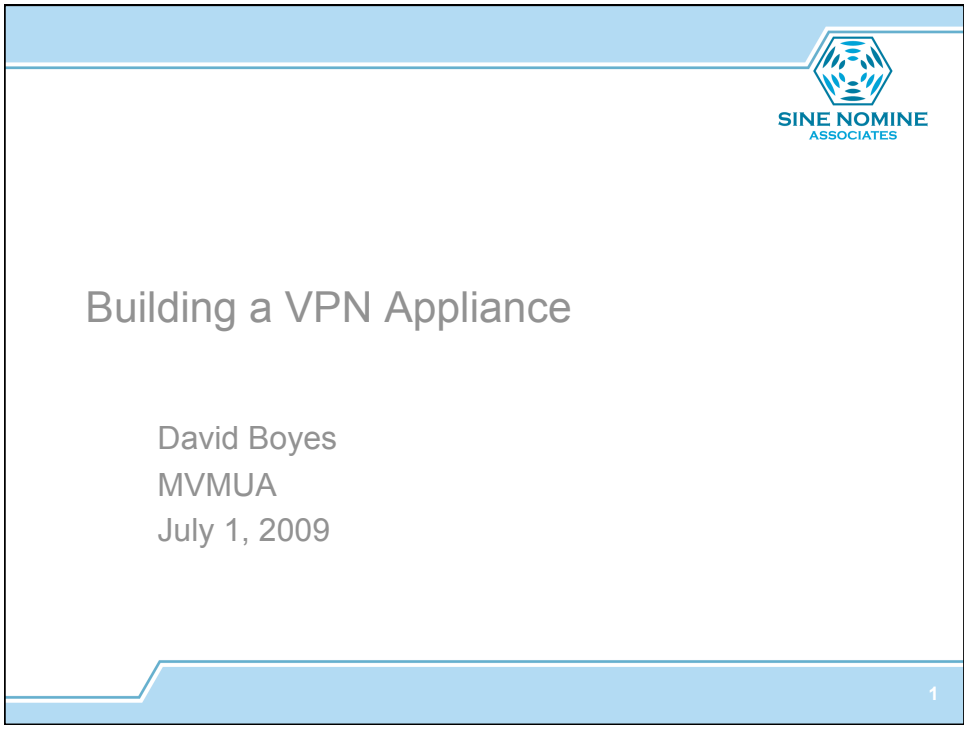
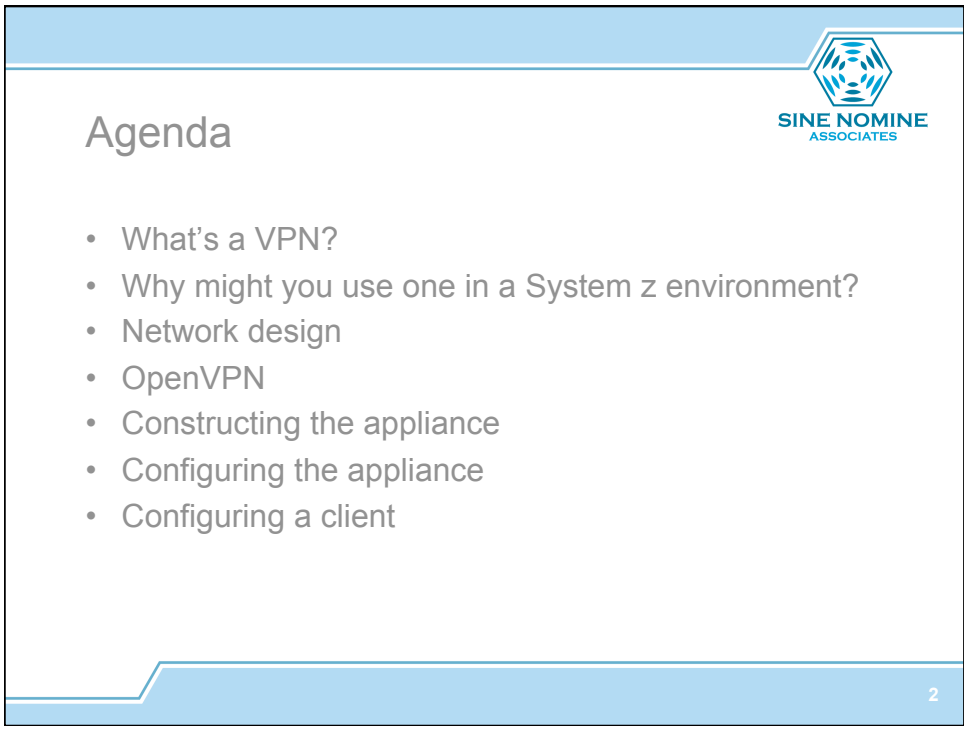

SINE NOMINE
ASSOCIATES
Building a VPN Appliance
David Boyes
MVMUA
July 1, 2009
1

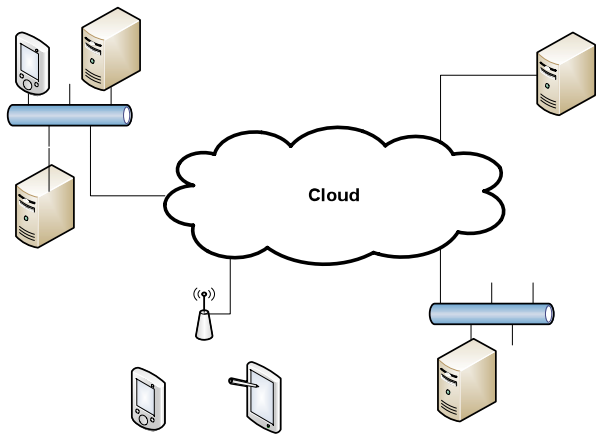

SINE NOMINE
ASSOCIATES
Agenda
• What's a VPN?
• Why might you use one in a System z environment?
• Network design
• OpenVPN
• Constructing the appliance
• Configuring the appliance
• Configuring a client
2

## What's a VPN?

- Virtual Private Network
  - A way to extend or bridge two network segments via another connected network
  - Passes data packets as the payload in the packets between two endpoint servers
  - Generally encrypted
  - Provides fine-grained authentication, authorization and access control to network segments

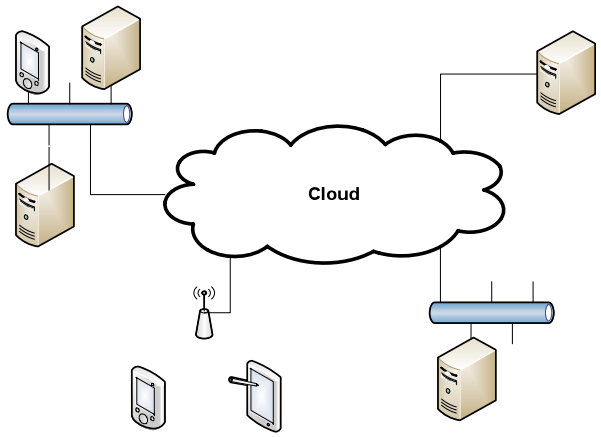
3

## Biggest Picture




4

## Biggest Picture




5

## Why on System z?

- Obvious case: let client systems access network resources via most reliable system in the network
- Not so obvious cases:
  - More granular access control to certain network services without modifying application code
  - Server to server dedicated paths w/o compromising network integrity
  - Protect sensitive traffic even in memory-based networks
  - Dynamic network reconfiguration if using virtual machines as cloud/grid servers
- May cost some additional CPU over external VPN server but often delivers substantially superior flexibility in configuration management

6

## Network Design

- Basic characteristics:
  - VPN service can be both layer 2 and layer 3 (bridge vs routed)
    - Layer 2 bridge used for non-IP protocols (SNA, etc)
    - Layer 3 for most common cases (IPv4, IPv6)
  - Both require a IP subnet ***DIFFERENT*** from the ones you are connecting to use for the VPN connections!
    - This is a basic requirement for IP routing to work. No, you can't avoid it. Don't try. You'll be sad.

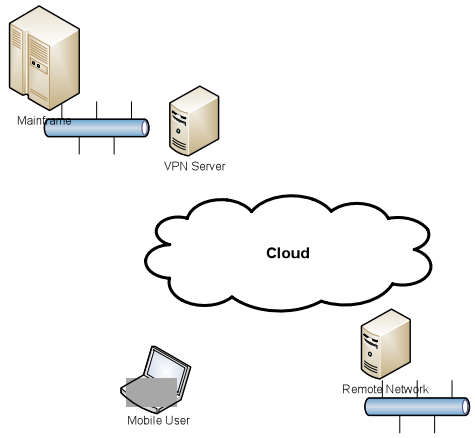
7

## Network Design

- You should work with your networking people
  - It makes them less cranky
    - If you do dynamic routing anywhere else in your network, this stuff may show up accidentally, and it will do strange things to routing tables
    - It tends to help them understand that all this virtual stuff is GOOD for them

8

## Big Picture (not so big as before)




9

## Tips on Network Design

- Avoid 192.168.x.x as your VPN subnet
  - Too many home router vendors use it (particularly 192.168.1.x)
  - With NAT involved and VPN stuff involved, address duplicates can easily occur
  - 172.x.x.x and middle of the 10.x.x.x space are more sparsely used and are equally valid.

10

## Tips on Network Design

- Make sure the client and VPN servers on each end of the VPN can reach each other somehow
  - The two can be the same machine
  - Seems obvious, but this is a common firewall problem that gets overlooked
  - Only the VPN port between the two VPN endpoints needs to be open (other traffic will flow through the VPN to the other side)

11

## OpenVPN

- SSL/TLS based open source VPN server and client application
- Uses OpenSSL encryption engines
- Included in both major distributions (RHEL, SLES)
- Clients on many platforms (sample):
  - MacOS - Solaris
  - Linux - AIX
  - PalmOS - Windows
  - iPhone (new) - Etc.

12

## Certificates

- Where there is SSL, there goes certificate hell
  - Can use self-signed certs
  - Recommended to use public or CAcert certificates
- Two certs to manage for each connection:
  - CA certificate and private key (once per OpenVPN server)
  - Client/user-specific cert and private key (once per connection)

13

## Certificates

- Total mutual authentication model:
  - Server only needs it's own certificate key to operate – doesn't need copies of all the client keys
  - Server accepts only clients whose certs were signed with CA master cert
  - If private key compromise, single keys can be easily disabled
  - Server can enforce client-specific access based on embedded certificate fields in client cert

14

## Constructing the Server Appliance

- Build a Linux guest with external access and access to the network segment you want to protect
- Harden guest according to your site requirements
- Install OpenVPN RPM

15

## Build A Guest

- Use your standard process. Works pretty much the same on RHEL and SLES
- Omit anything that is not absolutely necessary – this guest may be exposed to hostiles

16

## Install OpenVPN

- Install:

  rpm –ivh openvpn-[version].rpm
- Upgrade:

  rpm –Uvh openvpn-[version].rpm

17

## Configuring the Server Appliance

- Configure Certificate Authority

  Copy /usr/share/doc/packages/openvpn to /etc/openvpn

  Edit vars in file “vars”

  Must set all variables BEFORE proceeding!

18

## Configuring the Server Appliance

- Initialize PKI infrastructure:

  . ./vars (note initial dot)
  ./clean-all
  ./build-ca

19

## Configuring the Server Appliance

- Generate server key and certificate:

  ./build-key-server <serverid>

  <serverid> usually = <1st token of FQDN>

20

## Configuring the Server Appliance

- Generate a few client keys and certs:

  ./build-key client1
  ./build-key client2
  ./build-key client3

  client ids do not have to match actual hostnames, but remember names for later

21

## Configuring the Server Appliance

- Generate Diffie-Helman parameters:

  ./build-dh

  Running this during the day may be a job killer – very CPU intensive for a long time (several minutes on z10, 30-40 minutes on z800)

22

## Configuring the Server Appliance

- Edit server config file:
  - Update server directive to address range for VPN subnet
  - Update ca, cert, key, and dh parameters to point at files generated in earlier step (/etc/openvpn/<file>)
  - Uncomment user and group entries
  - Uncomment “client-to-client” if you want clients to be able to talk to each other

23

## Configuring the Server Appliance

- Start the server:

  /etc/init.d/openvpn start

  Startup script scans /etc/openvpn for conf files and starts openvpn instances for each conf file it finds

24

## Configuring A Client

- Install OpenVPN client
- Copy cert and key files to client
- Edit client config file

25

## Configuring a Client

- Same install as for the server (on Linux)
  - Client packages for Windows and Mac are native apps and install as per expected for platform
- Any file transfer tool can be used to transfer certs and keys:
  client.key
  client.crt
  ca.crt

26

## Configuring a Client

- Edit client conf:
  - Update ca, cert, and key lines to point to files generated in earlier step
  - Edit remote line to point to IP address of server

27

## Configuring a Client

- Start the client:

  /etc/init.d/openvpn start

  A few lines of text will fly by, and you should be able to ping hosts on the other side of the VPN server

28

## Summary

- There's lots more to do here, but this short tutorial will get you a working VPN capability that can serve clients inside and outside your System z host.

  Another good thing to have in your toolkit when someone asks for it.

29

## Questions

30


Contact Info
SINE NOMINE
ASSOCIATES
David Boyes
Sine Nomine Associates
dboyes@sinenomine.net
www.sinenomine.net
31