



# Lock up your Servers!

Protecting your Domino servers against internet attacks

Warren Elsmore  
BE Systems



# Agenda

- Access
- Authentication
- Server Topologies
- Tools and Resources
- Q & A



# Before we begin...



# Before we begin...

- Don't be complacent - no list is complete
- This presentation is based upon IBM Lotus Domino 6.5.x and above
- What am I showing?
- What am I NOT showing?
- Use this information responsibly.



# Agenda

- Access
- Authentication
- Server Topologies
- Tools and Resources
- Q & A



# Access - Server Platform

- Windows/Linux/Sun/AIX/S390....?
- OS ports
- File system
- User Accounts
- DON'T use the server as a client.



# Access - Notes Client access

- Do you need this?
- Turn on Port Encryption
- Turn on Password Checking
- Turn on Public Key Checking
- Turn off Anonymous Notes Connections.



# Access – IBM Lotus Domino Web Server

- Security model follows the Lotus Domino model
  - Server
  - Database
  - Site
    - Document
    - Field
  
- (Generally) no public key infrastructure
  
- (Generally) some anonymous access.



# Access - Server Level

- Follow good Lotus Notes security practice
  - 'Access server'
  
  - 'Not access server'
  
  - 'Run Restricted'
  
  - 'Run Unrestricted methods and operations'
  
- Turn off what you don't need
  - DIIOP
  
  
  - Remote Debug etc.



# Access - Port Level (HTTP)

- HTTP port security
- “Enforce Server Access Settings”
- Browse databases
- IP Address Allow/Deny lists
- Logging.



# Access - Site

- Internet Site Documents
- Introduced with Domino 6
- Are 'Internet Site' based, rather than 'Server' based
- Far more flexible than web site documents
- Allow for multiple, different, web site configurations.



# Access - Database Level

- Remove unnecessary databases AND templates
- SET YOUR ACLs !!!!!
- 'Maximum Internet Access' ACL entry
- 'Don't allow URL Open' - Database Property
- 'Require SSL Connection' – Database Property
- Configure event monitoring to look for ACL changes.



# Access – Review of Lotus Domino URL's

- Domino URLs are logically generated
  - `http://Host/DominoObject?Action&Arguments`
  - `http://Host/database.nsf/view/key?opendocument&login`
  
- Eg. <http://www.server.com/database.nsf/Myview/4?opendocument>
  
- There are a number of other valid URLs
  - Host/database/UNID
  - Host/UNID
  
- Check the 'URL Cheat Sheet' in Developerworks.



# Access - View

- Your views may contain data
- There is NO SUCH THING as a hidden view on the web
- Set view Readers field
- Create view templates for all your views, or create a `$$ViewTemplateDefault`
- `$$ViewTemplateDefault` *Page*
- Form Formulas can be bypassed.



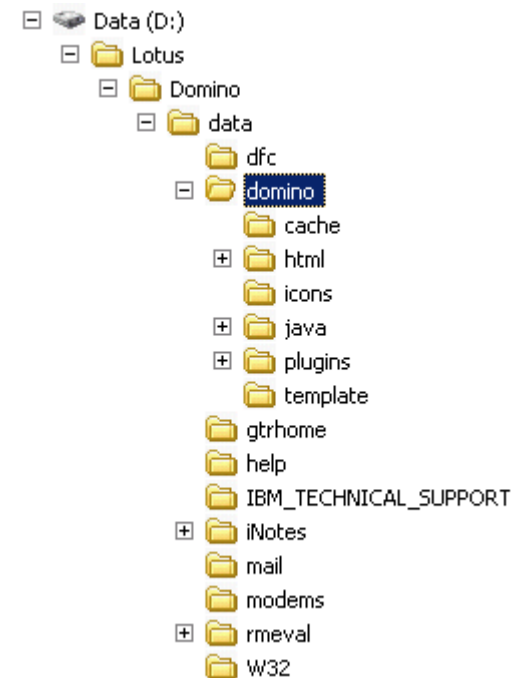
# Access - Document and Field

- Set your Readers and Authors fields correctly
- Don't rely on hidden elements
- Be aware – Hide-when sections can be read by DIOP.



# Access - Non-NSF objects

- Domino serves more than NSF;
  - HTML
  - JPG, Gif etc
  - Perl & CGI
  - Javascript files
  - Templates (.NTF)
- Most do not have ACLs
- File protection documents
- (plus) Directory rules.



# Access – Non-NSF objects

- Protection Documents apply ACL-like security to files or directories
- GET = read access
- POST = write (upload)
- File protection can be applied to CGI scripts – but NOT to any resources they access
- Don't protect 'java' or 'icons' – these are used by Lotus Domino.



# Agenda

- Access
- Authentication
- Server Topologies
- Tools and Resources
- Q & A





# Authentication - 'Domino Web Configuration' Db

- Must be created from 'Domino Web Server Configuration' template
- Must be called 'Domcfg.nsf'
- Allows you to provide
  - Custom login screens
  - Custom password change screens
  - Custom Error messages
- Can be redirected, or edited directly in the database
- With SSO, this database MUST be SSL Encrypted.



# Authentication – SSL

- Secure Sockets Layer
- Private/Public key infrastructure
- Verifies peer identity and (optionally) encrypts HTTP traffic
- Two types – Client and Server
- Server certificates are a MUST for site security.



# Authentication – SSL Server Certificates

- Verify the Identity of the server
- Can be self certified or purchased
- SSL Port must be enabled
- Redirect users to SSL.



# Authentication – SSL Client Certificates

- Verify the identity of your users
- Follow a similar format to Notes certificates
- Require specific maintenance to issue, renew and revoke certificates
- Plus – client certificates install into the browser.



# Authentication - Passwords

- THE most important layer of security
- Consider two factor authentication
- Should you allow password synchronisation?
- Set 'Fewer Internet Authentication variations'
- Pre 4.6 domains – “Upgrade to more secure Internet Password Format”.



# Authentication – Passwords

- Use a Security policy to enforce password quality
  - Length
  - Quality ('Notes' Quality)
  - Expiration times
  - Change intervals
- HTTP Password caching
  - New passwords – user must wait
  - Changed passwords – old password will still be valid
  - `HTTP_PWD_CHANGE_CACHE_HOURS = 0.`



# Agenda

- Access
- Authentication
- Server Topologies
- Tools and Resources
- Q & A

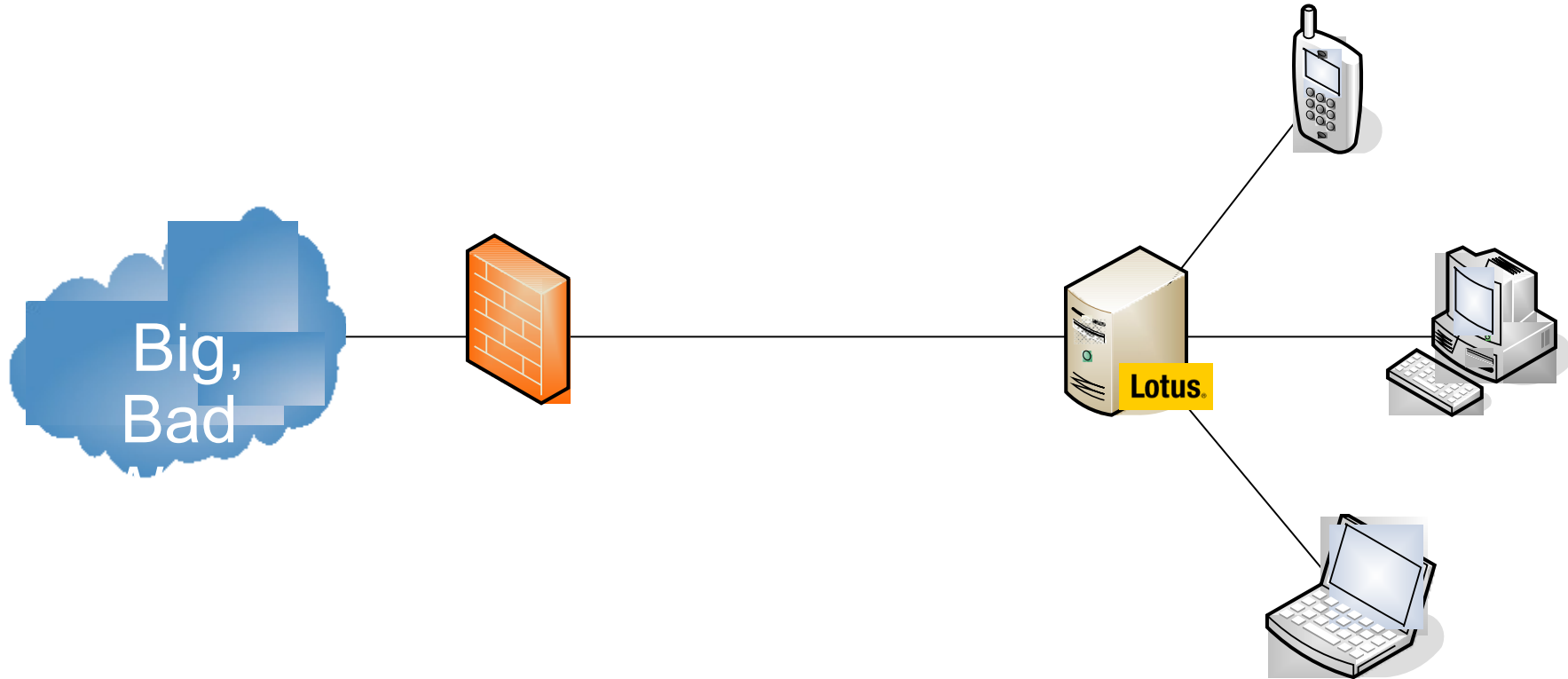


# Server Topologies

- Single Lotus Domino Server
- Two (or more) Lotus Domino Servers
- Multiple Web Servers



# Single Server

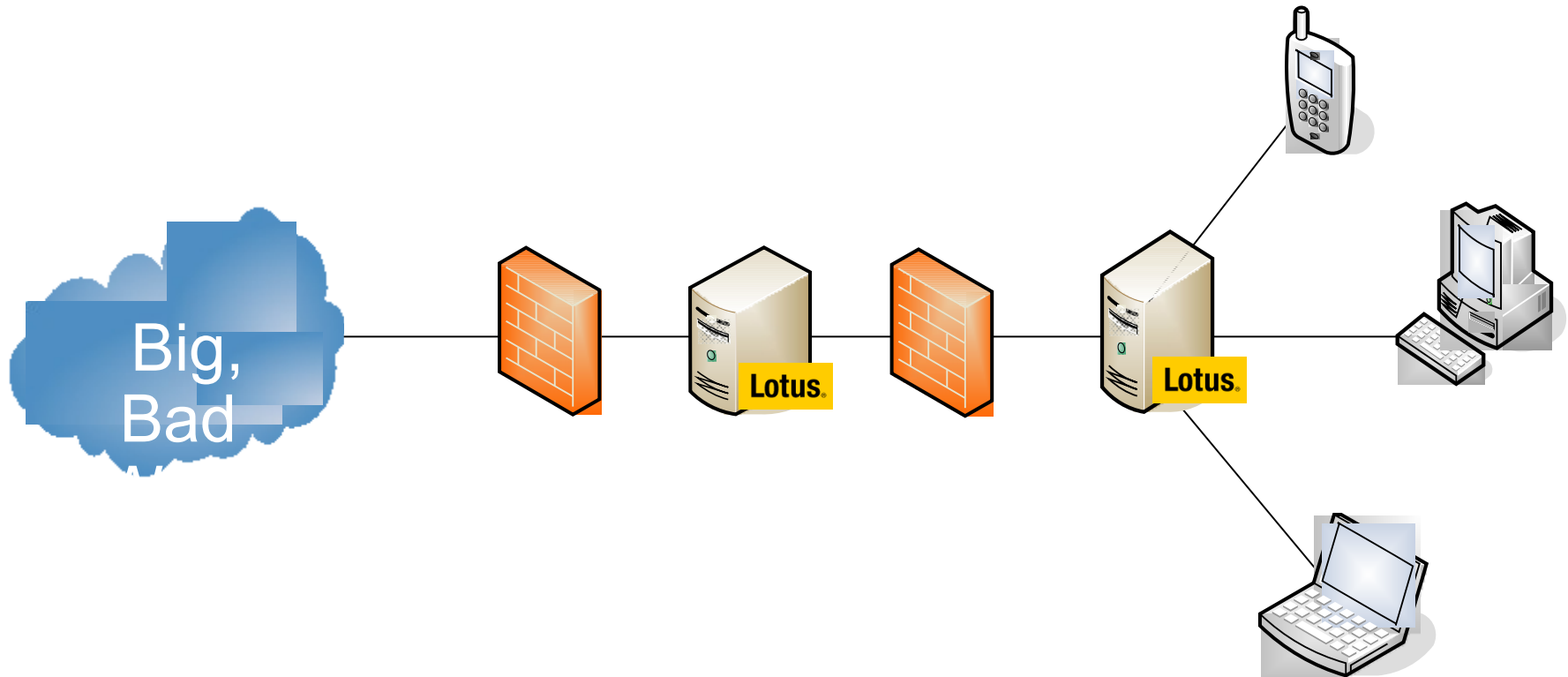


# Single Server

- All your data is on one server
- The same server that you are opening to the internet
- Be VERY careful.



# Two Lotus Domino Servers

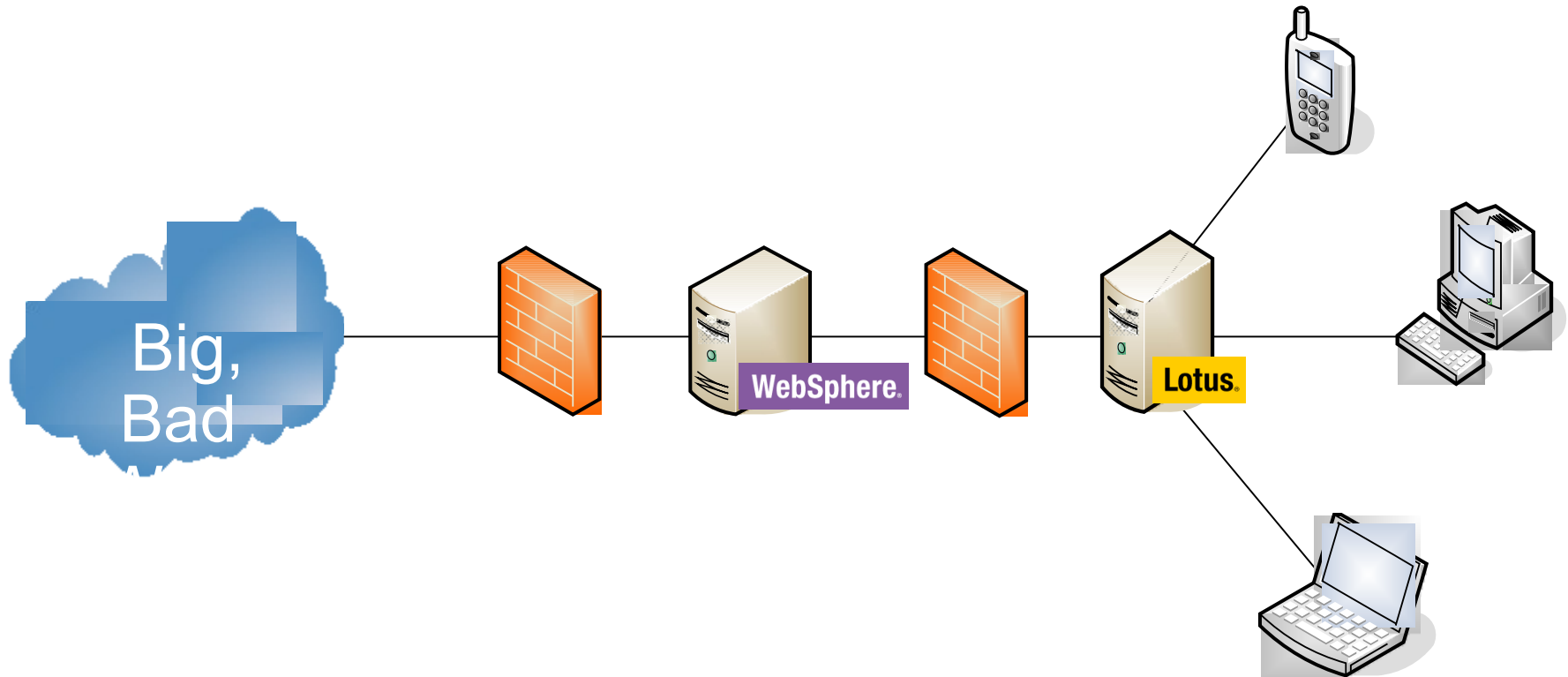


# Two Servers – Lotus Domino Servers

- Think about what the server is for and replicate only what you need to the DMZ
- Create a separate domain and certifier for the DMZ server
- Cross certify the new server and create adjacent domain documents
- Configure directory assistance for the new domain
- Create one way replication connections from the inside server for names.nsf, etc.



# Two Servers – Front End Server



# Two Servers – Front End Servers

- What is a Front End Server?
  
- Lotus Domino supports both IHS and IIS out of the box
  
- Advantages
  - Initial requests are not handled by Domino
  - May provide better protection for non-nsf resources
  - Allows for easier load balancing and fault tolerance
  
- Disadvantages
  - \*.nsf is still directed to the Domino Server
  - Domino must still be secured.



# Agenda

- Access
- Authentication
- Server Topologies
- Tools and Resources
- Q & A



# Security Tools

- Google
  - [www.google.com](http://www.google.com)
  - “site:www.mysite.com +nsf”
- DominoHunter
  - [sourceforge.net/projects/dominohunter](http://sourceforge.net/projects/dominohunter)
- Third Party Intrusion tools



# Resources

- Administration help file
- Redbooks
  - ‘The Domino Defense: Security in Lotus Notes 4.5 and the Internet’ - SG24-4848
  - ‘Lotus Notes and Domino R5.0 Security Infrastructure Revealed’ - SG24-5341
  - ‘Lotus Security Handbook’ - SG24-7017-00
  - ‘Security Considerations in Notes and Domino 7’ - SG24-7256 (in draft)
- IBM Technote
  - ‘Guide to Secure Domino Applications’ - 7002555
- Developerworks Article
  - ‘Securing a Lotus Domino Web server’ article – July 2005
- My blog and presentation
  - [www.elsmore.net](http://www.elsmore.net)



# Q & A

- Questions?

[www.elsmore.net](http://www.elsmore.net)

[warren.elsmore@bewithus.com](mailto:warren.elsmore@bewithus.com)

