University of Colorado **Boulder**

CSCI 3403 INTRO TO CYBERSECURITY

Lecture: 14-1

Topic: Firewalls

Presenter: Matt Niemiec

Announcements

- Project 3 (final project) is posted
- Assignment 10 due Thursday at 1:30PM
- Upcoming guest lecturers
  - From Rule4 on 4/21
  - From Twitter on 4/23 (Andy Sayler)

Exam Extra Credit

- Research a topic that won't be discussed in class
- Get credit in one of the following ways
  - Record a 10-minute (updated) video explanation of your topic for up to 10%. To receive credit for this, see Moodle
  - Present your topic for 5 minutes in recitation for up to 15%. Depending on demand, this may be first-come-first-serve. If you got an 85% or better on the midterm, please leave this for others. Poll opens right after class
  - If you're selected as an outstanding project from recitation, give a 10-minute presentation for up to 25% (total)
- Percentages apply to your higher exam score

Exam Extra Credit Criteria

- Will be graded on at least the following:
  - Interesting topic/information relevant to cybersecurity
  - Quality, professional preparation and presentation
  - Inspires the listener to want to learn more and provides resources to do so
  - Shows insight and depth in research presented in an appropriate manner for the given timeframe
  - Responds knowledgeably and accurately to any questions asked

Some Extra Credit Potential Topics

- Network security
  - Wireless security, honeypots, cloud security, SIEM, Tor
- Applied security
  - OWASP Top 10, reverse engineering, penetration testing
- Crypto
  - Common crypto libraries, homomorphic encryption
- Windows
  - Windows/AD security, Windows CLI
- Miscellaneous
  - Ethics in security, auditing, data provenance
- Or anything else! Just run it by Matt or your TA

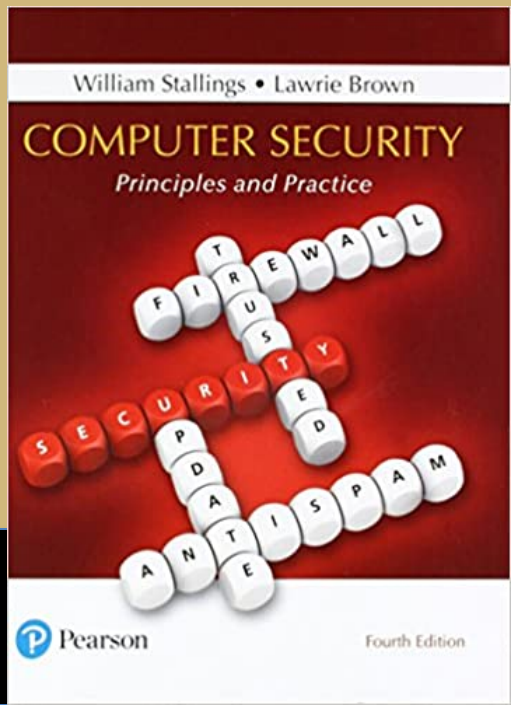
Technology Recap 3/17 (Old stuff)

- Piazza is used for content-related questions
- Feedback: https://forms.gle/WRUUbPkmFNsa6q3D6
- Instructor/TA email is used for individual circumstances
- cyber@Colorado.edu is used for accommodations/logistical questions
- Moodle is used for assignments, slides, and additional resources

Technology Recap 3/17 (New stuff)

- Calendar is used for holding all Zoom meetings, instructions, and meeting IDs
  - May contain due dates, but not guaranteed
- Lecture Zoom ID: https://cuboulder.zoom.us/j/633893668
  - This and others found in Google Calendar
- Lecture capture folder: https://drive.google.com/drive/folders/1VMrHEigP4AgDwRnRPTsgQS35EAozc19-?usp=sharing

Firewalls


William Stallings • Lawrie Brown
COMPUTER SECURITY
Principles and Practice
FIREWALL
TRUSTED
SECURITY
PDA
ANTE
SPAM
Pearson
Fourth Edition

Our Network

- For this lecture, we'll assume our network looks like this
- Imagine we're a company. Employees work in the internal net
- Demilitarized Zone (DMZ) exists on every network
  - Normal traffic for users is not normal for servers!

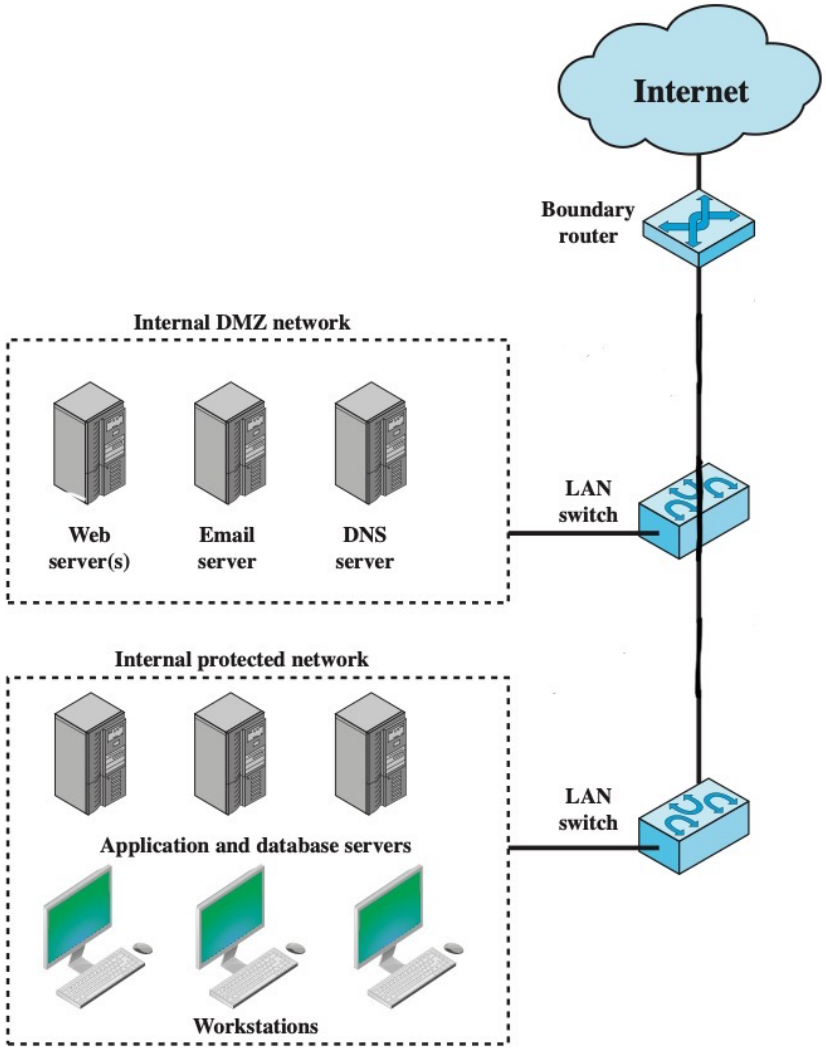


Figure 9.2 Example Firewall Configuration

Problems?

- Our employees can set up unauthorize Django servers
- If malware gets on our computer, it can communicate with the C&C server freely
- Traffic going in and out of the network isn’t monitored

Solution: Firewalls

- Firewalls can permit or deny certain *types* of traffic
- Analyze the traffic signature to decide if it's allowed
  - Ports, IP addresses, protocol, direction, etc.
  - Everything has to make sense!
- Question: Where to put the firewall on our network?

Goals of a Firewall

1. “All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.”
2. “Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used [...]”
3. “The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operation system”

Types of Firewalls

- Host-based firewalls
  - Runs on a machine
  - Filters traffic coming in and out of that machine
- **Network-based firewalls**
  - A separate machine on the network
  - All traffic on interface goes through firewall
  - Focus of lecture today
- Within these, there are many types of firewalls
  - Application-level gateway, **packet filtering**, circuit-level gateway, stateful packet inspection firewall, and more

Place Firewall on Network

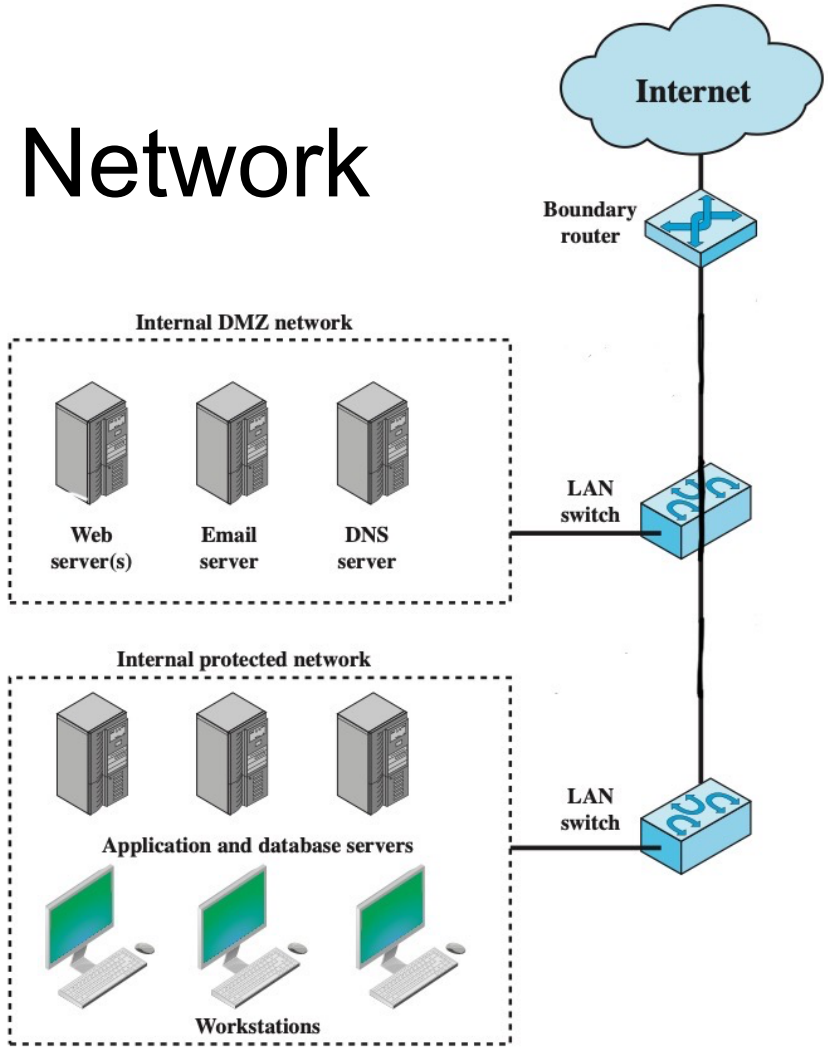


Figure 9.2 Example Firewall Configuration

Place Firewall on Network

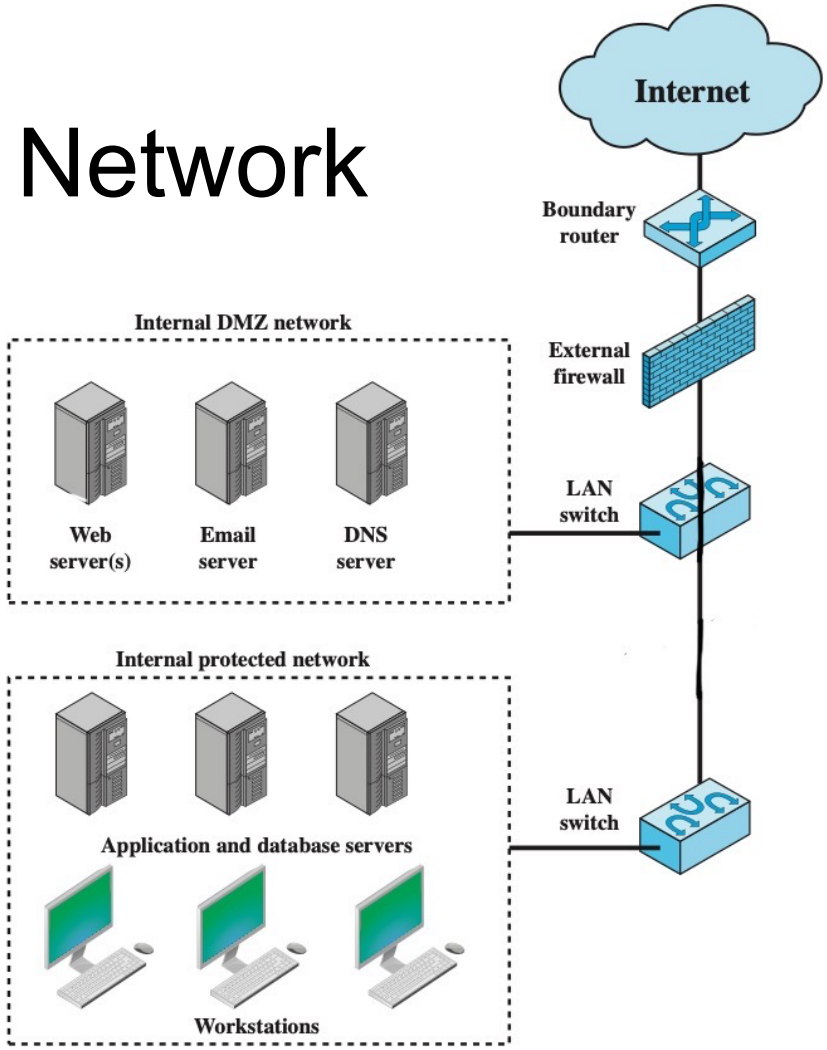


Figure 9.2 Example Firewall Configuration

Quick Note

- Blacklisting
  - Deny types of known bad traffic
  - Default allow
- Whitelisting
  - Allow types of known good traffic
  - Default deny
  - More secure
  - Always use for firewalls

Firewall Rules: Attempt 1

- Goal: Allow inbound and outbound SMTP traffic
- Inbound SMTP traffic:

Rule	Direction	Src Address	Dest Address	Protocol	Dest Port	Action
1	In	External	Internal	TCP	25	Permit

Firewall Rules: Attempt 1

- Goal: Allow inbound and outbound SMTP traffic
- Response to inbound SMTP traffic (Client ports >1023)

Rule	Direction	Src Address	Dest Address	Protocol	Dest Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit

Firewall Rules: Attempt 1

- Goal: Allow inbound and outbound SMTP traffic
- Outbound SMTP traffic:

Rule	Direction	Src Address	Dest Address	Protocol	Dest Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit

Firewall Rules: Attempt 1

- Goal: Allow inbound and outbound SMTP traffic
- Response to outbound SMTP traffic:

Rule	Direction	Src Address	Dest Address	Protocol	Dest Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit

Firewall Rules: Attempt 1

- Goal: Allow inbound and outbound SMTP traffic
- What's left?

Rule	Direction	Src Address	Dest Address	Protocol	Dest Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit

Firewall Rules: Attempt 1

- Goal: Allow inbound and outbound SMTP traffic
- Default deny: **Always include!!!**

Rule	Direction	Src Address	Dest Address	Protocol	Dest Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Firewall Rules: Attempt 1

- Problems?

Rule	Direction	Src Address	Dest Address	Protocol	Dest Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
1	In	1.2.3.4	192.168.0.5	TCP	8080	?
2	Out	192.168.0.5	1.2.3.4	TCP	5150	?

- Unauthorized programs still allowed!
- Solution?

Rule	Direction	Src Address	Dest Address	Protocol	Dest Port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Firewall Rules: Attempt 2

- Include source port number
- Removes vulnerability. Yay!

Rule	Direction	Src Address	Dest Address	Protocol	Src Port	Dest Port	Action
1	In	External	Internal	TCP	>1023	25	Permit
2	Out	Internal	External	TCP	25	>1023	Permit
3	Out	Internal	External	TCP	>1023	25	Permit
4	In	External	Internal	TCP	25	>1023	Permit
5	Either	Any	Any	Any	Any	Any	Deny

Packet	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	Action
1	In	1.2.3.4	192.168.0.5	TCP	25	8080	?
2	Out	192.168.0.5	1.2.3.4	TCP	8080	25	?

- Oops!

Rule	Direction	Src Address	Dest Address	Protocol	Src Port	Dest Port	Action
1	In	External	Internal	TCP	>1023	25	Permit
2	Out	Internal	External	TCP	25	>1023	Permit
3	Out	Internal	External	TCP	>1023	25	Permit
4	In	External	Internal	TCP	25	>1023	Permit
5	Either	Any	Any	Any	Any	Any	Deny

Firewall Rules: Attempt 3

- Use flags!
  - Many types of flags: SYN, ACK, **EST** (established), FIN, etc.
- Only connected connections should use certain rules
  - Most malicious traffic is on TCP
  - Take advantage of TCP flags!

Firewall Rules: Attempt 3

- Use the established flag to avoid bad connections

Rule	Direction	Src Address	Dest Address	Protocol	Src Port	Dest Port	Flags	Action
1	In	External	Internal	TCP	>1023	25		Permit
2	Out	Internal	External	TCP	25	>1023	Est.	Permit
3	Out	Internal	External	TCP	>1023	25		Permit
4	In	External	Internal	TCP	25	>1023	Est.	Permit
5	Either	Any	Any	Any	Any	Any		Deny

Firewall Rules: Attempt 3

- Use the established flag to avoid bad connections
- Now try malicious connections...
  - The security holes are all patched up!

Rule	Direction	Src Address	Dest Address	Protocol	Src Port	Dest Port	Flags	Action
1	In	External	Internal	TCP	>1023	25		Permit
2	Out	Internal	External	TCP	25	>1023	Est.	Permit
3	Out	Internal	External	TCP	>1023	25		Permit
4	In	External	Internal	TCP	25	>1023	Est.	Permit
5	Either	Any	Any	Any	Any	Any		Deny

Firewall Rules: Attempt 3

- Our firewall is secure
- No unauthorized servers will work
- One *tiny* problem...

Firewall Rules: Attempt 3

- Our firewall is secure
- No unauthorized servers will work
- One *tiny* problem...
  - Each policy has two rules
  - Not good engineering, and difficult to maintain

Firewall Rules: Attempt 4 (And Final)

- Have one rule that allows all established connections
  - Last two rules will **always** stay the same
  - Each of the two policies has exactly one rule
- Only vet connections that are being established

Rule	Direction	Src Address	Dest Address	Protocol	Src Port	Dest Port	Flags	Action
1	In	External	Internal	TCP	>1023	25		Permit
2	Out	Internal	External	TCP	>1023	25		Permit
3	Any	Any	Any	TCP	Any	Any	Est.	Permit
4	Either	Any	Any	Any	Any	Any		Deny

Different Zones

- The firewall for the DMZ is the same firewall for the internal network
- Problems?

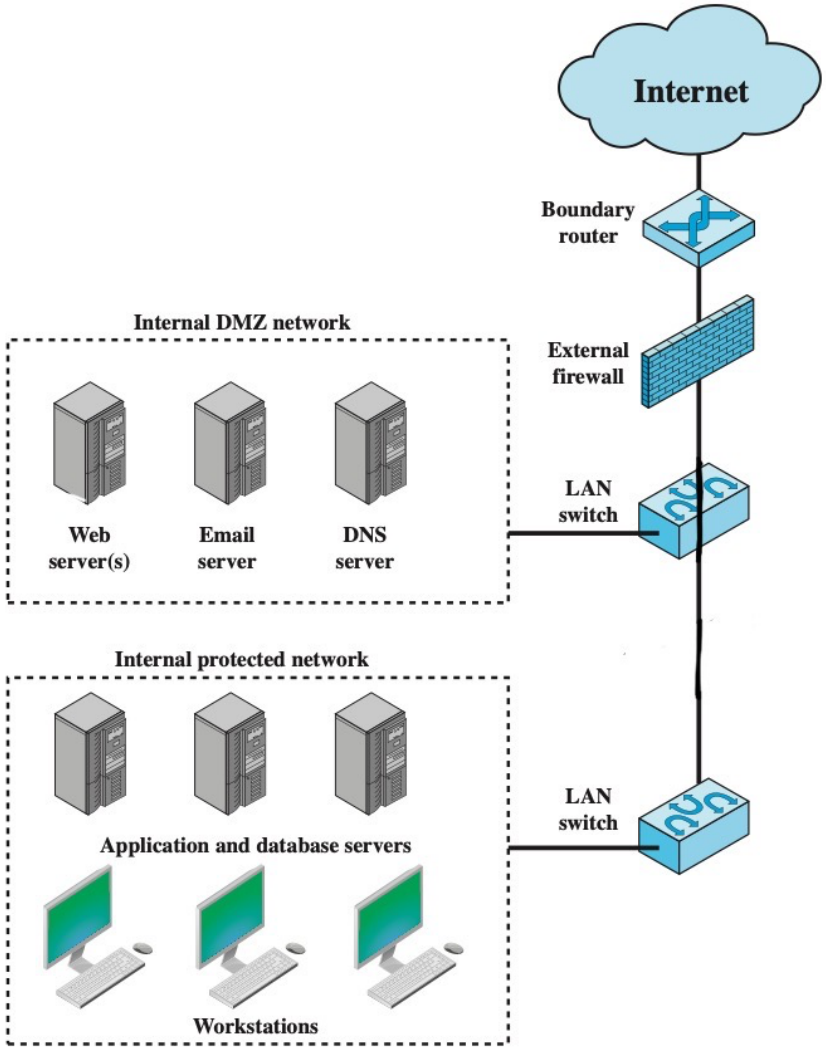


Figure 9.2 Example Firewall Configuration

Different Zones

- The firewall for the DMZ is the same firewall for the internal network
- Problems?
  - Our web servers can browse Facebook (use client ports)
  - Our employees with root can open authorized ports

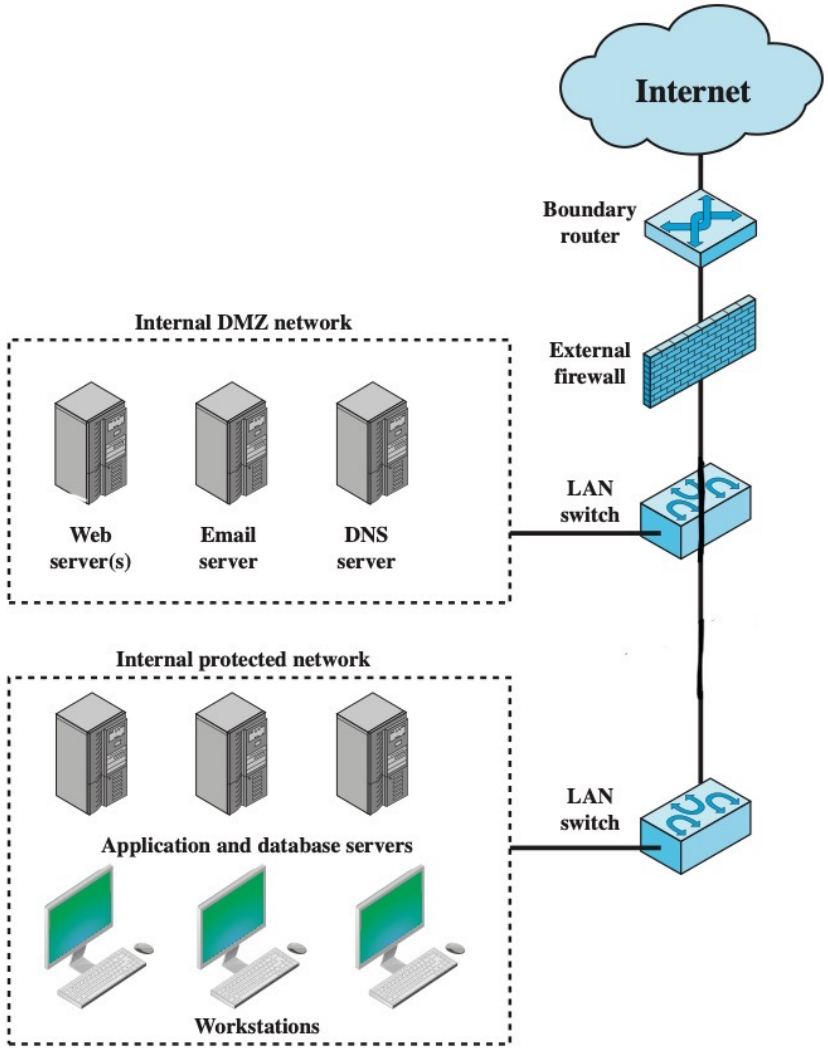


Figure 9.2 Example Firewall Configuration

Complete Picture

- Add a firewall between DMZ and internal
- Each firewall has own set of rules
- Won't worry about second firewall in this class
- Happy firewall rule making!

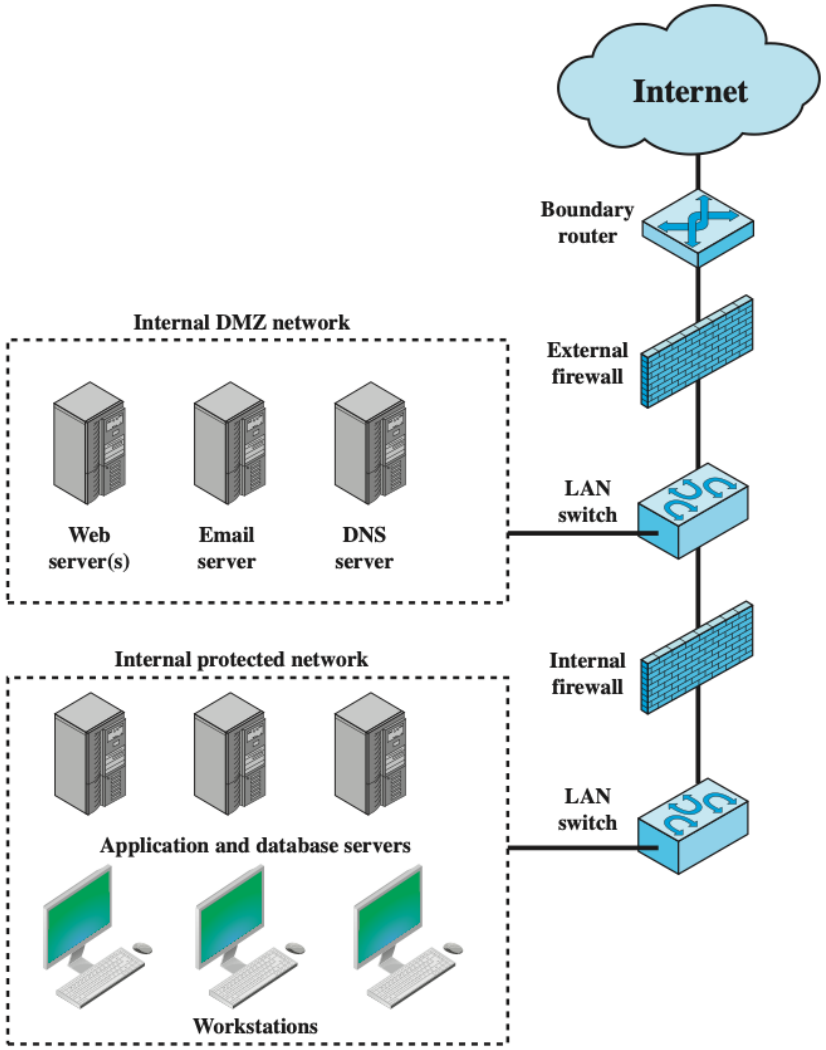


Figure 9.2 Example Firewall Configuration