

Network Security - ISA 656

Intro to Firewalls

Angelos Stavrou

August 30, 2007

Why Use Firewalls?

- Intro to Firewalls
- What's a Firewall
- Why Use Firewalls?**
- Traditional Firewalls by Analogy
- Should We Fix the Network Protocols Instead?
- Firewall Advantages
- Schematic of a Firewall
- Conceptual Pieces
- The DMZ
- Positioning Firewalls
- Why Administrative Domains?
- Splitting a Location
- Firewall Philosophies
- Blocking Outbound Traffic?
- Next: Packet Filtering

- Most hosts have security holes. Proof: Most software is buggy. Therefore, most security software has security bugs.
- Firewalls run much less code, and hence have few bugs (and holes).
- Firewalls can be professionally (and hence better) administered.

What's a Firewall

- Intro to Firewalls
- What's a Firewall**
- Why Use Firewalls?
- Traditional Firewalls by Analogy
- Should We Fix the Network Protocols Instead?
- Firewall Advantages
- Schematic of a Firewall
- Conceptual Pieces
- The DMZ
- Positioning Firewalls
- Why Administrative Domains?
- Splitting a Location
- Firewall Philosophies
- Blocking Outbound Traffic?
- Next: Packet Filtering

Devices examining traffic making access control decisions

- Divide the world between trusted and not
- Only authorized traffic is allowed to pass
- Act as Barrier between *us* and *them*.
- Limits communication from the outside world.
- ⇒ The outside world can be another part of the same organization.
- Only a very few machines exposed to attack.

Why Use Firewalls?

- Intro to Firewalls
- What's a Firewall
- Why Use Firewalls?**
- Traditional Firewalls by Analogy
- Should We Fix the Network Protocols Instead?
- Firewall Advantages
- Schematic of a Firewall
- Conceptual Pieces
- The DMZ
- Positioning Firewalls
- Why Administrative Domains?
- Splitting a Location
- Firewall Philosophies
- Blocking Outbound Traffic?
- Next: Packet Filtering

- Firewalls run less software, with more logging and monitoring.
- They enforce the partition of a network into separate security domains.
- *Without such a partition, a network acts as a giant virtual machine, with an unknown set of privileged and ordinary users.*

Traditional Firewalls by Analogy

Intro to Firewalls
What's a Firewall
Why Use Firewalls?
Traditional Firewalls by Analogy
Should We Fix the Network Protocols Instead?
Firewall Advantages
Schematic of a Firewall
Conceptual Pieces
The DMZ
Positioning Firewalls
Why Administrative Domains?
Splitting a Location
Firewall Philosophies
Blocking Outbound Traffic?
Next: Packet Filtering

- Passports are (generally) checked at the border.
- My office doesn't have a door direct to the outside.
- My bedroom doesn't have a real lock.
- But a bank still has a vault. . .

5 / 17

Firewall Advantages

Intro to Firewalls
What's a Firewall
Why Use Firewalls?
Traditional Firewalls by Analogy
Should We Fix the Network Protocols Instead?
Firewall Advantages
Schematic of a Firewall
Conceptual Pieces
The DMZ
Positioning Firewalls
Why Administrative Domains?
Splitting a Location
Firewall Philosophies
Blocking Outbound Traffic?
Next: Packet Filtering

If you don't need it, get rid of it.

- No ordinary users, and hence no passwords for them
- Run as few servers as possible
- Install conservative software, don't get the latest fancy servers, etc.)
- Log everything, and monitor the log files.
- Keep copious backups, including a "Day 0" backup.

Ordinary machines cannot be run that way.

7 / 17

Should We Fix the Network Protocols Instead?

Intro to Firewalls
What's a Firewall
Why Use Firewalls?
Traditional Firewalls by Analogy
Should We Fix the Network Protocols Instead?
Firewall Advantages
Schematic of a Firewall
Conceptual Pieces
The DMZ
Positioning Firewalls
Why Administrative Domains?
Splitting a Location
Firewall Philosophies
Blocking Outbound Traffic?
Next: Packet Filtering

- Network security is not the problem.
- Firewalls are *not* a solution to network problems. They are a network response to a host security problem.
- More precisely, they are a response to the dismal state of software engineering; taken as a whole, the profession does not know how to produce software that is secure, correct, and easy to administer.
- Consequently, better network protocols will not obviate the need for firewalls. The best cryptography in the world will not guard against buggy code.

6 / 17

Firewall Advantages

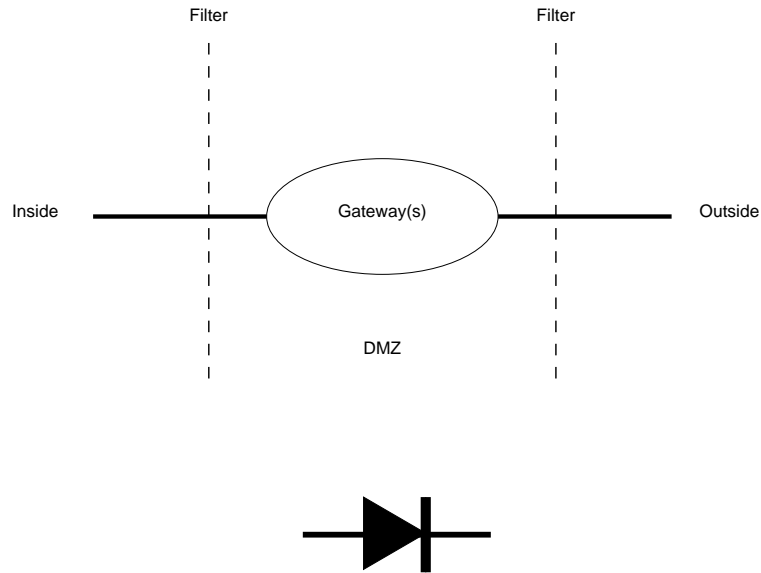
Intro to Firewalls
What's a Firewall
Why Use Firewalls?
Traditional Firewalls by Analogy
Should We Fix the Network Protocols Instead?
Firewall Advantages
Schematic of a Firewall
Conceptual Pieces
The DMZ
Positioning Firewalls
Why Administrative Domains?
Splitting a Location
Firewall Philosophies
Blocking Outbound Traffic?
Next: Packet Filtering

- Can operate at various levels in the stack
- Link, network, application
- Examines packet headers of the appropriate layer
- Transparent vs. proxy
- Stateful vs. stateless

8 / 17

Schematic of a Firewall

- Intro to Firewalls
- What's a Firewall
- Why Use Firewalls?
- Traditional Firewalls by Analogy
- Should We Fix the Network Protocols Instead?
- Firewall Advantages
- Schematic of a Firewall**
- Conceptual Pieces
- The DMZ
- Positioning Firewalls
- Why Administrative Domains?
- Splitting a Location
- Firewall Philosophies
- Blocking Outbound Traffic?
- Next: Packet Filtering



Conceptual Pieces

- Intro to Firewalls
- What's a Firewall
- Why Use Firewalls?
- Traditional Firewalls by Analogy
- Should We Fix the Network Protocols Instead?
- Firewall Advantages
- Schematic of a Firewall
- Conceptual Pieces**
- The DMZ
- Positioning Firewalls
- Why Administrative Domains?
- Splitting a Location
- Firewall Philosophies
- Blocking Outbound Traffic?
- Next: Packet Filtering

- An “inside” — everyone on the inside is presumed to be a good guy
- An “outside” — bad guys live there
- A “DMZ” (Demilitarized Zone) — put necessary but potentially dangerous servers there

The DMZ

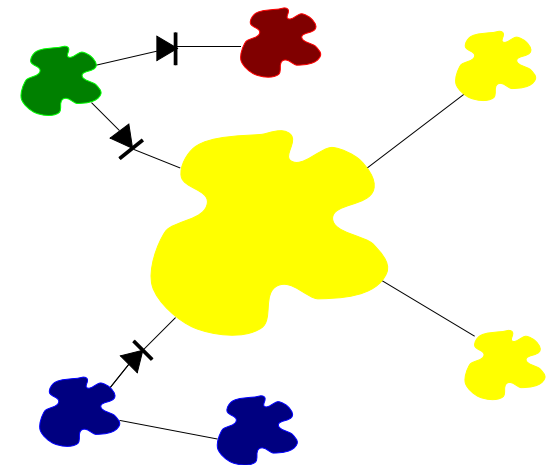
- Intro to Firewalls
- What's a Firewall
- Why Use Firewalls?
- Traditional Firewalls by Analogy
- Should We Fix the Network Protocols Instead?
- Firewall Advantages
- Schematic of a Firewall
- Conceptual Pieces
- The DMZ**
- Positioning Firewalls
- Why Administrative Domains?
- Splitting a Location
- Firewall Philosophies
- Blocking Outbound Traffic?
- Next: Packet Filtering

- Good spot for things like mail and web servers
- Outsiders can send email, retrieve web pages
- Insiders can retrieve email, update web pages
- Must monitor such machines very carefully!

Positioning Firewalls

- Intro to Firewalls
- What's a Firewall
- Why Use Firewalls?
- Traditional Firewalls by Analogy
- Should We Fix the Network Protocols Instead?
- Firewall Advantages
- Schematic of a Firewall
- Conceptual Pieces
- The DMZ
- Positioning Firewalls**
- Why Administrative Domains?
- Splitting a Location
- Firewall Philosophies
- Blocking Outbound Traffic?
- Next: Packet Filtering

Firewalls protect *administrative* divisions.



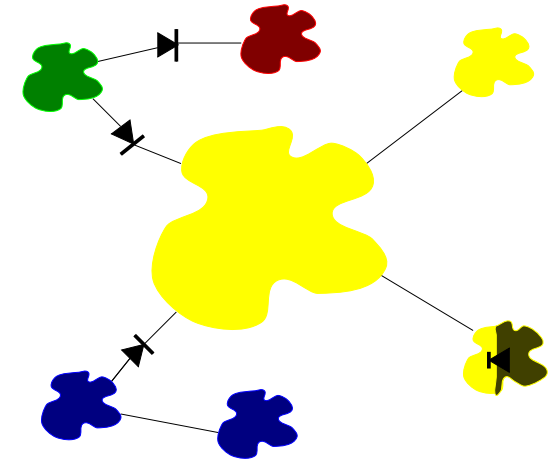
Why Administrative Domains?

Intro to Firewalls
 What's a Firewall
 Why Use Firewalls?
 Traditional Firewalls by Analogy
 Should We Fix the Network Protocols Instead?
 Firewall Advantages
 Schematic of a Firewall
 Conceptual Pieces
 The DMZ
 Positioning Firewalls
Why Administrative Domains?
 Splitting a Location
 Firewall Philosophies
 Blocking Outbound Traffic?
 Next: Packet Filtering

- Firewalls enforce policy
- Policy follows administrative boundaries, not physical ones
- Example: separate protection domains for Legal, HR, Research, etc.

Splitting a Location

Intro to Firewalls
 What's a Firewall
 Why Use Firewalls?
 Traditional Firewalls by Analogy
 Should We Fix the Network Protocols Instead?
 Firewall Advantages
 Schematic of a Firewall
 Conceptual Pieces
 The DMZ
 Positioning Firewalls
 Why Administrative Domains?
Splitting a Location
 Firewall Philosophies
 Blocking Outbound Traffic?
 Next: Packet Filtering



Firewall Philosophies

Intro to Firewalls
 What's a Firewall
 Why Use Firewalls?
 Traditional Firewalls by Analogy
 Should We Fix the Network Protocols Instead?
 Firewall Advantages
 Schematic of a Firewall
 Conceptual Pieces
 The DMZ
 Positioning Firewalls
 Why Administrative Domains?
 Splitting a Location
Firewall Philosophies
 Blocking Outbound Traffic?
 Next: Packet Filtering

1. Block all dangerous destinations.
2. Block everything; unblock things known to be both safe and necessary.

Option 1 gets you into an arms race with the attackers; you have to *know* everything that is dangerous, in all parts of your network. Option 2 is much safer.

Blocking Outbound Traffic?

Intro to Firewalls
 What's a Firewall
 Why Use Firewalls?
 Traditional Firewalls by Analogy
 Should We Fix the Network Protocols Instead?
 Firewall Advantages
 Schematic of a Firewall
 Conceptual Pieces
 The DMZ
 Positioning Firewalls
 Why Administrative Domains?
 Splitting a Location
 Firewall Philosophies
Blocking Outbound Traffic?
 Next: Packet Filtering

- Many sites permit arbitrary outbound traffic, but...
- Internal bad guys?
- Extrusion detection?
- Regulatory requirements?
- Other corporate policy?

Next: Packet Filtering

Intro to Firewalls

What's a Firewall

Why Use Firewalls?

Traditional Firewalls

by Analogy

Should We Fix the

Network Protocols

Instead?

Firewall Advantages

Schematic of a

Firewall

Conceptual Pieces

The DMZ

Positioning Firewalls

Why Administrative

Domains?

Splitting a Location

Firewall Philosophies

Blocking Outbound

Traffic?

Next: Packet

Filtering

- Read the Readings list posted online
- Ask questions
- Are firewalls a full-proof solution?