IT 609
Network and System Administration

Network Security

Thursday November 04, 2021

Network Security

Network Security

Networks open up limitless new security risks, but networks are also 100% essential to normal business and life today

- Restrict who can be on the network
- Restrict the kind of traffic moving in/out/over the network
- Monitor the network for badness

Restricting Access

DHCP = bad

Dynamic DNS = bad

Open Wi-Fi AP's = bad

Public Ethernet ports = bad

Network Access Control

Restricting who can use your network

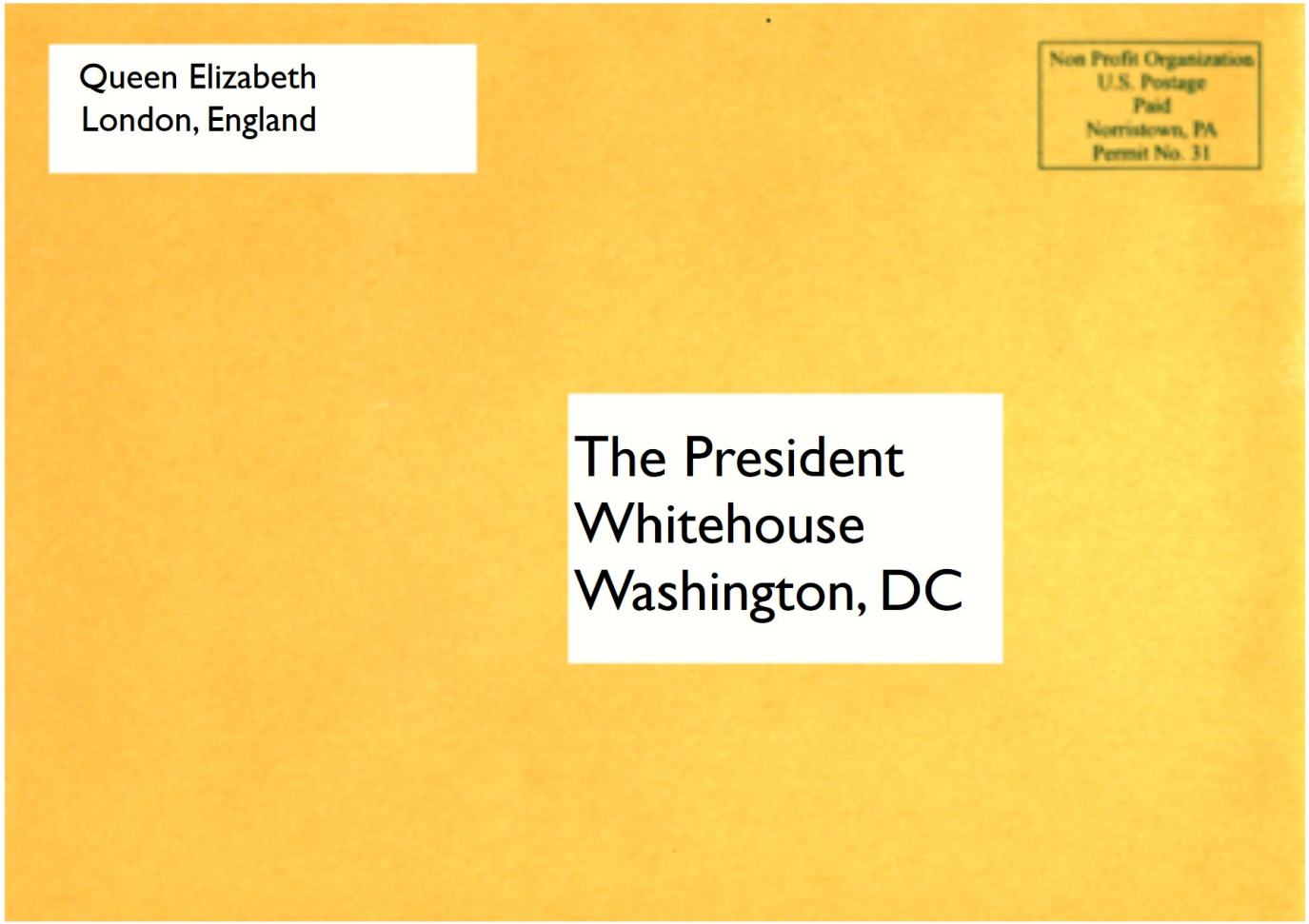
- Only known devices
- Only known users
- Only devices that meet certain standards
  - Malware protection
  - Certain OS versions or patches

Usually done through a registration system and a technology like 802.1x

Restricting Access - Firewalls

How do firewalls work?

Restricting Access - Firewalls

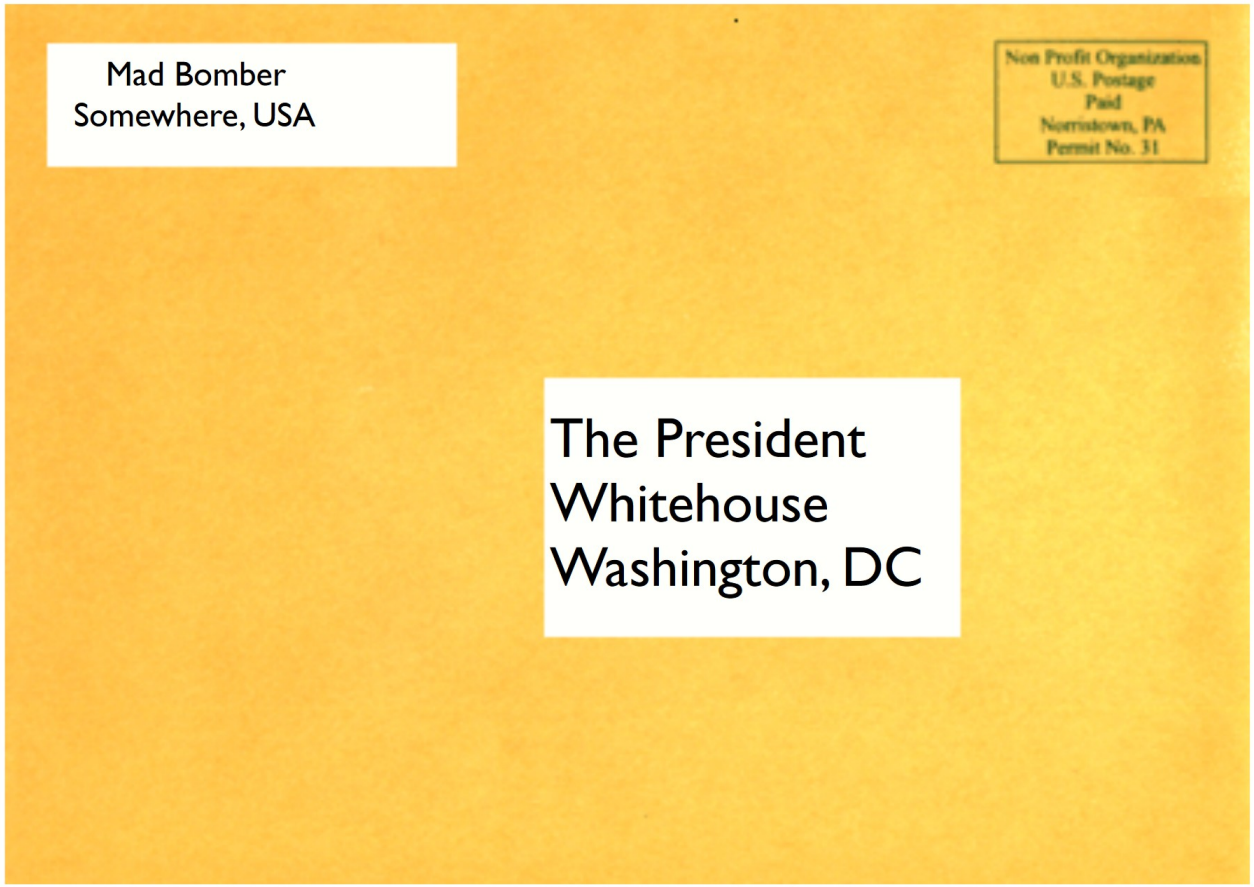


Would you deliver and open this?

Restricting Access - Firewalls

How about this one?

Restricting Access - Firewalls



Or this one?

Restricting Access - Firewalls

Decide whether to forward a network communication or not

List of rules based on:

- Protocol
- Sender information
- Receiver information
- IP network
- IP address
- Port

Firewalls are not foolproof!

Restricting Access - Firewalls

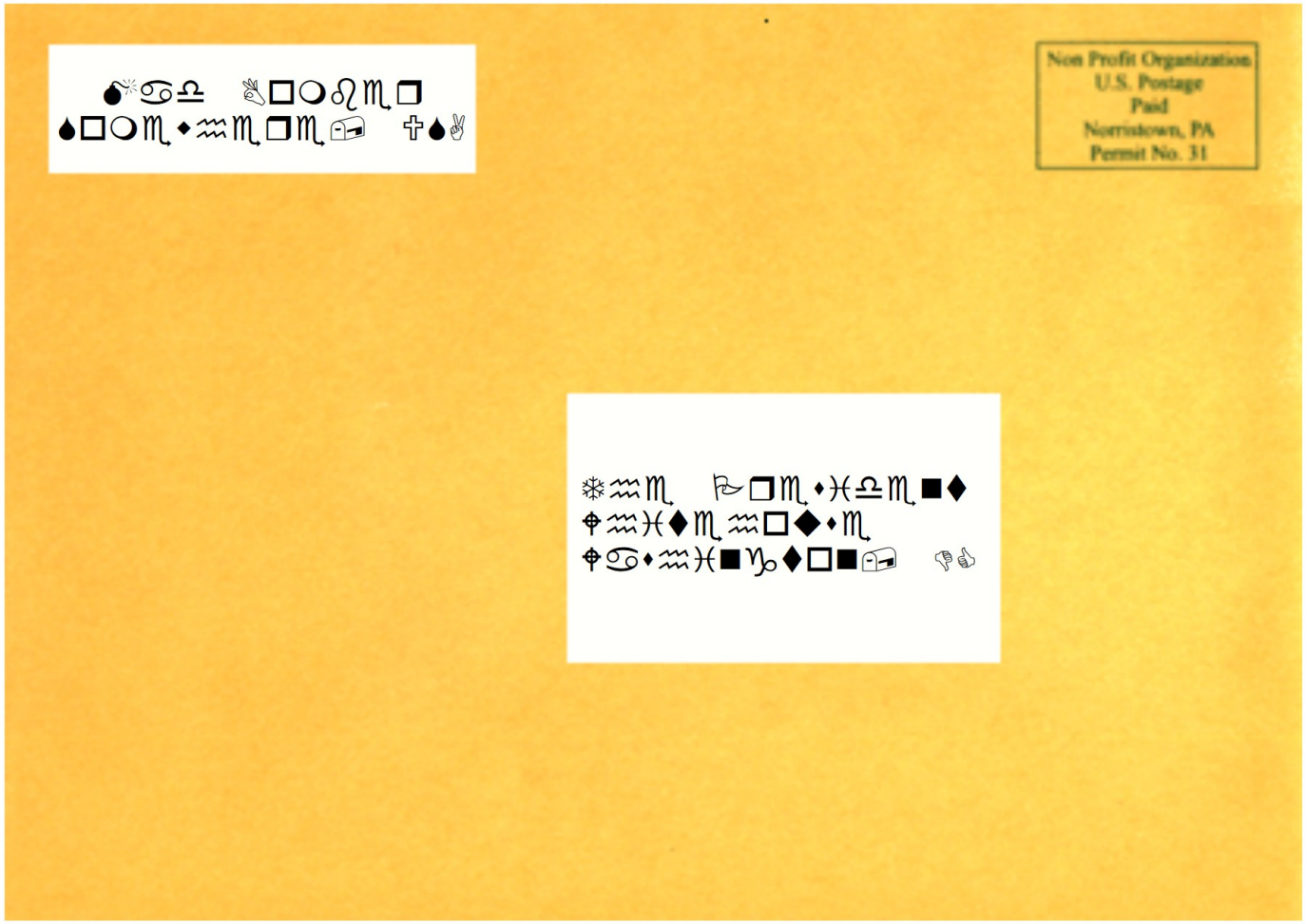
Decide whether to forward a network communication or not

List of rules based on:

- Protocol
- Sender information
- Receiver information
- IP network
- IP address
- Port

Firewalls are not foolproof!

Restricting Access - Firewalls



Now what?

Restricting Access - Firewalls

Looks ok, but...

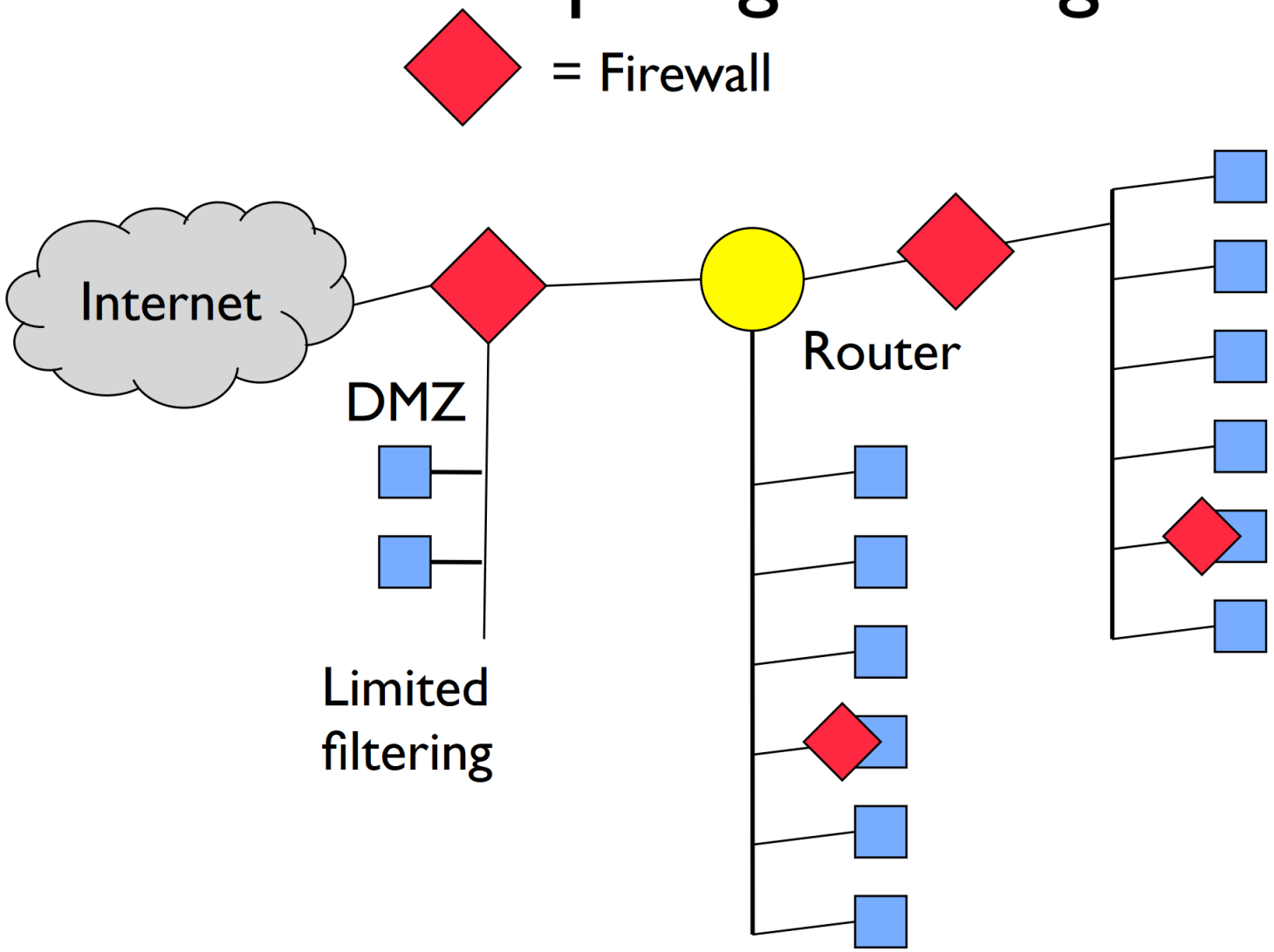
Restricting Access - Firewalls

Looks ok, but... ...see what's really inside?

Firewalls - Issues & Problems

- Outgoing traffic leads to incoming traffic
  - Firewalls must remember state information about connections that originate internally
  - Especially "hard" with UDP!
- Every packet must be checked, even those that are allowed - can be a bottleneck
- Software designed to be "firewall friendly"
  - Port 80 usually open for incoming traffic so let's run our service on that port!
  - Peer-to-peer systems can use referrals to get around incoming blocks

Firewalls - Topological Diagram



Restricting/Allowing Users - Proxy

- Firewall restricts outgoing traffic
- Users can get to outside via a proxy server
  - Firewall rules allow outgoing traffic from proxy server's IP address
- Proxy can regulate the kind of traffic
  - Logging use
  - Restricting destinations
  - Restricting content
- Proxies can also increase performance via caching

Next Gen Firewalls

Deep packet inspection plus application awareness intelligence

Block/Allow based on:

- Username
- Website or application
  - E.g. Allow salesforce.com, but block facebook.com
- End-point physical location
- Plus all of the usual IP, TCP, etc header info

Can potentially decrypt communications to watch encrypted traffic (to local systems only!)

Hide the Netwrok - NAT

NAT - Network Address Translation

- A means of using a single public Internet address to provide access to many hosts on a private network
- A way of hiding a private network from public access

NAT is commonly built-in to SOHO routers

- DHCP hands out private IP addresses
- Router bridges the connection between the network
- NAT translates network source/destination info

VPN - Virtual Private Network

VPN's allow external access into your network that is blocked by a firewall

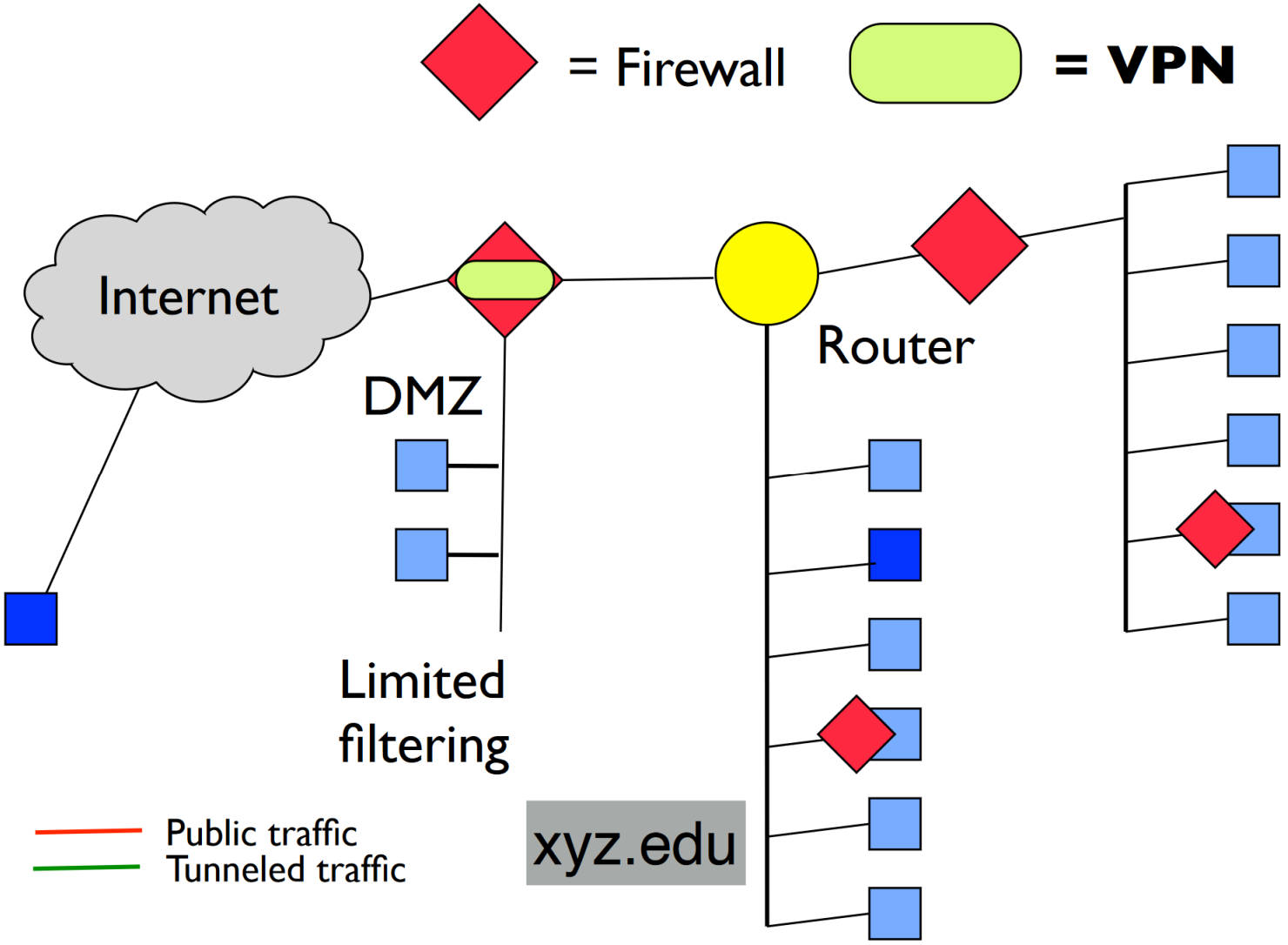
Require authentication

Create an encrypted channel over the public Internet so that communications from the remote site to the VPN server are secure

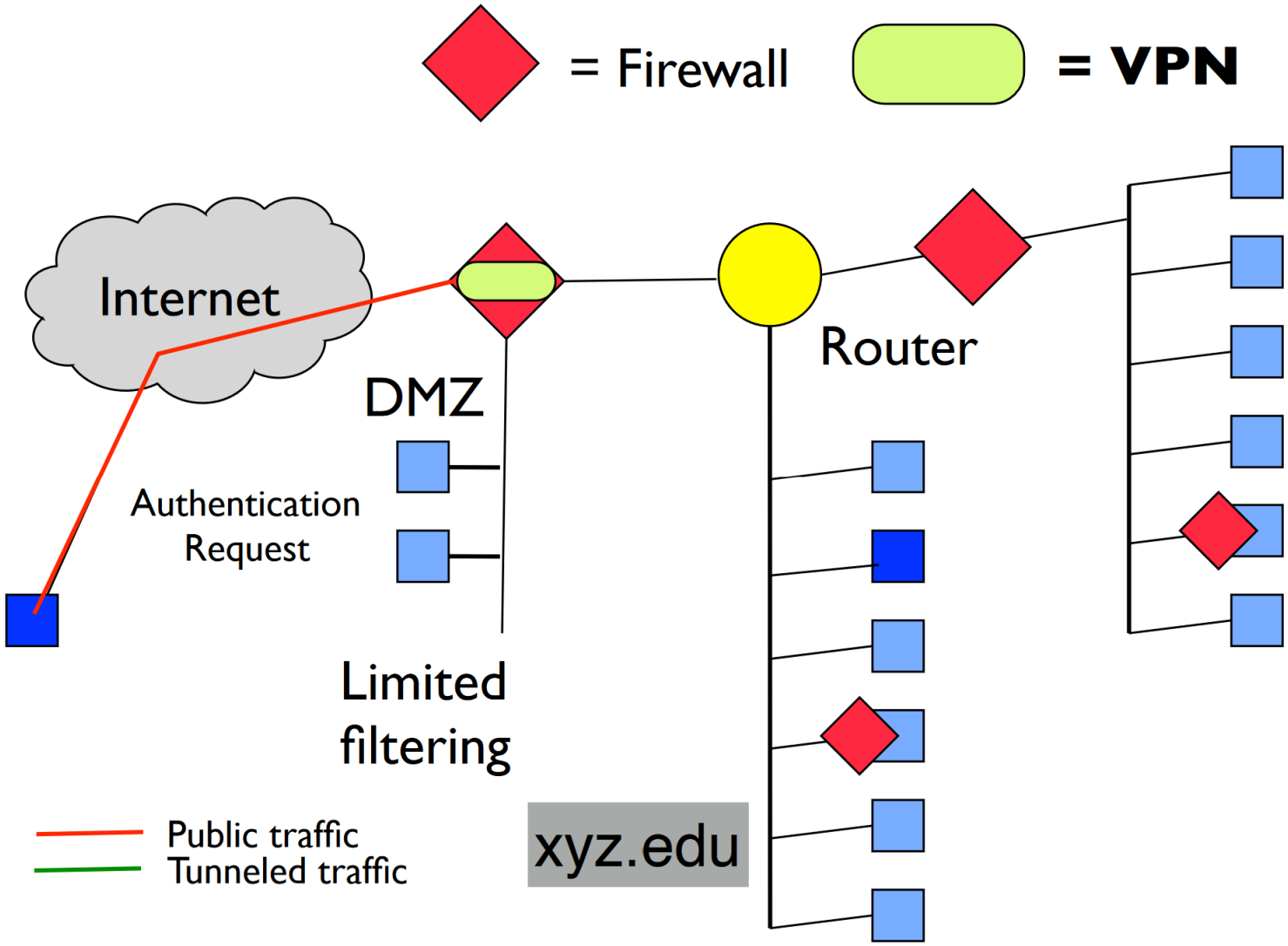
Port forwards the incoming traffic to a local, internal IP address so it appears that traffic originates on the local network

!!!Can expose a network to external threats!!!

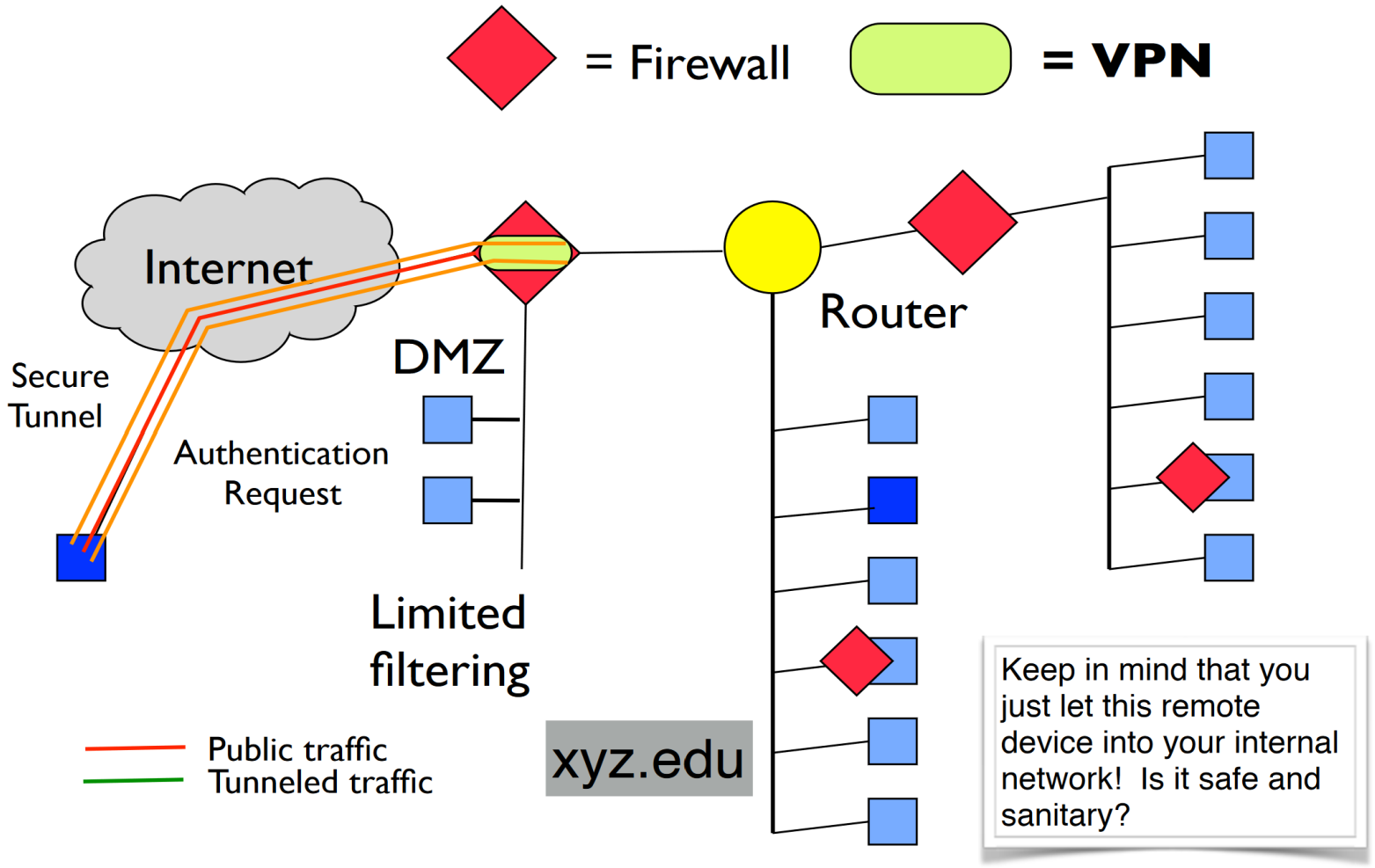
VPN - Topological Diagram



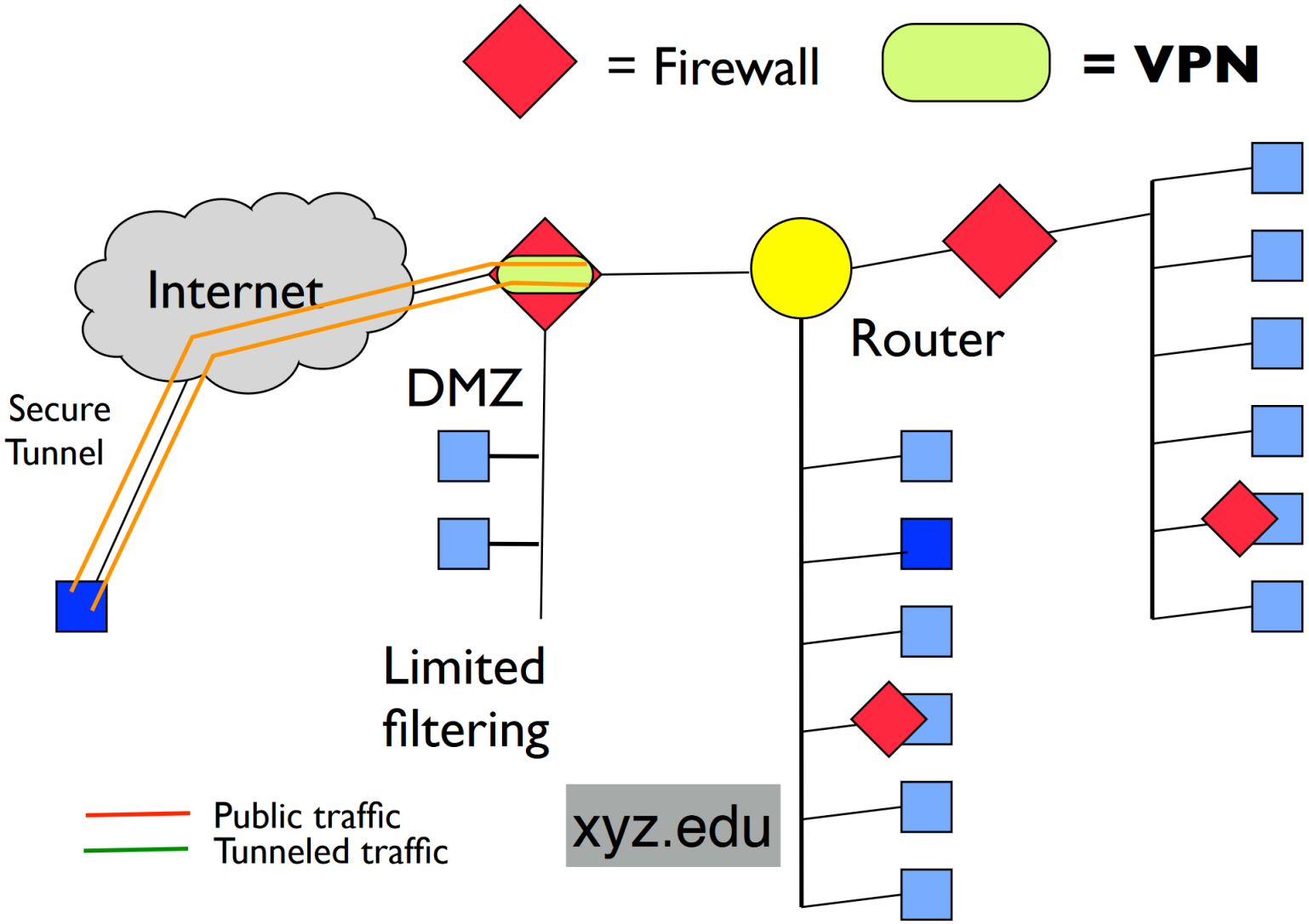
VPN - Topological Diagram



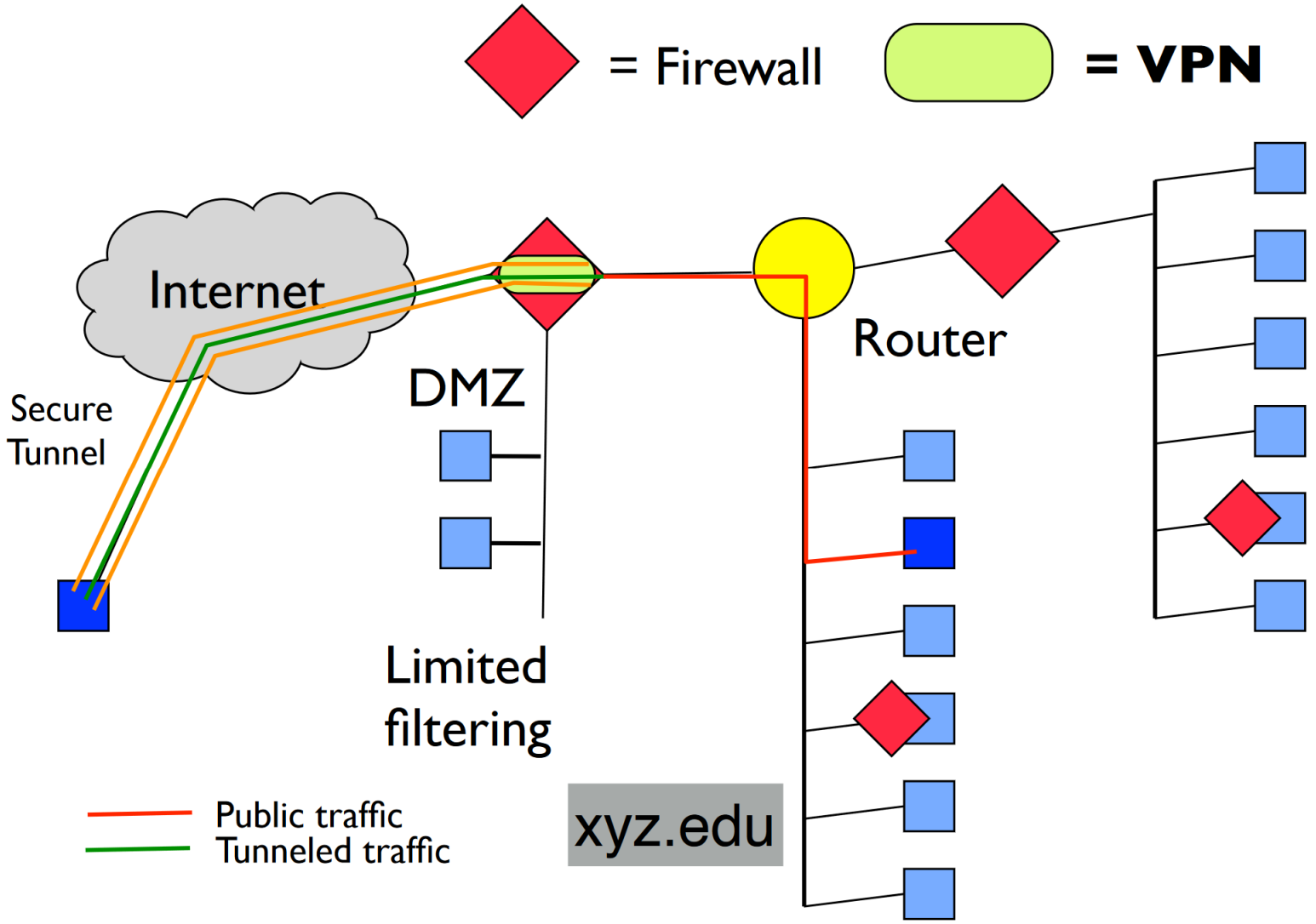
VPN - Topological Diagram



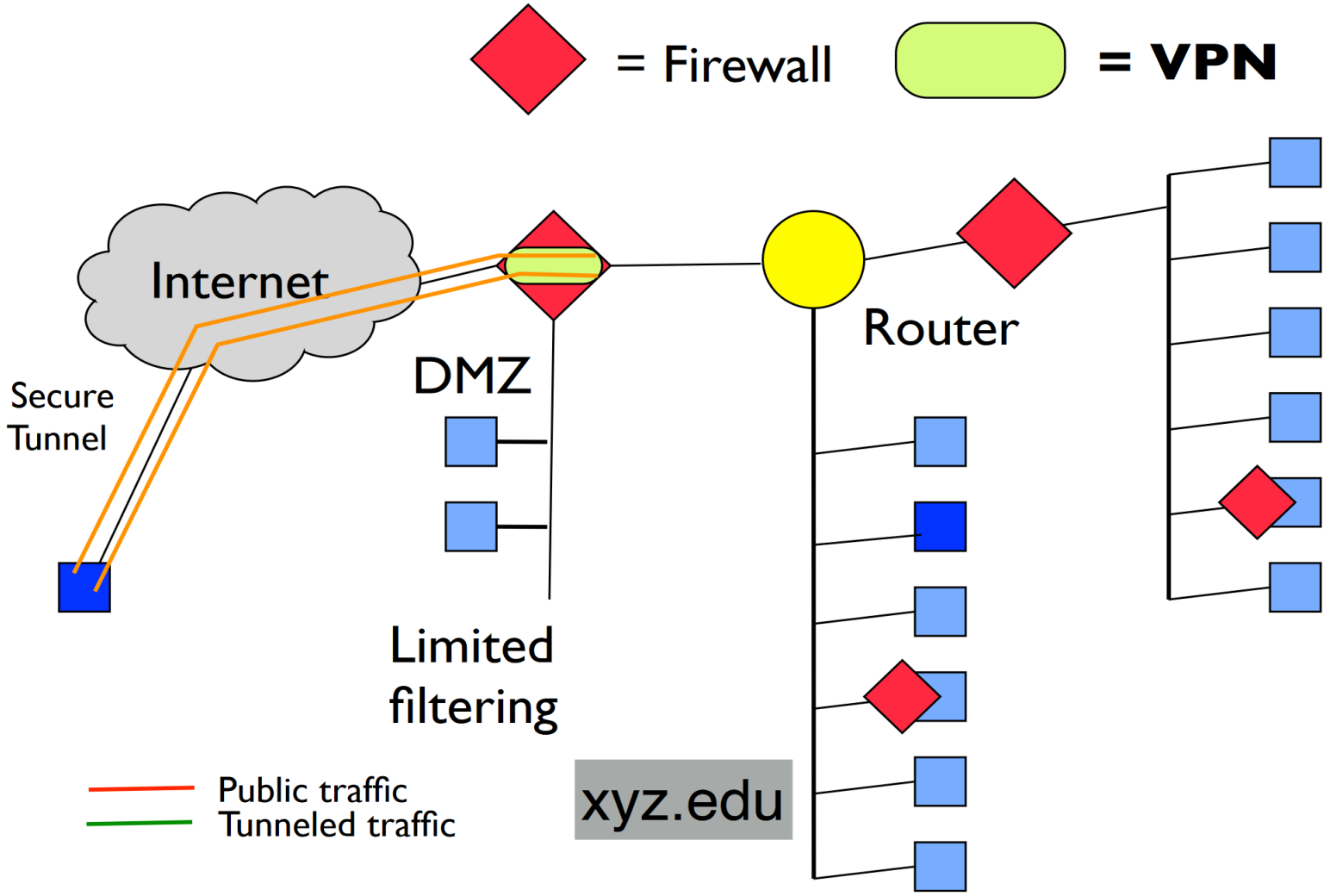
VPN - Topological Diagram



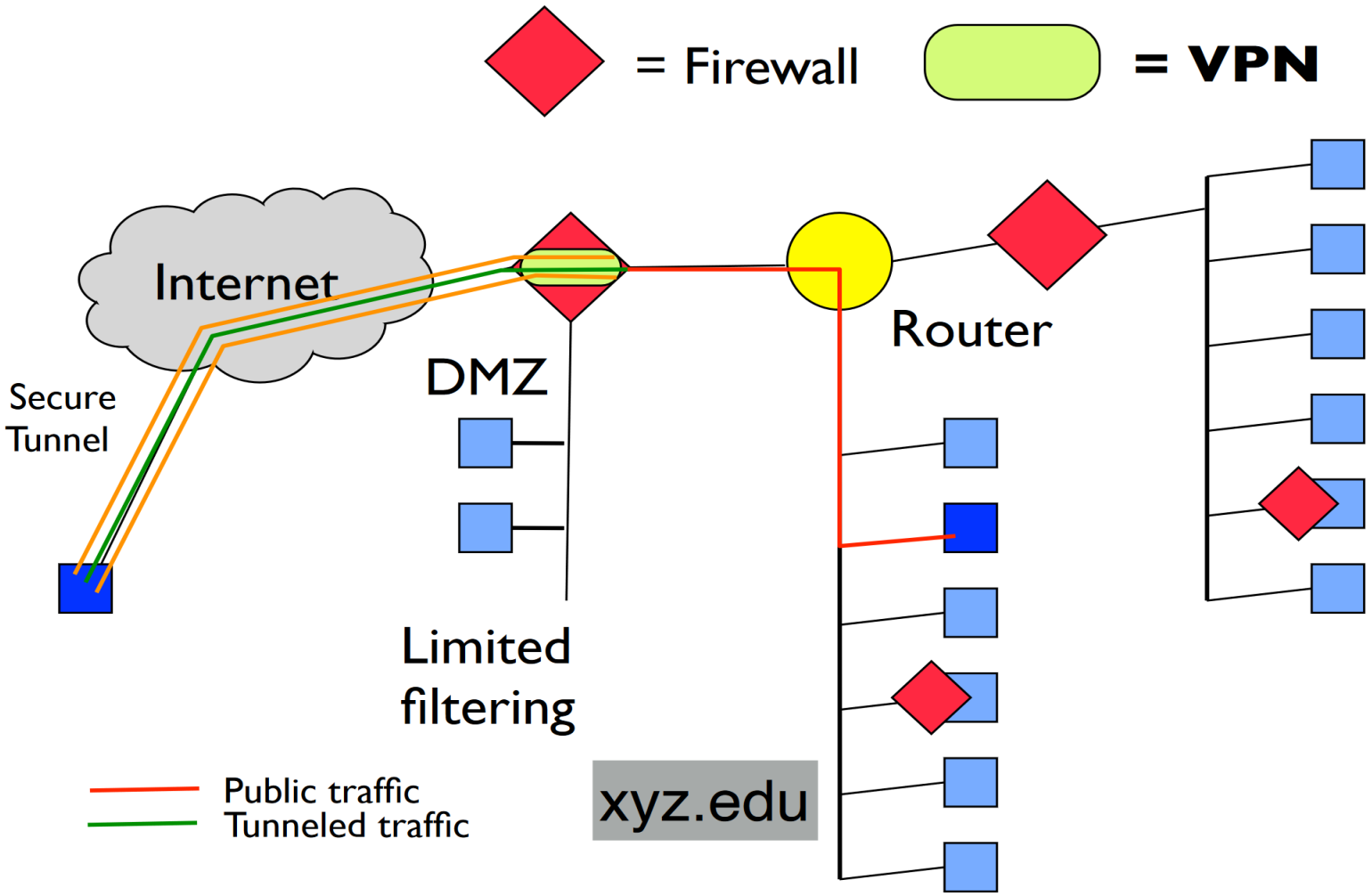
VPN - Topological Diagram



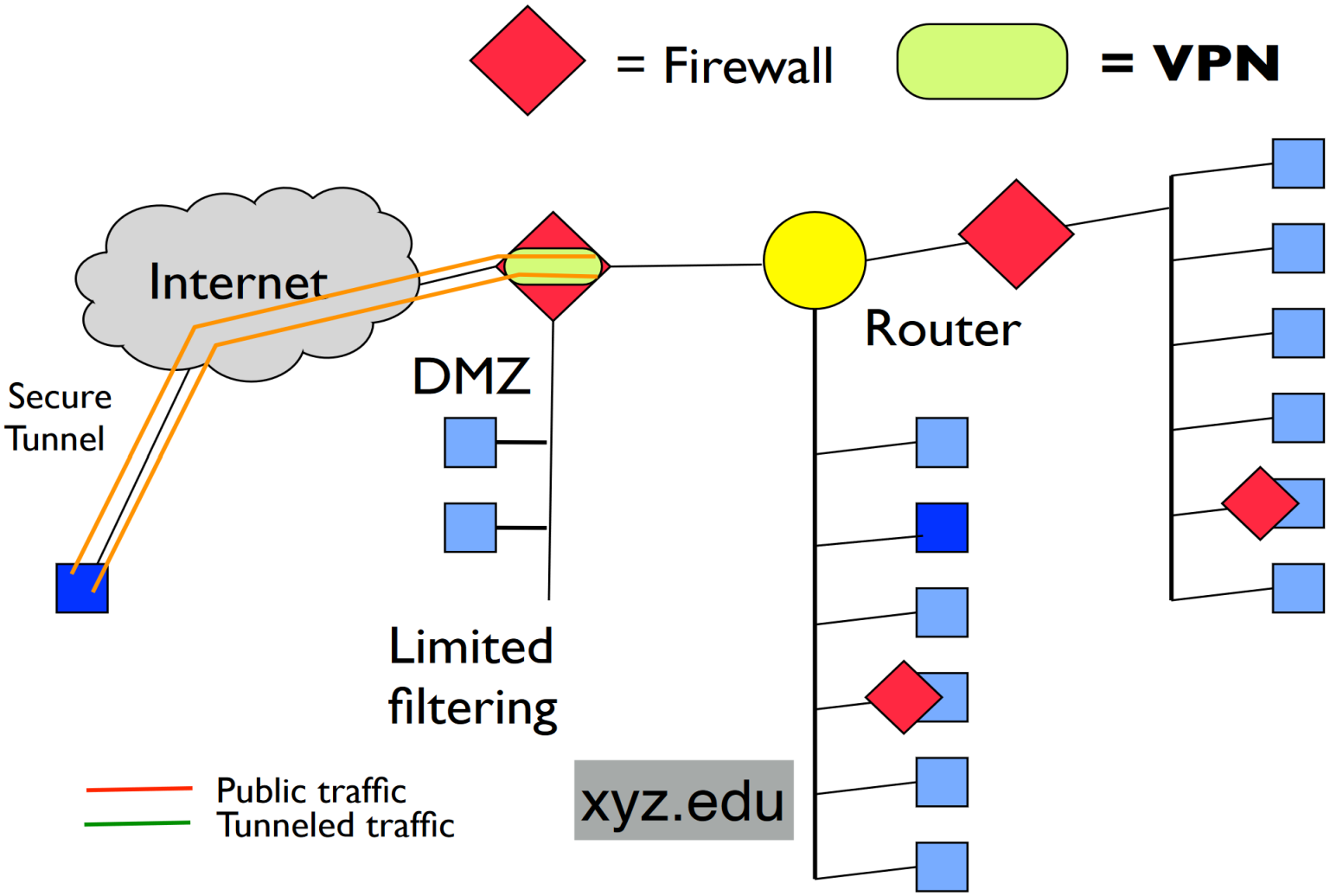
VPN - Topological Diagram



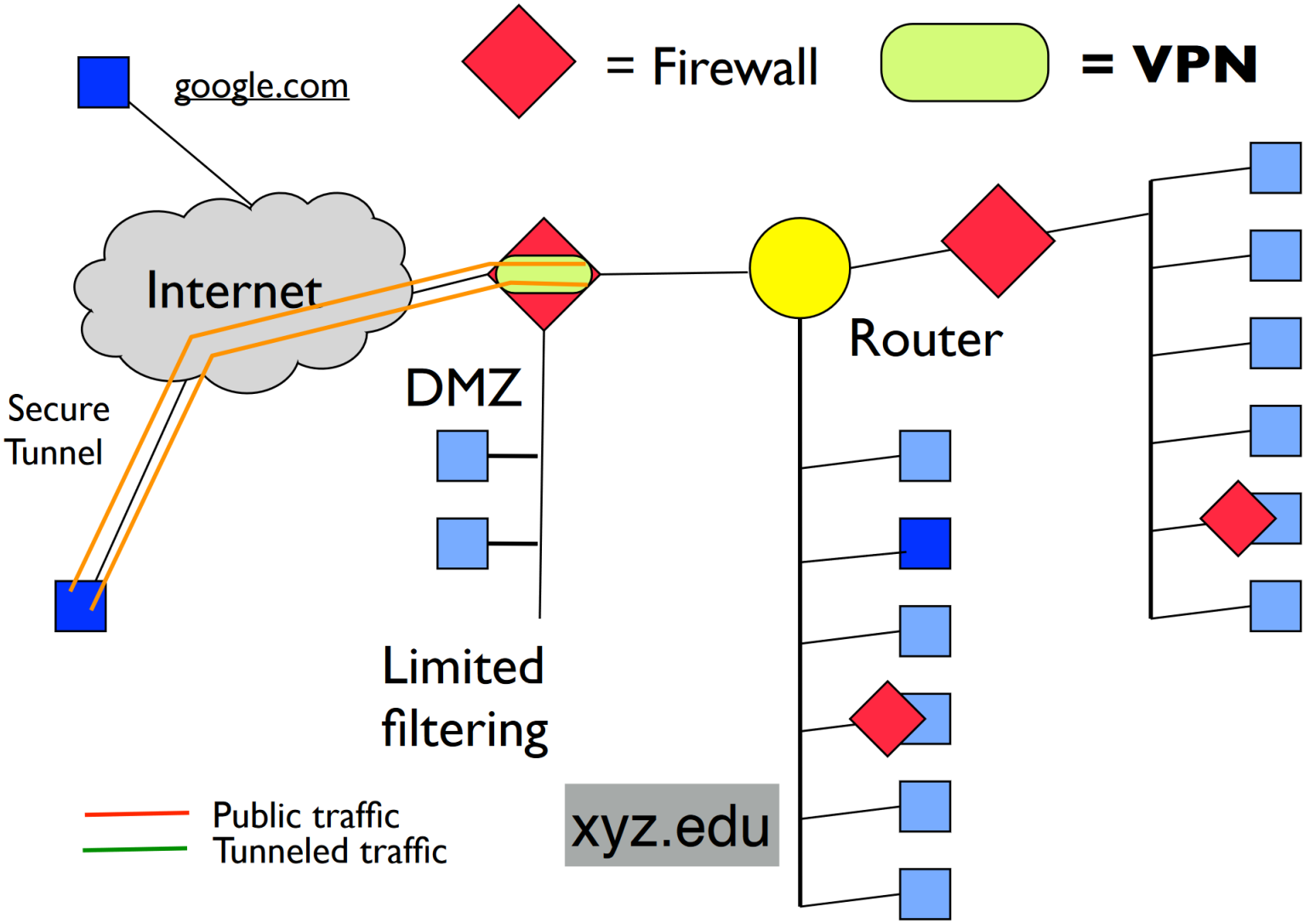
VPN - Topological Diagram



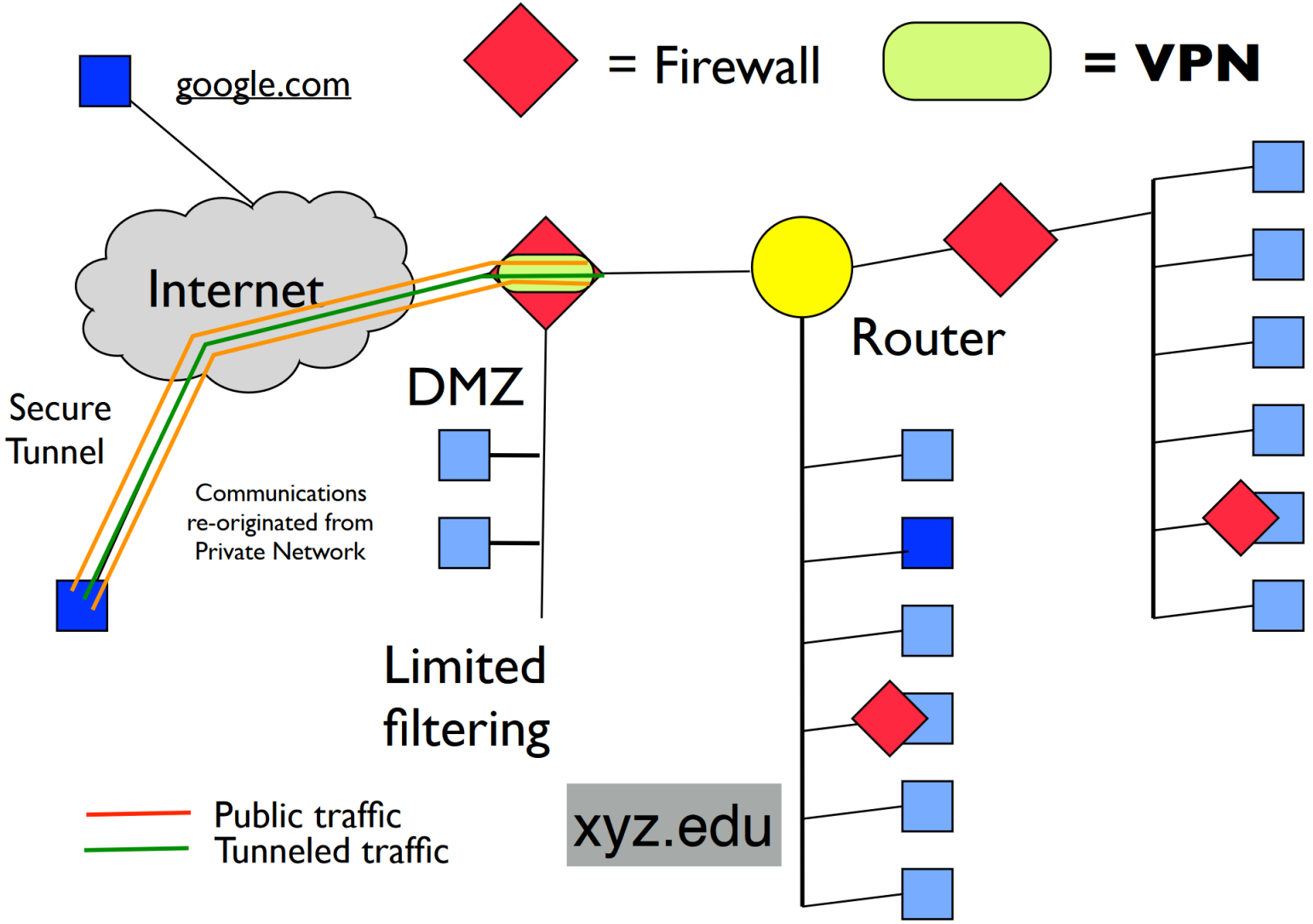
VPN - Topological Diagram



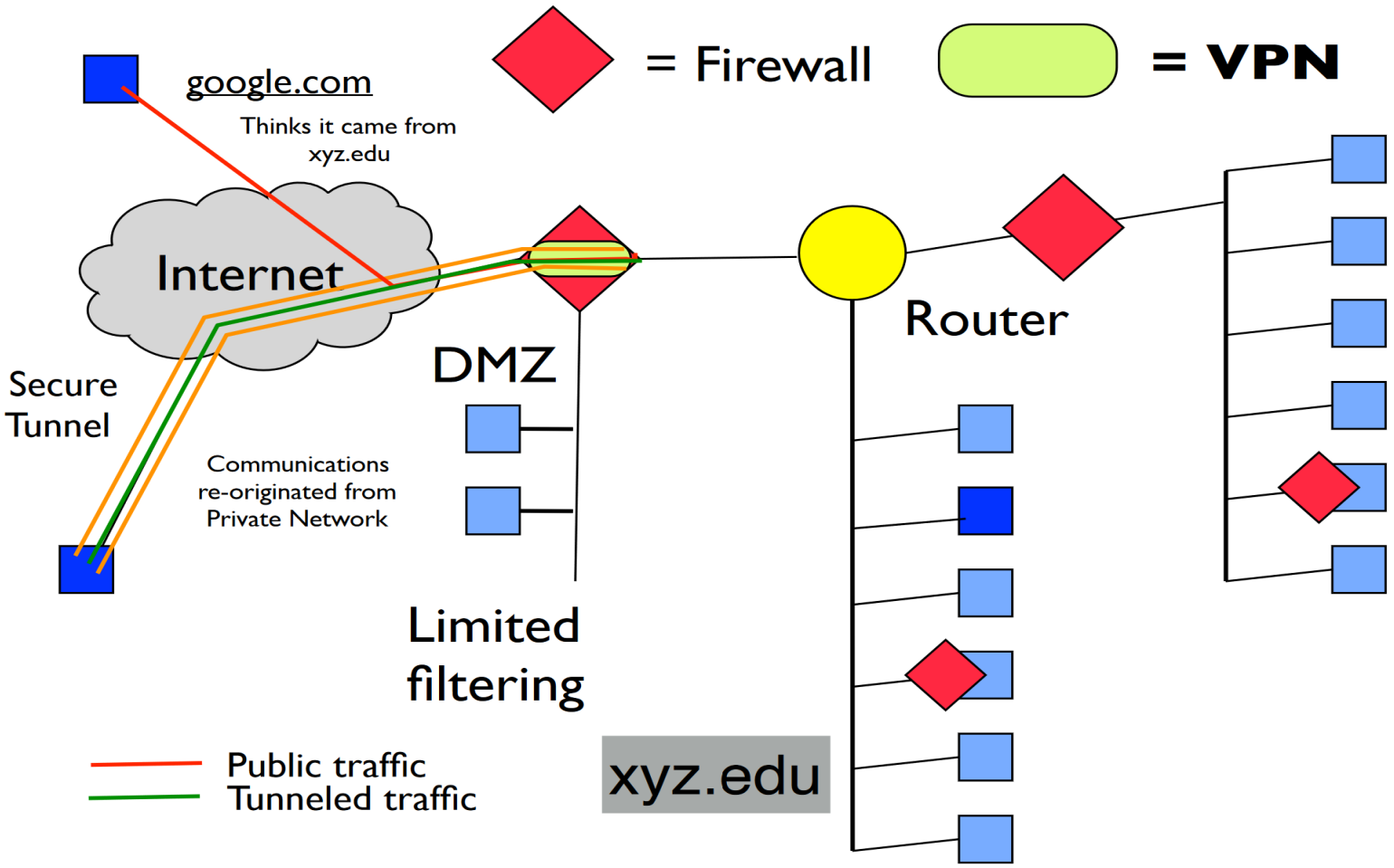
VPN - Topological Diagram



VPN - Topological Diagram



VPN - Topological Diagram



Security Scans

Computers can be checked using automated tools to see if there are possible vulnerabilities

Can be done using ping, telnet, etc

- Automated, dedicated tools are better (nmap)

Nessus - http://www.nessus.org/

- Most popular, tool available today
- Freely available
- Can tie into automated monitoring systems

Shields Up - http://www.grc.com/

- Popular on-demand scan website

Security Scans - The Results

How to use the results of a security scan:

1. Does the list of open ports match what you thing you have for running services?
2. Do you really need these services?
3. Are there any known vulnerabilities?
4. Is the firewall functioning as expected?

Intrusion Detection/Prevention

Automated monitoring of network traffic can detect security issues as they happen

IDS senses and analyzes communications at key network points

Can setup a "honeypot" to attract and study the bad actors

Active IDS or Intrusion Prevention System

- Re-write firewall rules
- Change DHCP system
- Change switch port policies

Intrusion Detection/Prevention

Automated monitoring of network traffic can detect security issues as they happen

IDS senses and analyzes communications at key network points

Can setup a "honeypot" to attract and study the bad actors

Active IDS or Intrusion Prevention System

- Re-write firewall rules
- Change DHCP system
- Change switch port policies

No, some device trying to SSH into your server 43 times a minute is not normal.