



Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

August 20, 2008



AUGUST



FUN

RELAXATION

REST

SURF

SAND

VACATION



ISOAG August 2008 Agenda

- | | | |
|-------|---|---|
| I. | Welcome and Opening Remarks | Peggy Ward, VITA |
| II. | Altiris at Longwood University | Dr. Brian Kraus, Longwood University |
| III. | Telework Expense Policy | Mark Murray, DOA |
| IV. | Telecommuting Policy & Practice | Rue White, DHRM |
| V. | Secure Telework Connectivity | Peggy Ward, VITA |
| VI. | Remote Access at Corrections | Rick Davis & Felicia Stretcher, DOC |
| VII. | Monitoring Internet Use Successfully | Cameron Caffee, VDOT |
| VIII. | Intro to Blue Coat Reporter | Kevin Ferlazzo, DJJ |
| IX. | COV IT Partnership Security Open Forum | Don Kendrick & Matt Slaight,
COV IT Infrastructure Partnership |
| X. | IT Infrastructure Security Letters of Assurance | Cathie Brown, VITA |
| XI. | Network Security at Home - Defending the Castle | Bob Baskette, VITA |
| XII. | Commonwealth Security Annual Report | Peggy Ward, VITA |
| XIII. | Upcoming Events & Other Business | Peggy Ward, VITA |



Losing the "T"

We are moving this year from Information
"Technology" Security and "Cyber" Security
to

Information Security!!

A comprehensive approach to information safeguards
that includes ALL media such as the spoken word & hard
copy documents as well as electronic media!



Information Security Awareness Month

Governor Kaine has signed a proclamation designating

October, 2008

as

Information Security Awareness Month

in the

Commonwealth of Virginia!!



2008 Information Security Awareness Tools

The Information Security Toolkit has been updated with new materials

Thank you MS-ISAC!

For printing cost estimates you can contact DMV's Damian McInerney @

367-0925

Thank you DMV!

Thank You



NASCIO 2008 Finalists

The National Association of State CIOs, (NASCIO) has recognized the Commonwealth of Virginia as a finalist in 3 categories for excellence! See all submissions & finalists on the NASCIO Web site

www.nascio.org/awards



NASCIO 2008 Finalists

Categories & Commonwealth finalists are:

Information Security & Privacy

*Commonwealth of Virginia - Information Security:
Interlocking Spheres of Collaborative Protection*

Enterprise IT Management Initiatives

*Commonwealth Information Technology Infrastructure
Partnership*

Data, Information & Knowledge Management

Commonwealth of Virginia Knowledge Center

NASCIO 2008 Finalists

Merci

Dikey

Gracias

Teşekkürler



Grazie



شكراً

Obrigado!



*Thank
You!*

Hvala



धन्यवाद

Ευχαριστώ

תודה

*Vielen
Dank*



Altiris at Longwood University

Dr. Brian Kraus
Director of Instructional Technology

Challenges faced by Longwood

- 1200 clients across campus
- No standardization
- All users with local admin rights
- Inaccurate hardware inventory
- No software inventory
- No computer imaging solution

Solution: Altiris Client Management Suite

- Director of Instructional Technology had prior experience with the product
- Already on state contract
- Powerful tool to help overcome challenges

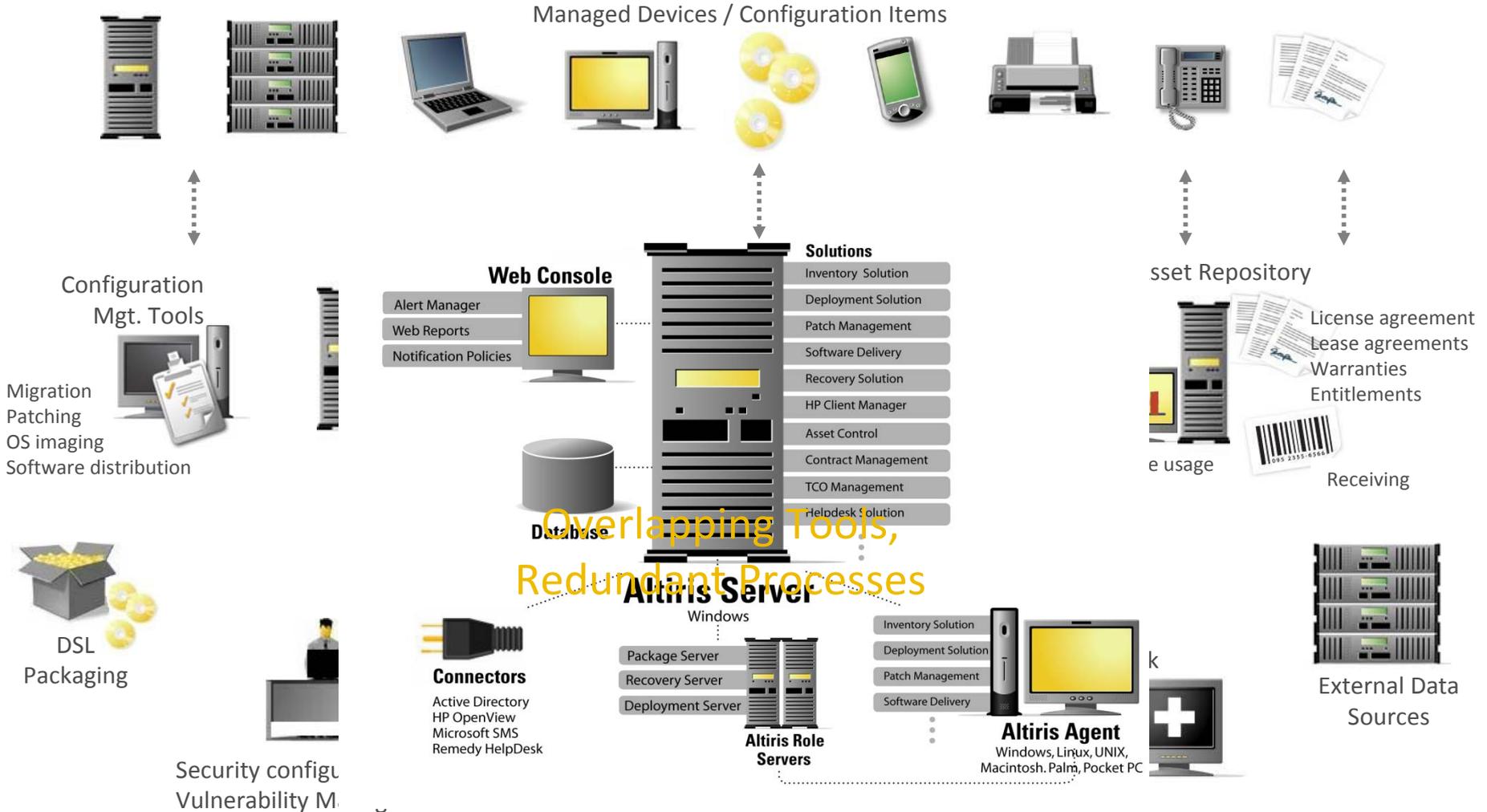
LONGWOOD UNIVERSITY

LANCERS

What is Altiris Client Management Suite?

- “Altiris Client Management Suite is an easy-to-use systems management solution that reduces the total cost of ownership for desktops, notebooks, and handheld devices. Developed for IT professionals who manage computing devices on a regular basis, the suite enables administrators to deploy, manage, and troubleshoot systems from virtually anywhere.”
- Recently purchased by Symantec

Integrated Solution



Challenge One: 1200 Clients Across Campus

- Carbon Copy allows for remote assistance reducing travel time between offices
- Remote Sessions are by Altiris (support can't connect anonymously)

LONGWOOD UNIVERSITY

LANCERS

Challenge Two: No Standardization

- Altiris allows us to create software delivery packages by job function
- Local Administrator passwords can be changed across the board

LONGWOOD UNIVERSITY

LANCERS

Challenge Three: Admin Rights

- All users had administrative rights and were able to install anything anytime.
 - Widely used software (Office 07, Adobe, etc) can be packaged in MSI files for remote silent installs.
 - Less widely used software can be installed using Carbon Copy.

Challenge Four: Inaccurate Hardware Inventory

- Altiris reports offer complete hardware inventories including:
 - Processor type
 - Hard Drive size/available space
 - NIC type and MAC address
 - Amount of RAM

The Console

Altiris Console 6.5 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail Print Mail Print Mail Address <http://localhost/Altiris/Console/> Go

altiris console localhost - MFSERVER\Administrator Search

Home View Manage Tools Reports Configure Help >

Altiris Console Home Edit

Information for Altiris solutions at a glance

Quick Starts

- [Dell Client Manager Standard Quick Start](#)
- [Software Portal](#)

Resource Manager

Resource: [Click to select](#)

View

Solution Licenses

Solution	In Use	Total
Altiris Software Delivery Solution	0	1...
Altiris Inventory Solution for Windo...	180	1...
Inventory Solution for UNIX and Linux	32	1...
Altiris Inventory Solution for Servers	32	1...
Real-Time System Manager	0	1...
Carbon Copy	31	1...
Inventory Solution for RIM	6	1...

Agent Rollout Status

javascript: __doPostBack('lnkEditPage','') Local intranet

Challenge Five: No Software Inventory

- Altiris gives a complete list of all software being used (works with Mac, PC, and Linux).
- Individual software products can be located.
- Undesirable software can be blocked and/or uninstalled.
- Software can be metered for usage statistics.

Challenge Six: No Imaging Solution

- Imaging solution allows us to reimagine computers in place
 - Especially useful for computer labs
- When used in conjunction with software delivery, images can be very small

Communication Plan

- Although Altiris can be installed and set to run silently we chose to communicate the plan to the faculty and staff
- We also chose to leave an icon in the system tray, allowing support to easily identify the computers with the Altiris client

Communication Plan (cont.)

- Presented the product to cabinet (VP level)
- Presented the product to middle management level
- Communicated via email
- Held open forums to allow for any employees to ask questions

“Big Brother” Effect

- Most common reaction to the Altiris Install:
“Sounds Like Big Brother.”
- Response:
 - Altiris does not monitor anything that could not be monitored through other means (web traffic, email, local storage, etc.)
 - Carbon Copy provides extra security since all computer access is logged by Active Directory credentials
 - With a better hardware inventory we can make more intelligent decisions about who gets new PCs

Post Implementation Challenges

- Despite fairly massive communication effort, some users still unaware of the change
- Create and modify remote assistance policies
- Users blame every computer problem on Altiris
 - “Since Altiris has been installed my monitor is blurry.”

Lessons Learned

- Plan your architecture carefully
 - If a firewall is involved many ports will need to be opened
 - If using multiple VLANs consider using a separate server for each VLAN
 - Run SQL on a separate server

Telework Expense Payment



Virginia Department of Accounts

Photo by Karl Steinbrenner

Financial Accountability. Reporting Excellence.

Agenda

- DOA's New Telework Expense Payment Policies and Procedures
- Executive Committee Developed Policy Draft
 - Karen Jackson – Office of Telework Promotion & Broadband Assistance
 - Rueyenne White – Department of Human Resource Management
 - Peggy Ward – Virginia Information Technologies Agency
 - Mark Murray – Department of Accounts, Chair



Issues, Policies and Procedures for Agencies and Institutions

- Commonwealth Accounting Policies and Procedures (CAPP) Manual
- CAPP Organized Into Sections Based on Topic
 - Topic 20310 Expenditures – Contains new topic entitled Telework Expenditures
- Until CAPP update published: DOA Home Page under “New Information” or “Telework Expense Payment Policy:



Telework Policy Basics

- Teleworkers Defined: Employees who work at a remote or alternate location a minimum one day per week or 32 hours per month
- Intermittent Teleworker: Less than above standard
- Certain necessary expenses can be paid by the agency
- Expense payments must consider the nature of work responsibilities

Telework Policy Basics

- Responsibilities must be documented in the Employee Work Profile (EWP)
- Different EWPs and different telework arrangements may produce different expense justifications
- Voluntary teleworking is viewed primarily as a personal convenience (no reimbursement)



Allowable Expenses

- Office supplies and operating expenses supporting Commonwealth owned equipment (i.e. PC's, communications devices, etc.)
- Single telephone service connection per employee
- Single internet service connection per employee
- NOTE: Determine reimbursement from documented justification based on:
 - Telework frequency
 - EWP requirement, work profile
 - actual costs
 - portion used only for business



Prohibited Expenses

- Employee home expenses (utilities, insurance, home maintenance, etc.)
- Purchase costs or maintenance expenses associated with employee-owned equipment
- Advance payment reimbursements for allowable connectivity services
- This list is not all-inclusive
- Agencies may always implement more restrictive standards



Documentation Requirements

- Telework arrangement must be in accordance with DHRM Policy Number 1.61 – Telecommuting
- Telework arrangement must adhere to all applicable policies and standards issued by other State agencies such as VITA, DHRM, and DOA.
- Justification for payment of telework expenses supported by documented business case
- Payments or reimbursements supported by original invoice
- Control over Commonwealth assets
 - Employee termination checklist
 - Records/logs for issuance and return



Income Reporting Requirement

- Internal Revenue Service “Taxable Fringe Benefit Guide Publication 15-B”
- Taxable fringe benefits must be processed through payroll to be reported as taxable income



Questions?

DHRM Policy 1.25 - Telework



Virginia Department of
HUMAN RESOURCE
M A N A G E M E N T

Why a revised policy?

The primary reason for this revision is the change to the definition of telecommuter in the Code of Virginia. Effective July 1, 2008. COV § 2.2-2817.1 defines a teleworker as someone who performs his/her job duties away from the central work place at least one day per week.

What's new?

- Definition of Teleworker
 - Alternate work place
 - At least one day per week, or
 - At least 32 hours per month

What's new?

- Telework Agreement Form
 - Streamlined / Condensed document.
 - Includes “Safety Confirmation” – Removing need for separate Safety Checklist.
 - Note: Agencies may require an Agreement for all employees teleworking any number of hours per month.

Compliance with VITA

- While the use of non-Commonwealth-owned or issued equipment is permissible, teleworkers and their agencies must be in compliance with the VITA's Information Technology Standard "Use of Non-Commonwealth Computing Devices to Telework". (SEC511-00) (07/01/2007)

Compliance with DOA

- Agency reimbursement procedures must comply with DOA's Telework Expense Payment Policy and must be consistently applied to all similarly situated employees.

The Green Touch

- Original intent was to produce administrative efficiencies (i.e., real estate and overhead costs) which is sometimes difficult to translate to government.
- Now notes additional benefits
 - work/life balance
 - easing traffic congestion
 - decreasing pollution
 - recruitment and retention tool

Questions?





Secure Telework Connectivity

Peggy Ward
Chief Information Security Officer





Secure Telework Connectivity Goals

Support telework by providing accessibility to Commonwealth systems and information from remote locations

Prevent access to Commonwealth systems and information by unauthorized parties



Secure Telework Connectivity Options

- Provide remote workers with a Commonwealth tablet or laptop with a Virtual Private Network Secure Socket Layer connection (VPN SSL)
(RECOMMENDED!)
- Exercise 1 of the 3 options authorized by Commonwealth Standard SEC 511 - *Use of Non-Commonwealth Computing Devices to Telework*
- Provide an alternative method while obtaining an exception from the Commonwealth Standard SEC 511 - *Use of Non-Commonwealth Computing Devices to Telework*



Options under SEC 511 - *Use of Non-Commonwealth Computing Devices to Telework*

The Standard permits using a Non-COV device:

- for standalone research
- to access web based applications
- via a “remote desktop” solution where applications are run from a remote desktop server or terminal server preferably secured within the COV infrastructure.

If these do not apply AND the agency has a better solution submit an exception request

[Exception Request Form - COV IT Security Policy and Standard](#)



Options under SEC 511 - *Use of Non-Commonwealth Computing Devices to Telework*

NOTE:

The Standard prohibits storage of Commonwealth information on any non-COV device!

RISKS:

Non-COV machine has malware such as keystroke logging!
Malware leads to any of the following

- Stolen credentials
- Stolen sensitive data
- Infection spreads to COV systems

Improper data storage on non-COV systems

- Temporary data not deleted after use
- Downloading email to the home system instead of webmail



Other Considerations

- Any internet connection needed should be reliable and have sufficient bandwidth.
- Meet Records retention and FOIA requirements.
- Sensitive information must have encryption at rest and in motion.
- Meet DOA and DHRM requirements.



Security Incident Response

- In the event a non-Commonwealth owned or leased computing device used for Commonwealth business is involved in the investigation of a security incident, the employee may be required to release the device to law enforcement or the COV Computer Security Incident Response Team (CIRT) for forensic purposes.
- The COV CIRT is obligated to report any illegal activity uncovered during a security incident investigation, whether the activity is related to the incident being investigated or not.
- While all investigations are confidential, the remote user concedes any expectation of privacy related to information stored on a personally owned computing device involved in a security incident.



Questions?

!!Thank you!!



Virginia Department of **corrections**

Securing Remote Network Access



FirePass[®]

Business Case

VirginiaCORIS



VirginiaCORIS is an initiative to modernize the way that offender information is managed, to provide real-time data and enhance our ability to share this data with State, Federal and local law enforcement Agencies, as well as other authorized users.

The simple sharing of information identified yet another challenge - *What means shall the DOC use to provide secure remote access across a wide range of client devices?*

Challenges

- Remote Access Issues - 'DOC VPN' Cisco IPSec VPN
- Utilizing Managed and Unmanaged Devices
- Scalability - Growing Number of Users and Mobile Workforce
- Security Requirements
- Cost Effective Solution

Vendor Demonstrations

- Cisco SSL VPN Solutions
- Juniper Networks Firewall/SSL VPN
- Citrix Access Gateway
- F5's SSL VPN FirePass

Solution



FirePass

Unlike an IPsec VPN, FirePass does not require the user to pre-install or configure any software, however the first time remote network access is requested, the user is required to install an ActiveX component. It works directly through a Web browser using a virtual desktop Web page.

Benefits

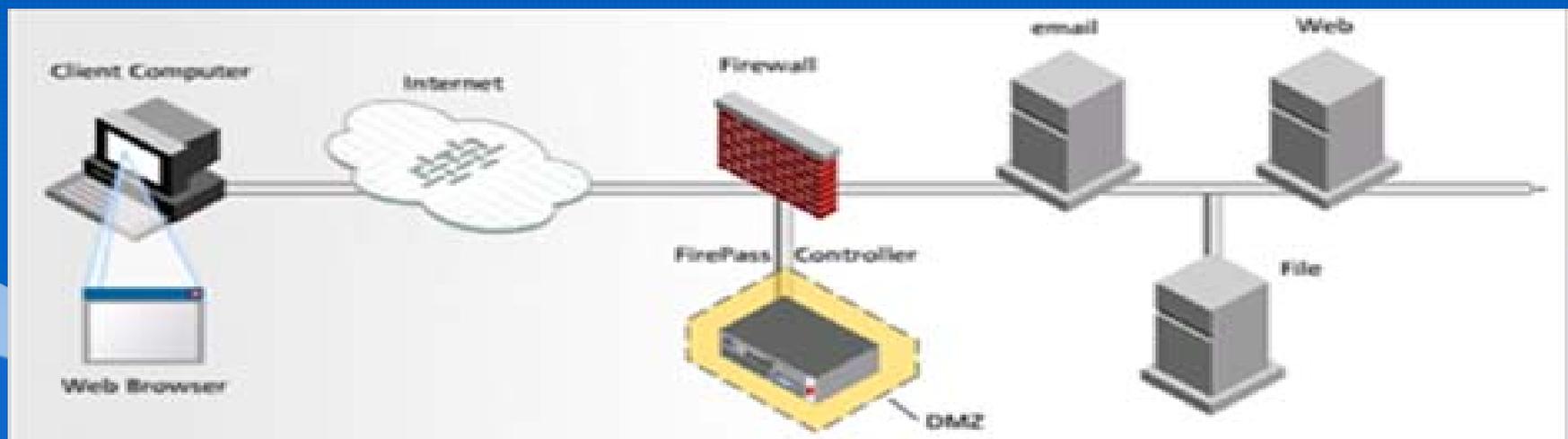
- ✓ Application and Client Access Ready
- ✓ Endpoint Integrity Checks
- ✓ Scalability
- ✓ Internet Explorer, Netscape and Mozilla browsers successfully established a SSL connection
- ✓ Cost Effective
- ✓ Solution Widely use by the Public and Private Sectors
- ✓ Simplified End-User Experience

Portal Access

<https://vpn.vadoc.virginia.gov>

Web Applications, Files and Email

- Provides portal page customization
- Automatic drive mapping
- Allows users access to network file servers
- Provides secure and full access to Outlook email
- Provides granular access control to the DOC servers, applications and Intranet resources
- Allows or restrict access to specific applications providing increased security



Client Security

firepass.vadoc.virginia.gov - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address <https://205.247.116.10/my.logon.php?check=1&fromjavalauncher=1&frommaxinstaller=1>



My Account

[Logon](#)

**Remote Access Logon
for Virginia Department
of Corrections**

Username:

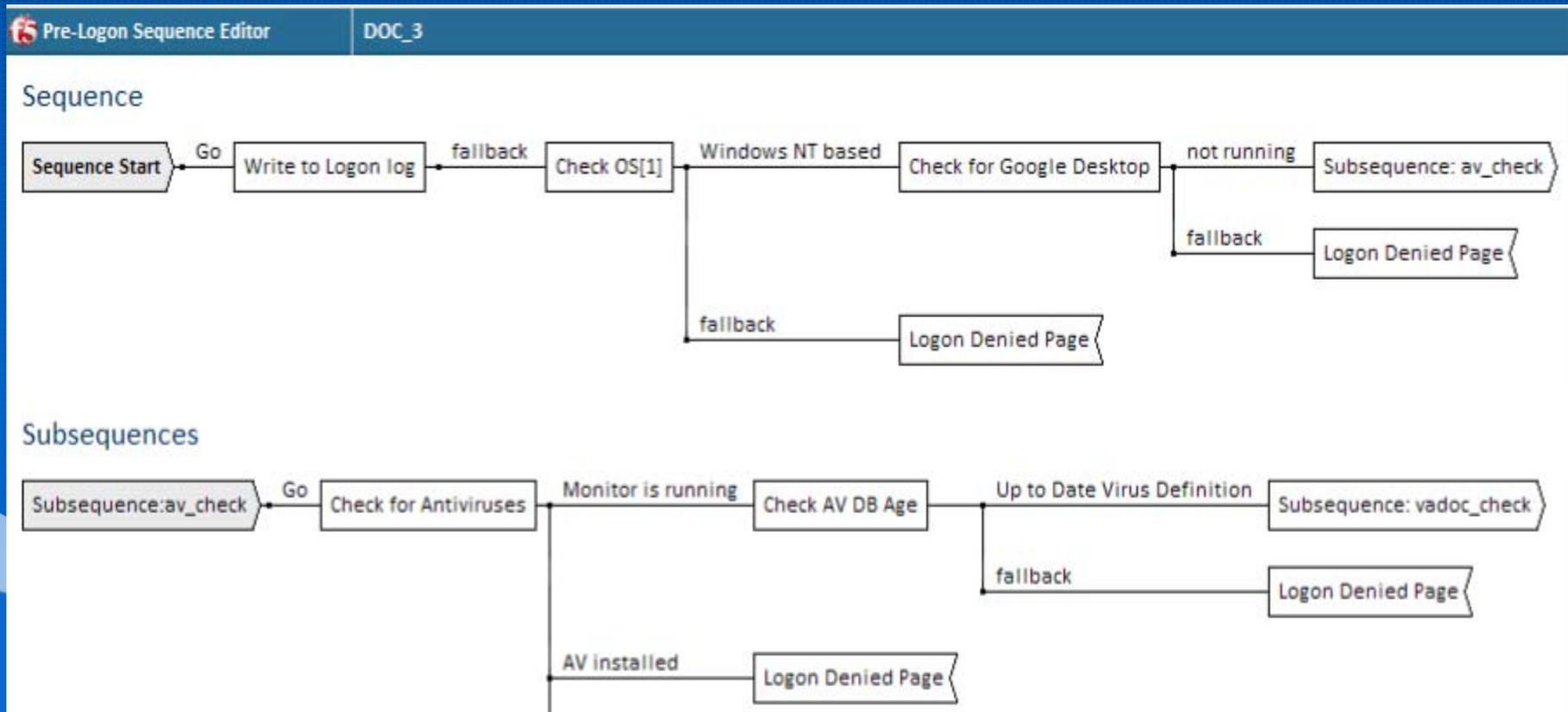
Password:

Client Integrity Checking - Increased security by detecting specific processes on a device before allowing full network access. The FirePass Controller can validate that:

- The client has a current antivirus
- Client firewall
- OS patch levels
- Google Desktop
- User-defined policy in place before allowing a full network connection.
- Cache cleanup control empties recycle bin, removes cookies, browser history and cache, auto-complete info and ActiveX controls installed during the session.

Client Security cont'd

Visual Policy Editor – GUI view of DOC access policies – giving you point-and-click ease in profiling and managing groups, users, devices or any combination of the three. This tool enables the creation of custom template policies based on the endpoints accessing the DOC's network and security profile.



Unmanaged Device

Felicia Stretcher's Home - Windows Internet Explorer

https://vpn.vadoc.virginia.gov/vdesk/?langchar=en.iso-8859-1

mywebsearch Search

Felicia Stretcher's Home

Public Safety
Department of Corrections

Felicia Stretcher's Home Logout

System Warnings

⚠ You have 2 System Warning(s)

Web Applications

- DOCnet
- Oracle Warehouse Inventory
- Outlook Web Access (OWA)
- Virtual Library
- VirginiaCORIS
- KIRS

Internet 100%

Unmanaged Device

System Warnings - Windows Internet Explorer

https://vpn.vadoc.virginia.gov/vdesk/index.php3?Z=0,a

File Edit View Favorites Tools Help

mywebsearch Search

System Warnings

Public Safety
Department of Corrections

Felicia Stretcher's Home : Tools : System Warnings Logout

System Warnings

[Clear system warnings >>](#)

Policy restriction

Access to resource group *rg_MyExtra* has been denied by the Policy Engine.
The reason is:

- File system check failed

Policy restriction

Access to resource group *rg_NetworkAccess* has been denied by the Policy Engine.
The reason is:

- File system check failed

Done

Internet 100%

Managed Device

The screenshot shows a web browser window with the following elements:

- Address Bar:** <https://vpn.vadoc.virginia.gov/vdesk/index.php?Z=5,17>
- Page Header:** Public Safety Department of Corrections
- User Profile:** Felicia Stretcher's Home (Logout)
- Navigation Menu:**
 - Network Access
 - Web Applications
- Network Access Section:**
 - MyExtra
 - Network Access
- Web Applications Section:**
 - DOCnet
 - Oracle Warehouse Inventory
 - Outlook Web Access (OWA)
 - Virtual Library
 - VirginiaCORIS
 - KIRS

Endpoint Trust Management

Integrated Endpoint Security delivers pre-login endpoint integrity checks and endpoint trust management.

1st – Automatic detection of security compliant systems

2nd – Automatic protection of resources by enabling a secure workspace preventing the theft of sensitive data.

3rd - Make sure no session residue is left behind.

Address  https://205.247.116.10/my.logon.php?no_inspectors=1&check=1&fromjavalauncher=1&frommaxinstaller=1



My Account

[Logon](#) |

Logon denied

Your device does not comply to current client security policies.

Error Code: 0201
(Error number is needed by support staff to troubleshoot)

The Google Desktop component must be disabled prior to access.

Please use the following [link](#) to notify support staff of the error.

To open a new session, please [click here](#)

Clientele

SIEMENS



SAP® Certified
Integration with SAP NetWeaver®

**SPORTS
AUTHORITY.**



Transportation
Security
Administration

Q & A



Rick Davis
Applications & Development Manager
rick.davis@vadoc.virginia.gov
804.674.3461 x1788



Felicia Stretcher
Operations Analyst
felicia.stretcher@vadoc.virginia.gov
804.674.3492 x1809



Sandy Phelps
Major Account Manager
sandy@f5.com
404.353.4343

Corrections Technology Services Unit



Monitoring Internet Use Successfully

Cameron C. Caffee CPA, GCFA, GCIH
IT Audit Manager
Internal Audit Division
Office of the Inspector General

August 20, 2008

VDOT Internet Monitoring

Background

Purpose

Tool

Reports

Discussion

Internet Use/Abuse Audits Early 2002 – The beginning

Case referred by Office of the Attorney General

Employee maintaining Yahoo! Profile

Profile name search hit for “VCU”

Firewall logs

- Substantial personal use
- Sexually explicit material

Investigation broadened to high volume users

10K log records in one day of selected week

93 IP addresses sampled

Raw firewall logs examined

Results

75 substantial personal use

16 accessed sexually explicit material

Recommendations

Timely monitoring

Policy change

Richmond Times-Dispatch October 4, 2002

VDOT CITES 86 FOR PC MISUSE WORKERS EITHER FIRED OR SUSPENDED

In the largest state disciplinary action in recent memory, the Virginia Department of Transportation has fired or suspended almost 90 employees for "gross abuse" of the Internet.

What the department's auditors found was that, during the week of April 8, workers were spending up to five hours browsing the Internet during work time ...

"We had a culture in some places that managers didn't realize that 90 employees had that much time to waste"

Richmond Times-Dispatch

October 8, 2002

CENTRAL COMPUTER PLAN LACKING STATE AGENCIES DO OWN POLICING OF INTERNET USE BY EMPLOYEES

Virginia's state government does not have a central means of policing Internet use by its more than 112,000 employees, officials say.

And the state does not intend to do a statewide check of what its workers are doing on the Internet ...

"My reaction was, 'Oh I've got to watch what I'm doing now,' " one state employee said yesterday.

"In a time of limited resources, we need everybody focused on their jobs," Qualls said, "but at the same we don't need to lower employee morale by promoting a culture of fear."

Richmond Times-Dispatch

October 12, 2002

VDOT MAY PAY FOR WASTED TIME U.S. FUNDS AT ISSUE IN INTERNET ABUSE

The Virginia Department of Transportation may have to pay back the U.S. government for the time highway agency workers wasted on the Internet when they should have been working on federally funded road projects.

Just figuring out how much the state improperly billed to the federal government because VDOT employees were looking at porn sites or shopping on the Internet carries its own cost for the taxpayer, Shucet said.

Internet Use/Abuse Audits

FY 2004 Follow-up Audit

Usage sample

- 10 K firewall log records for one day in selected week
- 67 IP addresses sampled
- 8e6 reporting examined
- Automated analysis tool developed

Results

- 44 excessive personal use
- 5 accessed sexually explicit material

Changes

- DHRM 1.75 in lieu of agency zero-tolerance policy
- 8e6 site-filtering appliance implemented

Recommendations

- Implement usage reporting for individual trend analysis
- Authenticated access to Internet
- Prohibit personal streaming/auto-updating media

Richmond Times-Dispatch February 4, 2004

VDOT COMPUTER ABUSE REPORTED MORE WILL MEAN DISCIPLINE, STATE TRANSPORTATION CHIEF WARNS AGENCY'S EMPLOYEES

An internal investigation at the Virginia Department of Transportation has turned up as many as 44 employees wasting taxpayer-paid work time on the Internet.

Conducted July 21-27, the computer-abuse sweep rounded up about half the number of VDOT workers caught in a similar investigation made public 16 months ago.

Richmond Times-Dispatch February 11, 2004

VDOT TO PUNISH 31 WORKERS FOR INTERNET USE

The Virginia Department of Transportation will discipline 31 employees for using their work computers to waste time or look at porn on the Internet.

Punishments will range from two-week suspensions without pay to being fired.

"We'll continue to monitor this activity on a regular basis," Shucet said, "and I hope to see this particular issue go away for us."

Internet Use/Abuse Audits FY 2006 Follow-up Audit

Usage sample

8,500 firewall log records for one day in selected week
67 IP addresses sampled

Results

11 excess personal use, 6 known to management
1 accessed sexually explicit material

Changes

Weekly usage summary reports to managers
Authenticated Internet access

Recommendations

Regular monitoring works

- Improve time measurement method
- Improve authentication to ensure identity capture

Internet Monitoring Purpose

Protect Public Trust

Assist Managers

Improve Productivity

Block Risk-Intense Access

Support Acceptable Use Policy

Minimize Litigation Exposure

Develop Trends of Web Use or Misuse

Improve Internet Utilization

Richmond Times-Dispatch

July 23, 2008

**No time for rush jobs at City Hall print shop
Instead, Web surfing occupies its workers,
auditor's report says**

In-house customers of Richmond City Hall's print shop have found it takes a long time to get work done - but then some of the shop's workers have been awfully busy lately. Surfing the Internet, that is, a city inspector general's report said yesterday.

One employee's computer logged 349,170 Web site visits from December to April, averaging more than 4,700 a day. The employee tried more than 600 times to see inappropriate sites, including one labeled "webdate" and one labeled "pornotube."

Reporting Introduction (2004)

8e6 site filter/blocking appliance

- Passive capture
- Reporting appliance

Weekly reporting by user

- Usage summary
- Site
- Category/Site
- Wall-clock summary

Challenges

- Multiple counting of minutes
- Qualitative assessment of reported data

Internet Monitoring Tool



China | Taiwan | Sitemap

Contact Us **877.369.8686**

Home | Solutions | Industry | Resource Center | Support | Press Room | Channel | About 8e6

Spot the Security Threat

Monitor and mitigate insider threats in real-time with the **8e6 Professional Edition**

[Click Here](#)



Business

Improve Productivity & Optimize Your Network

[Next Steps](#)

Education K-12

Secure Your Learning Environment

[Products](#)

Government

Manage Threats from Within

[Resources](#)

Latest News:

- Government agencies deploy Internet monitoring and filtering technology to oversee employee activity
Wednesday, 21 May 2008
- Vendor claims to nix URL-bypassing sites
Tuesday, 15 April 2008
- Exclusive Insights from Security Solutions Leaders
Tuesday, 08 April 2008

8e6 R3000 Categories

URL Inventory is Updated Daily

Threats Liability	Bandwidth/ Productivity		General Productivity	
Adult Content Child Porn Explicit Art Obscene/Tasteless Pornography/Adult Content R-rated	Bandwidth Image Server Internet Radio Peer-to-Peer (P2P) File Sharing Streaming Media Video Sharing Voice Over IP (VoIP) Web Storage	Business/Investments Business Employment Financial Online Trading/Brokerage Real Estate	Government/ Law/ Politics Government Legal Military Appreciation Military-Official Political Opinion	News/Reports News Sports Weather/ Traffic
Illegal/Questionable Criminal Skills Dubious/Unsavoury Hate Illegal Drugs School Cheating Terrorist	Internet Communication Chat Instant Messaging (IM) Message Boards Online Communities Web E-mail Web logs Web-based Productivity Applications	Community/ Organizations Community Organizations Local Community	Health/Fitness Fitness Health Holistic Self Help	Religion/Beliefs Paranormal Religion
Security Bad Reputation Domains Botnet Hacking Malicious Code Phishing Spyware Web Proxies	Internet Productivity Adware Banner Ads Dynamic DNS Fantasy Sports Free Hosting Remote Access Web Hosts	Education Education Education Cheating Educational Games Online Classes Reference	Information Technology Freeware/Shareware Information Technology Internet Service Providers Portals Search Engines Web-based Newsgroups	Shopping Classifieds Online Auction Online Greeting Cards Shopping
		Entertainment Art Comics Entertainment Gambling Games Humor Kids - Kid Friendly Sites Movies & Television Music Online Greeting Cards Restaurants/Dining Theater	Miscellaneous Domain Landing Edge Content Server / Infrastructure Intranet/ Internal Servers Invalid Web pages Reviewed/ Miscellaneous	Society/ Lifestyles Alcohol Animals/ Pets Books & Literature/ Writings Personals / Dating Drugs Fashion Lifestyle Recreation Self-Defense Social Opinion Tobacco Weapons
<div style="border: 1px solid black; padding: 5px; display: inline-block;"> Prohibited Categories in Red </div>				
				Travel/Events Tickets Travel Vehicles

Internet Monitoring Reports

Produced Weekly

Vendor and VDOT Developed

Provided Electronically

Wall Clock Use by Date/User

Internet Category Access by Date/User

Internet Site Access by Date/User

Wall Clock Use by Date/User

----- Section=CO-ITD -----

User Name	Sun May 25	Mon May 26	Tue May 27	Wed May 28	Thu May 29	Fri May 30	Sat May 31	Max Day	Total	Blocked	Porn
User.Name01	4	195	198	461	46	77	4	461	985	1	0
User.Name02	.	12	101	119	149	318	.	318	699	0	0
User.Name03	.	.	66	179	263	187	.	263	695	0	0
User.Name04	.	.	61	69	121	236	.	236	487	1	1
User.Name05	.	.	.	204	126	54	.	204	384	2	1



Internet Category Access by Date/User

----- Section=CO-ITD date=29MAY2008 -----

User Name	Tot User Time	Tot Cat Time	Category	Pages	Objects	IP Address
User.Name01	159	118	Unknown	405	552	172.30.94.123
		14	Banner	59	58	172.30.94.123
		8	Entertainment	31	180	172.30.94.123
		6	Weather/Traffic	14	12	172.30.94.123
		5	News	11	97	172.30.94.123
		3	Chat	8	150	172.30.94.123
		2	General Business	3	79	172.30.94.123
		1	Information Technology	1	579	172.30.94.123
		1	Reference	1	2	172.30.94.123
		1	VDOT	1	2	4
User.Name02	153	87	Unknown	179	244	172.30.91.123
		20	Banner	44	63	172.30.91.123
		17	Employment	64	172	172.30.91.123
		14	Information Technology	28	664	172.30.91.123
		7	Search Engines	9	3	172.30.91.123
		2	Entertainment	9	54	172.30.91.123
		2	General Business	6	51	172.30.91.123
		1	Movies & Television	3	0	172.30.91.123
		1	Music Appreciation	1	86	172.30.91.123
		1	R-Rated	1	0	172.30.91.123
		1	Streaming Media	1	87	172.30.91.123



Internet Site Access by Date/User

Dist	Group	Date	User	IP	Category	Sitename	Site Obj	Site Page	Site Time	Cat Time	User Time	Usr TmSum
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Unknown	209.133.65.11	0	135	27	45	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Unknown	il.sinaimg.cn	238	8	7	45	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Unknown	164.106.10.175	0	15	5	45	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Unknown	bbeshop.com	9	5	4	45	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Unknown	aision-int.com	1	3	1	45	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Unknown	rm04.net	4	2	1	45	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Unknown	egreetings.com	1	0	0	45	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Unknown	ruceci.com	4	0	0	45	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Government	virginia.gov	0	135	27	29	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Government	209.96.148.192	26	7	2	29	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Education	vccs.edu	693	20	9	16	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Education	164.106.81.251	238	8	7	16	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	General Business	Entrust.net	0	15	5	5	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Information Tech	liveperson.net	6	15	2	3	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Information Tech	209.96.149.107	0	2	1	3	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	Information Tech	adobe.com	2	0	0	3	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	VDOT	virginia.gov	28	7	2	3	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	VDOT	state.va.us	13	5	1	3	101	69
CO	CO-ITD	29-May-08	User.Name01	172.30.191.107	VDOT	vipnet.org	3	0	0	3	101	69

Reporting Issues

Frequency

Trend or sample

Data Retention

90 days

2 year archive desired

Judgment Required

Each employee's use evaluated against assignments

Internet Monitoring Questions

Audit:

Cameron.Caffee@VDOT.Virginia.gov
(804) 786-4882

Security:

James.Austin@VDOT.Virginia.gov
(804) 786-9315

Engineering:

Tom.Hutton@VITA.Virginia.gov
(804) 786-6578

Introduction

Dashboard

Report Filtering

Overall Traffic

Activity Summary

Conclusion

Intro to Blue Coat Reporter

Kevin Ferlazzo

Data Base Administration and Security
VA Department of Juvenile Justice



Introduction

Dashboard

Report Filtering

Overall Traffic

Activity Summary

Conclusion

Introduction

- Blue Coat Reporter is the tool provided by the VITA/NG Partnership for Network Transformed sites to monitor Internet activity.
- BCR runs on a network appliance at the CESC.
- Before you can use it you must obtain a BCR login from the NG Network Operations Center.



Introduction

Dashboard

Report Filtering

Overall Traffic

Activity Summary

Conclusion

Introduction

- How to use it (three simple steps)
 - Filter according to your search criteria.
 - Download your chosen report in the generic Comma Separated Values format.
 - Load the CSV file into a spreadsheet or database for analysis.
 - This part is still pretty much do-it-yourself.
 - I have yet to need to do very much analysis here.



Introduction
Dashboard
Report Filtering
Overall Traffic
Activity Summary
Conclusion

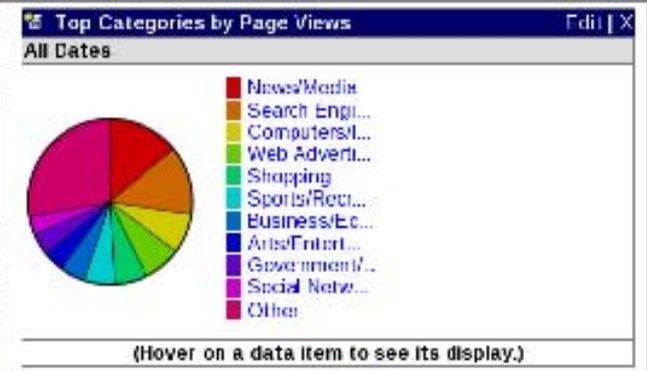
The Dashboard

- Gives Agency level general information
- Is divided into five sections ...
 - Log Reader Activity
 - Top Client IP by Requests
 - Top Users by Page Views
 - Top Categories by Page Views
 - Top Domains by Requests
- Many other top level reports available



Log Reader Activity		Edit X
Files	25,579	
Log Lines	138,410,841	
Bytes	7.5 GB	
Average Performance	11,329 lines/sec	
History		
Log Reader 0		
Logfile directory	/home/bluecoat/	
Logfile pattern	[*]*	
Next check	59 seconds	
Check Interval	60 seconds	

Top Client IP by Requests		Edit X
All Dates		
10.132.109.79	697,678	
10.132.56.172	685,559	
10.132.56.53	550,597	
10.132.56.112	479,375	
10.132.54.199	473,780	
10.132.59.63	473,635	
10.132.113.53	472,149	
10.135.3.152	468,393	
10.132.52.230	454,933	
10.132.795.118	445,368	
Full Report		



Top Users by Page Views		Edit X
All Dates		
-	478,319	
	107,322	
	105,678	
	104,880	
	100,899	
	99,037	
	91,368	
	91,197	
	88,428	
	85,812	
Full Report		

Top Domains by Requests		Edit X
All Dates		
www.com	5,107,545	
www.msnbc.msn.com	4,762,871	
www.msn.com	4,040,879	
msn.foxsports.com	3,287,028	
www.state.va.us	2,436,151	
lads.myspace.com	1,665,455	
www.mspquest.com	1,505,136	
www.facebook.com	1,366,590	
profile.myspace.com	1,317,609	
sportillusira.ed.cnm.com	1,123,107	
Full Report		

Introduction
Dashboard
Report Filtering
Overall Traffic
Activity Summary
Conclusion

The Dashboard

- Very configurable (just click Edit) ...
- For example, you can have two or more “Top Users” sections
 - One by Page Views (showing most active)
 - One by Volume (showing who is using up most of your bandwidth)
 - And even one by Volume as a Pie chart
- Remember, all the Pie charts you could ever want, right at your fingertips!



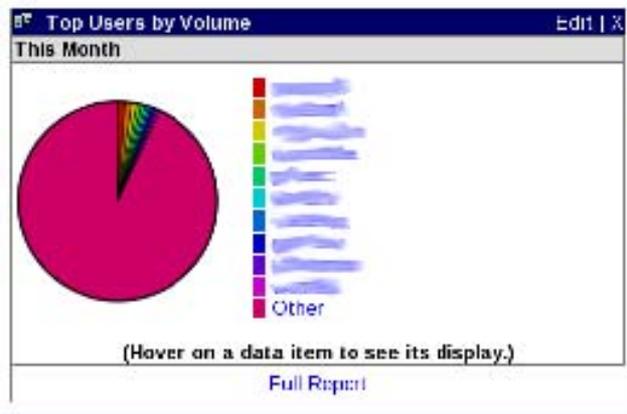
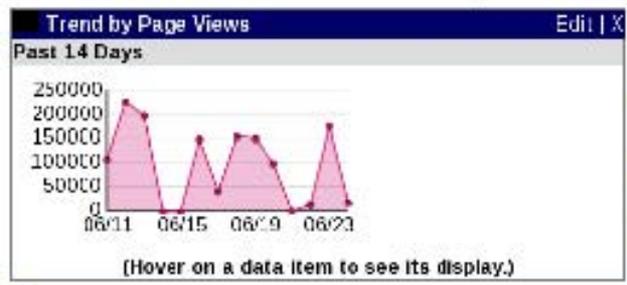
Log Reader Activity

Files	25,765
Log Lines	138,844,825
Bytes	7.6 GB
Average Performance	11,352 lines/sec

History

Log Reader 0

Logfile directory	/home/bluecoat/
Logfile pattern	DJJ*
Next check	43 seconds
Check Interval	60 seconds



Top Client IP by Requests

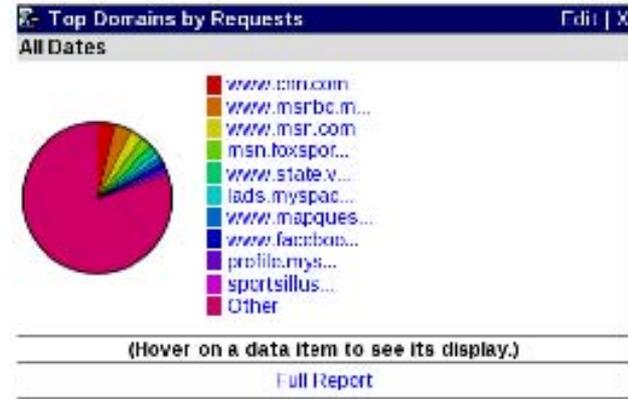
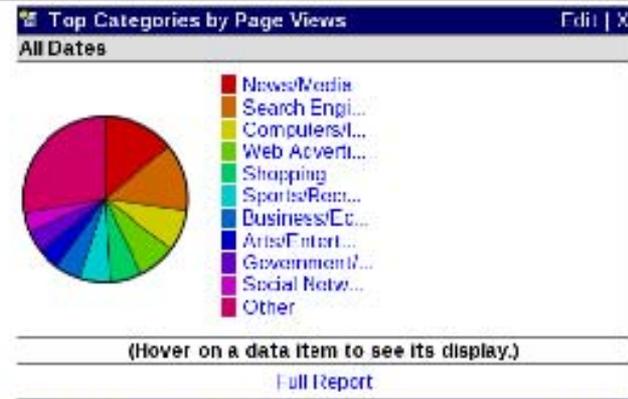
All Dates	
10.132.109.79	703,051
10.132.56.177	666,029
10.132.56.53	550,597
10.132.68.117	481,260
10.132.54.199	474,775
10.132.69.63	473,635
10.132.113.53	473,433
10.132.0.152	472,240
10.132.52.230	455,103
10.132.225.118	445,388

Full Report

Top Users by Page Views

All Dates	
	479,983
	107,496
	106,951
	105,043
	101,042
	99,460
	91,526
	91,273
	86,426
	65,812

Full Report



Report Filtering

Introduction

Dashboard

Report Filtering

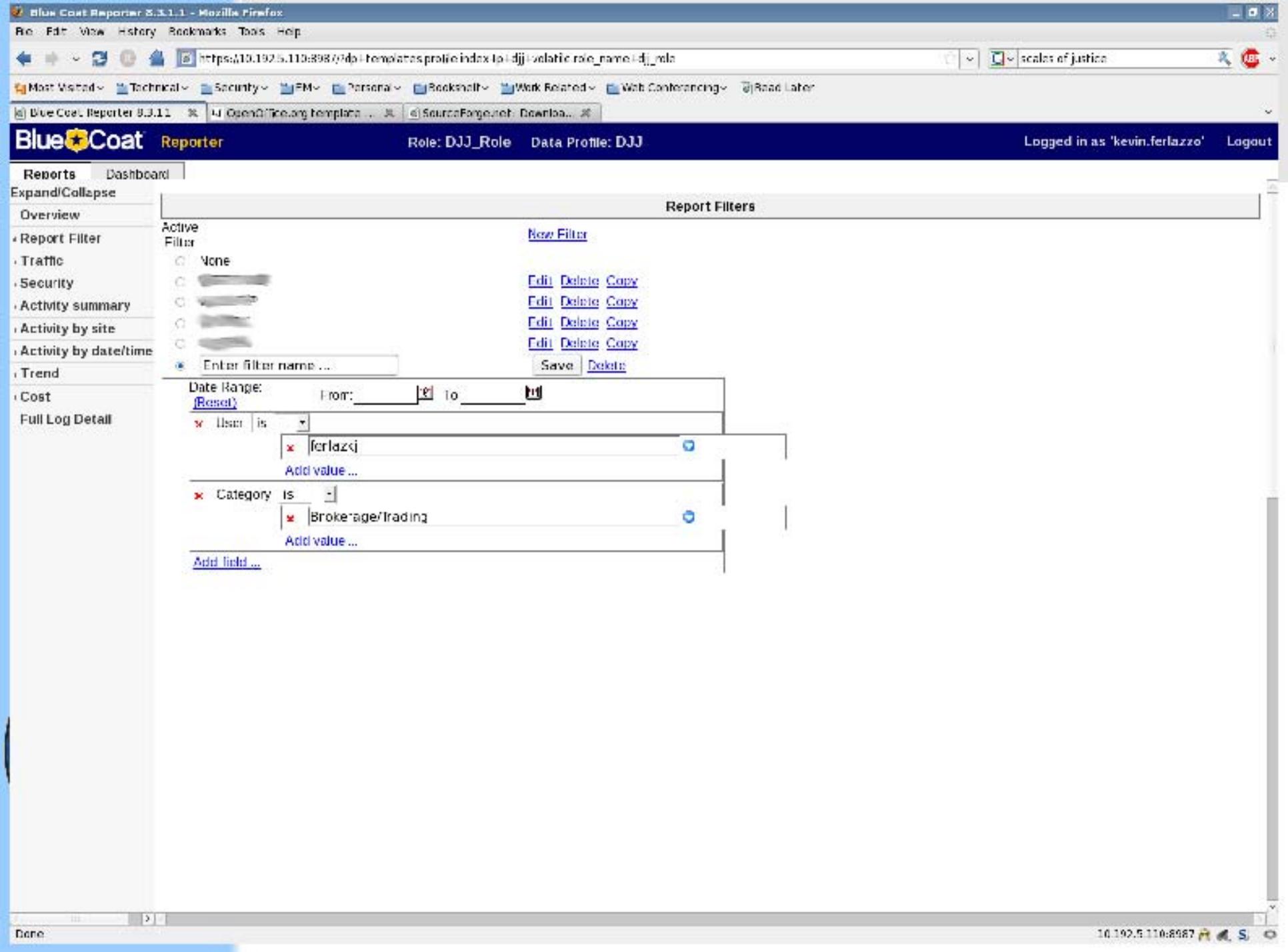
Overall Traffic

Activity Summary

Conclusion

- Any combination of ...
 - Begin/End Dates
 - User Account
 - Category
 - Client IP Address
 - File Extension
 - Group
 - Host
 - Port
 - And others ...





Overall Traffic Reports

Introduction

Dashboard

Report Filtering

Overall Traffic

Activity Summary

Conclusion

- General reports that track traffic by ...
 - Date
 - Days of Week
 - Hours of Day
 - Month



Introduction

Dashboard

Report Filtering

Overall Traffic

Activity Summary

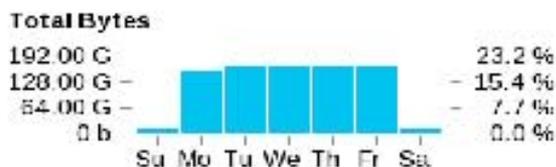
Conclusion

Overall Traffic Reports

- Example Day of the Week Report ...

Statistics for 13/Dec/2007 - 19/Jun/2008, 189 days

Days of Week Report



Page 1 of 1

"Click to zoom" report type:

Export to: CSV | PDF

Day of Week	Total Bytes	Bytes Received	Bytes Sent	Page Views
1 Wednesday	167.17 G	147.12 G	20.05 G	4,029,363
2 Friday	165.26 G	144.86 G	20.40 G	3,960,404
3 Thursday	162.98 G	142.92 G	20.06 G	3,941,870
4 Tuesday	162.92 G	143.17 G	19.75 G	3,891,522
5 Monday	149.43 G	130.99 G	18.44 G	3,522,620
6 Saturday	11.03 G	9.49 G	1.54 G	341,732
7 Sunday	9.71 G	8.43 G	1.28 G	322,327



Introduction

Dashboard

Report Filtering

Overall Traffic

Activity Summary

Conclusion

Overall Traffic Reports

• Example Month Report ...

Statistics for 13/Dec/2007 - 19/Jun/2008, 189 days

Month Report

Total Bytes



- 1 May/2008 21.6 %
- 2 Apr/2008 17.4 %
- 3 Mar/2008 14.3 %
- 4 Feb/2008 14.2 %
- 5 Jan/2008 13.3 %
- 6 Jun/2008 11.3 %
- 7 Dec/2007 7.8 %

Page 1 of 1

"Click to zoom" report type:

Export to : CSV | PDF

Month	Total Bytes	Bytes Received	Bytes Sent	Requests	Page Views
1 Dec/2007	65.37 G	57.21 G	8.16 G	10,489,329	1,712,943
2 Jan/2008	111.38 G	97.82 G	13.56 G	18,330,485	2,766,660
3 Feb/2008	118.62 G	103.70 G	14.94 G	19,231,791	2,800,009
4 Mar/2008	119.45 G	103.77 G	15.68 G	19,545,842	3,014,503
5 Apr/2008	144.68 G	127.40 G	17.28 G	22,301,357	3,468,805
6 May/2008	180.50 G	159.31 G	21.20 G	27,203,488	4,159,482
7 Jun/2008	94.13 G	82.66 G	11.47 G	14,294,975	2,110,061



Activity Summary Reports

Introduction

Dashboard

Report Filtering

Overall Traffic

Activity Summary

Conclusion

- Are the more specific reports that track activity by...
 - Most Active
 - Most Blocked
 - By Date
 - By User (if filtering for more than one)
 - By Group (useful if your site has defined more than one group in your AD domain)
 - By Category
- Full Log Detail Report (the Kitchen Sink Report)



- Reports
- Dashboard
- Expand/Collapse
- Overview
- Report Filter
- Traffic
- Security
- Activity summary
- Activity by site
- Activity by date/time
- By user
- By group
- By category
 - Activity Detail by Category
- Trend
- Cost
- Full Log Detail

Statistics for 01/Jun/2008 - 19/Jun/2008, 19 days
Activity Detail by Category Report

Report is filtered and shows data for User is: **ferlazzk**
[Save](#) [Print](#) [Regenerate](#)

Page 1 of 9 [1](#) [2](#) [3](#) [4](#) [5](#) > > Rows per page: 100

Export to: CSV | PDF [Table Viewing Options](#)

Category / Date and Time	Url	Verdict	Total Bytes	Requests
Blogs/Personal Pages				
02/Jun/2008 15:51:22	http://jeffkemptoncrade.blogspot.com/1e...	Allowed	975 b	1 0.1 %
02/Jun/2008 15:51:22	http://jeffkemptoncrade.blogspot.com/20...	Allowed	4.66 k	5 0.3 %
02/Jun/2008 15:51:24	http://www.blogger.com/v-css/navbar/129...	Allowed	745 b	1 0.1 %
02/Jun/2008 16:51:24	http://www.blogger.com/	Allowed	2.88 k	1 0.1 %
09/Jun/2008 09:04:39	http://indiah.wordpress.com/2007/09/06/o...	Allowed	519.00 k	14 0.9 %
18/Jun/2008 11:33:39	http://nixcraft.com/linux-software/690...	Allowed	109.14 k	40 2.5 %
18/Jun/2008 11:33:40	http://nixcraft.com/clientscript/vbulle...	Allowed	12.35 k	5 0.3 %
Subtotal			650.00 k	67 4.2 %
Business/Economy				
18/Jun/2008 13:08:14	http://www.bluecoat.com/user/password	Allowed	1013 b	1 0.1 %
Subtotal			1013 b	1 0.1 %
Computers/Internet				
02/Jun/2008 08:32:55	http://forums.cradle.com/forums/thread...	Allowed	124.85 k	14 0.9 %
02/Jun/2008 08:33:04	http://forums.cradle.com/forums/thread...	Allowed	5.86 k	2 0.1 %
02/Jun/2008 15:38:05	http://www.arydatabasesupport.com/forums...	Allowed	39.55 k	2 0.1 %
02/Jun/2008 15:38:41	http://forums.cradle.com/forums/thread...	Allowed	97.25 k	16 1.0 %
02/Jun/2008 15:40:55	http://forums.cradle.com/forums/thread...	Allowed	43.34 k	14 0.9 %
02/Jun/2008 15:42:51	http://www.cradle.com/technology/index...	Allowed	133.23 k	36 2.4 %

Introduction

Dashboard

Report Filtering

Overall Traffic

Activity Summary

Conclusion

Importing a CSV file

- Typically, the CSV file exported from BCR will be loaded into a spreadsheet.
 - This is useful for analysis of what a single user is doing, for example.
- If examining multiple users/groups, it is more useful to load the CSV file into a database.
 - For example, the CSV file can be loaded into an Oracle database



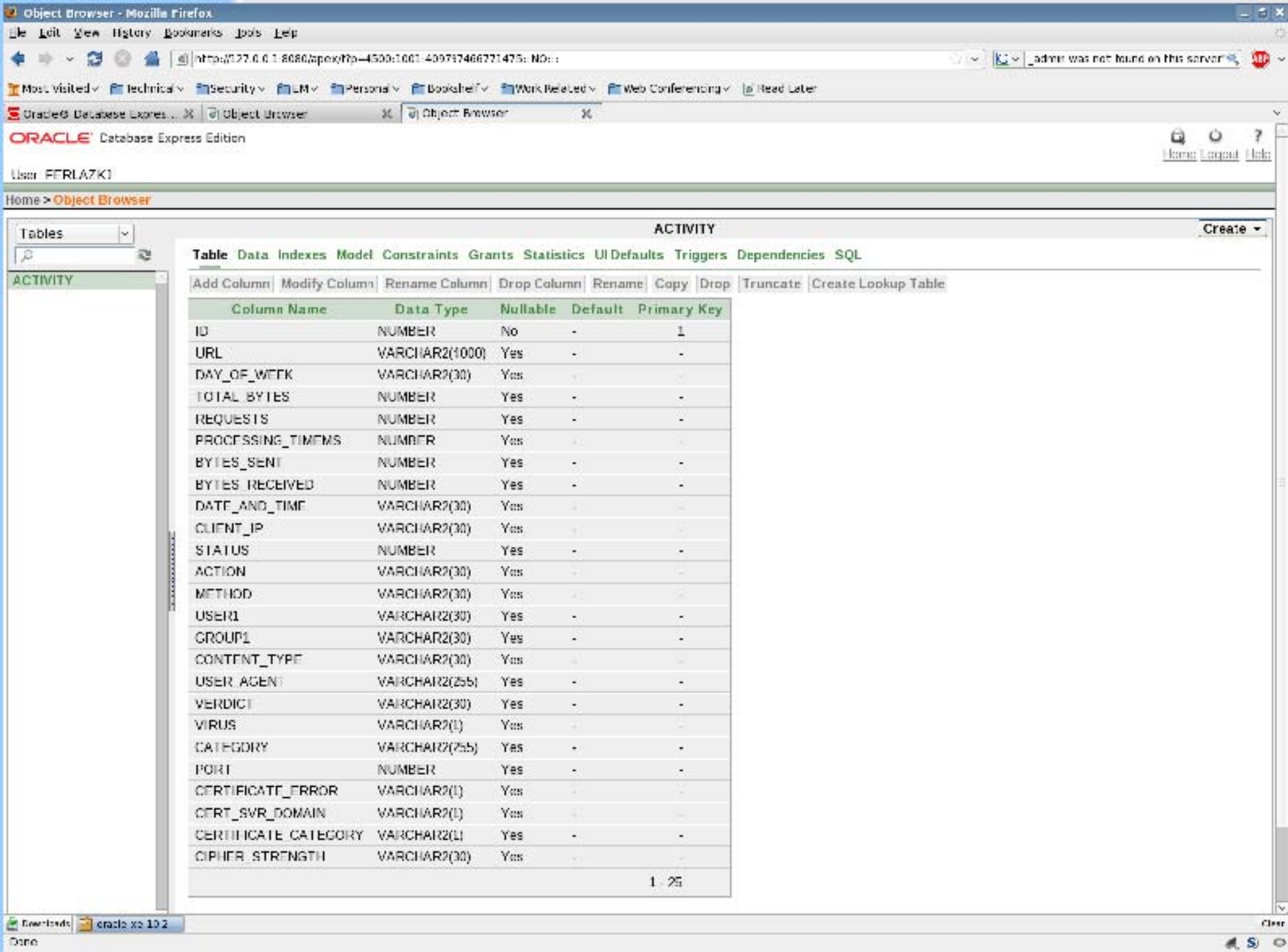


Table Data Indexes Model Constraints Grants Statistics UI Defaults Triggers Dependencies SQL

Add Column Modify Column Rename Column Drop Column Rename Copy Drop Truncate Create Lookup Table

Column Name	Data Type	Nullable	Default	Primary Key
ID	NUMBER	No	-	1
URL	VARCHAR2(1000)	Yes	-	-
DAY_OF_WEEK	VARCHAR2(30)	Yes	-	-
TOTAL_BYTES	NUMBER	Yes	-	-
REQUESTS	NUMBER	Yes	-	-
PROCESSING_TIMES	NUMBER	Yes	-	-
BYTES_SENT	NUMBER	Yes	-	-
BYTES_RECEIVED	NUMBER	Yes	-	-
DATE_AND_TIME	VARCHAR2(30)	Yes	-	-
CLIENT_IP	VARCHAR2(30)	Yes	-	-
STATUS	NUMBER	Yes	-	-
ACTION	VARCHAR2(30)	Yes	-	-
METHOD	VARCHAR2(30)	Yes	-	-
USER1	VARCHAR2(30)	Yes	-	-
GROUP1	VARCHAR2(30)	Yes	-	-
CONTENT_TYPE	VARCHAR2(30)	Yes	-	-
USER_AGENT	VARCHAR2(255)	Yes	-	-
VERDICT	VARCHAR2(30)	Yes	-	-
VIRUS	VARCHAR2(1)	Yes	-	-
CATEGORY	VARCHAR2(255)	Yes	-	-
PORT	NUMBER	Yes	-	-
CERTIFICATE_ERROR	VARCHAR2(1)	Yes	-	-
CERT_SVR_DOMAIN	VARCHAR2(1)	Yes	-	-
CERTIFICATE_CATEGORY	VARCHAR2(1)	Yes	-	-
CIPHER_STRENGTH	VARCHAR2(30)	Yes	-	-

ACTIVITY

ACTIVITY	
<input type="checkbox"/>	DATE AND TIME
<input checked="" type="checkbox"/>	CLIENT_IP
<input type="checkbox"/>	STATUS
<input type="checkbox"/>	ACTION
<input type="checkbox"/>	METHOD
<input type="checkbox"/>	USER1
<input type="checkbox"/>	GROUP1
<input type="checkbox"/>	CONTENT_TYPE

Conditions SQL Results Saved SQL

Column	Alias	Object	Condition	Sort Type	Sort Order	Show	Function	Group
ID	ID	ACTIVITY		Asc		<input checked="" type="checkbox"/>		<input type="checkbox"/>
TOTAL_BYTES	TOTAL_BYTES	ACTIVITY		Asc		<input checked="" type="checkbox"/>		<input type="checkbox"/>
PROCESSING_TIMEMS	PROCESSING_TIMEMS	ACTIVITY		Asc		<input checked="" type="checkbox"/>		<input type="checkbox"/>
CLIENT_IP	CLIENT_IP	ACTIVITY		Asc		<input checked="" type="checkbox"/>		<input type="checkbox"/>

Introduction
Dashboard
Report Filtering
Overall Traffic
Activity Summary
Conclusion

Final Thoughts

- Automatic Report Generation is possible, but that needs to be set up with/by the NOC staff.
- Reports can be automatically emailed to users, but that also needs to be set up with/by the NOC staff.



Conclusion

Introduction
Dashboard
Report Filtering
Overall Traffic
Activity Summary
Conclusion

- If you have any questions about BCR:
 - Read The Fine Manual (I have a PDF of it that I can share)
 - Join the Blue Coat Forum at
 - <http://forums.bluecoat.com/>
 - Or you can email me ...

Kevin Ferlazzo

Data Base Administration and Security

VA Department of Juvenile Justice

Email: Kevin.Ferlazzo@djj.virginia.gov





COV IT Partnership Security Topic

Matt Slaight, Partnership Program Security Officer, NG
Don Kendrick, Senior Manager of Security Operations, VITA

August 20, 2008



NORTHROP GRUMMAN

OPEN QUESTION AND ANSWER SESSION



IT Infrastructure Security Letters of Assurance

Cathie Brown, CISM, CISSP
Deputy Chief Information Security Officer

August 20, 2008



Background

- Goal of the COV Information Assurance process is to assist customer agencies in their responsibility for security of their agency's systems and information.
- Assurance in 2007
 - the first Letters of Assurance of security controls over customer agency's infrastructure were provided in August, 2007.
- Assurance in 2008
 - Letters of Assurance for 2008 are in process to be distributed no later than September, 2008.
- Assurance is not a guarantee, rather an assessment of security controls over the infrastructure.



2008 Data Points for Assurance

Data points for July 1, 2007 – June 30, 2008 include:

- 2008 SEC501 Self Assessment and Remediation Plans (Provided to All Customer Agencies)
- 2007 Deloitte & Touche SAS 70 Type II Remediation Plans (26 Agencies)
- 2007 Deloitte & Touche IT Security Audit Remediation Plans (8 Agencies)
- Current APA Reports with Infrastructure findings



Assurance Process

- Assurance provided on IT Security Domains with respect to infrastructure components:
 - IT Contingency Planning
 - IT System Security
 - Logical Access Control
 - Data Protection
 - Facilities Security
 - Personnel Security
 - Threat Management
 - IT Asset Management
- Assess the control requirements and findings related to each of the IT Security Domains

Assurance Process

- Measure the vulnerabilities by quantifying the number of findings relative to the total requirements in each IT Security Domain.
 - None – 0
 - Few – >0% -33%
 - Some - >33% - 66%
 - Many - >66%



COV Information Assurance Team

Meet the COV Information Assurance Team

- **Benny Ambler**
Enterprise Risk, Assurance and Standards Manager
- **Bill Freda**
Security Analyst
- **Jonathan Smith**
Security Analyst
- **Aarona Brooks**
Security Analyst
- **Mauri Shaw**
Risk Management Analyst



Questions





Network Security at Home Defending the Castle

Bob Baskette, CISSP, CCNP
Incident Management Engineer



Defense in Depth – The need

- Home computer systems have an inherent value to both the computer system owner and those malicious individuals who seek the data stored on the computer systems and the available processing power the computer systems possess.
- Malicious individuals may be interested in taking over the computer system to store illegal materials or launch attacks that will be traced back to the compromised system instead of the malicious individual.
- It is the responsibility of the computer system owner to protect the home network and the computer systems attached to that network.

Defense in Depth – The Issues

- Studies have shown that a non-patched Microsoft Windows 2000/XP system connected to the Internet can be compromised in as little as 5-minutes.
- A compromised home computer system can send 200,000 spam emails an hour.
- Details on new vulnerabilities are published on an hourly basis.
- Software publishers require time to provide software updates.



Defense in Depth – The Golden Age

- Defense in Depth concepts have not changed in over 1000 years
- Confront the attacking force with as many overlapping obstacles as possible to discourage the attack or at least delay the attacking force until response measures can be deployed.
- Castle defenses started with the use the natural terrain
 - Moat
 - High-wall Outer-Shell
 - Sentries
 - Building walls with windows only above the second floor.



Defense in Depth – Modern Approach

- Firewalls
- Network Address Translation (NAT)
- Wi-Fi Security
- Operating System Hardening
- Email Security
- Anti-Virus / Anti-Spam / Anti-Spyware Software
- Secure Browsers
- Virtualization



Firewall Information

- Firewalls are hardware devices or software programs that can be configured to filter both inbound and outbound traffic between the home network and the public Internet.
- Firewalls add a layer of protection by blocking unauthorized and potentially dangerous traffic from entering the home network. Firewalls are essential for home networks that have an “always on” connection to the Internet.



Firewall Information

- The selection of a firewall is dependent upon the sensitivity of the computer systems and data to be protected. The value of the assets, the complexity of the computers or networks, and the usage of the Internet will dictate the type and size of firewall that should be used.
- A software-based firewall can be deployed in those cases where the computer system is used simply access websites and sending emails.
- A hardware-based firewall would be more appropriate for those computer systems used for on-line banking, on-line bill paying, on-line shopping, or file hosting services.
- A software-based firewall can be used in combination with a hardware-based firewall to implement the "Defense-in-Depth" best practice, thereby providing multiple layers of traffic filtering.



Basic Firewall Configuration

- Implement a “Client-Only” or “Established/Related” traffic filtering list.
 - Allow only the inbound network traffic that is needed.
 - Define the programs, protocols and ports that should have access to the home network.
 - Block unsolicited traffic from connecting to the home network.
 - Prevent LAN traffic from leaving the home network .
 - Filter all inbound traffic with a source IP-address in the RFC-1918 Private IP-address range.
 - Filter all inbound traffic with a source IP-address that matches the IP-address range used on the home network.
- Enable the “automatic update” feature if one exists for the firewall.
- Periodically check the firewall vendor’s website for the latest software updates.
- Change the default “administrator” account and password.
- Disable the remote management option.
- Firewalls should be configured to log activity. These logs should be reviewed at least once a month to identify any anomalous or unexpected activity.



Additional Firewall Information

- Stateful Packet Inspection (SPI) technology will examine traffic destined for the home network to determine if the inbound traffic is arriving in response to an authorized request.
- MAC address filtering should be employed to prevent rogue devices from connecting to the home network.
- Administrative functions should be limited/assigned to a specific computer system IP-address on the home network.
- If the firewall administrative interface is web-based, only enable the SSL/TCP-port 443 option. Disable the HTTP/TCP-port 80 option.
- If the firewall administrative interface is text-based, only enable the SSH/TCP-port 22 option. Disable the Telnet/TCP-port 23 option.
 - PuTTY is a SSH program for Microsoft Windows.
- Firewalls should be used in concert with Network Address Translation, operating system hardening, anti-virus, anti-spyware, and anti-spam software as part of a "Defense-in-Depth" strategy for protecting the computer systems attached to the home network from various forms of remote attacks by malicious individuals who want to steal personal information or use the computer systems for illegal activities.



Network Address Translation

- Most hardware-based firewalls and wireless access points provide Network or Port Address Translation.
- NAT/PAT will obfuscate the home network's actual IP-address space.
- NAT/PAT will allow every computer system on the home network to appear as the same IP-address to the Internet so a malicious individual cannot easily determine the actual number of computer systems attached to the home network or which system is utilizing a specific service.



Network Address Translation

- By default, most home networking NAT/PAT devices will use the 192.168.0.0/24 IP-address range for the home network. This IP-address range should be changed to another private IP-address range defined in RFC-1918.
- Available RFC-1918 IP-address ranges include:
 - 10.0.0.0/8
 - 172.16.0.0/16 – 172.31.0.0/16
- Change the administrative interface on all home routers/firewalls/wireless access points to use something other than 192.168.0.1 or 192.168.0.100. These two IP-addresses are default on most consumer-grade equipment.



Wi-Fi Security

- Physical lay-out
 - Place the wireless access point at center of the home.
 - Limit broadcast distance
- Wireless access point configuration
 - Operate in the 802.11n range if possible.
 - Most current equipment operates at 802.11b or 802.11g.
 - Change the SSID (Service Set Identifier) from the default vendor value.
 - Disable the SSID broadcast if possible.
 - Enable MAC-address filtering.
 - Include all Ethernet and wireless MAC-addresses on the home network in the filter list.
 - Enable Wi-Fi Protection
 - WPA-2 Personal security provides the best protection for a home network
 - WPA security provides adequate protection for a home network
 - WEP has been compromised, but is still better than clear text



Wi-Fi Security

- Disable “Bridge” mode on the wireless access point if only one wireless access point will be installed on the home network.
- Configure the computer systems on the home network that use a wireless connection to operate in an “Infrastructure Mode” only.
 - Wireless “Ad-Hoc” mode will allow a direct connection between two computers using wireless network adapters.
 - Microsoft Windows 2000/XP will bridge an active wireless connection to the wired network in certain network configurations.
 - An “Ad-Hoc” connection to a computer system on the home network will allow a malicious individual to “by-pass” all security measures and connect to the home network.

Operating System Hardening

- Every modern Operating System has vulnerabilities and available exploits with which to attack those vulnerabilities.
- To protect the Operating System:
 - Enable the “Automatic Software Update” feature.
 - Remove software that is no longer needed.
 - Remove trial software once the trial has ended.
 - Do not install unsolicited software from any source.
- Remember, “Free” Software can be VERY Expensive!!



Operating System Hardening

- Turn off File Sharing, Print Sharing, NetBios or other services that are not needed.
- Employ the Least Privilege concept
 - Create a separate account for system administration on the computer system.
 - Do not use the name Admin, Superuser, Root, or any other term that would suggest that the account is the Administrator account. The "Administrative" account should only be used to install software and make system modifications.
- Create separate accounts for each user on the computer system. The user accounts should be used for the day to day activities. Limiting access to the system privileges associated with the Administrator account will prevent some of the malicious content spreading across the Internet from getting installed on the computer system.



Operating System – Password Selection

- Ensure that each account on the computer system uses strong passwords.
 - Do not use anything that can be associated with the user such as name, birth date, family member/pet name, or words found in the dictionary.
 - Use phrases or build a password by pulling out the first and last letter of every word of a phrase and use that as the password.
 - Replace characters with numbers such as the '0' (zero) instead of the 'O', 'i' instead of a '1', '3' instead of an 'e', or '4' instead of an 'a'.
 - Do not use the same password on every site.
- To verify the strength of a password, visit the Microsoft password checking site:
<http://www.microsoft.com/protect/yourself/password/checker.aspx>



Email Security

- Email Security Best Practices

- To mitigate the potential threat presented by a spam or phishing email campaign, never open attachments or click links contained in unsolicited email messages.
- If possible, check with the person who supposedly sent the email to make sure that it is legitimate prior to opening any attachments.
- Scan any attachments with anti-virus software before opening the attachment.
- Do not reveal personal or financial information in an email, and not to respond to email solicitations for this information.
- Always examine the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain extension such as .com vs. .net.
- If the legitimacy of an email request needs to be verified, try to verify the origin of the email by contacting the company directly. Never use the contact information provided on a web site connected directly to the email request.
- An additional step to help mitigate the risk of a phishing campaign is to limit the administrative rights of the local users through the implementation of the Least-Privileged best practice.



Email Security – Additional Steps

- Disable automatic image loading.
- Configure the email client software to send and display email in text format. This will prevent the embedded links in the email from being clickable and will prevent malicious code hidden in the email from running when the email is opened.
- Establish an unique domain name for email accounts. Domains can be registered with companies such as:
 - Network Solutions <http://www.networksolutions.com>
 - Verisign <http://www.verisign.com>
 - GoDaddy <http://www.godaddy.com>
- Create a separate email account for website forms and contact lists.



Anti-X software

- Every computer system on the home network needs an up-to-date version of anti-virus, anti-spyware, anti-spam, and anti-phishing software.
- The leading vendors for Anti-X software are:
 - Norton (Symantec)
 - McAfee
 - Trend Micro
 - Zone Alarm (CheckPoint)
 - Each of these vendors provide a complete software solution for Anti-X and firewall functions.
- Configure the Anti-X software to check for product updates on a daily basis.
- Configure the Anti-X software to scan the entire contents of the hard drive at least once a week.
- Configure the Anti-X software to scan ALL removable media each time the removable media is attached to the computer system.
- Scan ALL installation CD/DVDs for malicious code prior to installing the software.
- Please renew the software update license each year or purchase a new copy of the software at the end of each year. Do not let the Anti-X software expire.



Anti-X Notes

- USB storage devices such memory cards (for digital cameras or MP3 players), flash drive/thumb drives, removable hard drives or digital photo frames are formatted at the factory to simplify installation. During the past three years, these devices have been shipping with additional features such as viruses, trojans, and key logging programs.
 - 500Gbyte and 1Tbyte hard drives purchased by the Federal Government contained a trojan.
 - Digital photo frames sold by Best Buy and CompUSA contained a key logging program.
- Before any USB device is used for the first time:
 - Turn off the Operating System Autorun feature.
 - Scan the device for malicious software.
 - Format memory cards using the built-in digital camera function.
 - Format (zero the drive) new USB hard drives.
- Monitor the computer system:
 - Monitor hard disk space to determine if the available space decreases for an unknown reason – This may indicated a backdoor has been installed on the computer system and the system is storing information for a malicious individual.
 - Monitor the log files and Event Viewer logs for unexpected error messages
- Avoid P2P programs. Multimedia download services such as Limewire, Bearshare, Gnutella and Kazaa can expose the computer system to massive exploits.



Secure Web Browser Information

- Modern-day Browsers
 - Microsoft Internet Explorer 7
 - Mozilla Firefox 3
 - Opera
 - Safari 3
- Browser configuration
 - Disable Active-X controls and applets if possible.
 - Disable the Adobe Flash plug-in if possible.
 - Disable form auto-fill functions.
 - Disable password caching.
 - Install security plug-ins from the software vendor's website to improve the security inspection of the displayed website.
 - Configure the browser to clear all browser information when the browser window is closed.
 - Only accept cookies from the sites that you visit.
- Avoid Tab browsing when sending sensitive information.
- Prior to initiating a secure connection to a website where confidential information will be sent to or received from the web server:
 - Close all browser windows.
 - Clear the browser cache.
 - Clear all browser cookies.
- Enable private browsing if supported by your browser.
- Do not ignore SSL certificate warnings.



Secure Web Browsing Concerns

- Take care when surfing the Internet. Even trusted websites can become compromised with code that will redirect your browser to malicious websites or attempt to download malicious code to the computer.
- Beware of the “Pop-Up” window. Never install a program just because a “Pop-Up” window appears with message indicating that a software update or applet is needed. Remember, if a trusted website prompts to install a program, err on the side of caution and say no. Contact the company by telephone and confirm the software update.
 - A popular exploit mechanism is to use an Anti-Virus “Pop-Up” window informing the user of a potential infection on the computer system and to install “Anti Virus Software” to remove the infection. This exploit will either install a program that does nothing but prompt the user for money to remove the “infection” or will attempt to ransom the contents of the computer system. Either way, clicking “Yes” to remove the “infection” actually results in the installation of malicious software.



Secure Web Browsing Password Security

- Use strong passwords for any websites requiring a login.
- Use unique passwords for all websites. Avoid using the same password for similar websites.
- Carefully consider the questions used by a website for automated password resets. Most websites use the same set of common questions for password reset. Most of the answers to these questions can be found in public records or on-line.
 - Place of birth, mother's maiden name, and school information are available in public records.
 - Friends, color preference, hobbies, and pet information often found on Social Network sites.
 - Make of first car can be guessed based on purchasing trends.
- Consider using the option to create your own question/answer combination if possible.



Virtualization Information

- Virtualization is a mechanism to run multiple instances of an operating system on the same computer.
- Virtualization can also be used to allow different operating systems to run at the same time on the same computer system.
- Popular Virtualization software products include:
 - VMware Workstation for Microsoft Windows and Linux
 - VMware Player for Microsoft Windows and Linux
 - Parallels Workstation for Microsoft Windows and Linux
 - Parallels Desktop for Mac
 - VMware Fusion for Mac



Virtualization Techniques

- Virtualization can be used to fortify the computer system when accessing external resources through the use of “Snapshot” images.
- “Snapshot” images allow the virtual system to be reset to a pre-determined point, removing any changes to the virtual system that have been made since the last snapshot. Reverting to a previous “Snapshot” would remove any malicious code installed within that virtual system while browsing the Internet from that virtual system.
- Virtual systems can be installed to provide specific functions such as:
 - General Internet surfing
 - On-line shopping and on-line banking
 - Email
 - File-sharing and website hosting
- VMware Player is a free software product from VMware. VMware Player can use pre-configured virtual machines from VMware.



Helpful URLs

- To learn more about home network security, please visit the following sites:
 - <http://www.securityfocus.com>
 - <http://www.isc.sans.org>
 - <http://www.microsoft.com/protect/default.mspx>
 - <http://www.microsoft.com/security/default.mspx>
 - <http://www.us-cert.gov>
 - <http://secunia.com/>
 - <http://www.cert.org/homeusers/HomeComputerSecurity/>
 - http://www.cert.org/tech_tips/home_networks.html



Helpful URLs

- Additional information on firewall configuration can be found at the following URLs:
 - <http://www.us-cert.gov/cas/tips/ST04-004.html>
 - <http://onguardonline.gov/tutorials/firewall-xp-instruct.html>
 - <http://onguardonline.gov/tutorials/firewall-osx-instruct.html>
 - <http://www.firewallguide.com>



Final Thoughts

- The security of the home network is ultimately decided by how the computer systems are used.
- A “Fully-Patched” computer system is only fortified against known vulnerabilities. “Zero-Day” exploits and unpublished vulnerabilities can still have a negative impact on the computer systems.
- Most home computer systems that become compromised have two components in common.
 - The computer system had outdated anti-virus programs
 - The computer systems were used to download music and movies from the Internet.
- Keep the software on the computer systems up-to-date.
 - Install the latest security updates from the software vendor.
 - Enable Automatic Updates for the operating system, anti-virus, and user applications.
 - Secunia PSI is the FREE security tool that is designed to scan the computer system for installed software and determine if any applications lack security updates. <https://psi.secunia.com/>



Final Thoughts

- Scan the computer system for malicious software at least once a week.
- Back-up your files on a regular basis.
- Keep all installation CD/DVD media and license keys in a safe place.
- Visit computer security websites to become aware of the current malicious threats.
 - www.isc.sans.org
 - www.us-cert.gov
 - www.securityfocus.com



Questions???

For questions or more information, please
contact VITA Security Services at:
VITASecurityServices@VITA.Virginia.Gov

Thank You!



Commonwealth Security Annual Report

Peggy Ward
Chief Information Security and
Internal Audit Officer



§ 2.2-2009

§ 2.2-2009. (Effective until July 1, 2008) Additional duties of the CIO relating to security of government information.

- C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.



Explanation

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
XYZ	Current	YES	1	YES	YES	1 of 1

Agency

- Agency Abbreviation

Security Audit Plan Rec'd

- Indicates whether agency has submitted a Security Audit Plan to Commonwealth Security and Risk Management for all systems classified as sensitive based on confidentiality, integrity, or availability.
- Options: Current = Received and up to date,
No = Not Received,
Outdated = Audit Plan was submitted but requires update,
Extension Expired = An Exception was filed but has expired and Audit Plan has not been received.

Information Security Officer (ISO) Designated

- Indicates whether agency head has designated an ISO for the agency and provided the person's name, title and contact information to VITA no less than biennially.
- Options: YES/NO

Explanation – Continued

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
XYZ	Current	YES	1	YES	YES	1 of 1

Attended Information Security (IS) Orientation (Extra Credit)

- Indicates the number of attendees that an agency has sent to attend Information Security Orientation.
- This data point is an “Extra Credit” data point where as it is not currently a requirement, but attendance is highly encouraged for ISO’s and all interested parties.
- Options: 0 - ∞

Information Technology Disaster Recovery (IT DR) Plan Rec'd

- Indicates whether agency has submitted an IT DR Plan.
- Options: YES = Submitted,
 YES/UPD = Submitted an updated IT DR Plan,
 NO = Has not submitted IT DR Plan,
 N/A = Not Applicable (Agency is not a customer of the IT Partnership)

Explanation – Continued

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
XYZ	Current	YES	1	YES	YES	1 of 1

Corrective Action Plan's (CAP's) Rec'd

- Indicates whether the agency has submitted Corrective Action Plans (CAP's) for vulnerabilities identified in Security Audits.
- *Note* CAP's should be submitted to Commonwealth Security and Risk Management one month after the completion of an audit and updates submitted quarterly for open vulnerabilities.
- Options: YES = Agency performed Security Audits & submitted CAP's,
 NO = Agency's Security Audit Plan indicates Security Audit was scheduled but has not submitted CAP,
 N/A = Not applicable, either Agency did not have Security Audits scheduled to date or Agency has not submitted a Security Audit Plan.

CAP's Status

- Indicates the number of Corrective Action Plans submitted and the number of Security Audits scheduled based on the Security Audit Plan.
- Options: [Numbers of CAP's received] of [number of Security Audits scheduled] (example - 1 of 1, 0 of 1, 1 of 2, etc...), N/A = either Agency did not have Security Audits scheduled to date or Agency has not submitted a Security Audit Plan.



Secretariat: Administration

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
CHR	NO	YES	0	YES	N/A	N/A
DGS	Current	YES	0	YES	NO	0 of 3
DHRM	Current	YES	0	YES/UPD	N/A	N/A
DMBE	NO	YES	2	YES	N/A	N/A
EDR	Current	YES	3	YES/UPD	N/A	N/A
SCB	Current	NO	1	YES	NO	0 of 6
SBE	Current	NO	1	YES	N/A	N/A



Secretariat: Agriculture & Forestry

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DOF	Current	YES	1	YES	N/A	N/A
VADACS	Current	YES	3	YES	N/A	N/A



Secretariat: Commerce & Trade

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DBA	NO	YES	1	YES	N/A	N/A
BOA	Current	YES	1	YES	NO	0 of 3
DHCD	Current	YES	0	YES	NO	0 of 4
DMME	Current	YES	1	YES	YES	1 of 3
DOLI	NO	YES	3	YES	N/A	N/A
DPOR	Current	YES	1	YES	NO	0 of 5
TIC	NO	NO	0	NA	N/A	N/A
VEC	Current	YES	2	YES/UPD	NO	0 of 6
VEDP/VTA	NO	YES	0	YES	N/A	N/A
VHDA	NO	NO	1	NA	N/A	N/A
VNDIA	NO	NO	0	NA	N/A	N/A
VRA	NO	NO	0	NA	N/A	N/A
VRC	EXTENSION EXPIRED	YES	2	YES	N/A	N/A



Secretariat: Education (excluding Higher Ed)

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DOE	Current	YES	1	YES	NO	0 of 5
FCMV	NO	YES	0	NO	N/A	N/A
GH	NO	YES	0	NO	N/A	N/A
JYF	Current	YES	1	YES	NO	0 of 3
LVA	Current	YES	1	YES	N/A	N/A
SCHEV	EXTENSION EXPIRED	YES	0	YES	N/A	N/A
SMV	NO	YES	0	YES	N/A	N/A
VCA	NO	NO	0	YES	N/A	N/A
VMFA	Current	YES	2	YES	YES	2 of 2



Secretariat: Education (Higher Ed only)

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
CNU	Current	YES	0	NA	N/A	N/A
GMU	Current	YES	1	NA	YES	11 of 22
JMU	Current	YES	0	NA	YES	3 of 3
LU	Current	YES	1	NA	YES	1 of 2
NSU	NO	YES	2	NA	N/A	N/A
ODU	Current	YES	1	NA	YES	3 of 4
RU	Current	YES	0	NA	N/A	N/A
UMW	Current	YES	1	NA	NO	0 of 1
VCCS	Current	YES	3	NA	YES	1 of 2
VMI	Current	YES	0	NA	N/A	N/A
VSU	Current	YES	2	NA	NO	0 of 10



Secretariat: Finance

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DOA	NO	YES	4	YES	N/A	N/A
DPB	Extension Expired	Yes	2	YES/UPD	N/A	N/A
TAX	Current	YES	1	YES	YES	10 of 16
TRS	Current	YES	2	YES	YES	1 of 9



Secretariat: Health & Human Resources

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DHP	Current	YES	0	YES	N/A	N/A
DMAS	Current	YES	1	YES	NO	0 of 5
DMHMRSAS	Current	YES	13	YES	N/A	N/A
DRS (VBPD, VDBVI, VDDHH, WWRC)	Current	YES	0	YES	NO	0 of 5
DSS (CSARYF)	Current	YES	2	YES/UPD	NO	0 of 18
TSF	NO	NO	0	NO	N/A	N/A
VDA	Current	YES	1	YES	N/A	N/A
VDH	Current	YES	3	YES	YES	9 of 11



Secretariat: Natural Resources

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DCR	Current	YES	1	YES	NO	0 of 1
DEQ	Current	YES	4	YES	YES	1 of 1
DGIF	NO	YES	1	YES	N/A	N/A
DHR	Current	YES	2	YES	N/A	N/A
MRC	Current	YES	2	YES/UPD	YES	4 of 4
VMNH	NO	YES	1	YES	N/A	N/A



Secretariat: Public Safety

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
ABC	Current	YES	1	YES	YES	5 of 5
CASC	NO	NO	0	NO	N/A	N/A
DCJS	Current	YES	0	YES	NO	0 of 5
DFP	NO	YES	1	NO	N/A	N/A
DFS	Current	YES	1	N/A	N/A	N/A
DJJ	Current	YES	3	YES	NO	0 of 1
DMA	NO	NO	0	YES	N/A	N/A
DOC	Current	YES	3	YES	NO	0 of 6
DOCE	NO	YES	1	YES	N/A	N/A
DVS	NO	YES	1	YES	N/A	N/A
VDEM	NO	YES	1	YES	N/A	N/A
VSP	Current	YES	3	YES	N/A	N/A



Secretariat: Technology

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
CIT	Current	YES	1	YES	NO	0 of 1
VITA	Current	YES	7	YES	N/A	N/A



Secretariat: Transportation

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
DMV	Current	YES	2	YES	NO	0 of 7
DOAV	NO	YES	2	YES	N/A	N/A
DRPT	Current	YES	1	YES	N/A	N/A
MVDB	NO	YES	0	YES	N/A	N/A
VDOT	Current	YES	5	YES	YES	1 of 3



Independent Branch Agencies

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
IDC	NO	YES	4	N/A	N/A	N/A
SLD	NO	YES	2	N/A	N/A	N/A
SCC	NO	YES	3	N/A	N/A	N/A
VCSP	YES	YES	3	N/A	NO	0 of 3
VOPA	NO	NO	0	N/A	N/A	N/A
VRS	NO	YES	2	N/A	N/A	N/A
VWCC	NO	NO	0	N/A	N/A	N/A



Other

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	IT DR Plan Rec'd	CAP's Rec'd	CAP's Status
GOV	Extension Expired	YES	1	YES	N/A	N/A
OAG	NO	YES	1	NA	N/A	N/A



Questions?





Upcoming Events





UPCOMING EVENTS! 9/7-8

COVITS 2008

Commonwealth of Virginia Innovative Technology Symposium

September 7 – 9, 2008
Williamsburg Marriott

Don't miss this opportunity to see the latest in digital government solutions, keep abreast of current policy issues and network with key government executives, technologists and industry specialists.

www.govtech.com/events/COVITS2008



UPCOMING EVENTS! 9/11

IS Orientation

Thursday, September 11th, 9:30 am to 12:00 pm @ CESC

Information Security Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV IT Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

To register email VITASecurityServices@vita.virginia.gov



UPCOMING EVENTS! 9/15

Commonwealth Information Security Council Meeting

Monday, September 15th, 12:00 - 2:00 p.m. @ CESC with Committee meetings from 2:00 - 3:00 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to VITASecurityServices@vita.virginia.gov (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at:
<http://www.vita.virginia.gov/security/default.aspx?id=5128>



UPCOMING EVENTS! 9/18

NEXT ISOAG MEETING!

September 18th, 1:00 – 4:00 pm @ CESC

DRAFT Agenda

FBI InfraGard – Melissa McRae, FBI

DMV Security Awareness – Doug Mack, DMV

Commonwealth & COV Partnership Security

Incident Handling – Michael Watson & Don

Kendrick, VITA



UPCOMING EVENTS! 9/24

The University of Virginia is hosting the SANS Security 537: Identifying and Removing Malware course on September 24th. The discounted rate is \$325 for employees of accredited educational institutions, state and local government, and state and local law enforcement.

The standard SANS price is \$1264. All course materials, parking, snacks, and lunch buffet are included.

Details at <http://itc.virginia.edu/security/sansedu>



UPCOMING EVENTS! 10/6-7

VA SCAN – October 6-7, 2008

The VA SCAN 2008 conference registration is \$125; pre-registration is required.

The fee includes the conference program, a Monday evening reception, and lunches and breaks for both days. Special room rates are available at The Inn at Virginia Tech, as well as the Hawthorn Suites.

Registration deadline is September 29, 2008. Register at:
<http://www.cpe.vt.edu/vascan2008/registration.html>

<http://www.cpe.vt.edu/vascan2008/index.html>



Any Other Business ???????



ADJOURN

THANK YOU FOR ATTENDING!!

