Rividium Whites - White papers on leading edge technologies

Cost-Efficient Network Security Architecture

Security and Efficiency for Start-ups

Andrew Bruce, CISSP, PMP, FITSP-D
CTO, RiVidium Corporation (http://www.rividium.com/)
andy.bruce@rividium.com

25 September 2010

Topic Summary:

- Core functions for your network: what does it do and who is it designed for?
- Logical versus physical architectures: Constructing the network for success.
- Security and defense-in-depth: Layers of protective assurance.
- Starting and Staying Secure: Maintaining your operating systems over time.
- Recommendations and Best Practices: Providing Assurance without breaking the bank!

Table of Contents

Illustration Index

About the Author

Andrew Bruce is Chief Technical Officer for RiVidium Incorporated, a Service Disabled Veteran Owned Small Business in the suburban Washington, DC area. RiVidium provides professional services to the Federal Government and the Department of Defense, specializing in customizing and developing architecture and governance models that leverage our proprietary technologies. Mr. Bruce's job responsibilities include: working directly with customers and partners for new business development, supporting proposal efforts, overseeing RiVidium's network infrastructure, working with project managers to ensure project completion, managing software development efforts throughout the entire system life-cycle, and leading new technology research and proofs-of-concept. After a career spanning decades in shrink-wrap, commercial, and corporate software development, Mr. Bruce is focusing on Information Assurance to achieve his goal of building and managing large data centers providing cloud computing utility services for commercial and Government customers.

1.0 Introduction

In this white paper, we look at a notional (but typical) small business. This notional organization faces unique challenges as a small company competing in a difficult business environment. As an information systems services provider, its network must provide a high degree of confidentiality, integrity, and availability (the CIA Triad)[i] – the loss of any of these elements translates to a loss of its customers' trust. At the same time, it must be economical; overhead personnel must be funded from existing revenues. Our notional network infrastructure must satisfy these conflicting goals to provide the best cost-benefit. Specifically, we look at the following:

- *Background* – The constraints under which our notional network must function.
- *Existing Landscape* – The business drivers for our notional network's configuration, the logical architecture we use to address these drivers, and our notional physical implementation.
- *Defensive Posture* – How we protect our notional network from external and internal attacks.
- *Recommendations* – Suggestions and alternatives for applying new resources to our notional network.

Gartner identifies both virtualization and activity monitoring as top strategic IT technologies for 2010.[ii] In our notional infrastructure, we address both of these technologies, but temper our adoption based on **reliability** as the single most important consideration for us, closely followed by **affordability**. We analyze existing shortcomings and suggest new solutions with these constraints in mind.

2.0 Background

Our notional organization is a start-up with strong funding sources, currently active customers / revenue generation, and strong business development efforts. However, it recognizes that sustainable success demands prudent management of corporate expenses. Today's hyper-competitive business environment requires our notional network infrastructure to be highly secure while simultaneously keeping the overhead rate low and the billable rate high.

Network success is a *sine qua non*[iii] for our start-ups own success – our notional network must run in an automated and highly-available mode. It must account for power outages, equipment failures, system failures, data corruption, and external auditing requirements all while minimizing our overhead expenditures. Additionally, our notional network must be scalable; we must be able to expand its functionality without extensive retooling of the existing infrastructure.

3.0 Existing Landscape

3.1 Core Functions

Computer networks exist to satisfy business drivers,[iv] and our notional network is no exception. Our business drivers specify the core functions that our notional network must provide, and include the following:[v]

1. **Corporate presence** (corporate Web pages, company contact information, news feeds, search engine support, and so on);
2. **Secure communication** via email and phone;
3. **Managed Internet access** for team members;
4. **Collaboration functions** to allow internal groups and customers to work together in a secure environment; and,
5. **Compliance and accreditation** requirements to satisfy contractual and legal obligations. This last requirement includes the ability for the network to protect itself against internal and external attacks.

3.2 Network Structure

Our notional network infrastructure directly addresses these business drivers, as shown by the following drawing:

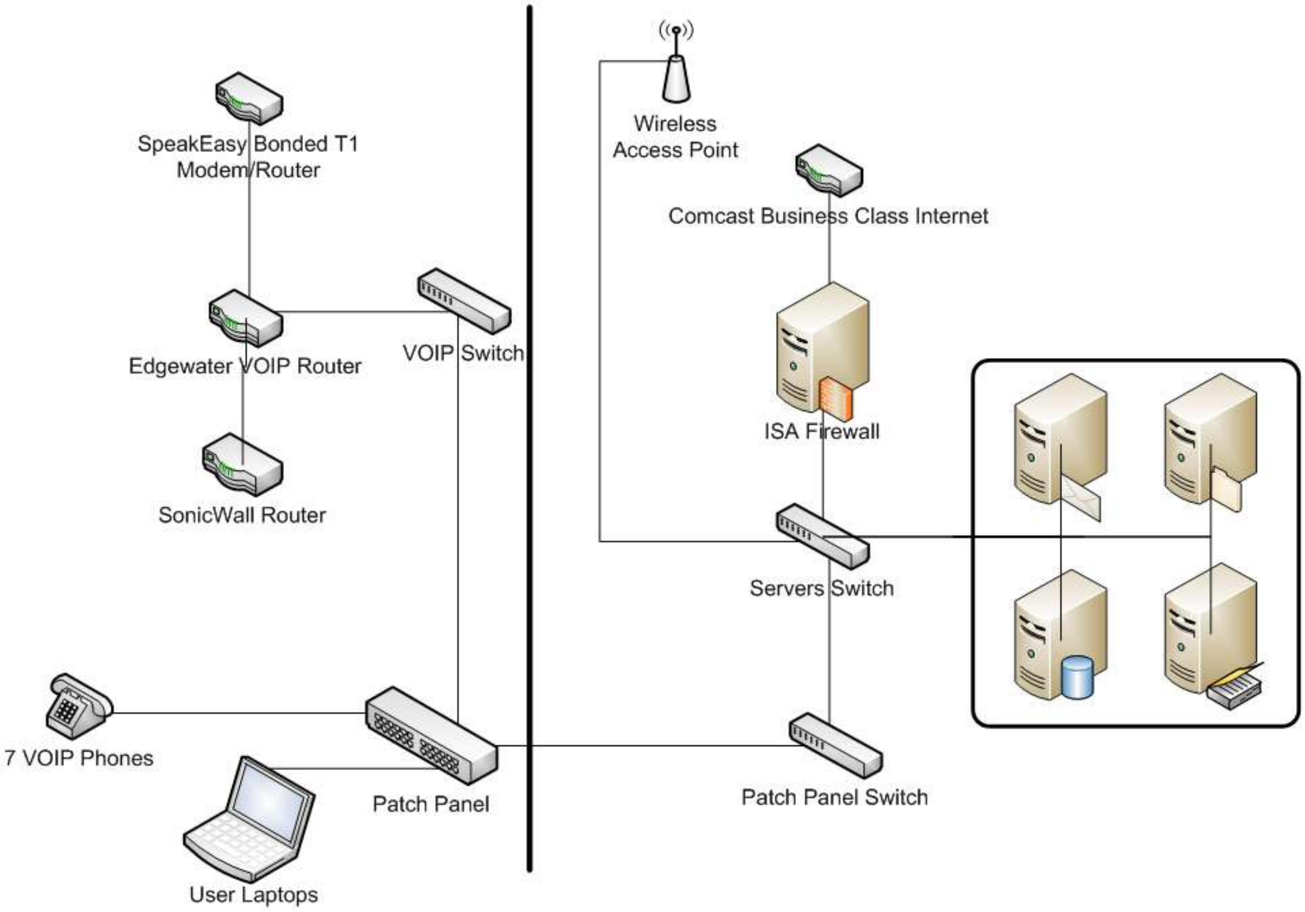


Illustration 1: Our notional organization's logical computer network

Our existing network landscape includes voice and data support, multiple Internet Service Provider (ISP) lines, application-level gateways[vi] providing firewall support,[vii] back-end Web servers providing corporate presence and internal collaboration, a segmented architecture that segregates network servers from end-users, and support for guest access via wireless connectivity. In conformance with general enterprise information security architecture principles, our notional network must not impede information flow or affect the company's productivity.[viii]

3.3 Physical Layout

Due to our notional organization's small size and the constraints we have on its overhead positions, we have designed the physical local area network (LAN) with centralization and minimal administrative cost in mind. The diagram below shows this physical layout; as can be seen, the primary rack uses the most common LAN configuration: the *star-wired bus* (all servers are connected to a single switch).[ix] We provide uninterrupted power from a separate dedicated rack, and we provide external links through one of two ISP providers via cable modem.

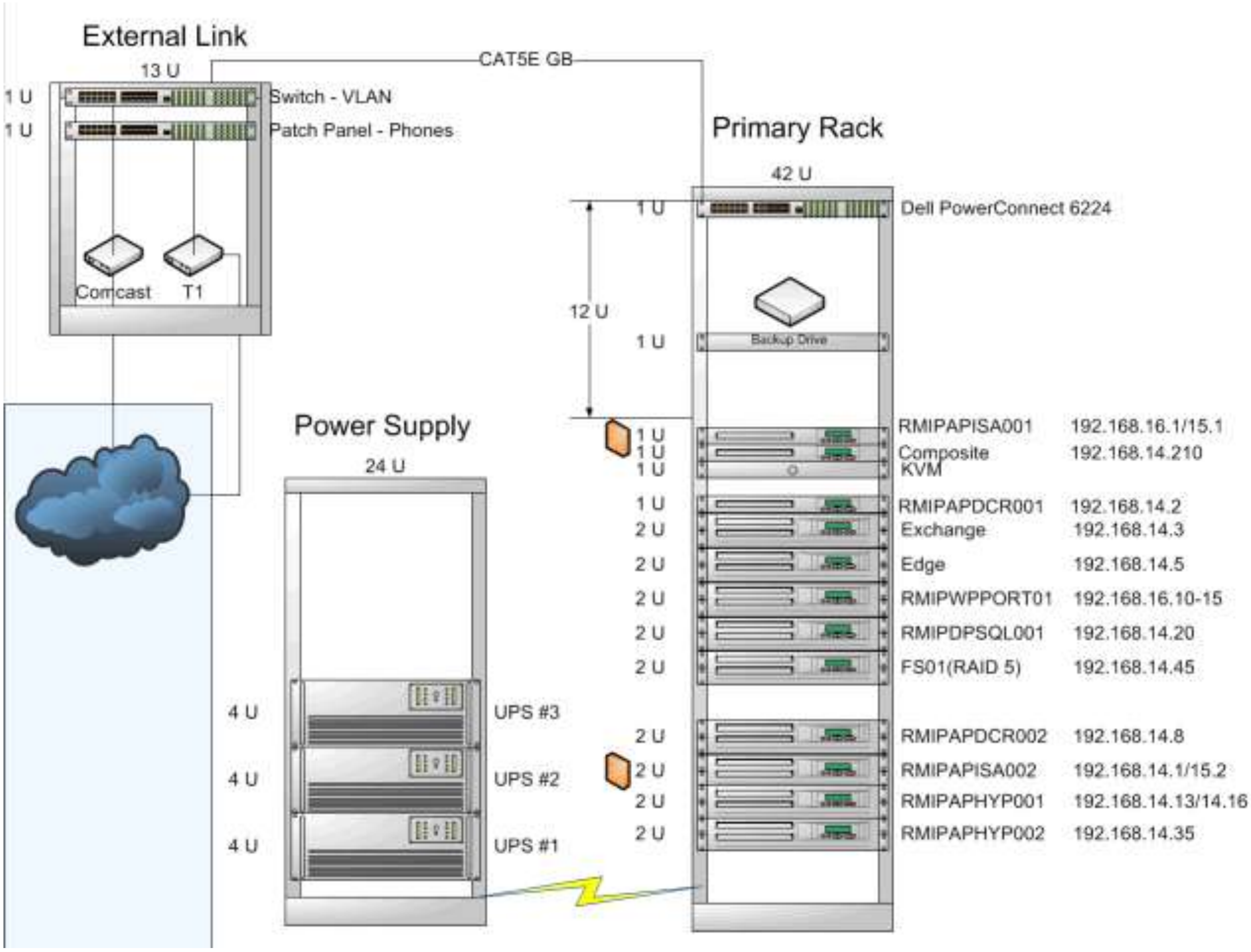

External Link
13 U
1 U
1 U
Switch - VLAN
Patch Panel - Phones
Comcast
T1
CAT5E GB
Primary Rack
42 U
1 U
Dell PowerConnect 6224
12 U
1 U
Backup Drive
1 U
1 U
1 U
RMIPAPISA001 192.168.16.1/15.1
Composite 192.168.14.210
KVM
1 U RMIPAPDCR001 192.168.14.2
2 U Exchange 192.168.14.3
2 U Edge 192.168.14.5
2 U RMIPWPPORT01 192.168.16.10-15
2 U RMIPDPSQL001 192.168.14.20
2 U FS01(RAID 5) 192.168.14.45
2 U RMIPAPDCR002 192.168.14.8
2 U RMIPAPISA002 192.168.14.1/15.2
2 U RMIPAPHYP001 192.168.14.13/14.16
2 U RMIPAPHYP002 192.168.14.35
Power Supply
24 U
4 U UPS #3
4 U UPS #2
4 U UPS #1

Illustration 2: Our notional organization's physical computer stack

This design consciously accepts certain risks. For example, the primary rack is connected to the external link by a single set of high-capacity network cables (the CAT5E GB cables above)[x] via the virtual LAN (VLAN) switch. Obviously, if either the cables or the switch fail, we effectively lose our entire network communications. However, the risk is justified based on our notional organization's need to minimize overhead (there's only a single cable to check if a network problem is detected). Additionally, by using two cables instead of one, we effectively reduce the risk of failure by half. This type of decision-making repeats itself throughout the network infrastructure as we attempt to balance competing pressures to find the the best possible value (overhead cost vs. required reliability vs. ease of maintenance).

4.0 Defensive Posture

Our notional corporate network applies defense-in-depth[xi] by using a variety of protective measures:

- Redundancy (both hardware and data).
- Logical network segmentation to help prevent unauthorized access.
- Proactive network protection via firewalls, VPN,[xii] anti-virus, and intrusion detection / prevention.
- Operating system compliance, including regularly scheduled patch applications.

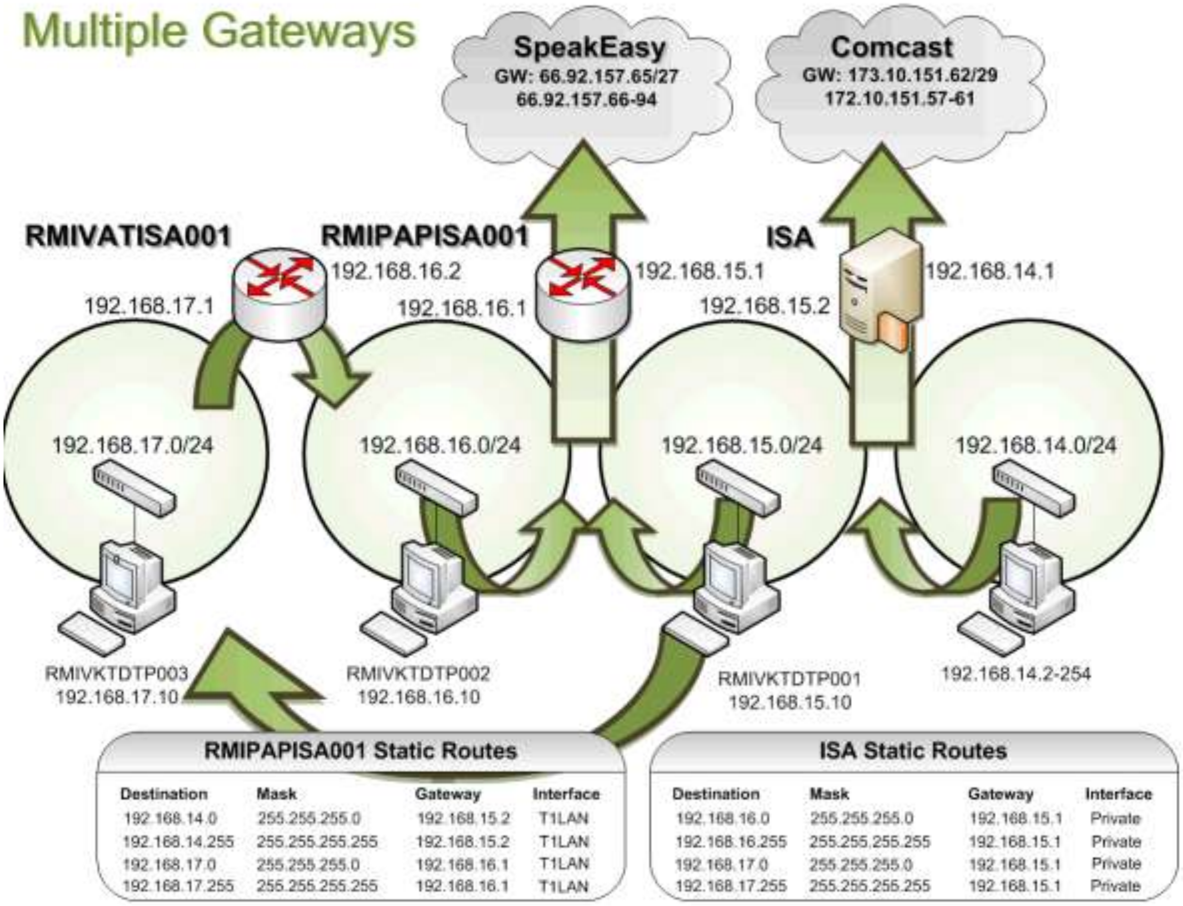
4.1 Redundancy

The first line of defense guards against both physical failure (e.g. a disk crash) and logical failure (e.g. an infected system) by providing redundancy. These defenses include:

1. Using fault-tolerant disk storage such as RAID 1[xiii] (mirroring between two disks, the most expensive overall but easiest to setup) or RAID 5 (data striping at the block level over multiple disks with distributed parity; less expensive but harder to setup). In our notional setup, both approaches allow us to replace a failed disk without powering down the server and without losing any data. However, let's consider that in our notional environment we do not using RAID for *all* physical servers and are therefore at risk of disk crashes. (Haven't we all personally experienced this problem?)
2. Some critical servers have two power supplies, each of which is connected to a separate UPS[xiv] device. In the event of power supply failure, this approach protects the servers against unexpected crashes and allows us to replace the failed power supply without powering down the server. However, let's assume that this approach is not used for all servers.
3. We've designed a high-capacity external disk for data backups, and we suggest that detailed recovery instructions for many of systems. While this is an excellent start, is this enough storage capacity to maintain full monthly backups for five years as best practices suggest?[xv]

4.2 Logical Network Segmentation

As Lai and Dai point out, for “sensitive systems...segregation in networks should be employed”[xvi] in order to prevent unauthorized access. We use our network switches to implement virtual LANs (VLANs);[xvii] these VLANs allow us to separate the higher-risk wireless guest access network from internal protected network servers. Also, this approach allows us to maximize our notional network throughput by having critical servers configured to use the higher-quality leased line (the T1[xviii] connection from the network drawing) instead of the less-expensive Comcast connection. The drawing below shows our notional segmentation architecture:



RMIPAPISA001 Static Routes

Destination	Mask	Gateway	Interface
192.168.14.0	255.255.255.0	192.168.15.2	T1LAN
192.168.14.255	255.255.255.255	192.168.15.2	T1LAN
192.168.17.0	255.255.255.0	192.168.16.1	T1LAN
192.168.17.255	255.255.255.255	192.168.16.1	T1LAN

ISA Static Routes

Destination	Mask	Gateway	Interface
192.168.16.0	255.255.255.0	192.168.15.1	Private
192.168.16.255	255.255.255.255	192.168.15.1	Private
192.168.17.0	255.255.255.0	192.168.15.1	Private
192.168.17.255	255.255.255.255	192.168.15.1	Private

Illustration 3: A segmented network architecture with gateways and VLANs

While the above is a strong start, it does not fully account for all weaknesses. For example, an individual corporate server must still be tied to a specific gateway. As many have found to their chagrin, it is quite possible for one (or both) of the Internet service providers (ISPs) to have an outage. The current design requires manual intervention to switch the server to the other ISP. Thus, this violates our notional organization's primary need for automation and reliability.

4.3 Proactive Network Protection

Our notional network uses a number of protective defensive layers, including:

1. Invested in commercial application-level firewalls and anti-virus for network edge connections. Each firewall scans inbound as well as selected outbound network messages thoroughly for problems (such as Web-based buffer overflow attacks), while the anti-virus uses signature- and behavior-based algorithms to detect harmful activity on individual host computers. As part of the corporate domain security policy, our notional infrastructure ensures that each member computer (including all corporate servers like the email and Web servers) use both the corporate anti-virus as well as the built-in operating-system provided firewall. Member computers must meet these requirements to use this network.

2. The corporate VPN (virtual private network) allows external access to trusted team members and partners by using the organization's public key infrastructure (PKI). Remote access to the network requires that the client receive (from us!) a special keypair for Layer 2 Tunneling Protocol / Internet Protocol Security connectivity (L2TP/IPsec). The VPN server allows connections only from clients with this valid keypair.

3. At the hardware level (specifically, the Data Link Layer or Layer 2 from the OSI model),[xix] our notional network implements packet filtering within the network switches. This protection is of limited use because it can check only the IP address and port number of each data packet, but it is an easy way to limit network traffic to known protocols.

What is lacking in the above are automated responses when dangerous situations occur. For example, if the anti-virus detects a security breach within a production Web server, manual intervention must occur for the network administrators to remediate the situation (such as restoring the server from a verified backup). Such manual intervention is costly, error-prone, and can result in downtime that may affect Service Level Agreements (SLAs) with our notional organization's customers; for an organization's security breach response to be effective it must be automated!

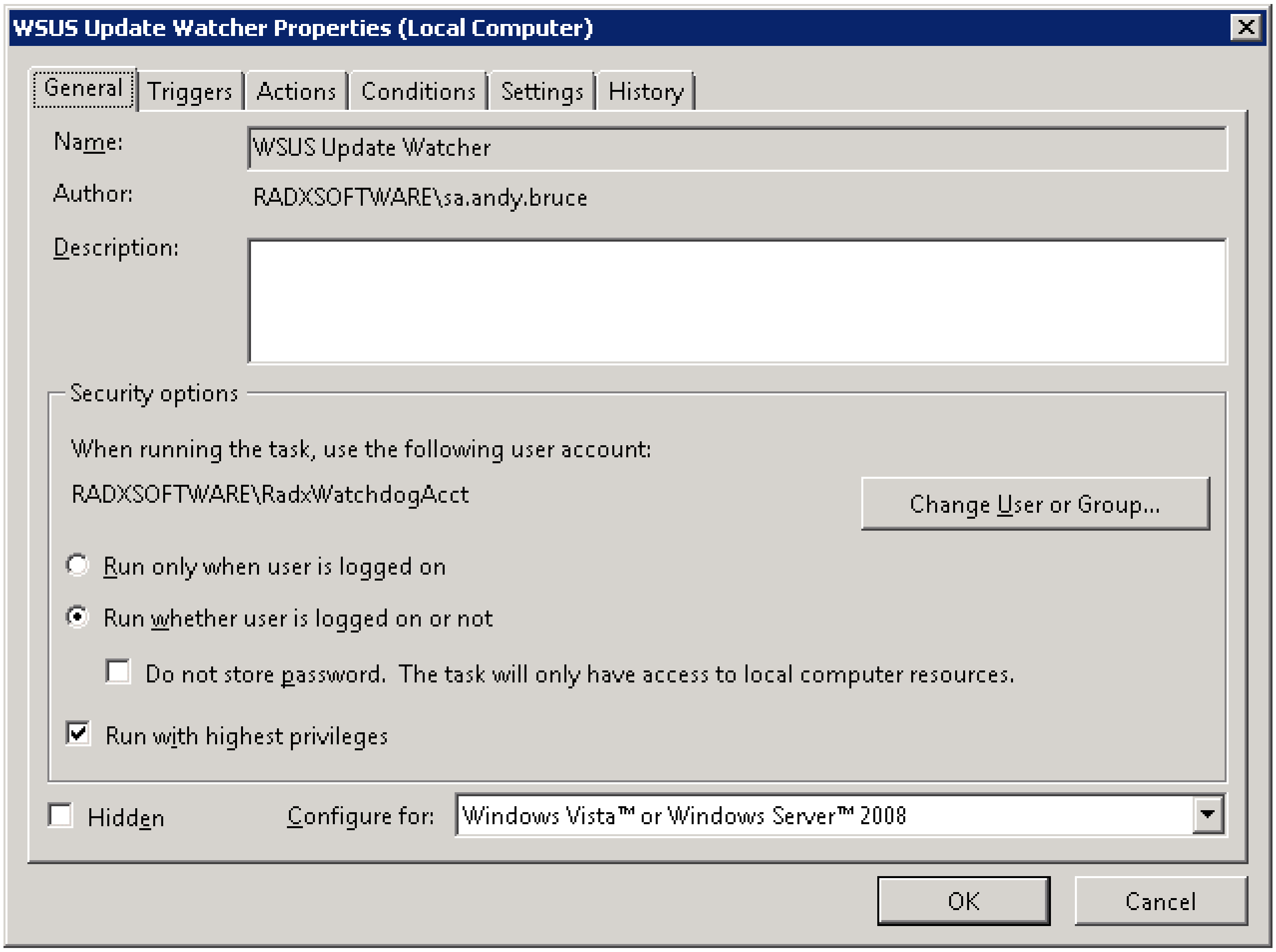
4.4 Operating Systems

Within our notional network, we assume standardized variants of the Microsoft systems, from XP Professional up through Windows 7. However, let's acknowledge that additional platforms such as RedHat Enterprise Linux (RHEL) must be hosted in support of customers. As the 2010 Black Hat Forum points out, each of these operating system platforms is made up of insecure software that we must protect against.[xx]

This is where virtualization comes into play. Initially, we can use a virtualization manager (Microsoft Hyper-V) to assist with provisioning new servers. Hyper-V allows our notional organization to create base images and to use these images as “templates” for new systems (both virtual and physical). For any organization doing work for DoD and per NIST SP 800-123, the network administrators should typically build servers using the highly-secured Army Golden Master baseline (AGM).[xxi] This provides the assurance that our notional customers require to know that the systems we build are strong from the beginning.

We ensure continued security compliance by applying the managed patching process from NIST SP 800-123 (document the process, identify / evaluate patches and map to vulnerabilities, install patches).[xxii] Specifically, we combine the built-in Windows Update Service with an in-house solution. As SP 800-123 points out, patches can be dangerous to apply to production servers because they occasionally result in side effects.[xxiii] We therefore use Windows Update in “Download Only but Do Not Install” mode and use our custom solution to detect changes. As seen below, our custom system consists of three pieces.

1. On each server to be monitored, a nightly task runs and uses WMI (Windows Management Instrumentation) for checking for software updates.



WSUS Update Watcher Properties (Local Computer)

Name: WSUS Update Watcher

Author: RADXSOFTWARE\sa.andy.bruce

Description:

Security options

When running the task, use the following user account:

RADXSOFTWARE\RadxWatchdogAcct

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

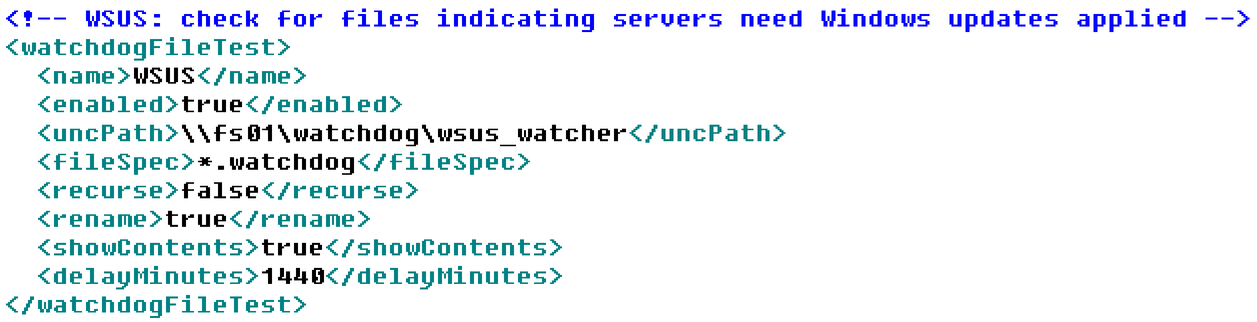
☑ Run with highest privileges

□ Hidden

Configure for: Windows Vista™ or Windows Server™ 2008

Illustration 4: Nightly job for running operating system patch checker

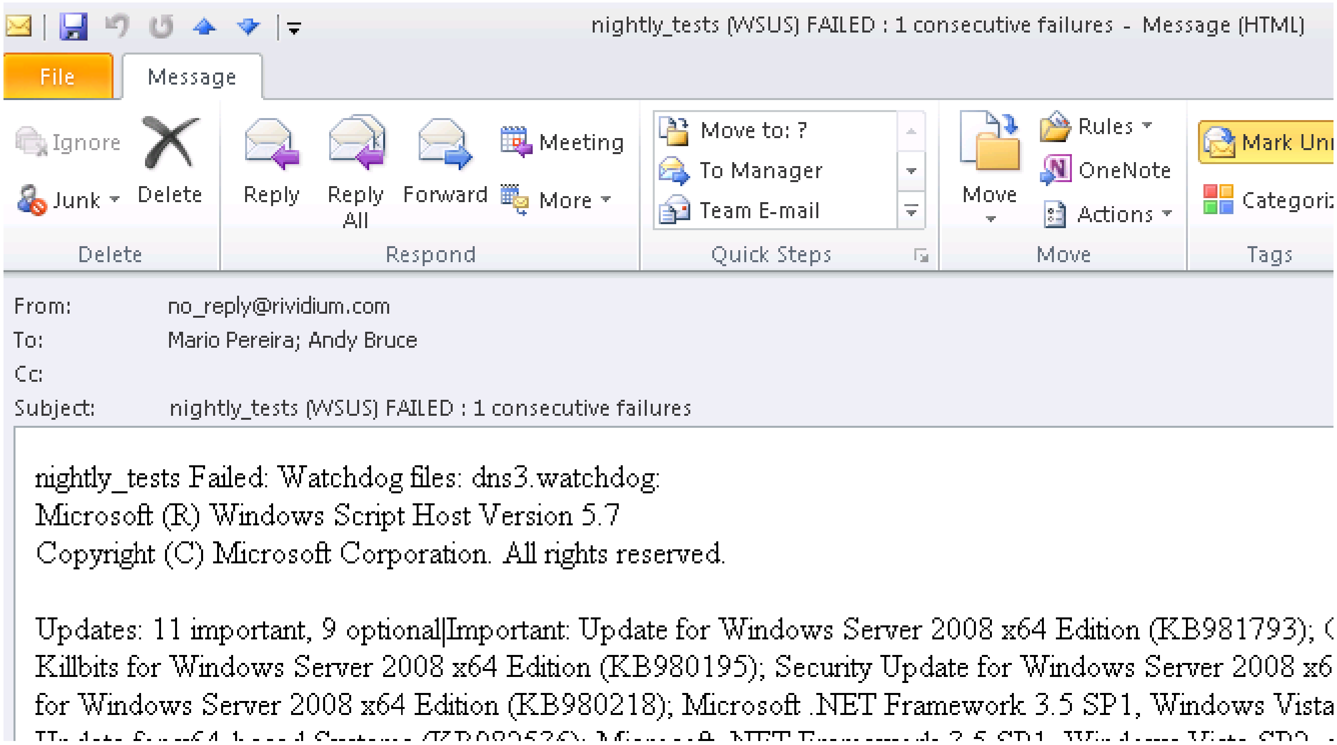
2. On **one** server (we chose our corporate anti-virus server), a master service runs a nightly check that scans a shared directory for any out-of-date patches:



```
<!-- WSUS: check for files indicating servers need Windows updates applied -->
<watchdogFileTest>
  <name>WSUS</name>
  <enabled>true</enabled>
  <uncPath>\\fs01\watchdog\wsus_watcher</uncPath>
  <fileSpec>*.watchdog</fileSpec>
  <recurse>false</recurse>
  <rename>true</rename>
  <showContents>true</showContents>
  <delayMinutes>1440</delayMinutes>
</watchdogFileTest>
```

Illustration 5: Data file defining a test for required critical OS patches

3. System administrators receive notification about required updates:



nightly_tests (WSUS) FAILED : 1 consecutive failures - Message (HTML)

From: no_reply@rividium.com
To: Mario Pereira; Andy Bruce
Cc:
Subject: nightly_tests (WSUS) FAILED : 1 consecutive failures

nightly_tests Failed: Watchdog files: dns3.watchdog:
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Updates: 11 important, 9 optional|Important: Update for Windows Server 2008 x64 Edition (KB981793); (
Killbits for Windows Server 2008 x64 Edition (KB980195); Security Update for Windows Server 2008 x6
for Windows Server 2008 x64 Edition (KB980218); Microsoft .NET Framework 3.5 SP1, Windows Vista

Illustration 6: Email notification for a missing OS patch

The above process and checks are good, but not sufficient. It does not properly account for non-Windows operating systems, and the proprietary system requires maintenance as new servers are added to the stack.

5.0 Recommendations

Given our notional organization's small size and resource constraints, we highlight specific recommendations both for the physical and logical network layers.

5.1 Physical Servers

Two efforts will decrease manual operations overhead at a minimum cost:

1. *Use at least RAID 1 for all servers* – In the notional diagram above, we use RAID to protect ourselves from disk crashes only for certain servers. Available for less than $100 each,[xxiv] one can install an additional disk drive for each physical server. Perhaps this was not done in the past because a classic "hardware RAID" requires a rebuild of the entire server. However, by using "software RAID" we can avoid that expense.[xxv] While software RAID is less efficient, our primary goal of reliability over maximum efficiency makes this a better solution. Also, software RAID has few if any risks associated with it.
2. *Redundant power supplies* – For each physical server, we need two power supplies. At a cost of around $100 per server,[xxvi] we can add a second power supply (powered from a separate battery) that protects us from this type of equipment failure.

5.2 Logical Protection

1. *Anti-virus automated response* – Our existing corporate anti-virus software can identify malicious activity but can take no action other than sending email. For approximately two weeks worth of effort, we can leverage the built-in automated response capabilities in our existing package to define custom actions.[xxvii] For example, upon detection of malware activity on an end-user's box, outbound network connectivity can be suspended and a message displayed to the user with instructions and help desk contact information.
2. *Replacement of Windows Update package.* Our current in-house Windows Update solution requires periodic maintenance to account for Windows changes as well as manual integration as we add new servers to our network. Also, it does **not account for non-Windows systems.** By investing in a commercial product, we can alleviate both of those concerns.[xxviii]

By implementing these low-cost and highly effective solutions, we can continue to provide the availability, integrity, and confidentiality that our customers and partners demand while keeping overhead costs low.

Reference List and End-notes

End-notes immediately follow this section.

Bosworth, Seymour, M.E. Kabay, Eric Whyne, eds., *Computer Security Handbook: Volume 1, 4th ed.* Hoboken, NJ: John Wiley & Sons, Inc., 2009.

Gartner Corp. "Gartner Identifies the Top 10 Strategic Technologies for 2010." Gartner Corp. press release, October 20, 2010. Gartner Corp. Web site. http://www.gartner.com/it/page.jsp?id=1210613 (accessed: September 15, 2010).

Harris, Shon. *CISSP All-in-One (AIO), 4th ed*. New York: McGraw-Hill, 2007.

Howe, Denis. *Dictionary.com*. http://dictionary.reference.com/browse/sine+qua+non (accessed: September 20, 2010).

Lai, Yeu-Pong and Ruan-Han Dai. "The implementation guidance for practicing network isolation by referring to ISO-17799 standard." *Computer Standards & Interfaces* 31 (2009).

Microsoft Press, "Overview of Disk Management," *Microsoft Technet*, http://technet.microsoft.com/en-us/library/dd163558.aspx.

Pfleeger, Charles P., Shari Lawrence Pfleeger. *Security in Computing, 3rd ed*. (Upper Saddle River, NJ: Prentice Hall, 2003).

Scarfone, Karen, Wayne Jensen, and Miles Tracy. "Guide to General Server Security." *NIST Special Publication 800-123* (July, 2008). National Institute of Standards and Technology, available online at http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf (accessed: September 12, 2010).

Stephenson, Peter R., ed. Information Security Essentials: Section 2. Auerbach Publishing, ISBN 978-1-4398-0030-0, 2009.

Worthington, David. "Black Hat forum exposes software security issues." *SD Times*. August 15, 2010.

[i] Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing*, 3rd ed. (Upper Saddle River, NJ: Prentice Hall, 2003), pg. 10. Dr. Pfleeger is widely credited with the first mention of the term CIA Triad in his first edition of this book (same publisher, dated 1989).

[ii] "Gartner Identifies the Top 10 Strategic Technologies for 2010," Gartner Corp. press release, October 20, 2010, on the Gartner Corp. Web site, http://www.gartner.com/it/page.jsp?id=1210613 (accessed: September 15, 2010).

[iii] Sine qua non, "Dictionary.com," *The Free On-line Dictionary of Computing*, Denis Howe, http://dictionary.reference.com/browse/sine+qua+non (accessed: September 20, 2010). Definition: "an indispensable condition, element, or factor; something essential."

[iv] Seymour Bosworth, M.E. Kabay, Eric Whyne, eds., "Chapter 1: Brief History and Mission of Information System Security," *Computer Security Handbook: Volume 1*, 4th ed. (Hoboken, NJ: John Wiley & Sons, Inc., 2009), pg. 50. Even the original ARPANET (Advanced Research Projects Agency Network) in 1969 had as a primary business driver to "increase productivity through resource sharing."

v Interview with Chief Network Engineer, September 17, 2010.

vi Bosworth et. al., *CSH,* "Chapter 5: Data Communications and Information Security," pg. 155. The older term *gateway* here has the same meaning as *router*: a device connecting individual networks together and allowing information to be passed ("routed") between the networks.

vii Ibid., "Chapter 26: Gateway Security Devices," pg. 734. An *application-level firewall* extends upon simple Layer 2 (port number filter) or Layer 3 (destination address filter) firewalls. An application-level firewall allows network messages to be fully "unwrapped" so that the entire data payload can be analyzed – including the application-specific commands contained within the payload. For example, a Layer 2 firewall might block all traffic on well-known port 23 (Telnet) but allow all traffic on well-known port 80 (HTTP). Thus, any vulnerabilities in the HTTP protocol can be attacked even with the Layer 2 firewall in place. An application-level firewall, however, can examine individual data packets on the allowed HTTP port to scan for malicious data (such as malformed Uniform Resource Locators or URLs) that exploit known vulnerabilities in the backing Web server. Thus, application-level firewalls provide a significantly finer grain of attack detection.

viii Peter R. Stephenson, ed. *Information Security Essentials: Section 2* (Auerbach Publishing, ISBN 978-1-4398-0030-0, 2009), pg. 6. Retrieved on September 21, 2010 from https://norwich.angellearning.com/AngelUploads/Content/MSIA_2_0/_assoc/msia_s2/msia_s2_readings/ise_section_2.pdf. This reading captures best practices for applying an enterprise security architecture to an organization, which certainly includes network security.

ix Bosworth et. al., *CSH,* "Chapter 6: LAN Topology," pg. 182. In our organization's case, our central switch in our primary server rack contains a bus connecting input / output ports such that when one station transmits a message, all stations receive that message. The term used in the text is "physical star, logical bus."

x In our shop, we use a CAT5E-rated RJ-45 cable that allows transmission speeds of up to 1Gbps ("Fast Ethernet," one gigabit per second). RJ-45 is the most common type of network cable connection and uses four "twisted-pair" wires to transfer data. Numerous resources exist online describing network cabling in general and Ethernet cabling in particular (as opposed to IBM Token Ring, for example). One not-for-profit resource with a very quick introduction to this topic can be found at http://www.ertyu.org/steven_nikkel/ethernetcables.html.

xi Stephenson, *ISE Section 2*, pg. 11. Defense-in-depth provides a layered approach to deter and delay attacks (perfect security is not possible; given sufficient time and resources a determined attack can always defeat an established defense). Defense-in-depth ensures that even if an outer layer is penetrated, additional layers stand in the way of an attacker. Key to any defense-in-depth approach is for the organization to define an overarching and high-level Security Policy that identifies and guides the more specific defenses applied at lower levels.

xii Bosworth et. al., *CSH,* "Chapter 32: Virtual Private Networks and Secure Remote Access," pg. 890. A VPN allows secure remote access from a client to the organization's network.

xiii Ibid., "Chapter 57: Data Backups and Archives," pg. 1501. RAID stands for "Redundant Array of Independent Disks" (formerly "Redundant Array of Inexpensive Disks"). Different RAID levels provide different levels of data assurance; RAID 0 (disk striping) provides improved performance and low cost but no data integrity, RAID 1 (mirroring) is the most expensive option but provides very high availability and cost, while RAID 5 (redundant disk striping with distributed parity) provides a reasonable balance between the two.

xiv Ibid., "Chapter 23: Protecting the Information Infrastructure," pg. 672. An uninterruptible *power supply (UPS) provides backup battery power for devices.* Most UPS devices also provide protection against power surges and sags and can help to ensure a conditioned input voltage for the protected device. UPS devices come in three flavors: activation upon failure (least expensive; battery kicks in when power loss is detected); always online (battery is always available); and battery-driven (power is *always* provided from the battery, in normal use the batteries are constantly drawing and recharging from the power source).

xv Ibid., "Chapter 57: Data Backups and Archives," pg. 1514. End-of-month backups should be maintained for a full five years, and end-of-year backups should be maintained for ten years.

xvi Yeu-Pong Lai and Ruan-Han Dai, "The implementation guidance for practicing network isolation by referring to ISO-17799 standard," *Computer Standards & Interfaces* 31 (2009), pg. 753.

xvii Shon Harris, "Telecommunications and Network Security," *CISSP All-in-One (AIO), 4th ed.*, (New York: McGraw-Hill, 2007), pg. 544. Ms. Harris, of course, is always ready with a quip and a definition. She does, however, provide a good overview of how VLANs allow system administrators to separate groups of computers based on business needs rather than physical proximity. This allows administrators to apply independent security policies to individual computer sets.

xviii Bosworth et. al., *CSH,* "Chapter 6: Network Topologies, Protocols, and Design," pg. 203. A *T1* line provides 1.544 Mbps connectivity over a *leased-line* (a dedicated connection between the service provider and the consumer). Because of housekeeping overhead associated with this direct connection, only 1.536 Mbps is actually available for use. However, a T1 connection generally provides extremely reliable and high-speed connectivity.

xix Pfleeger, *Security in Computing*, pg. 373. The seven layers of the TCP/IP model are actually defined in the International Organization of Standards' source document *ISO Publication 7498-2: 1989*.

xx David Worthington, "Black Hat forum exposes software security issues," *SD Times*, August 15, 2010.

xxi Karen Scarfone, Wayne Jensen, and Miles Tracy, "Guide to General Server Security," *NIST Special Publication 800-123* (July, 2008), National Institute of Standards and Technology, pg. 26, available online at http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf (accessed: September 12, 2010).

xxii Ibid., pg. 25.

xxiii Ibid., pg. 26.

xxiv eBay Corporation, "Add 500GB SATA Hard Drive Dell PowerEdge 2950 purchase," http://cgi.ebay.com/Add-500GB-SATA-Hard-Drive-Dell-PowerEdge-2950-purchase-/370419143805 (accessed: September 23, 2010).

xxv Microsoft Press, "Overview of Disk Management," *Microsoft Technet*, http://technet.microsoft.com/en-us/library/dd163558.aspx. This overview includes Windows Server 2008 instructions, making it very useful for us.

xxvi TXcess Surplus Corporation, "NEW, Dell 750 Watt Power Supply for PowerEdge 2950 Systems," http://www.txcesssurplus.com/servlet/the-4442/NEW-Dell-Y8132-PowerEdge/Detail (accessed: September 23, 2010).

xxvii Symantec Corporation, "Data Sheet: Virus Protection and Endpoint Security," available online at http://eval.symantec.com/mktginfo/enterprise/fact_sheets/b-datasheet_antivirus_ce_3-2009_11280731-1.en-us.pdf (accessed: September 23, 2010).

xxviii Lumension Corporation, "PatchLink Update 4.0 White Paper," http://www.contegosecurity.com/docs/PatchLink.pdf (accessed: September 23, 2010). PatchLink provides a cross-platform operating system patch solution featuring proactive notification of critical updates to system administrators.