Learn About Firewall Design

This *Learn About* briefly introduces guidelines for network firewall planning and design. It summarizes the processes entailed in creating a security policy for your organization that underpins effective firewall design. It also provides links to sites and publications that elaborate on or are related to these processes.

Firewall Planning and Design Processes

As everyone knows, firewall design entails far more than configuration of the firewall. Processes that comprise an organization's overall security policy inform decisions such as which firewall features will be used, where the firewall will be enforced, and, ultimately, how the firewall will be configured.

Firewall technology has evolved from packet filter firewalls to today's next-generation firewalls. At each stage of firewall evolution, new services and solutions emerged to address the expanding complexity of the cyber landscape, to protect resources, and to block and trap attempts by cyber attackers to breach 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.

This *Learn About* covers a set of five sequential steps to follow when designing a firewall, as shown in Figure 1, and best practices accenting firewall planning and design are provided throughout. These steps apply whether you plan to deploy a single firewall with limited features or full-featured firewalls for various areas of your environment.

Step 1. Identify Security Requirements for Your Organization

Step 2. Define an Overall Security Policy

Step 3. Define a Firewall Philosophy

Step 4. Identify Permitted Communications

Step 5. Identify the Firewall Enforcement Points

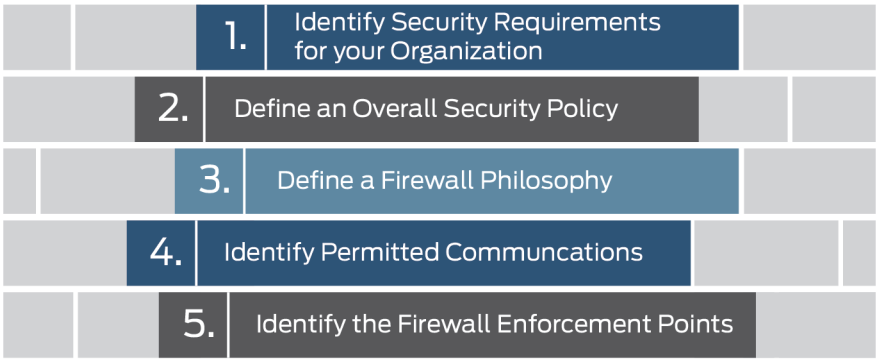

Figure 1 Five Best-Practice Steps to Optimal Firewall Design

Step 1. Identify Security Requirements for Your Organization

Security requirements differ among organizations. Before you can secure your network environment, you need to understand your organization's resources, evaluate their security requirements, and assess your current security posture.

You can use the information that you collect during this process as input to the remaining steps involved in defining the security requirements for your environment in preparation for configuring and deploying your firewall.

Here are some suggestions.

Conduct an inventory to identify what it is that you need to protect. Every environment is unique.

Catalog your environment's assets and resources. For example:

- Identify your organization's resources including the hardware and software that comprise your environment and network. Include resources deployed throughout your organization's campus, both at headquarters and branches.
- 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.
  - Organizations have many kinds of data to protect, some of it more valuable and sensitive than others. Your business data may include customer records, a range of employee information, account records, financial information, marketing plans, intellectual property, and state, local, and federal tax information. Specify how that data is handled and protected.
- Identify transaction flows in your environment.
  - Data is most at risk when it is moved and used throughout the organization. Every time data moves, it is exposed to risks.
- Identify your connections to partners and guest access networks.
- Scan your Internet address ranges.
- Assign quantifiable value and importance to your resources. For example:
  - Consider the degree of sensitivity of each type of data and who will use it.
  - Identify systems used by IT to manage your environment. Breaches to their security could disable the entire network and its resources.

Identify and assess the vulnerabilities or potential threats to each resource.

- A vulnerability assessment is the first step to improving your environment's security posture.
- Change hats: View your environment as it would be viewed by a cyber-attacker.

- Review the operating systems and applications used throughout your organization. Determine if they have been maintained and updated with the latest patches, especially when they are used in conjunction with sensitive data.
- Have a third-party conduct a vulnerability assessment. They can identify critical vulnerabilities in your network.

RECOMMENDATION There are many commercial products that you can purchase that include templates to help you define a security policy. Obtain a product that accommodates the information that you collect as you define your security policy, its firewall philosophy, the allowed communications, and the organization's network architecture.

Use an application that includes auto-generated topology features that build maps and graphical representations of your network architecture based on the information you capture and that renders revised topology maps as your network architecture changes. There are software applications available for purchase that include these features as well as asset management and workflow recording. These tools usually also include features that provide detailed views of LAN and Internet connectivity—what's connected to what.

Step 2. Define an Overall Security Policy

Before a network can be secured for business, a security policy must be defined. Firewalls and other security measures, such as deployment of VPNs, are designed to execute a portion of the security policy.

An overall security policy contains the following information and it encompasses the outcome of the work accomplished in two of the five steps: "Step 3: Define the Firewall Philosophy" and "Step 4: Identify Permitted Communications."

An effective security policy:

- Identifies all network resources belonging to the company and the required security for each resource. (See Step 1)
- Includes a network infrastructure map that is revised as systems are added to or removed from the topology. (See Step 1)
- Encompasses the organization's firewall philosophy. (See Step 3)
- Includes coverage of the organization's permitted communications and access policies, and it defines access rights and access levels based on employee job functions and roles. (See Step 4)
- Articulates the organization's position in regard to security. It defines the culture of the organization with respect to security and how its policies are applied.
- Identifies the authentication and authorization controls put in place, such as use of user IDs and passwords, single-instance password generators, and certificates.
- Defines security threats and the actions to be taken to thwart those threats and to respond to successful attacks.
- Contains a glossary that defines the terms used throughout its documentation to avoid misinterpretation.
- Is readily available on the LAN to employees and other responsible parties.

Many organizations rely on tools that maintain this information and record all changes. Use of these tools ensures consistent application of approved policies and processes.

In addition to other benefits, defining a security policy at the outset makes it easier to configure your firewall and ensures that the firewall addresses all of your security requirements. A security policy provides the logic that you apply in configuring the firewall – think of it as outlining what the firewall will implement.

Usually corporate policy for larger enterprises dictates security policy for headquarters as well as for branch and regional sites, but smaller enterprises should also define and document a security policy that their administrators can rely on for direction as the company scales to accommodate growth, supports new applications, and responds to advances in firewall security.

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

Table 1 summarizes some of the best-practice procedures that an organization might follow in establishing its security policy. Use the guidelines in Table 1 to help you begin defining your own security policy.

Table 1 Security Policy Definition

Task	Instructions
Define your environment.	Document network assets to be protected throughout your environment, at headquarters as well as at branch and regional offices. Identify the services and systems you want to protect. You cannot deploy a robust firewall to be used successfully unless you have 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 system 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, their configuration information, and which versions they run ▪ Location and description of any network management systems used
Define your current security policy implementation.	Describe your current security posture. Identify any existing security mechanisms used. For example, identify the following technology and any other mechanisms you use: ▪ Antivirus programs ▪ Firewalls, if any ▪ Security hardware, such as encryptors for servers ▪ VPNs
Define the main threats in plain language and the actions to be taken in the event of a security breach or attack.	Define threats to the system. Define the actions administrators will take after an attack has been identified and resolved. For example: ▪ Will you attempt to identify the attacker? If so, what software or other method will you ▪ use? ▪ Do you plan to prosecute? ▪ Will administrators contact the ISP to report the attack?

TIP The success of a meaningful security policy depends on whether it is maintained and kept current. Ensure that your security policy is updated as often as necessary.

This *Learn About* does not provide references to examples of corporate information technology security policies because most corporations make their security policies available to employees on private internal Web sites. However, you can view examples of security policies published by government, universities, and some companies on the Web.

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. Setting and documenting a firewall philosophy 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 as new hosts and software are added to the network. Documentation of the firewall philosophy 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 a philosophy to guide its implementation and administration, the firewall itself might become a security problem. Table 2 identifies some firewall philosophy components you can include in your own firewall philosophy review document.

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? ▪ To protect against insider attacks? ▪ To monitor user activity? ▪ 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. 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?
Specify if private addressing is to be used.	Identify the subnetworks to be used. Specify whether you plan to use Network Address Translation (NAT).
Specify how the firewall is to be managed and updated.	Identify management tools, audits, and scheduled downtime for periodic testing. Define how alerts and alarms are to be used.
Identify security vulnerabilities in the network and rectify them.	Record this information in your firewall philosophy document for historical purposes.
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.

NOTE Some sites might deploy the firewall inline, and set and use logs to capture information to identify common, successful attacks. In this case, parts of the network might succumb to an attack. However, based on the logged information, the network administrator can have a better sense of common attacks on the LAN. For example, for Junos OS, this deployment approach would allow the administrator to more definitively understand the appropriate firewall screens and thresholds to put in place.

Step 4. Identify Permitted Communications

Define an acceptable use policy to specify the types of network activities that are allowed and those that are denied. An acceptable use policy states explicitly what services and applications are allowed for use on the LAN and which Internet Web services and applications are allowed.

Before you can define polices for your firewall, you need to understand and characterize your network environment, including the applications that are currently used on the network. In some cases, network administrators are unaware of certain applications that employees use, especially in regard to use of the Internet. For example, employers might not know if employees are using instant messaging services or similar applications, and employees might not be aware that these kinds of 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. This kind of information can be maintained on your corporate intranet and made available to employees.

It is also important to understand and document the workflow in your organization based on employee roles and the applications allowed and required for each role. To maintain this information, use the workflow records feature of the software application tool that you purchased.

Table 3 gives a simplified example of how you might characterize information that is used for this purpose.

Table 3 Employee Roles, Access Rights, and Allowed Services and Applications

Employee Roles	Access Rights	Allowed Protocols, Services, and Applications as Applied to Employees
Bank Tellers	Allowed access to the customer checking and savings records database at corporate headquarters. Allowed access to banking applications for tellers. Not allowed Internet access.	▪ Client software for access to transaction processing software on a database server ▪ TellPro Accounting ▪ Proprietary custom applications
Bank Managers	Allowed access to both database servers at corporate headquarters: the customer checking and savings records and the customer special services records. Allowed access to Microsoft Office 365 suite of business applications for management and Internet access.	▪ Client software for access to transaction and special services software on a database server ▪ Microsoft Office 365 ▪ Proprietary custom applications
Financial Managers	Allowed access to both database servers at corporate headquarters: the customer checking and savings records and the customer special services records. Allowed access to financial management application software. Allowed access to Microsoft Office 365 suite of business applications for management and Internet access.	▪ Client software for access to transaction and special services software on a database server ▪ Section 5 Suite ▪ Microsoft Office 365 ▪ Proprietary custom applications
IT Operations Personnel	Allowed access to both servers at corporate headquarters: the customer checking and savings records and the customer special services records. Allowed access to private cloud-based firewall policy management software. Allowed access to Microsoft Office 365 suite of business applications for management and Internet access. Allowed remote access to LAN servers and other devices. Allowed access to intrusion detection and recovery software.	▪ Client software for access to transaction and special services software on a database server ▪ Nova Identity and Access Management ▪ Microsoft Office 365 ▪ SNMP ▪ FTP ▪ rlogon ▪ SSH ▪ HTTPS ▪ Telnet ▪ Microsoft Forefront
Bank Executives	Allowed access to both servers at corporate headquarters: the customer checking and savings records and the customer special services records. Allowed access to Microsoft Office 365 suite of business applications for management and Internet access. Allowed access to online collaboration software. Allowed access to online travel schedule management software.	▪ Client software for access to transaction and special services software on a database server ▪ Microsoft Office 365 ▪ Triangle ▪ Concurrence

Gathering this information can help you define your firewall. Most of the legwork will already be 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-filter 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-filter 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.

The emergence of application firewalls gave IT teams granular control over access to applications. Application firewalls examined the application and protocol with which a packet was associated and the ports that the applications used. They could inspect traffic contents and block specific content such as Web services and known viruses.

Application firewalls monitor and can block application traffic and system service calls. These firewalls allow administrators to permit and restrict access to specific services and applications that were previously made widely available. For example:

- FTP can be used for banner-grabbing, which allows IT administrators to take inventory of the systems on their network and the services running on open ports. But in the hands of intruders, FTP could be used to find network hosts and extract information about them such as the operating system and its version, any Web servers, and any other applications running on the hosts for which there are known exploits or holes.
- SSH can be a valuable tool for IT administrators. But in the hands of a malicious user it could be used to breach corporate policy by circumventing content checking, in addition to exposing internal services to outside attacks because of tunneling other IP applications.

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. While special requirements may warrant firewall complexity, unwarranted design complexity lends itself to configuration errors.

For example, for Juniper Network SRX Series devices that implement firewall security and related services, design and deployment simplicity might translate into:

- Creating zones that are specific to functional requirements. For example, a zone might consist of employees sharing the same job functions and the same access rights to applications and resources.
- Separating groups of users from servers. You could assign groups of users to a zone based on the group's subnet.
- Designing policies that are specific rather than general, and placing the general policies at the bottom of your policy list.

TIP Ensure that a zone containing servers does not include users.

Determining enforcement points is fundamental to firewall design. As a rule, the primary use of the firewall should largely 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, or deployments, to consider.

For example, an enterprise network generally comprises two areas: the core (or internal network) and the edge, but the network can also be extended to include an area called the Demilitarized Zone (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 4.

Table 4 Network Areas and Types of Firewalls

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 lock-out 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. Usually contains publicly accessible servers and bastion hosts. If these servers are attacked, hosts within the LAN are not compromised.

Maintaining a Secure Environment

One of the key elements in maintaining an effective firewall is understanding your network traffic patterns. Knowing what is normal for your network and setting a baseline enables you to measure what you think is irregular behavior and then to set thresholds to protect against attacks.

To develop a network profile that accurately reflects the network's state and allows you to establish effective firewall traffic thresholds and other firewall protection, you must understand the network's normal traffic patterns.

To define a baseline for your network, use a Real-Time NetFlow Analyzer under normal operating conditions and monitor the network for at least a week. There are many commercial and open-source tools you can use for this purpose, such as MRTG, NetMGR, and OpenNMS. You can also use SNMP. Table 5 lists the kind of information that contributes to a well-defined network traffic profile.

NOTE In most cases, you can use a device that is already deployed, such as an SRX Series device, to gather the information required to establish a network baseline. For example, after you have configured and deployed an SRX Series device, you can use the CLI to collect information about your normal network traffic patterns and then use that information to tune your network security.

Here are some of the tasks involved in creating a detailed profile of your network's normal behavior:

- Create a network traffic baseline profile.
- Create a profile to characterize network host connectivity.
  - For example, in Junos OS you can rate-limit the number of sessions per IP address to avoid a session table flood.
- Determine the type of ICMP messages to allow, for example, ping versus timestamp messages.
- Determine the normal ICMP traffic flow. (You can use this information to set boundaries on ICMP traffic to avoid an ICMP address sweep.)
  - Many systems use ICMP for error reporting. It is important to understand what normal ICMP traffic flow is so that you do not impede genuine error-reporting information by setting thresholds that are too low.
- Determine the normal TCP packet traffic flow. Many network attacks use malformed or hijacked TCP packets to carry out their malicious missions.

You can use the packet-filtering features in Junos OS to rate-limit certain types of traffic. For example, in Junos OS you can rate-limit the number of sessions per IP address to avoid a session table flood. However, you cannot effectively determine the thresholds to set for specific types of traffic unless you know the normal traffic flow patterns for your network

Table 5 suggests some of the methods that you can use to obtain information that will help you to define your network traffic baseline.

Table 5 Network Traffic Baseline Profile

What is it?	Detailed Layer 3 to Layer 7 Characterization of Network Traffic	
How do I create it?	1. Measure and collect session, flow, and packet statistics from real-time traffic. 2. From these statistics, create a model that describes both average aggregate behavior and average individual behavior on the network.	
Information the Network Traffic Baseline Profile Provides		
What Layer 3 to Layer 7 aggregate information can I deduce from the traffic baseline I create?	The number of users on the network How many applications these users are running What percentage of sessions are of a certain protocol type	NOTE For networks that incorporate user identify firewall features, consider that a single user could be logged into the network using more than one device.
What Layer 3 to Layer 7 individual information can I deduce from the traffic baseline I create?	The average bandwidth consumed per user The average number of sessions per user	
What information can I obtain by comparing this data with Layer 2 to Layer 3 statistics?	The average packet size on your network The normal error rate on your network The normal fragmentation rate on your network	
Measurements Required to Create a Network Traffic Baseline Profile		
What measurements do I need to collect to calculate the average Transport Layer statistics?	▪ Bandwidth: You can collect this data from SNMP using tools such as MRTG, NetMGR, and OpenNMS, or you can monitor it using the CLI of a currently deployed device. (You can use the Junos OS CLI for this purpose.) ▪ Session count ▪ Session rate The preceding three measurements contribute to determining the average aggregate model. These measurements plus the following one constitute the average individual model. ▪ User count	
Average Aggregate Model Calculations		
How do I calculate the average aggregate model?	▪ Session time = session count / session rate ▪ Bandwidth per session = bandwidth per user / sessions per user ▪ Data per session = bandwidth per session x session time	
Average Individual Model Calculations		
How do I calculate the average individual model?	▪ Session rate per user = session rate / user count ▪ Bandwidth per user = bandwidth / user count ▪ Session per user = session count / user	

NOTE After you create a traffic model, you can use it to validate the methodology that you used to define the baseline. One way to do this is to program traffic-generating test equipment to fit the traffic model and take the same measurements. If they match the

measurements, then the model is correct. You can use the SRX Series CLI to continue to collect this information. Then you can use the results to fine tune your firewall. You can obtain this information by:

- Setting SNMP for collecting bandwidth session, and possibly session rate (by zone or interface).
- Setting policy rules to generate traffic logs that you can collect with the system logs.

Security Policy Creation and Firewall Design Summary

Deploying an effective firewall for any area of your network entails a great deal more than configuration. This *Learn About* has explored the processes and best practices that contribute to creating a security policy for your organization and designing its firewall. These best practices enhance the firewall design and configuration process and allow you to deploy a firewall that meets the security requirements for particular areas of your environment.

Fundamental to designing and enforcing a strong firewall is keeping current all documentation that defines your environment, and its resources and their security requirements. This documentation should cover the firewall philosophy, reflect the organization's current security posture and its current network state, address allowed communications, and include role-based workflow documentation. It is a living document that should be updated dynamically to reflect ongoing changes. If your environment description is out-of-date, you will leave holes in your firewall configuration and weaken its enforcement.

Best practices recommend that you characterize your network, document your current security posture, and determine your organization's position in regard to security.

- Identify all network resources, their security requirements, and the culture of your organization in relation to its security policies.
- Create a network map and keep it updated and current as systems are added or removed.
- Identify known threats and how you will deal with attacks.
- Document your company's philosophy with respect to the firewall and share that information with your employees.
- Document operating systems and their versions and patches, and applications running on your systems and their versions and patches. Document how these resources are protected.
- Define your organization's workflow with respect to allowed communications, access rights based on employee roles, and individual user requirements and responsibilities.

It is vital to the security of your environment that you make this information available to employees in a visible way.

Determine the firewall enforcement points: Will you deploy a firewall to protect the

edge (Internet-facing), the core (corporate-facing), or the DMZ (bastion first line of defense)? Or does your environment require firewall enforcement at all of these points?

Design your firewall for simplicity, where possible, without sacrificing complete security coverage.

As ongoing measures of protection:

- Develop a network traffic baseline profile that identifies your network's normal traffic patterns to set a baseline to measure against for irregularities. You cannot determine the correct thresholds to set for types of traffic, such as ICMP traffic, without it.
- Take measurements to create a traffic model, then use the model to validate how you defined the baseline. You cannot set effective thresholds to protect against attacks without it.

References and Suggested Reading

Step 2. Define an Overall Security Policy

Take a look at these examples of government and university security policies made available to the public on the Web:

Government of Canada security policy
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text

Creighton University Information security policy
https://www.creighton.edu/fileadmin/user/doit/docs/security/SEC_PHILv7.pdf

Read the Google white paper, Google's Approach to IT Security, made available to the public on the Web. Although more general than a private corporate security policy, this document includes security policy and firewall philosophy content.
https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf

Although not part of an initial security policy, lifecycle management is used to gather and analyze security data and to "apply and enforce security objectives on the ground." Read the Juniper Networks brief on their partnership with Tufin Security Suite in offering security lifecycle management solutions.
http://www.tufin.com/media/32635/tufin_juniper_solution_brief_en.pdf

Step 3. Define a Firewall Philosophy

Read the definitive Junos Security guide to gain hands-on experience with Junos services gateways for the enterprise:
http://shop.oreilly.com/product/0636920001317.do

Learn about configuring and specifying the order of security policies for firewalls on SRX Series devices:
http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/pathway-pages/security/security-authentication-index.html

Take a look at information on configuring Junos OS access privilege levels, login classes, and access privilege user permissions for the M Series, MX Series, and T Series routers:
http://www.juniper.net/techpubs/en_US/junos13.3/information-products/pathway-pages/access-privilege/access-privilege.pdf

Step 4. Identify Permitted Communications

For rich, comprehensive coverage of security services on SRX Series devices and an enjoyable read, see the widely acclaimed Juniper SRX Series hands-on reference:
http://shop.oreilly.com/product/0636920026785.do

To learn more about Junos OS security zones, interfaces, and SRX Series devices, visit here:
http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/pathway-pages/security/security-basic-zone-interface.html

http://www.juniper.net/us/en/training/jnbooks/day-one/day-one-posters/srx-series/

Learn about Junos OS access privilege levels, login classes, and access privilege user permission configuration for the M Series, MX Series, and T Series routers:
http://www.juniper.net/techpubs/en_US/junos13.3/information-products/pathway-pages/access-privilege/access-privilege.pdf

Read about evolution of the firewall and its various stages. See Learn About: Firewall Evolution:
http://www.juniper.net/techpubs/en_US/learn-about/index.html

Maintaining a Secure Environment

For details on how to use SRX Series screens to protect against denial-of-service attacks, see:
http://www.int.juniper.net/marketing/product_marketing/gamma/docs/350097.pdf

For examples of how to configure firewall rate-limiting filters, see:
http://www.juniper.net/techpubs/en_US/junos13.2/topics/example/firewall-filter-stateless-example-rate-limits-based-on-destination-class.html

http://www.juniper.net/techpubs/en_US/junos14.1/topics/example/routing-state- less-firewall-filter-security-protect-against-tcp-and-icmp-flood-configuring.html

For details on Real-Time Performance Monitoring and Flow monitoring and measuring, see:
http://www.juniper.net/techpubs/en_US/junos14.1/information-products/pathway-pages/services-interfaces/real-time-performance-monitoring-services.pdf

http://www.juniper.net/techpubs/en_US/junos14.1/topics/concept/performance- measuring-junos-nm.html

For details on configuring SRX Series screens, see the following configuration information and the KB article *SRX Getting Started-Configure Screen Protection*:
http://www.juniper.net/techpubs/en_US/junos12.1x46/information-products/pathway-pages/junos-cli/junos-cli.html

http://kb.juniper.net/InfoCenter/index?page=content&id=KB16618

http://www.int.juniper.net/marketing/product_marketing/gamma/docs/350097.pdf

For facts on Junos OS SNMP, see:
http://www.juniper.net/techpubs/en_US/junos14.1/topics/reference/general/ snmp-junos-faq.html

For information on Junos OS firewall filters and policer, see:
http://www.juniper.net/techpubs/en_US/junos14.1/information-products/pathway-pages/config-guide-firewall-filter/config-guide-firewall-filter.pdf

Learn About Firewall Design

by Judy Thompson-Melanson

You cannot deploy a robust firewall to be used successfully unless you have determined what you must protect, and this **Learn About** provides you with all the essential elements that comprise any best-practice network firewall design. In a remarkable twelve pages, you'll know what information to collect, what to do with it, and how to process your network's demand for both connectivity and security.

Judy Thompson-Melanson is a Juniper Networks staff technical writer with over twenty-five years in the industry. She has written API documentation, design guides, and networking and security documentation for many companies including Apple, Sun Microsystems, Cisco Systems, and Intuit.
The author thanks the following for their engagement in this project: Patrick Ames, Editor in Chief; illustrator, Karen Joice; project promoter, Linnea Wickstrom, and Mark Smallwood, original sponsor.

ISBN: 978-1-941441-01-5 Version History: First Edition, October 2014 2 3 4 5 6 7 8 9

For more information *see*:
juniper.net/documentation