Standing up GIS Servers in the DOD Environment

GIS Servers

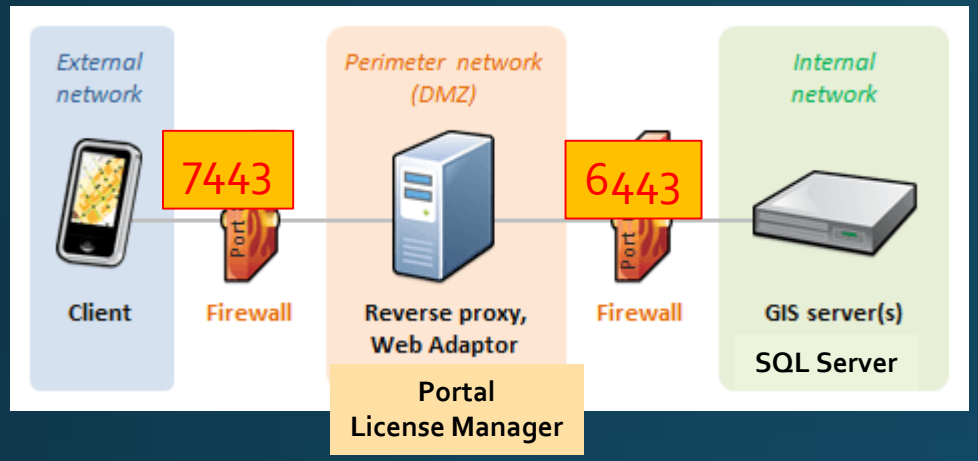
Jonathan Witcoski

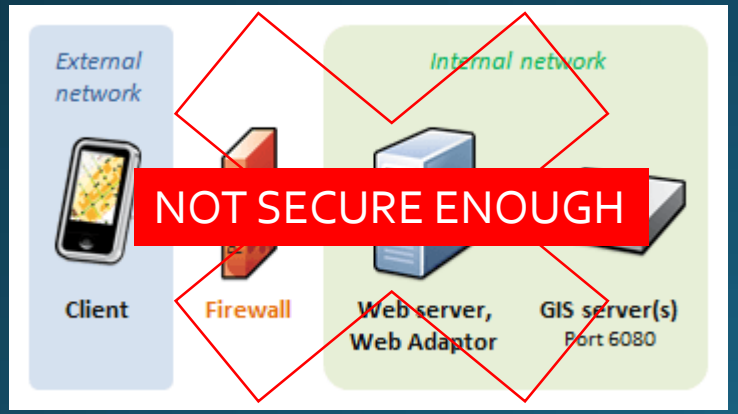
Contractor ARNG-ILE

Jonathan.f.Witcoski.ctr@mail.mil

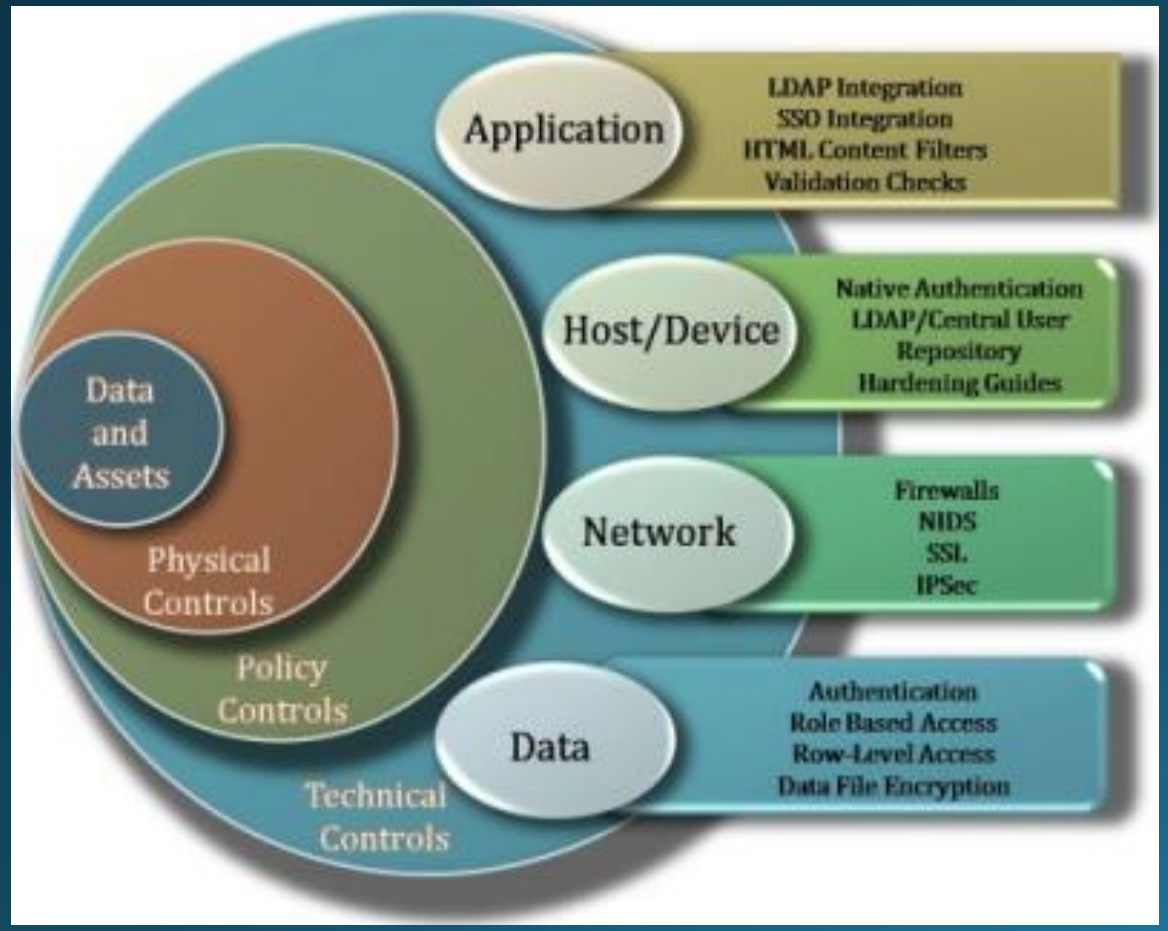
http://trust.arcgis.com/

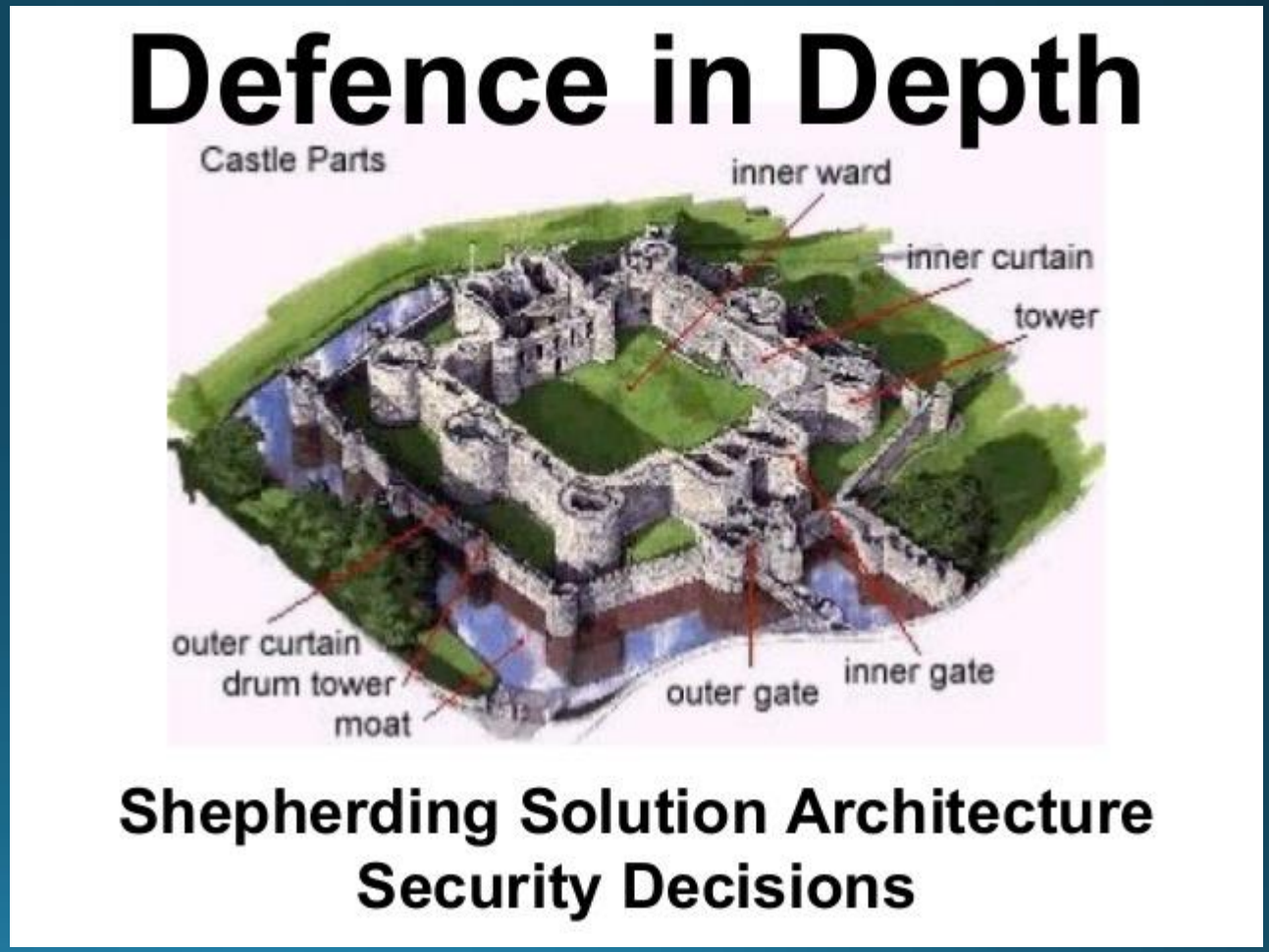
The Architecture





Defense in Depth Strategy





Differences

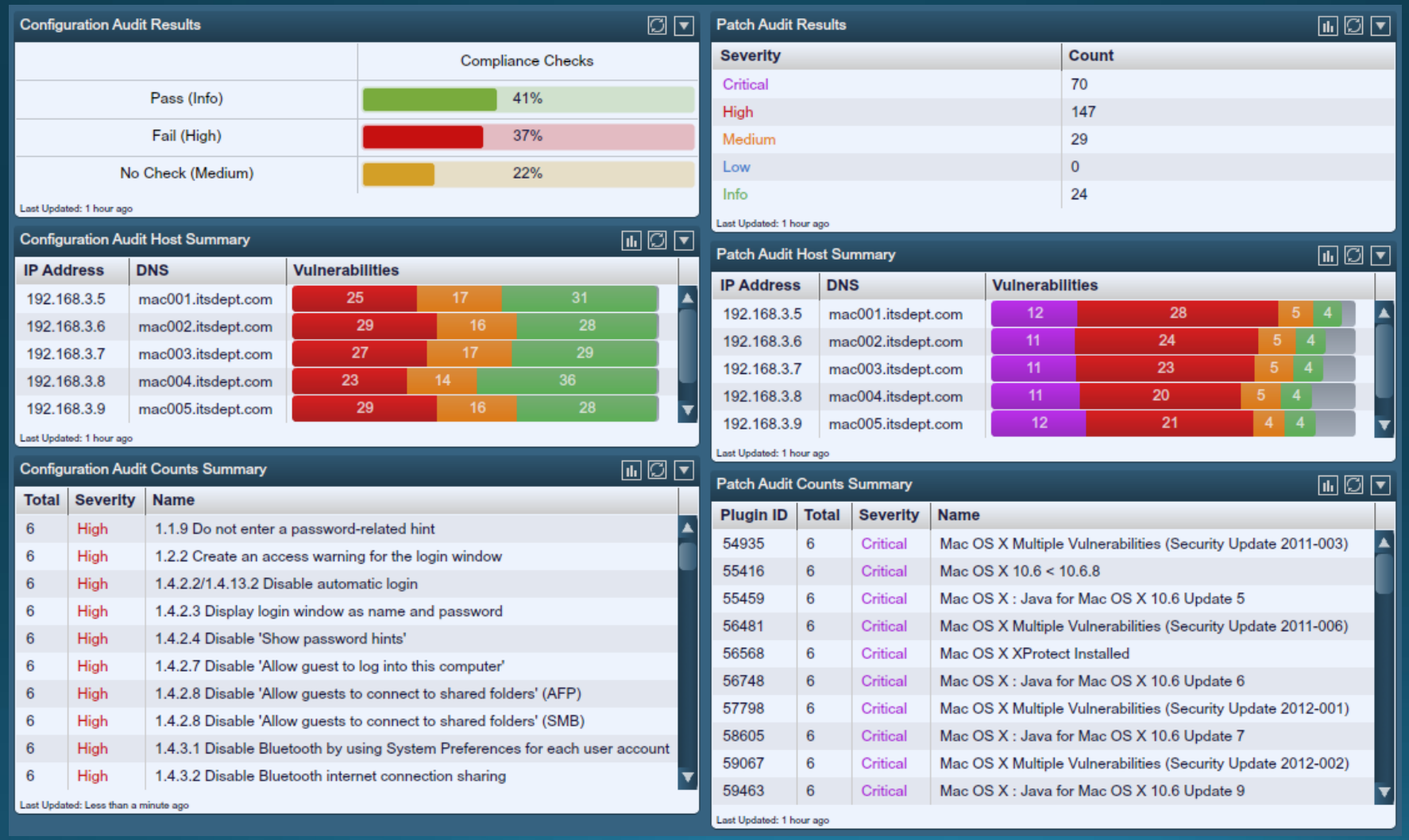
	Standard Install	DOD Install
Directory	C:	OS (C:) separate from data and app (D:)
Access	HTTP or HTTPS	HTTPS required with CAC authentication
Server Location	Anywhere	DOD secure facility
Internet Connectivity	No Firewall, any site	Firewall, Trusted Sites Only
Software	Anything	Only certified software
Installation	Directly on Production Machines	Development → Test → Production

Firewall Ports

License Manager	ESRI Server	ESRI Portal	SQL
27000-27009 inbound tcp	6443 inbound tcp	7080 inbound tcp	1433 inbound tcp
27000-27009 inbound tcp		7443 inbound tcp	1433 inbound udp
		7005 inbound tcp	1434 inbound tcp
		7099 inbound tcp	1434 inbound udp
		7199 inbound tcp	1433 outbound tcp
		7654 inbound tcp	1433 outbound udp
			1434 outbound tcp
			1434 outbound udp

TCP: Transmission Control Protocol (with Internet Protocol [IP], the main protocol of the Internet
UDP: User Datagram Protocol

Security (STIG) Compliance



Configuration Audit Results

	Compliance Checks
Pass (Info)	41%
Fail (High)	37%
No Check (Medium)	22%

Last Updated: 1 hour ago

Configuration Audit Host Summary

IP Address	DNS	Vulnerabilities
192.168.3.5	mac001.itsdept.com	25 17 31
192.168.3.6	mac002.itsdept.com	29 16 28
192.168.3.7	mac003.itsdept.com	27 17 29
192.168.3.8	mac004.itsdept.com	23 14 36
192.168.3.9	mac005.itsdept.com	29 16 28

Last Updated: 1 hour ago

Configuration Audit Counts Summary

Total	Severity	Name
6	High	1.1.9 Do not enter a password-related hint
6	High	1.2.2 Create an access warning for the login window
6	High	1.4.2.2/1.4.13.2 Disable automatic login
6	High	1.4.2.3 Display login window as name and password
6	High	1.4.2.4 Disable 'Show password hints'
6	High	1.4.2.7 Disable 'Allow guest to log into this computer'
6	High	1.4.2.8 Disable 'Allow guests to connect to shared folders' (AFP)
6	High	1.4.2.8 Disable 'Allow guests to connect to shared folders' (SMB)
6	High	1.4.3.1 Disable Bluetooth by using System Preferences for each user account
6	High	1.4.3.2 Disable Bluetooth internet connection sharing

Last Updated: Less than a minute ago

Patch Audit Results

Severity	Count
Critical	70
High	147
Medium	29
Low	0
Info	24

Last Updated: 1 hour ago

Patch Audit Host Summary

IP Address	DNS	Vulnerabilities
192.168.3.5	mac001.itsdept.com	12 28 5 4
192.168.3.6	mac002.itsdept.com	11 24 5 4
192.168.3.7	mac003.itsdept.com	11 23 5 4
192.168.3.8	mac004.itsdept.com	11 20 5 4
192.168.3.9	mac005.itsdept.com	12 21 4 4

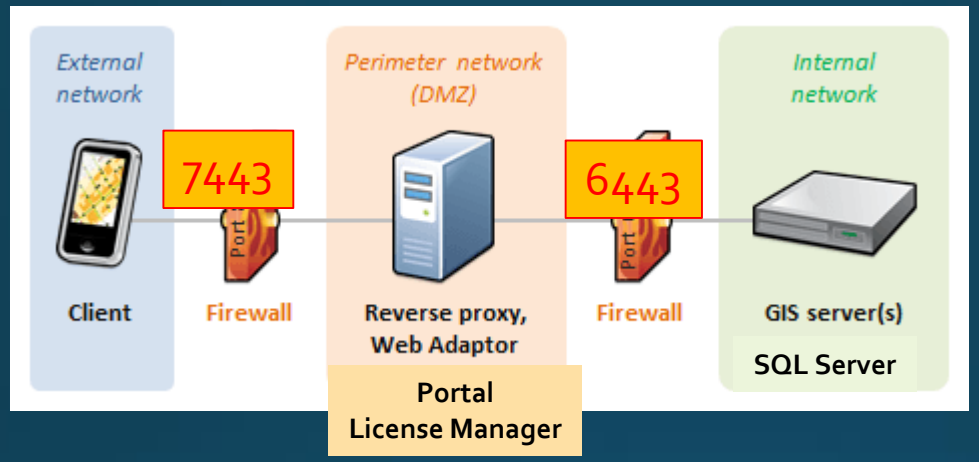
Last Updated: 1 hour ago

Patch Audit Counts Summary

Plugin ID	Total	Severity	Name
54935	6	Critical	Mac OS X Multiple Vulnerabilities (Security Update 2011-003)
55416	6	Critical	Mac OS X 10.6 < 10.6.8
55459	6	Critical	Mac OS X : Java for Mac OS X 10.6 Update 5
56481	6	Critical	Mac OS X Multiple Vulnerabilities (Security Update 2011-006)
56568	6	Critical	Mac OS X XProtect Installed
56748	6	Critical	Mac OS X : Java for Mac OS X 10.6 Update 6
57798	6	Critical	Mac OS X Multiple Vulnerabilities (Security Update 2012-001)
58605	6	Critical	Mac OS X : Java for Mac OS X 10.6 Update 7
59067	6	Critical	Mac OS X Multiple Vulnerabilities (Security Update 2012-002)
59463	6	Critical	Mac OS X : Java for Mac OS X 10.6 Update 9

Last Updated: 1 hour ago

iase.disa.mil/stigs



Standing up GIS Servers in the DOD Environment

GIS Servers

Jonathan Witcoski

Contractor ARNG-ILE

Jonathan.f.Witcoski.ctr@mail.mil

http://trust.arcgis.com/