

# D N S

Allen Hancock

Onsite Consultant - The Orchard Solutions

Technical Lead - Watchman Monitoring







# What is DNS?



DNS is like an address book we use to locate systems and services on the Internet.



# DNS Structure

## Local Servers →

The name server in System Preferences

## Root Servers →

Servers spread strategically around the world

## Top-level Domain (TLD) →

Top-level domain servers: .com .net .biz .io, etc.

## Start of Authority (SOA) →

Start of Authority is the name server for your company

## Zone File

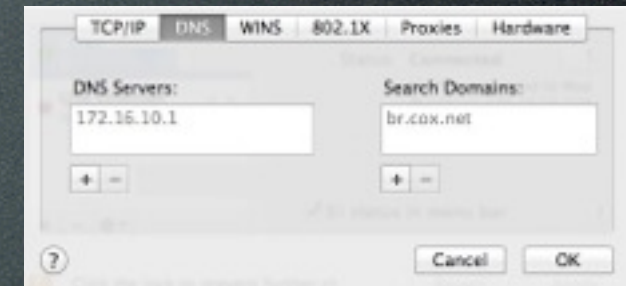
Configuration file for the SOA (Tells it who it is)



# DNS Structure

## Local Servers

- The IP address(es) in System Preferences.
- Recursive - configure to go look up whatever they don't host, or have in cache.
- Rely on forwarders to resolve unknown addresses.
- This is your window to the internet, a level of trust is implied.





# DNS Structure

## Root Servers →

- 13 Servers spread strategically around the world. These resolve the “.” which is at the end of every DNS request.
- These resolve to the ~20 generic Top Level Domains (.com, .net, .biz, ) and the ~248 country code top-level domains.



# DNS Structure

## Top-level Domain (TLD) →

- Top-level domain servers: .com .net .biz .io, etc.
- They are stepping stones on the way to your domain's SOA
- These are where your domain's nameserver records are stored when you register a domain at Network Solutions, Hover, GoDaddy & the like.



# DNS Structure

## Start of Authority (SOA) →

- Start of Authority is the name server for your company
- This is the actual record which designates ownership of a domain, where its name servers can be found, and as such, is truly where a domain's DNS begins.



# DNS Structure

## Zone File

- The actual configuration file held on your domain's Name Server.
- The information in the zone file is the target of all these name server lookups which define a domain's DNS
- Records in the Zone File become authoritative facts about your organization.



# What's a Zone File?

- A “Zone File” holds the records which make up your organization's DNS.
- Records in the Zone File become authoritative facts about your organization.



# What's in a Zone File?

- A - the IP address for an FQDN (www.apple.com).
- CNAME - Points to an A record.
- MX - A record where mail should be delivered.
- NS - Declares name servers for a given domain.
- TXT - Facts about the domain.
- SRV - Advanced way to define services



# Reading a Zone File

open <http://bit.ly/dnszone> to see this clearer

```
backupminder.org.      600  IN      A        216.70.89.143
www.backupminder.org.  3600 IN      A        216.70.89.143

calendar.backupminder.org.  3600 IN      CNAME    ghs.google.com.
docs.backupminder.org.    3600 IN      CNAME    ghs.google.com.
mail.backupminder.org.    3600 IN      CNAME    ghs.google.com.
community.backupminder.org. 3600 IN      CNAME    getsatisfaction.com.

backupminder.org.      3600 IN      MX       10 aspmx.l.google.com.
backupminder.org.      3600 IN      MX       20 alt1.aspmx.l.google.com.

backupminder.org.      3600 IN      TXT      "v=spf1 a include:_spf.google.com ~all"

_jabber._tcp.backupminder.org,  3600 IN      SRV      5 0      5269 xmpp-server.l.google.com.
_jabber._tcp.backupminder.org.  3600 IN      SRV      20      0      5269 xmpp-server1.l.google.com.
_xmpp-server._tcp.backupminder.org. 3600 IN      SRV      5 0      5269 xmpp-server.l.google.com.
_xmpp-server._tcp.backupminder.org. 3600 IN      SRV      20      0      5269 xmpp-server1.l.google.com.

backupminder.org.      86400 IN      NS       ns10.dnsmadeeasy.com.

backupminder.org. 86400 IN SOA ns10.dnsmadeeasy.com. dns.dnsmadeeasy.com. 2009010112 43200 3600 1209600 180
```



# Where does DNS “Live”?

To find out where your DNS “lives”  
(i.e. where the zone files are stored) use “whois”.

```
$whois backupminder.org
```

```
<snipped out contact info>
```

```
Name Server:NS10.DNSMADEEASY.COM
```

```
Name Server:NS11.DNSMADEEASY.COM
```

```
Name Server:NS12.DNSMADEEASY.COM
```

```
Name Server:NS13.DNSMADEEASY.COM
```



# Split DNS

- Common in SMB and SOHO markets with internal servers (rumpus, profile manager, etc)
- How will this look in LAN to WAN router?
  - External
    - files.backupminder.org A 198.13.84.190
  - Internal
    - files.backupminder.org A 172.16.1.10



# Split DNS

- Defining a Primary Zone
  - domain.com X
  - server.domain.com ✓
- Forwarding, Authoritative, and Recursive lookups with a DNS server
- Slave servers, when and why



# Split DNS

173.230.133.218 - Office's External IP address  
192.168.20.10 - Server's internal IP address  
Where will **ftp.backupminder.org** resolve?

External Lookup  
always gets WAN address

173.230.133.218 WAN

Router

192.168.20.1 LAN

Internal FTP Server  
ftp.backupminder.org  
192.168.20.10

Internal Client computer  
192.168.20.119



# Control DNS at the Router

**DNS Hosts Editor**

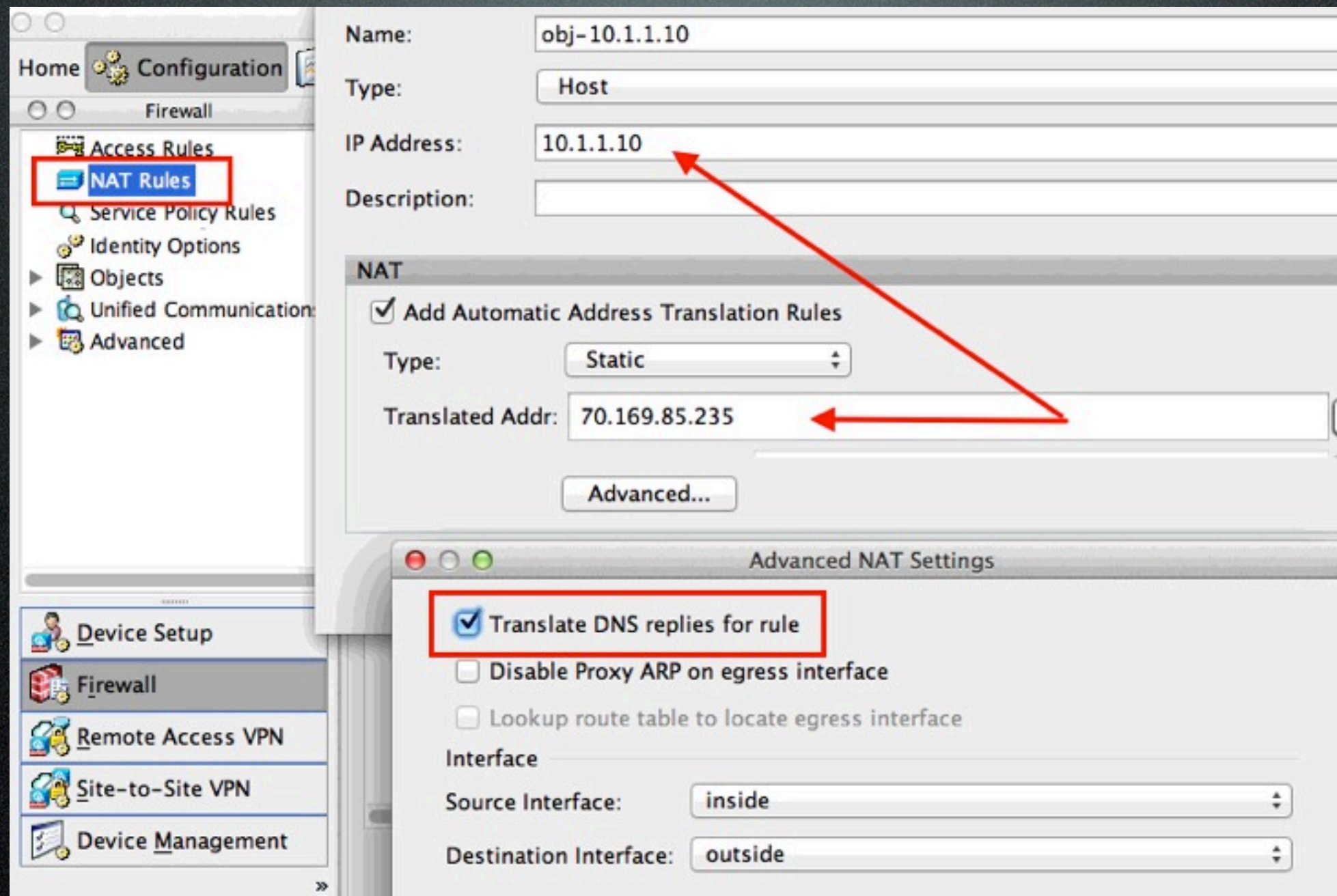
Find:

<input type="checkbox"/>	IP Address	Hostnames	Description
<input checked="" type="checkbox"/>	192.168.16.248	files	
<input checked="" type="checkbox"/>	192.168.16.245	mail;intranet;www;ltc	
<input checked="" type="checkbox"/>	192.168.16.245	files.home.eunicemanor.com	

Use semicolons ( ; ) to separate individual hostnames in a row.



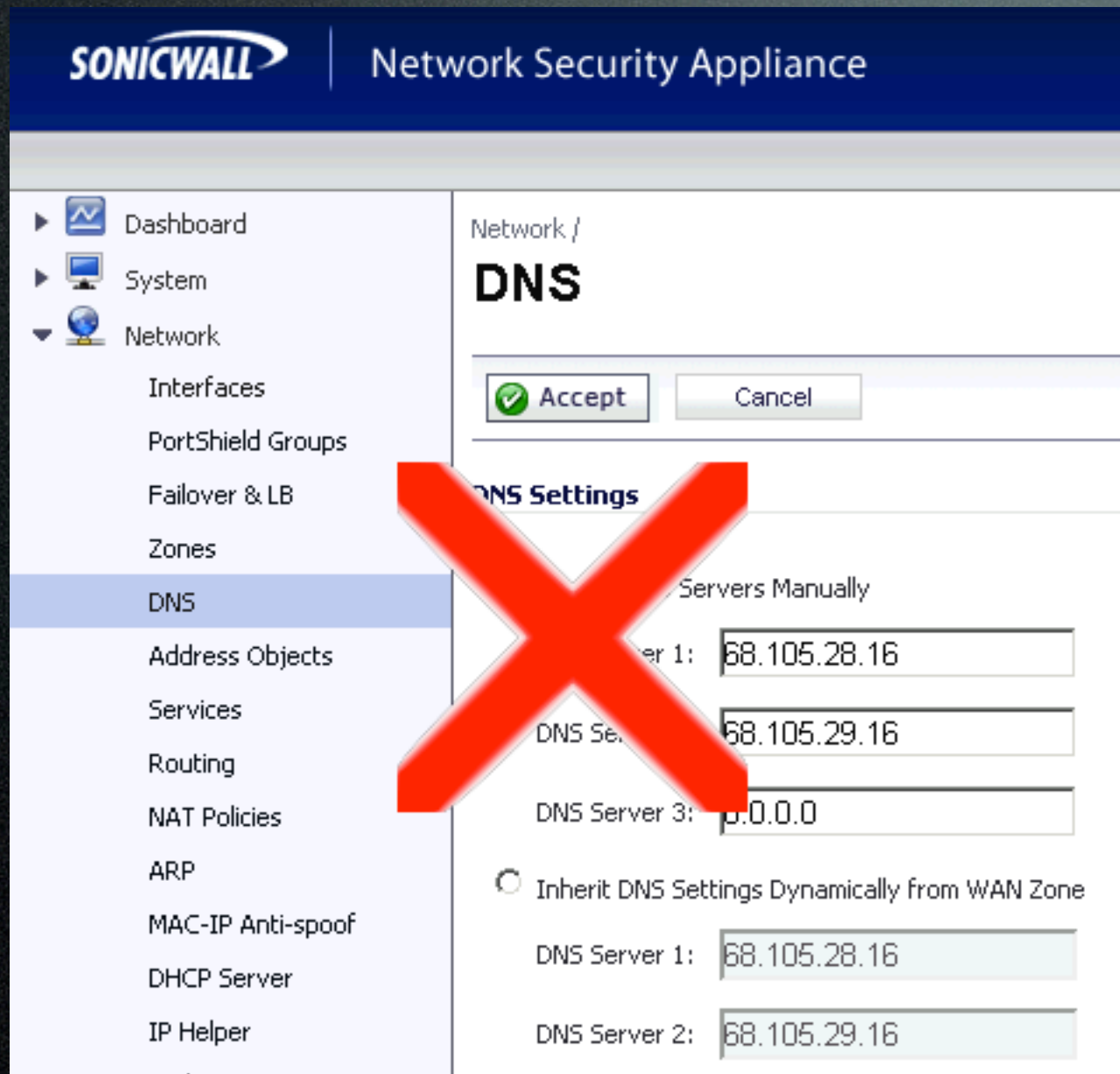
# Control DNS at the Router





# Control DNS at the Router

It's called DNS  
NAT LoopBack





# What if I don't have a public static IP?

## Dynamic DNS

- Providers - dyn.com, dnsmadeeasy
- DNS Update Clients
  - Software vs Router-embedded -

backupminder.dyn.org A 198.2.52.2 (TTL 60)

home.backupminder.org CNAME

backupminder.dyn.org (TTL 7200)



# The Importance of DNS

- Why is DNS important?
- What happens when DNS is “having issues”?



# Troubleshooting DNS

- Start at the beginning. Always.
- Use whois to confirm the domain & owner:

```
whois backupminder.org
```

```
Registrant:
```

```
Watchman Monitoring, Inc.
```

```
Name Server:NS10.DNSMADEEASY.COM
```

```
Name Server:NS11.DNSMADEEASY.COM
```

- Is the ownership correct?
- Can you make changes at the Name Servers?



# Troubleshooting DNS

- Next Confirm the active DNS Server!
  - Check system preferences
  - `ipconfig getpacket en0` (or `en1` for wifi)
- Check records locally, and at another NS
  - `host server.domain.com`
    - vs
  - `host server.domain.com 8.8.8.8`
  - Is there a difference, what does that mean?



# DNS Troubleshooting

- Using the built in resolution libraries vs query tools like nslookup dig
- DNS change propagation times / ttl
- dscacheutil -flushcache
- Host lookup:
  - host server.domain.com
  - host server.domain.com 8.8.8.8





**MACTECH**





# Q&A

- Bring them on... you know you have them!
- [consultants.apple.com](http://consultants.apple.com)
- <https://groups.google.com/forum/#!forum/acn-alumni>
- [watchmanmonitoring.com/acn-benefit](http://watchmanmonitoring.com/acn-benefit)