Rividium Whites - White papers on leading edge technologies

Network Perimeter Security

For a Small Network

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

26 October 2010

Topic Summary: For a notional small corporate network, identify:

- Security zones
- Perimeter architecture and defenses
- Guest access

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 “typical” notional small network and how it should implement perimeter security. Brussin and Opatrny identify an organization’s network devices and firewalls as “combin[ing] to form a least privilege gateway” which keeps traffic moving “only in expected and intended ways.”[1] For our notional network, this traffic includes data from internal users, guests, public-facing Web servers, and highly-protected application servers – all of which combine to support our notional organization’s business requirements, and each of which requires protection. In this paper we look at our notional organization’s network components from servers to thin clients and their *security perimeters*. We review these perimeters with an eye towards improving the organization’s overall security posture, and we make targeted recommendations that minimize acquisition and maintenance costs.

2.0 Background

In most small companies, the physical layout includes at least the following “security zones:”

- *public* – the organization’s “face” to the world (reception via secure entry)
- *protected* – the organization’s proprietary information (locked access requiring entry codes or a key – think a corporate safe)
- *internal* – employee workspaces (bullpen – normally an open or thinly partitioned area)
- *guest* – provides an area for visitors to be entertained (think the “nice” executive conference room)

Not coincidentally, many logical corporate networks are built to reflect and support that rather simplistic model. Adding to this simple network design is the fact that in most cases an organization will standardize on some single operating system (in this paper we’ll assume the ubiquitous Windows environment, but of course it could be anything). Given these typical constraints and notional logical network setup, we look at some common effects on the organization’s network security perimeter.

3.0 Network Diagram

The following diagram shows a simple but reasonable network diagram for our notional organization.

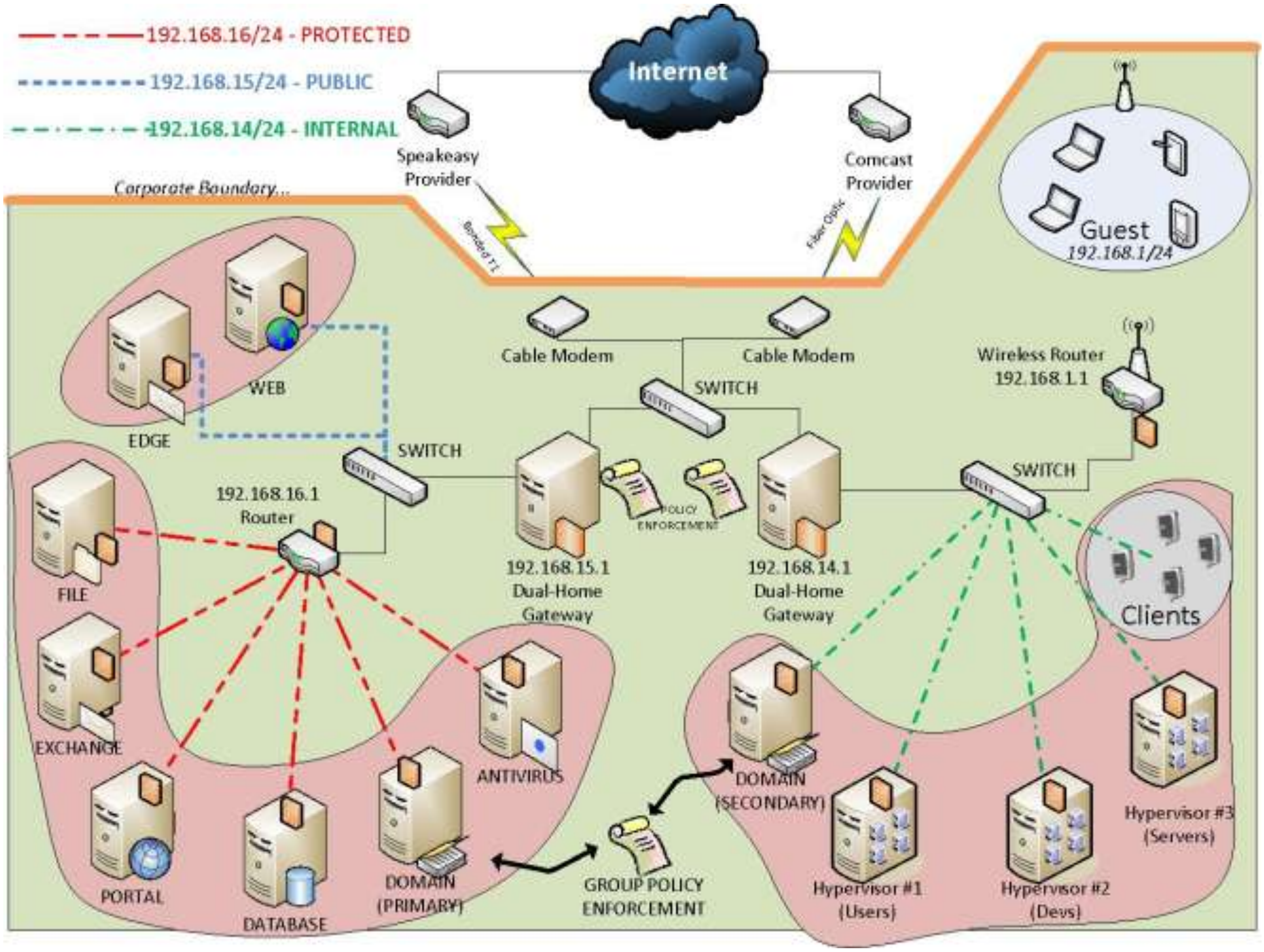


Figure 1 - Our notional corporate network's security zones

This notional corporate network defines four primary areas that map more-or-less to the standard four physical security zones identified above:

- *192.168.16/24* – A protected network containing file and database servers, an internal Exchange server, corporate antivirus, and the organization’s intranet portal.
- *192.168.15/24* – A DMZ (demilitarized zone) containing a public Web server and the organization’s public SMTP server for receiving email.
- *192.168.14/24* – An internal network containing primarily workstations and thin clients, although some development servers and our hypervisors can be found here in our notional display.
- *192.168.1/24* – A wireless network for guests and mobile devices.

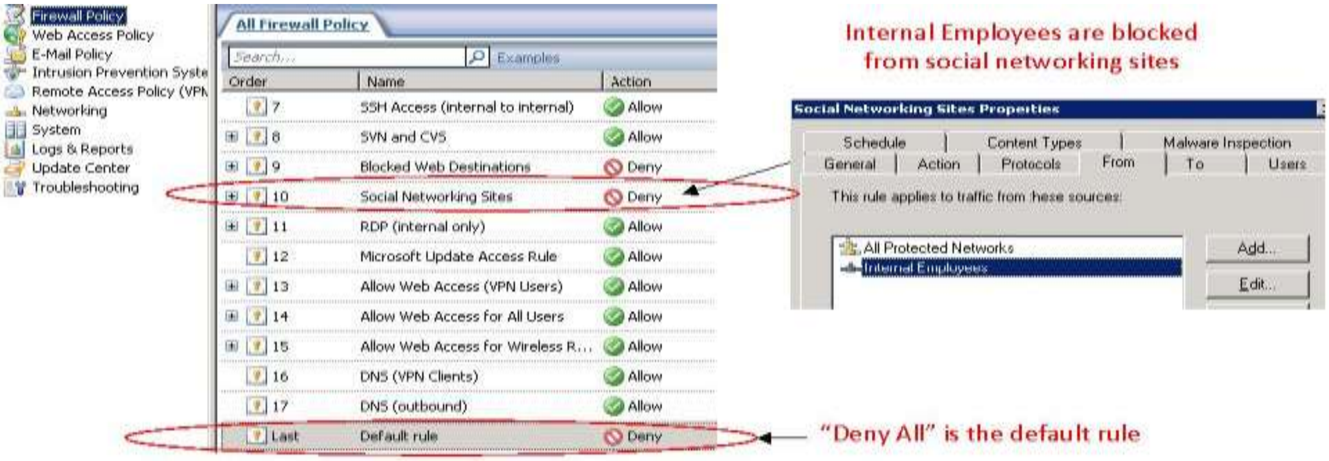
4.0 Perimeter Defenses

Each element in our notional organization's layered network defense strategy surrounds individual hosts much like an onion skin does – the closer one gets to a host the more perimeter layers one must have traversed. Consider a malicious application within the "guest" subnet: it must cross four different gateways (and the same number of firewalls) for even one data packet to be presented to the protected file server – which itself is hardened with *at least* three more perimeter defenses (host firewall, anti-malware solutions, and operating-system level access control lists).

4.1 Application Gateway

Our notional organization has at its outermost perimeter two physical Internet connections for two dual-homed application gateways. (While we realize that this is somewhat unusual – many companies use a single public Internet access point – the fact is that most small companies are already paying for a dedicated T1 line for Voice-over-IP [VoIP] for their telephones. Our drawing simply leverages that fact.) Each application gateway provides three supporting functions for our notional organization's network perimeter:

1. **Network Boundary Enforcement** – The gateways divide the organization's corporate network into two basic segments: servers and workstations. The servers' side includes the "protected" subnet and the DMZ, while the workstations' side includes the "internal" and "guest" subnets. The gateways allow controlled communications between the segments.
2. **Access Policy** – Hoefelmeyer and Phillips point out that the "first step" in overall security defense is a "security policy addressing the threat,"[2] and in this case we show below Internet access based on *default-deny*. For example, the workstations' side can deny access to social networking sites:



Order	Name	Action
7	SSH Access (internal to internal)	Allow
8	SVN and CVS	Allow
9	Blocked Web Destinations	Deny
10	Social Networking Sites	Deny
11	RDP (internal only)	Allow
12	Microsoft Update Access Rule	Allow
13	Allow Web Access (VPN Users)	Allow
14	Allow Web Access for All Users	Allow
15	Allow Web Access for Wireless R...	Allow
16	DNS (VPN Clients)	Allow
17	DNS (outbound)	Allow
Last	Default rule	Deny

Internal Employees are blocked from social networking sites

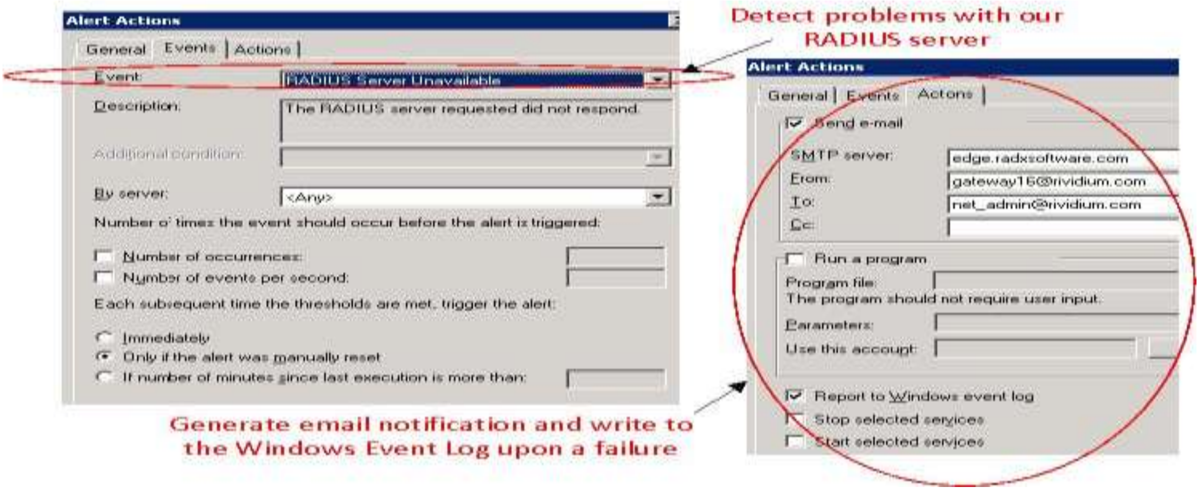
This rule applies to traffic from :hese sources:

All Protected Networks
Internal Employees

"Deny All" is the default rule

Figure 2 - Our notional organization's gateway firewall policy defaults to Deny All

3. **Monitoring Functions** – Each gateway should provide an Intrusion Prevention System (IPS) featuring automatic updates for known network attack signatures. The gateways should also provide monitoring and alert functions for problem detection and notification. For example, consider the problem of wireless users and authentication: by using a RADIUS (Remote Access Dial-In User Service) server our notional organization can support stronger wireless device authentication and can report failures automatically.



Detect problems with our RADIUS server

Alert Actions

Event: RADIUS Server Unavailable

Description: The RADIUS server requested did not respond.

Additional condition:

By server: <Any>

Number o' times the event should occur before the alert is triggered:

□ Number of occurrences:
□ Number of events per second:

Each subsequent time the thresholds are met, trigger the alert:

○ Immediately
● Only if the alert was manually reset
○ If number of minutes since last execution is more than:

Alert Actions

☑ Send e-mail

SMTP server: edge.radxsoftware.com
From: gateway16@rividium.com
To: net_admin@rividium.com
Cc:

□ Run a program

Program file:
The program should not require user input.
Parameters:
Use this account:

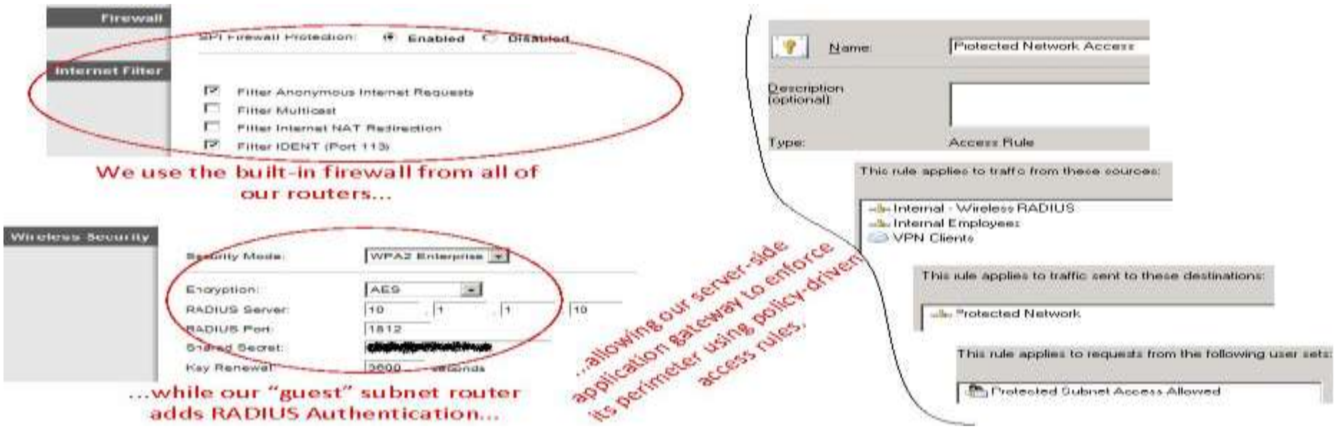
☑ Report to Windows event log
□ Stop selected services
□ Start selected services

Generate email notification and write to the Windows Event Log upon a failure

Figure 3 - Infrastructure problems generate logs and alerts

4.2 Router

Routers provide a Layer 3– the layer perimeter for any IP network – by using “store and forward” network communications. This effectively hides the IP address of each connected device via Network Address Translation (NAT) support. Even consumer-class routers include simple firewalls as well as Wi-Fi Protected Access v2 (WPA2) Enterprise to perform optional authentication of each guest user. This allows our notional organization’s team members to connect to the wireless network, authenticate using the RADIUS server, and gain access to the protected subnet – while guests cannot.



SPI Firewall Protection: ● Enabled ○ Disabled

☑ Filter Anonymous Internet Requests
□ Filter Multicast
□ Filter Internet NAT Redirection
☑ Filter IDENT (Port 113)

We use the built-in firewall from all of our routers...

Security Mode: WPA2 Enterprise
Encryption: AES
RADIUS Server: 10 . 1 . 1 . 10
RADIUS Port: 1812
Shared Secret: [redacted]
Key Renewal: 3600 seconds

...while our “guest” subnet router adds RADIUS Authentication...

...allowing our server-side application gateway to enforce its perimeter using policy-driven access rules.

Name: Protected Network Access

Description (optional):

Type: Access Rule

This rule applies to traffic from these sources:

Internal - Wireless RADIUS
Internal Employees
VPN Clients

This rule applies to traffic sent to these destinations:

Protected Network

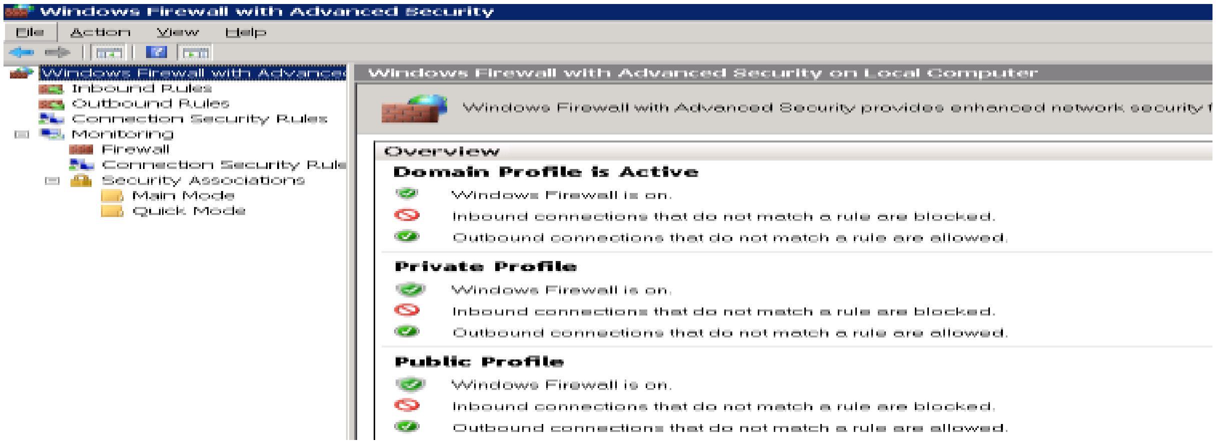
This rule applies to requests from the following user sets:

Protected Subnet Access Allowed

Figure 4 - Routers should use strongest available security

4.4 Host Firewalls

Each of our notional organization's Windows-based hosts should use *at least* the built-in firewall that ships with the operating system. While basic Windows Firewall is weak (no outbound port filtering; cannot specify a range of trusted IP addresses when enabling specific ports), it is much better than nothing. Server class machines (preferably running Windows Server 2008 R2 over Windows Server 2003) have Windows Advanced Firewall that allows quite sophisticated firewall policies to be applied based on Active Directory Group Policy settings, including separate scanning rules for packets based on their origination. Per NIST recommendations, we also recommend disabling IPv6 if not in use by the organization (and current small organizations typically have no use for the extensions that IPv6 allow).[3]



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides enhanced network security f

Overview

Domain Profile is Active

Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Private Profile

Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

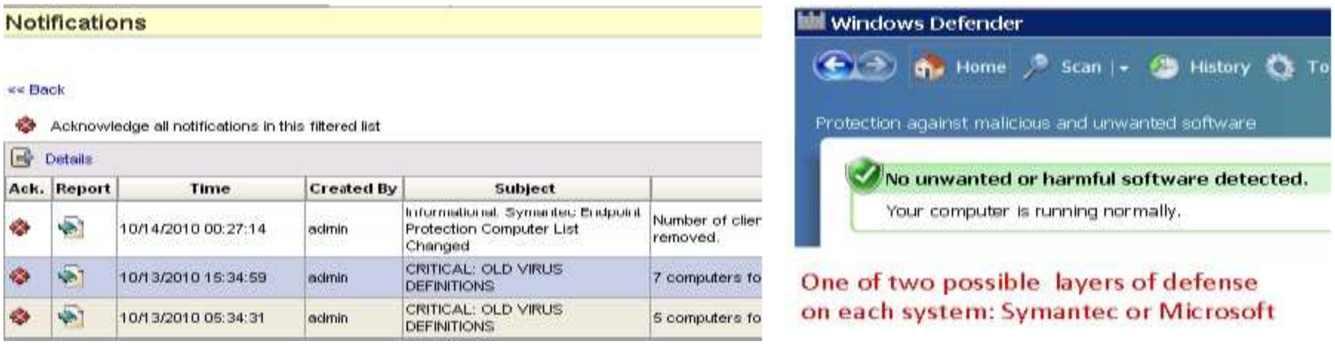
Public Profile

Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Figure 5 - All hosts should use at least the built-in firewall

4.3 Anti-malware

A key perimeter defense includes the ability to detect malicious software, whether originating from Web-based "drive-by" attacks from dangerous Web sites, or from downloaded viruses disguised as useful programs (Trojan Horses), or from infected portable media such as USB drives or compact discs. Our notional organization's standard defenses should include one of two possible solutions: a commercial product whenever possible, or Microsoft's built-in Defender application. For a commercial solution, one common choice is the Symantec product (we use that ourselves within RiVidium). The Symantec product runs from a central server within the "protected" subnet and distributes antivirus agents and virus "signature" updates to XP and laptop domain clients through the use of Active Directory Group Policies. Because it's possible that a given development server may not function with the Symantec anti-virus, smaller organizations are probably better off by installing such a solution to dedicated server hosts on a manual basis rather than automatically. In any case, it's generally much less common to provision and build a new server than to build and provision a new end-user machine, so the extra manual step for provisioning anti-virus on a server should not add appreciably to the organization's overall overhead costs.



Notifications

<< Back

Acknowledge all notifications in this filtered list

Details

Ack.	Report	Time	Created By	Subject	
		10/14/2010 00:27:14	admin	Informational: Symantec Endpoint Protection Computer List Changed	Number of clier removed.
		10/13/2010 15:34:59	admin	CRITICAL: OLD VIRUS DEFINITIONS	7 computers fo
		10/13/2010 05:34:31	admin	CRITICAL: OLD VIRUS DEFINITIONS	5 computers fo

Windows Defender

Protection against malicious and unwanted software

No unwanted or harmful software detected.

Your computer is running normally.

One of two possible layers of defense on each system: Symantec or Microsoft

Figure 6 - Hosts should use at least one layer of anti-malware software

4.5 Physical Security

The physical interface between human and host computer is a prime risk area – inserting an infected CD effectively bypasses every network firewall. One way our notional organization can defend the physical interface is by minimizing the number of physical hosts and maximizing the usage of virtual machines (VMs) within dedicated hypervisors. For example, at RiVidium our engineers and analysts typically work using a thin client instead of a physical desktop or laptop; these thin clients simply do not allow devices to be inserted – neither USBs nor CDs. For a user to install unauthorized software on a VM, that software must be copied electronically from a file share or downloaded; thus, it must run the gauntlet of every security perimeter we have created on our network. This type of control can actually improve employee morale; as Colwill points out in his well-reasoned article on the human factor in information security, "employees are reassured that the company they work for is safeguarded…this can protect jobs."[4]

Figure 7 - Thin Client

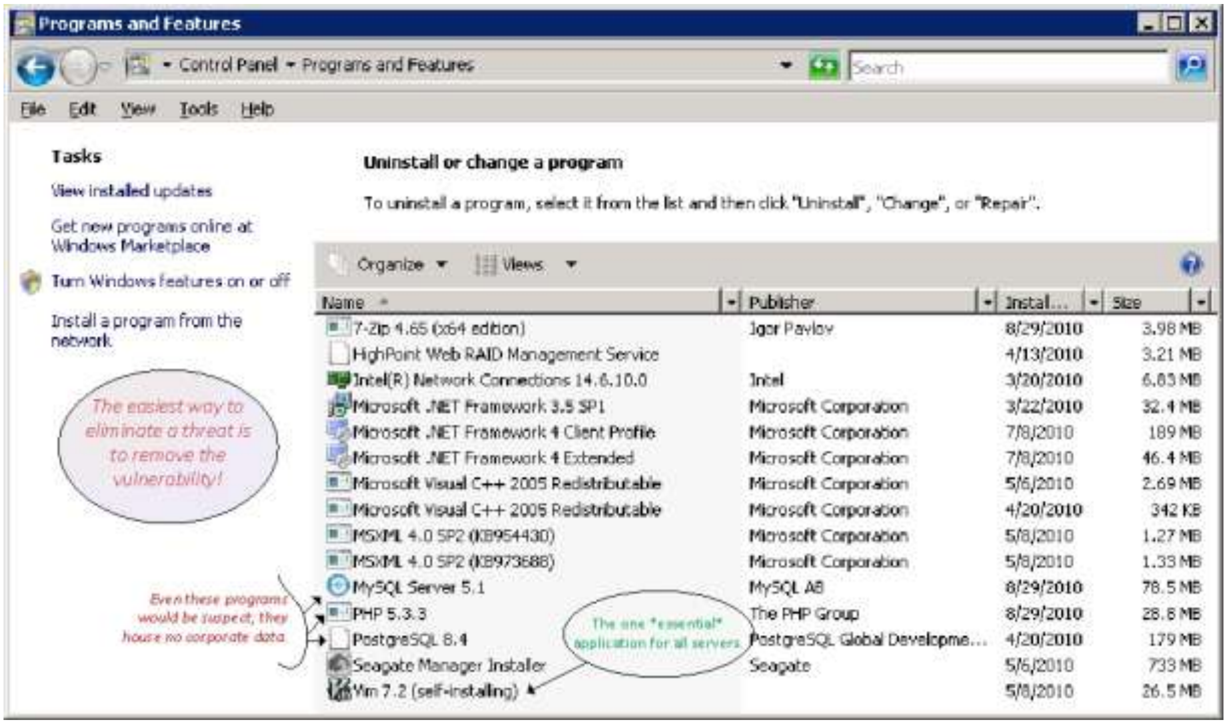
5.0 What our Perimeters Defend

NIST states that the goal of information technology security is to “enable an organization to meet all of its mission/business objectives,”[5] so a reasonable question to ask is what we are defending and how that defense supports our business drivers. In our notional organization’s case, we defend four logical security zones: *public*, *protected*, *internal*, and *guest*.

5.1 Public Network

Our notional organization’s public network defines the DMZ and allows people to access the corporate Web presence (Web site, blogs, etc.) as well as to communicate using email. In addition to the standard defenses listed above, we recommend employing a number of specific defenses on these servers:

1. *Minimal software environment* – Only software absolutely required is installed.


Programs and Features
Control Panel ▸ Programs and Features
Search
File
Edit
View
Tools
Help
Tasks
View installed updates
Get new programs online at Windows Marketplace
Turn Windows features on or off
Install a program from the network
Organize
Views

Uninstall or change a program

To uninstall a program, select it from the list and then click "Uninstall", "Change", or "Repair".

Name	Publisher	Instal...	Size
7-Zip 4.65 (x64 edition)	Igor Pavlov	8/29/2010	3.98 MB
HighPoint Web RAID Management Service		4/13/2010	3.21 MB
Intel(R) Network Connections 14.6.10.0	Intel	3/20/2010	6.83 MB
Microsoft .NET Framework 3.5 SP1	Microsoft Corporation	3/22/2010	32.4 MB
Microsoft .NET Framework 4 Client Profile	Microsoft Corporation	7/8/2010	189 MB
Microsoft .NET Framework 4 Extended	Microsoft Corporation	7/8/2010	46.4 MB
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	5/6/2010	2.69 MB
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	4/20/2010	342 KB
MSXML 4.0 SP2 (KB954430)	Microsoft Corporation	5/8/2010	1.27 MB
MSXML 4.0 SP2 (KB973688)	Microsoft Corporation	5/8/2010	1.33 MB
MySQL Server 5.1	MySQL AB	8/29/2010	78.5 MB
PHP 5.3.3	The PHP Group	8/29/2010	28.8 MB
PostgreSQL 8.4	PostgreSQL Global Developme...	4/20/2010	179 MB
Seagate Manager Installer	Seagate	5/6/2010	733 MB
Vim 7.2 (self-installing)		5/8/2010	26.5 MB

The easiest way to eliminate a threat is to remove the vulnerability!

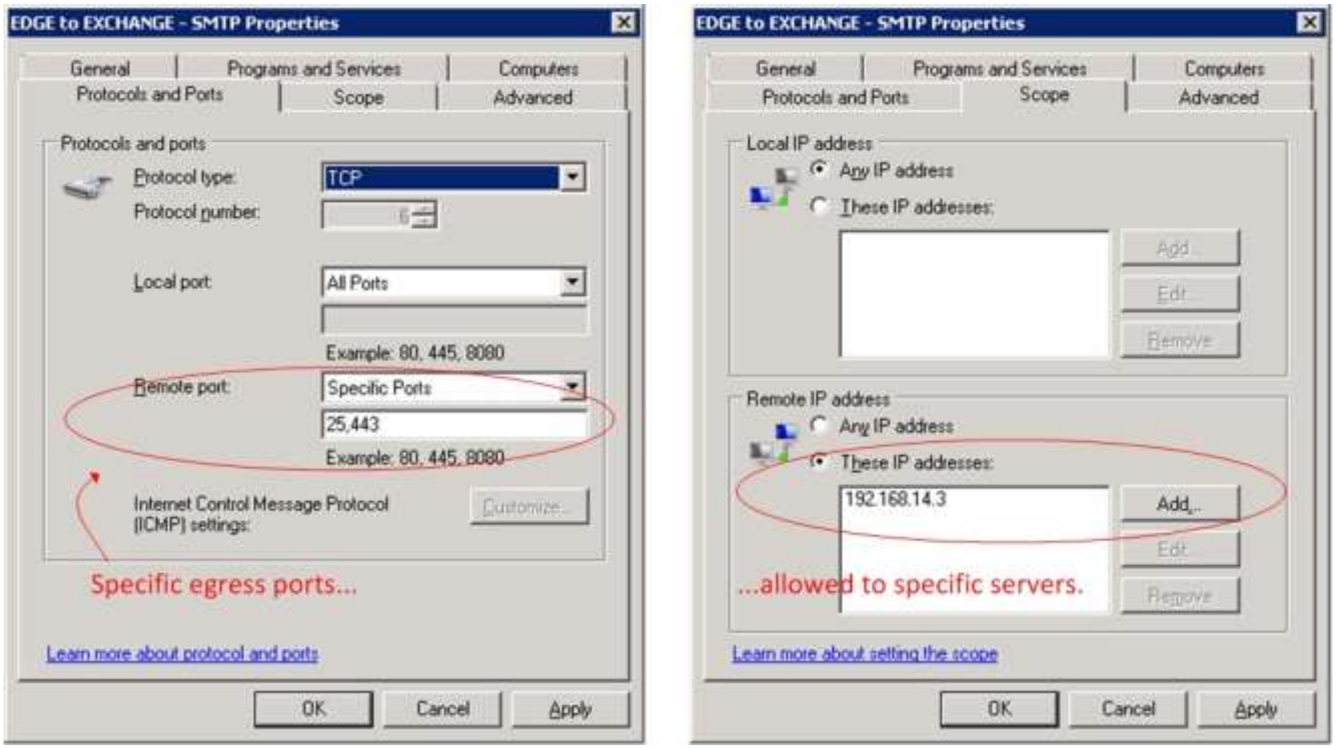
Even these programs would be suspect, they house no corporate data

The one "essential" application for all servers

Figure 8 - Minimal software installation minimizes attack surface

2. *Minimal allowed remote access* – By default, team members *should not be able* to connect directly to any server within the DMZ. This means that functions such as Remote Desktop are reserved only for administrative accounts stored within the Active Directory.

3. *Minimal outbound access allowed* – The servers within the DMZ can only initiate connections to particular services provided on particular target servers. For example, the corporate EDGE email server we defined in our drawing (an SMTP server) must be able to communicate with the internal Exchange server using ports 25 (SMTP) and 443 (HTTPS) – but no other outbound ports need to be allowed.



Protocols and ports

Protocol type: TCP

Protocol number: 6

Local port: All Ports

Example: 80, 445, 8080

Remote port: Specific Ports

25,443

Example: 80, 445, 8080

Internet Control Message Protocol (ICMP) settings:

Specific egress ports...

Local IP address

● Any IP address

○ These IP addresses:

Remote IP address

○ Any IP address

● These IP addresses:

192.168.14.3

...allowed to specific servers.

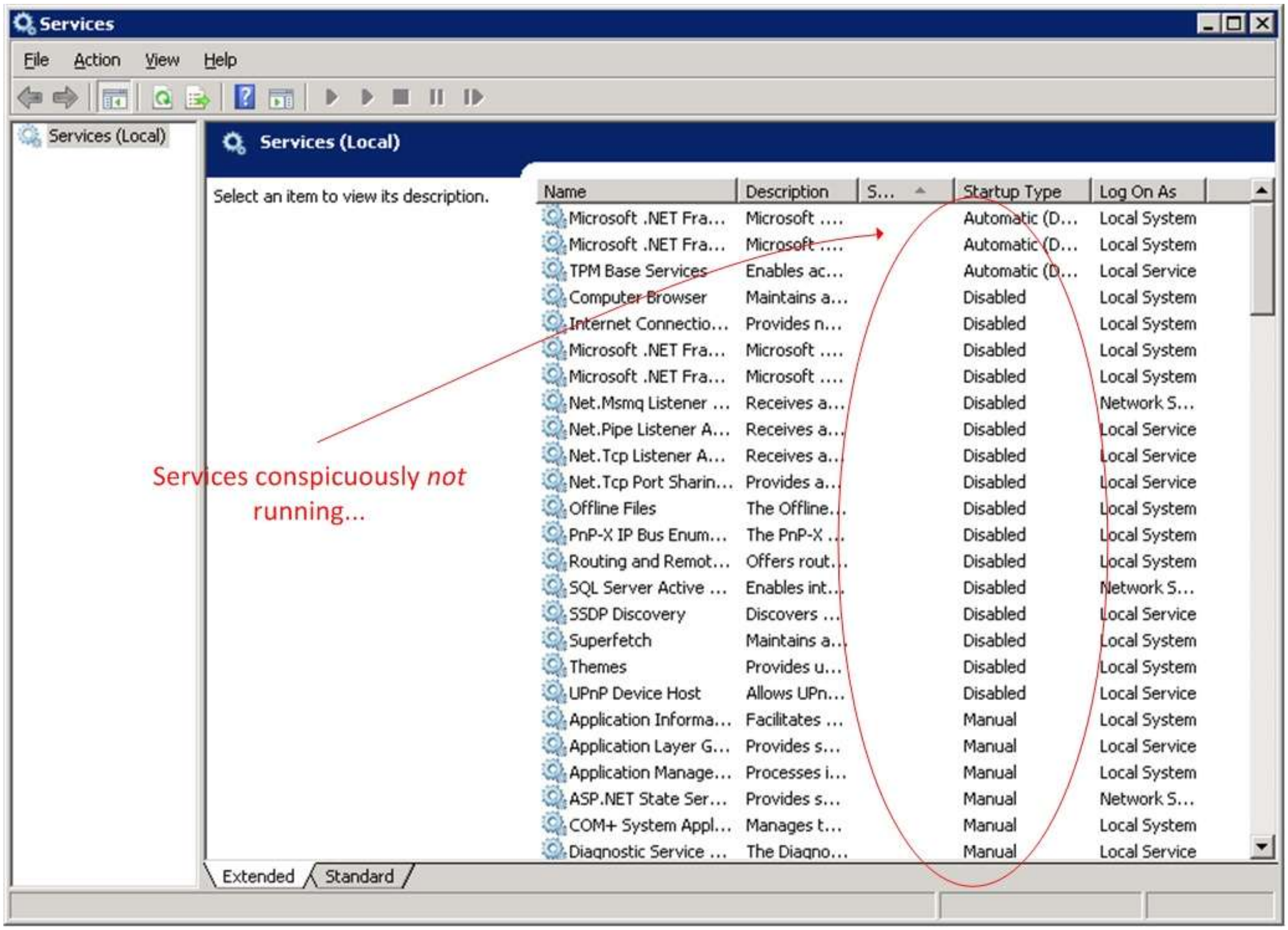
Figure 9 – Outbound firewall rules minimize DMZ security breach dangers

5.2 Protected Network

Our notional organization's protected network contains internal corporate servers. These servers provide the functional backbone for corporate activity and business; without them the ability to perform any type of meaningful work quickly deteriorates to zero. We recommend employing a significant number of protections on these servers to minimize the organization's risk if a security breach occurs. In many ways, the servers in this group constitute an organization's crown jewels and must be protected carefully:

1. *Hardened operating system* – Protected servers should start with a locked-down and minimal operating system. In our case, RiVidium starts with a Windows version built on the Army Golden Master (AGM). This version of the Windows operating system features a stripped-down and secured feature set.

2. *Minimal software install and execution* – As with the DMZ network, only critical functions should be installed on these servers. Additionally, the set of installed and running Windows services (automatic functions typically set to start with the computer; called *daemons* on UNIX) should be manually reviewed to be sure only to run only those critically needed services are enabled.

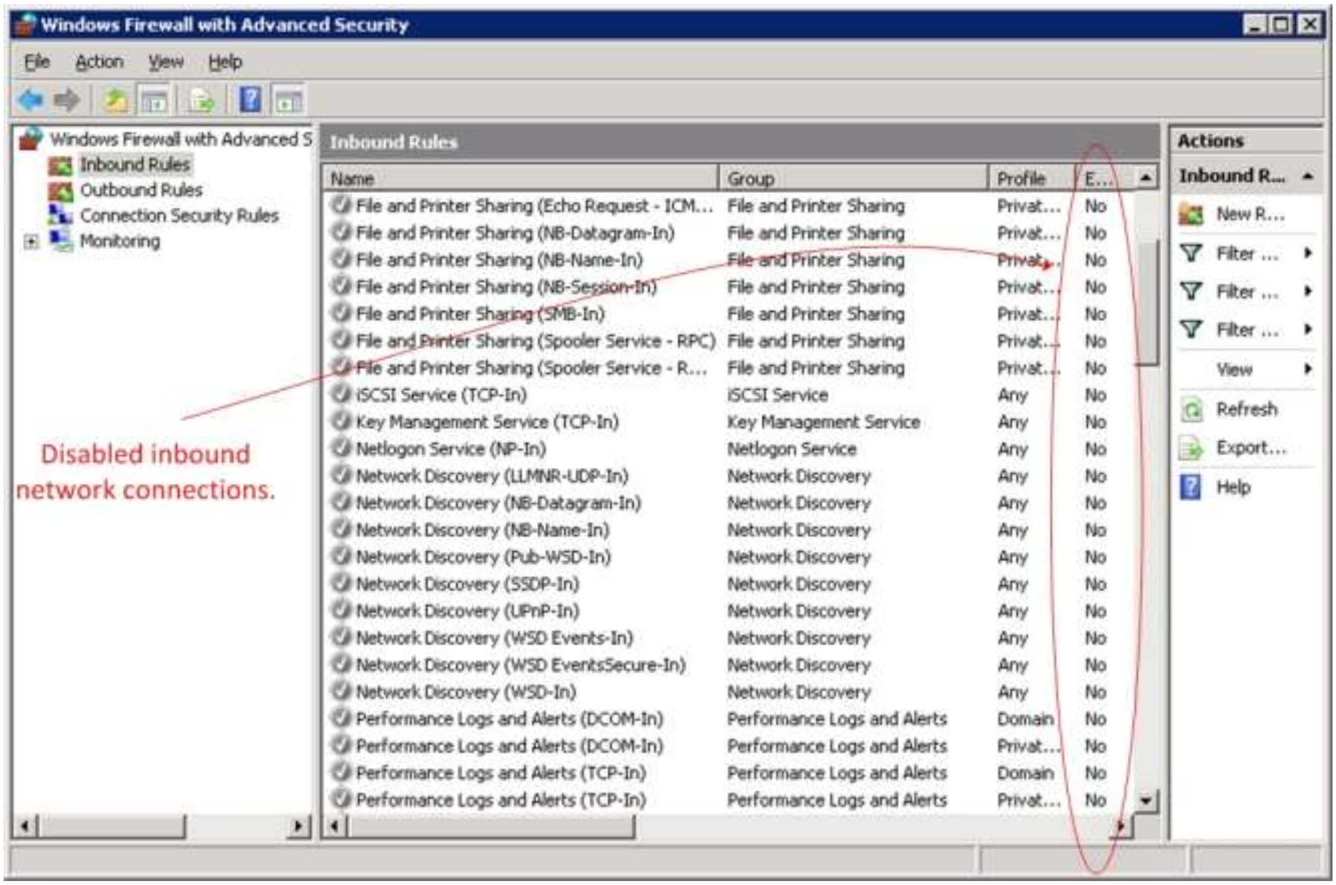


Name	Description	S...	Startup Type	Log On As
Microsoft .NET Fra...	Microsoft		Automatic (D...	Local System
Microsoft .NET Fra...	Microsoft		Automatic (D...	Local System
TPM Base Services	Enables ac...		Automatic (D...	Local Service
Computer Browser	Maintains a...		Disabled	Local System
Internet Connectio...	Provides n...		Disabled	Local System
Microsoft .NET Fra...	Microsoft		Disabled	Local System
Microsoft .NET Fra...	Microsoft		Disabled	Local System
Net.Msmq Listener ...	Receives a...		Disabled	Network S...
Net.Pipe Listener A...	Receives a...		Disabled	Local Service
Net.Tcp Listener A...	Receives a...		Disabled	Local Service
Net.Tcp Port Sharin...	Provides a...		Disabled	Local Service
Offline Files	The Offline...		Disabled	Local System
PnP-X IP Bus Enum...	The PnP-X ...		Disabled	Local System
Routing and Remot...	Offers rout...		Disabled	Local System
SQL Server Active ...	Enables int...		Disabled	Network S...
SSDP Discovery	Discovers ...		Disabled	Local Service
Superfetch	Maintains a...		Disabled	Local System
Themes	Provides u...		Disabled	Local System
UPnP Device Host	Allows UPn...		Disabled	Local Service
Application Informa...	Facilitates ...		Manual	Local System
Application Layer G...	Provides s...		Manual	Local Service
Application Manage...	Processes i...		Manual	Local System
ASP.NET State Ser...	Provides s...		Manual	Network S...
COM+ System Appl...	Manages t...		Manual	Local System
Diagnostic Service ...	The Diagno...		Manual	Local Service

Services conspicuously *not* running...

Figure 10 - Minimal Windows services

3. We recommend that our notional organization ensures that, by default, only a minimal set of inbound network connections are allowed:



Disabled inbound network connections.

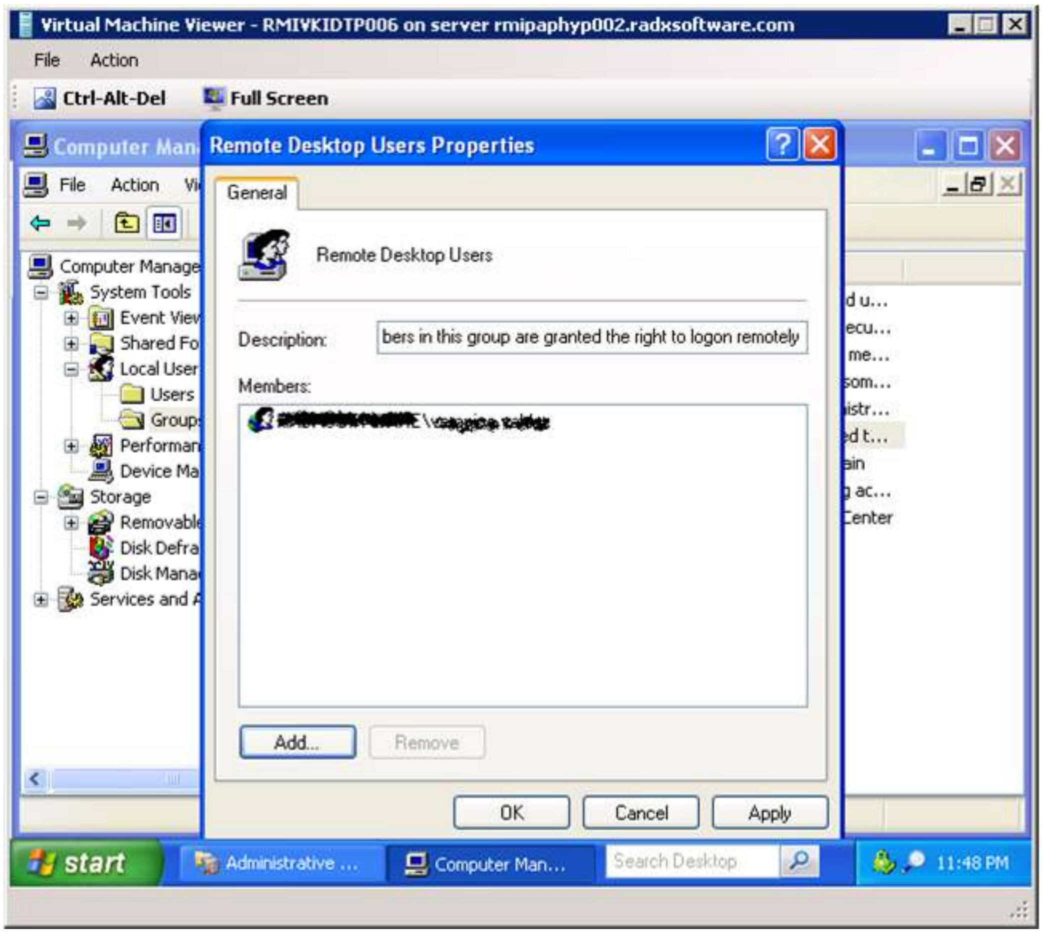
Name	Group	Profile	E...
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Privat...	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Privat...	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Privat...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Privat...	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Privat...	No
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Privat...	No
File and Printer Sharing (Spooler Service - R...	File and Printer Sharing	Privat...	No
iSCSI Service (TCP-In)	iSCSI Service	Any	No
Key Management Service (TCP-In)	Key Management Service	Any	No
Netlogon Service (NP-In)	Netlogon Service	Any	No
Network Discovery (LLMNR-UDP-In)	Network Discovery	Any	No
Network Discovery (NB-Datagram-In)	Network Discovery	Any	No
Network Discovery (NB-Name-In)	Network Discovery	Any	No
Network Discovery (Pub-WSD-In)	Network Discovery	Any	No
Network Discovery (SSDP-In)	Network Discovery	Any	No
Network Discovery (UPnP-In)	Network Discovery	Any	No
Network Discovery (WSD Events-In)	Network Discovery	Any	No
Network Discovery (WSD EventsSecure-In)	Network Discovery	Any	No
Network Discovery (WSD-In)	Network Discovery	Any	No
Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Domain	No
Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Privat...	No
Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Domain	No
Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Privat...	No

Figure 11 - Minimal inbound connections

By taking these simple and (almost!) risk-free steps, our notional organization can dramatically increase its level of protection for minimal cost.

5.3 Internal Network

In our network drawing, specified (and highly recommend) the use virtual machines (VMs) for most users (for example, developers and analysts. These VMs should be run by using thin clients rather than full workstations – making administration and ongoing maintenance costs much lower. These VMs should run within the *internal* organizational network, along with research and development servers. Critical system data or servers should *never be stored* within this network, and network egress (outgoing traffic) should be controlled by policy rules from the corporate gateway. Team members should be able to access only their assigned individual VM(s), and we group policy should be used to ensure that each VM has the correct anti-malware solution installed.



Description: bers in this group are granted the right to logon remotely

Members:

[redacted]

Figure 12 - VMs restrict remote access

5.4 Guest Network

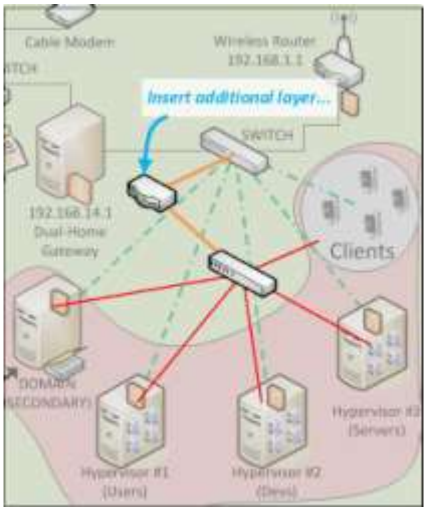
This network allows our notional organization's guests (and mobile devices) to access the Internet. This network should have the most restrictive set of policies that prohibit all network ingress and limiting Internet access to the standard Web protocols DNS (53), HTTP (80), and HTTPS (443).

6.0 Recommendations

We purposefully put in a common weakness: insufficient protection between the guest network and the internal network. We also speak to smaller organization's common lack of enterprise logging capabilities.

6.1 Protection from Guest Network

Ironically, a typical guest network is more protected from the internal network (via the firewall in the wireless router) than the internal network is from our guest network. This can be remediated by implementing another router between the switch and the internal network.



Step	Cost	Notes
Cisco router (RVS4000) and switch (SG300-10P)	$130 (router), $382 (switch)[*]	Switch connects systems, router provides firewall / NAT protection
Gateway client	Two days	Our gateway already applies policy to NAT'ed clients, but requires a custom agent.

This ensures that the internal network is secure from our guest network, similarly to our protected network.

6.1 Enterprise Log Event Management

Most small organizations do not have the ability to track or log event files and report problems to system administrators. While excellent commercial products abound, in order to minimize the initial expense we recommend the use of **OSSIM** (The Open Source Security and Information Event Management).[**]

Step	Cost	Notes
Inventory critical logs	Ten days	The major cost for any SIEM solution is to identify what servers to log, and what actions should be initiated based on logged events
Install SIEM	Two days	Free download
Configure SIEM	Five days	This SIEM has significant functionality, but requires extra configuration

Over time, the smaller organization can move to a full commercial solution; the initial "critical log" inventory will stand it in good stead then.

[*] Priced from Cisco Web site as of 20 October 2010

[**] See Web site http://tinyurl.com/ossiem.

7.0 Terminology

DMZ – Demilitarized Zone (a zone between the external untrusted network and the internal network)
DNS – Domain Naming Service
Dual-homed – Having two NICs (typically one for external traffic and another for internal traffic)
HTTP – Hyper-text Transfer Protocol (*HTTP**S*** adds security)
IP – Internet Protocol
NIC – Network Interface Card
NIST – National Institute of Standards and Technology
RADIUS – Remote Access Dial-in User Service (allows authentication of remote users)
SIEM – Security Information and Event Management
SMTP – Simple Mail Transfer Protocol
SP – Special Publication
VM – Virtual Machine
USB – Universal Serial Bus

Reference List and End-notes

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

Cowill, Carl. "Human factors in information security: The insider threat - Who can you trust these days?" *Information Security Technical Report 14* (2009), pp. 186-196.

Scarfone, Karen, Wayne Jensen, and Miles Tracy. "Guidelines on Firewalls and Firewall Policy." *NIST SP 800-41* (September, 2009). NIST, available online at http://tinyurl.com/sp80041 (accessed: October 20, 2010).

Stephenson, Peter R., ed. Information Security Essentials: Section 2. Auerbach Publishing, ISBN 978-1-4398-0030-0, 2009. Retrieved Sep. 21, 2010 from http://tinyurl.com/isevol2.

Stoneburner, Gary. "Underlying Technical Models for Information Technology Security." *NIST SP 800-33* (December, 2001). NIST, available online at http://tinyurl.com/sp80033 (accessed: October 25, 2010).

[1] Bosworth et. al., pg. 740.

[2] Stephenson, pg. 551.

[3] Scarfone and Hoffman, pg. 30.

[4] Cowill, pg. 194.

[5] Stoneburner, pg. 6.