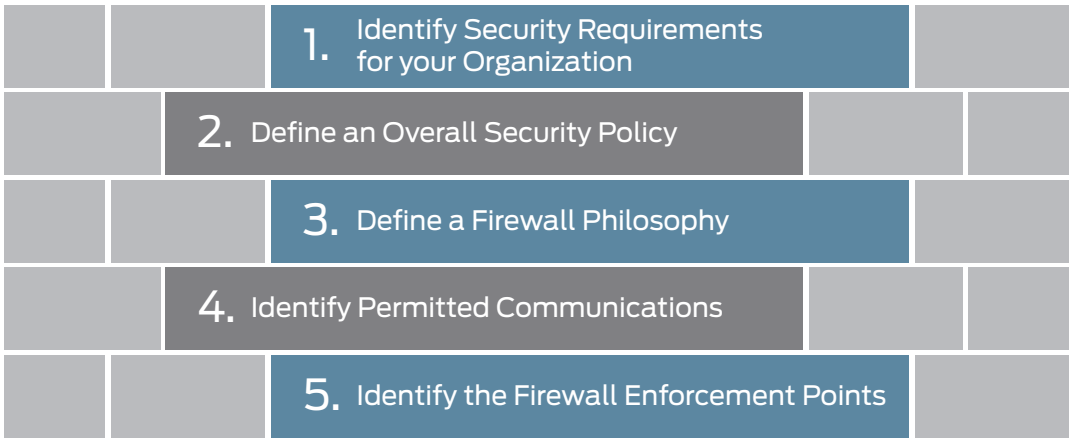

Figure 1: Five best-practice steps to optimal firewall design

Step 1. Identify Security Requirements for Your Organization

Before you can secure your network environment, you need to understand your organization's resources and security requirements, and your current security posture. Here are suggestions on how to carry out that assessment:

- Conduct an inventory to identify what it is that you need to protect.
- Catalog your environment's assets and resources. For example:
  - Identify resources deployed throughout your campus, including the hardware and software that make up your environment and network.
  - Characterize your resources. For example, identify publicly available databases and customer-facing systems, resources that have high concentrations of sensitive data, and legacy security devices.
  - Identify your data. Specify how to handle and protect it. Assign quantifiable value to your resources. Consider data sensitivity and who uses the data. Identify transaction flows. Data is most exposed to risk when it moves.
  - Note vulnerabilities and potential threats to each resource. Identify systems used by IT—breaches to IT security could disable the entire network.
  - Scan your Internet address ranges.
  - Identify your partners and guest access network connections.
  - Change hats—view your environment as a cyberattacker would.
  - Ensure that your operating systems and applications are updated with the latest patches.
  - Have a third-party group conduct a vulnerability assessment. The group can identify critical vulnerabilities in your network.

©2015, Juniper Networks, Inc.

Step 2. Define an Overall Security Policy

Regardless of its size, before an enterprise can secure its assets, it requires an effective security policy that does the following:

- Identifies all network resources and their required security
- Includes a network infrastructure map that is revised as systems are added to or removed from the topology
- Encompasses the organization's firewall philosophy
- Covers permitted communications and access policies and defines access rights and access levels based on employee job functions and roles
- Defines the culture of the organization with respect to security and how its policies are applied
- Defines security threats, how to thwart them, and how to respond to successful attacks

A well-documented security policy can guide network administrators in maintaining and managing the firewall.

Table 1 summarizes some security policy best practices that you can use to begin defining your own security policy.

Table 1. Security Policy Definition Process

Task	Instructions
Define your environment.	Identify the services and systems you want to protect. You cannot deploy a robust firewall unless you have first determined what you must protect.
Identify resources, systems critical to the network, and other systems that require strong defense tactics.	Create network diagrams and maps that identify the following information: • The locations of all hosts in your environment and the operating systems that they run • The types and locations of other devices, such as bridges, routers, and switches • The types and locations of terminal servers and remote connections • Descriptions and locations of any network servers, including the operating system and any installed application software (including version numbers), and their configuration information • Location and description of any network management systems used
Define the main threats in plain language and the actions to be taken in the event of a security breach.	Define threats to the system. Define the actions that administrators take after an attack has been identified and resolved. For example: Do you attempt to identify the attacker? If so, what software or other method do you use? Do you plan to prosecute? Do administrators contact the ISP to report the attack?

Step 3. Define a Firewall Philosophy

A firewall philosophy is the part of your site's security policy that applies strictly to the firewall and defines your overall goals for the firewall. It provides written guidelines that any administrator can follow in implementing the firewall deployment. If you identify how resources, applications, and services are to be protected, it is much easier to define and configure the firewall itself.

A firewall philosophy is also essential when new hosts and software are added to the network. It can serve as a means of communicating the current firewall deployment, and factors that contribute to its deployment, to successive IT personnel.

Even simple firewalls need a well-documented firewall philosophy to guide their design, deployment, and maintenance. Without one, the firewall itself might become a security problem. Table 2 suggests some components you can include in your own firewall philosophy review document.

©2015, Juniper Networks, Inc.

Table 2. Firewall Philosophy Guidelines

Task	Steps
Identify the objectives for your firewall deployment.	Define your primary goals: • Are they to protect against threats from outside your organization? • Are they to protect against insider attacks? • Are they to monitor user activity? • Are they for uses unrelated to security, such as maintaining control over network usage? Define your goals in regard to integrity, confidentiality, and availability. Define your requirements for manageability versus sophistication.
Specify how the firewall is to be managed and updated.	• Identify the subnetworks to be used. • Specify whether you plan to use Network Address Translation (NAT).
Identify security vulnerabilities in the network and rectify them.	• Record this information in your firewall philosophy document for historical purposes. • Define what constitutes an attack. Determine, for example, whether you consider information gathering (reconnaissance missions) an attack. Do you restrict qualification of attacks to incidents that do damage?
Test the network integrity before you deploy the firewall for production.	Test the network to ascertain that it has not been breached and to ensure that it is not infected with viruses before you deploy the firewall.

You can establish an overall approach or security stance of least privilege or greatest privilege to guide the development of your firewall philosophy, depending on your network requirements:

- **Least privilege**—Lock down the network. Block all network connections in both directions, within the LAN and in relation to the Internet. After all interzone and intrazone traffic is blocked, you can unblock it selectively through policy configuration. The policy configuration can then define precisely and incrementally what is allowed. Least privilege is the more common approach to deployment of a firewall.
- **Greatest privilege**—Trust everything inside the network. The policy can then designate specific denial of access to close down access as appropriate. This stance is sometimes taken when the firewall is deployed inline while network activity continues. In this case, the stance allows the firewall to be deployed without disturbing normal business activity that is conducted using the network.

Step 4. Identify Permitted Communications

Define an acceptable use policy to specify the types of network activities that are allowed for use on the LAN and allowed for Internet services and applications.

To design effective firewall policies, you must understand which applications are currently used. Network administrators are not always aware of all of them, especially in regard to use of the Internet. Employees might not be aware that social media and instant messaging applications open entry points into the network that provide easy access for attackers. Maintaining a list of allowed applications and services, any known security risks associated with them, and the means used to secure the application or service is a best practice.

Understand and document the workflow in your organization based on employee roles and applications allowed for each role.

Gathering this information can help you define your firewall. Most of the legwork is already done, and then the firewall configuration simply becomes a software configuration task.

When you define allowed communications and access permissions, take into account the type of firewall that you plan to deploy to enforce these requirements. Although packet-filtering firewalls that operate up to Layer 3 (transport) and stateful firewalls that operate up to Layer 4 (network) continue to serve specific purposes, they do not provide adequate network protection required to defend against Web-based attacks.

Web-based attacks can easily pass through well-known ports—HTTP (port 80), HTTPS (port 443), and e-mail (port 25). Packet-filtering and stateful firewalls that are based on protocols and ports are unable to distinguish legitimate applications that rely on those protocols and ports from illegitimate applications and attacks. They are unable to distinguish one kind of Web traffic that uses the port from another.

©2015, Juniper Networks, Inc.

The emergence of application firewalls has given IT teams granular control over access to applications. Application firewalls examined the application and protocol with which a packet was associated and the ports it used. They could monitor and block application traffic and system service calls, controlling access to services and applications previously made widely available.

After you have defined the allowed services and applications and your user access workflow, it is vital to communicate that information to employees in a way that is visible and available.

Step 5. Identify the Firewall Enforcement Points

Every network has unique characteristics that require equally unique firewall deployment solutions. Many companies deploy different types of firewalls throughout their environment based on the assets and access points they want to protect.

Regardless of where the firewall is enforced, simple firewall designs are more likely to be secure and are easier to manage than complex ones. While special requirements might warrant firewall complexity, unwarranted design complexity lends itself to configuration errors.

Determining enforcement points is fundamental to firewall design. As a rule, the primary use of the firewall should dictate its enforcement points and configuration. Firewalls are commonly deployed at the edge, or border, between the private LAN and a public network, such as the Internet. However, there are other firewall enforcement points to consider, such as the DMZ, also known as a perimeter or bastion network. Firewalls are designed and enforced differently in these areas of a network because each area has its specific security requirements, as detailed in Table 3.

Table 3: Network Areas and Firewall Enforcement

Edge: Internet-Facing Firewall • Protects the border of the network against unauthorized access from the Internet • Defends its hosts against all forms of attack from outside the LAN • Ensures that authorized users are able to perform required tasks by thwarting denial of service (DoS) and other forms of lockout attacks launched from outside the LAN • Guards the entry points to the LAN by checking each packet to determine if it is allowed through
Core: Corporate-Facing Firewall • Protects corporate resources from internal opportunistic, accidental, or malicious attacks, such as data theft or DoS floods instigated through a virus • Provides outgoing traffic-handling policies • Ensures that employees have access only to the Internet services they require • Protects against employee use of the network to launch outside attacks
Firewall in the DMZ • Provides additional security by creating a less secure area in front of the private network to provide a first line of defense behind which the internal LAN hosts can safely exist • Contains, as a rule, publicly accessible servers and bastion hosts—if servers are attacked, hosts within the LAN are not compromised

Conclusion

To deploy effective firewalls for your organization, you must take into account wide-ranging security concerns and assessments to implement a security policy and firewall philosophy whose plans and processes give your environment the kind of security it requires. The result of this work influences your decision about how many firewalls must be deployed, their types, and their enforcement points. The task is easier if you follow standard approved practices, which have been covered in this document. Briefly, they are as follows:

Conduct an inventory to identify the resources in your environment and network that must be secured. Catalog and characterize each resource, and assign quantifiable value and importance—identify networking equipment, publicly available customer-facing servers, internal servers, and all other equipment and data storage. Note which devices have high concentrations of sensitive data, which devices are legacy, and which devices are used by IT. Document your transactions to secure the data they move.

Create a security policy document that includes your inventory assessment and network diagrams and maps. Use a dynamic network topology application that maps your infrastructure initially and updates the map automatically as you add machines and enter the data. Define threats to your system and how administrators who manage and maintain the firewall should respond to them.

Include in your security policy a firewall philosophy document that applies exclusively to the firewall. Consider that current and future administrators will rely on it for direction. Note your firewall security goals: Should your firewall protect against outside attacks, insider attacks? Do you use it to maintain control over network usage? Do you require more than one type of firewall?

©2015, Juniper Networks, Inc.

Define an acceptable use policy that identifies permitted communications and program access rights. Take into account your organization's workflow and assign rights to roles and individuals.

Let these fundamental processes guide you through the work of implementing strong, effective security for your environment. To learn more about these guidelines and other important networking topics, visit http://www.juniper.net/techpubs/en_US/learn-about/index.html.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

Copyright 2015 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos and QFabric are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

2000591-001-EN Oct 2015