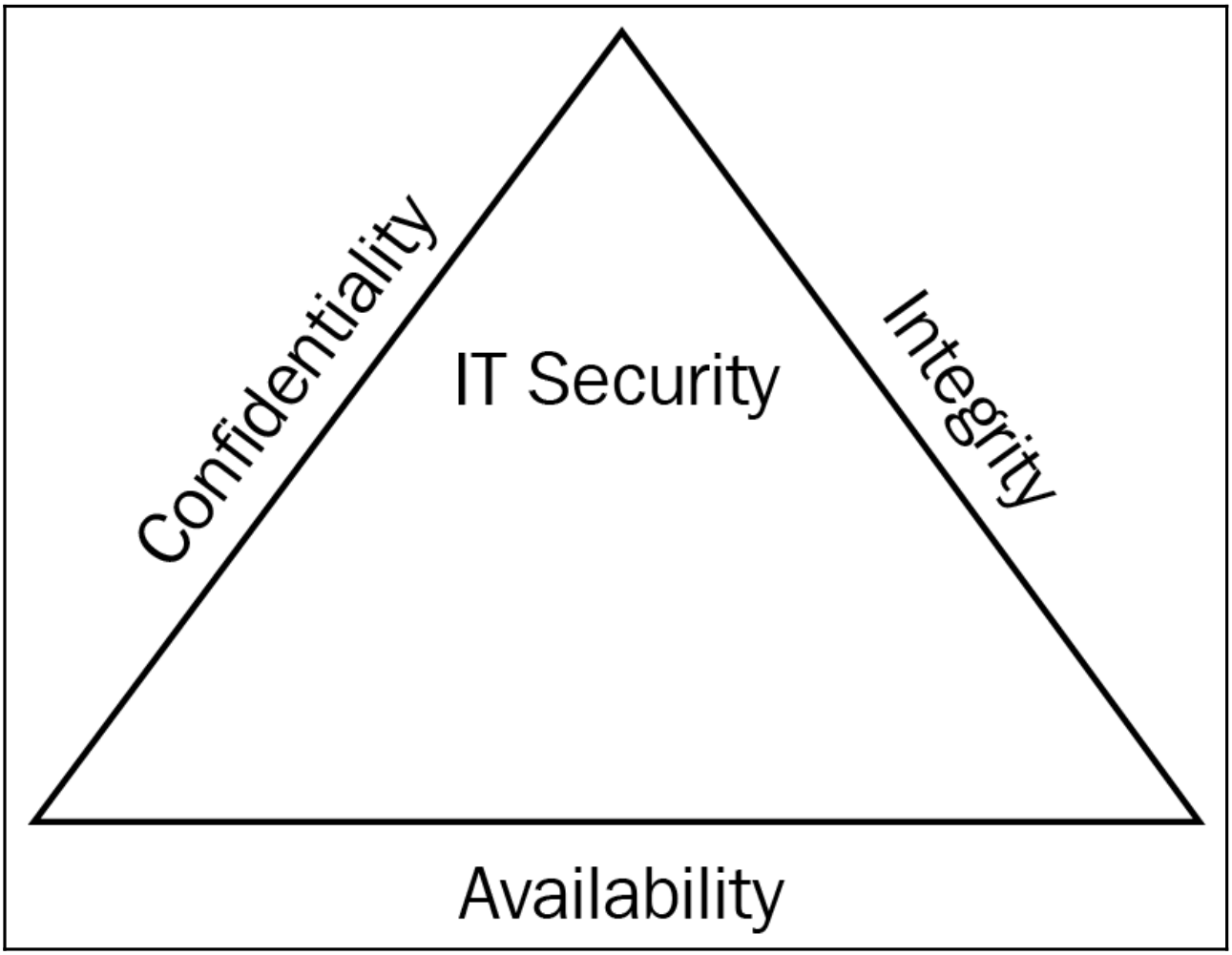
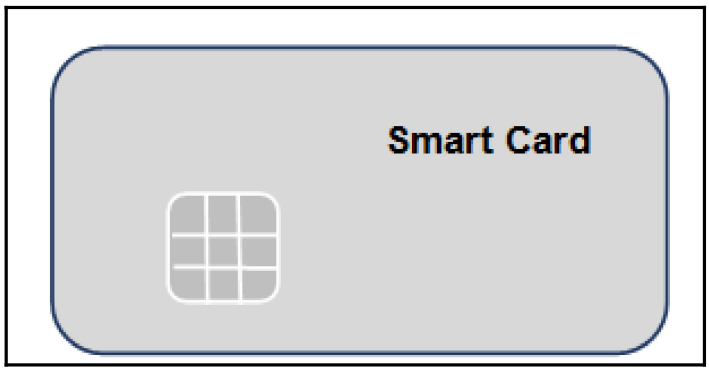
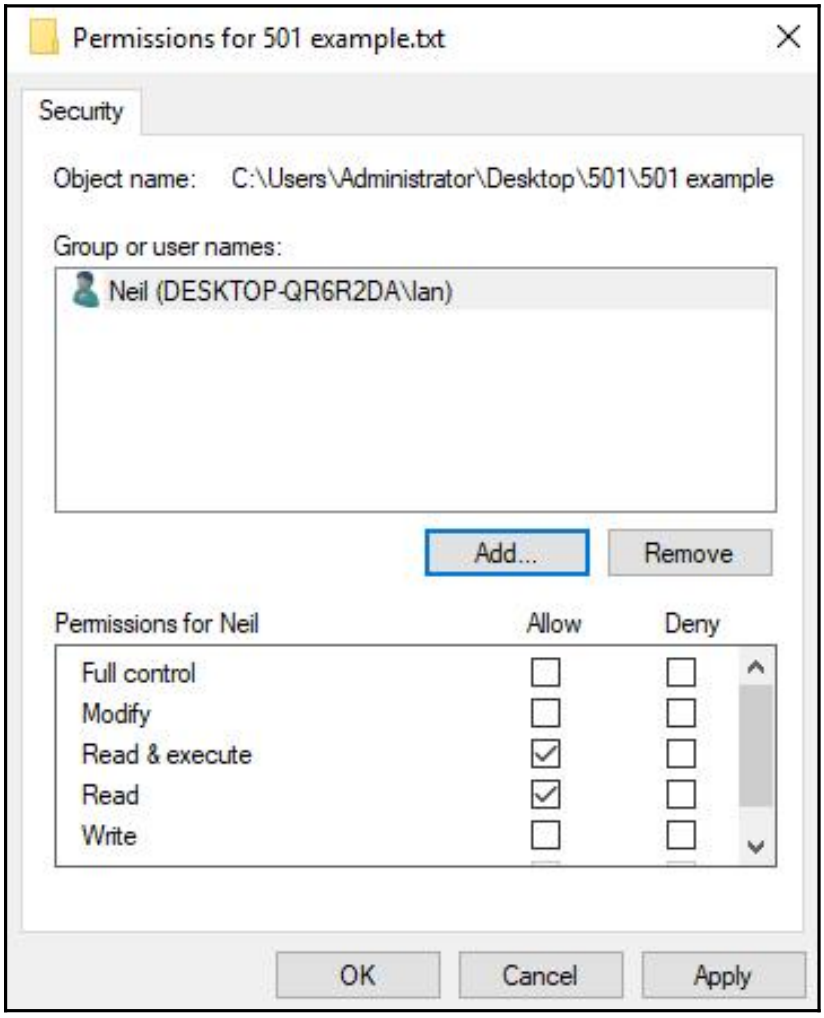
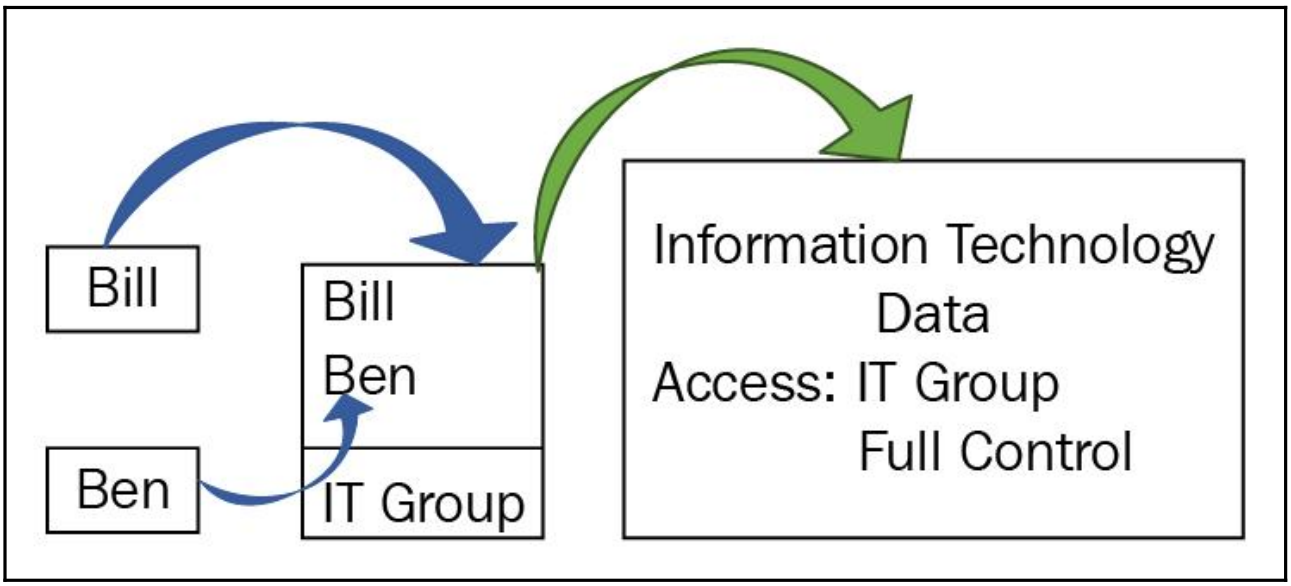
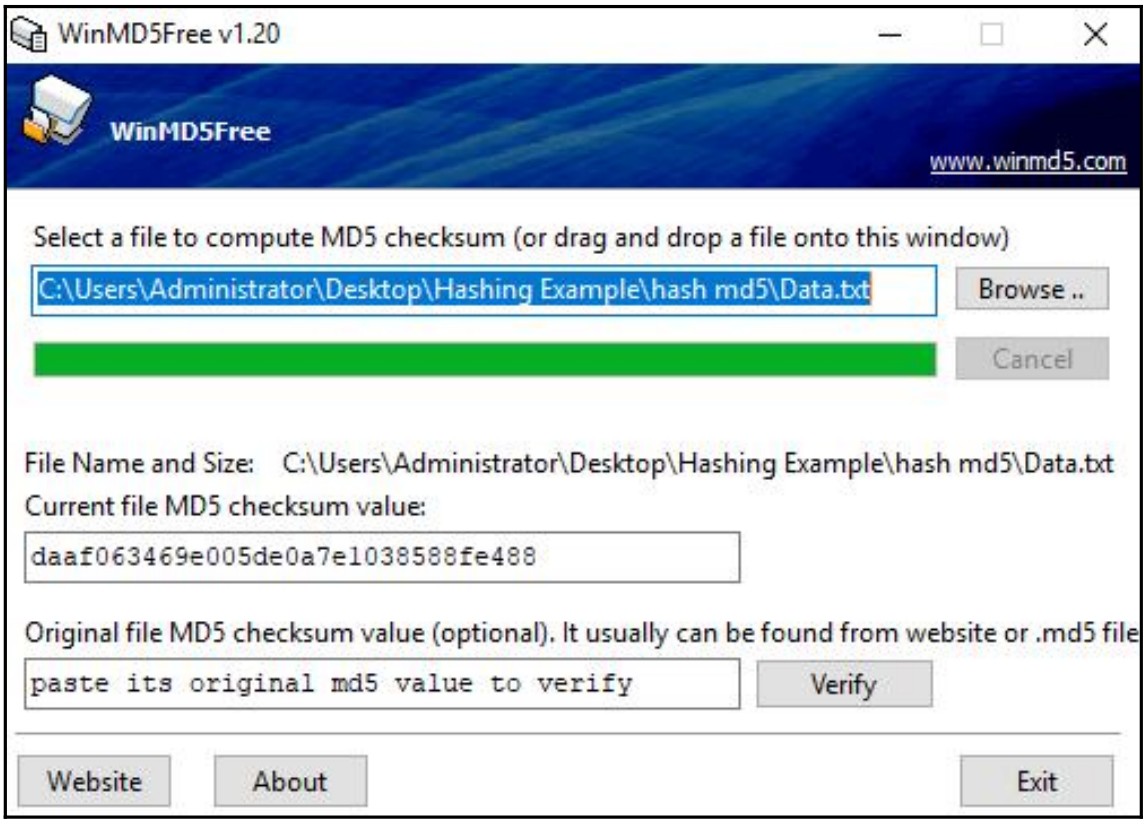
Chapter 01: Understanding Security Fundamentals

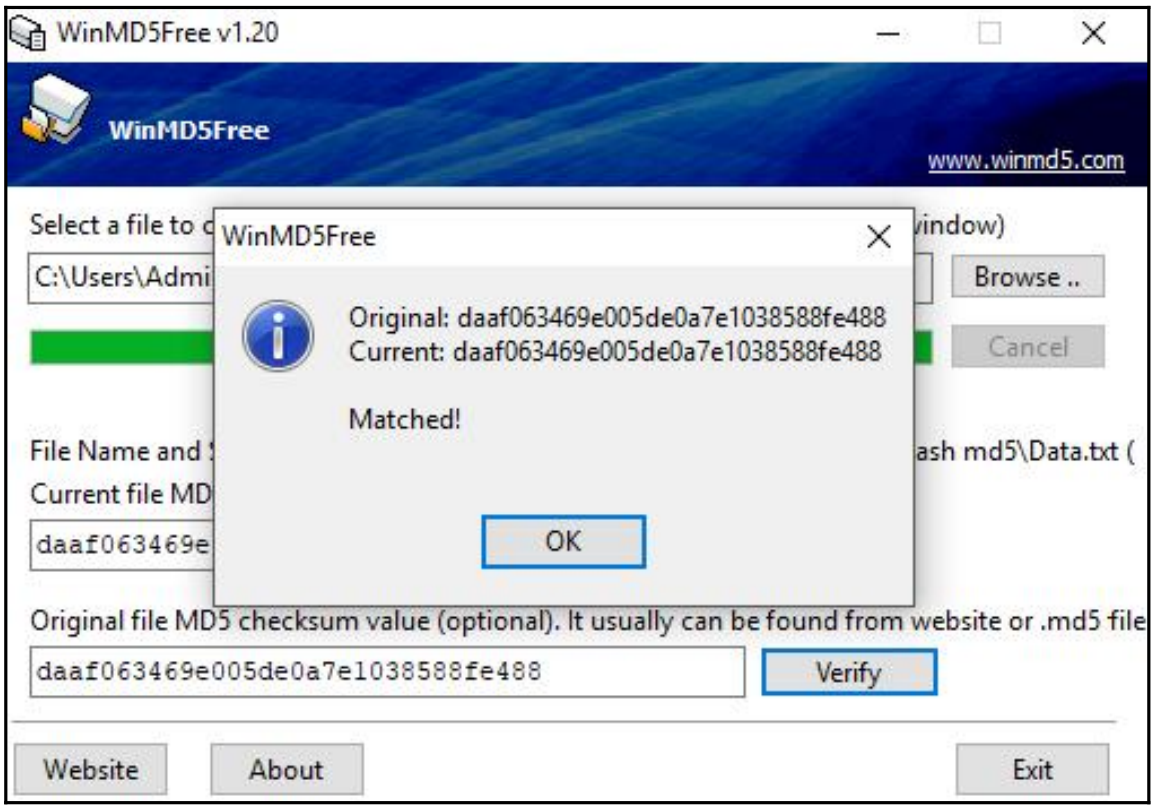


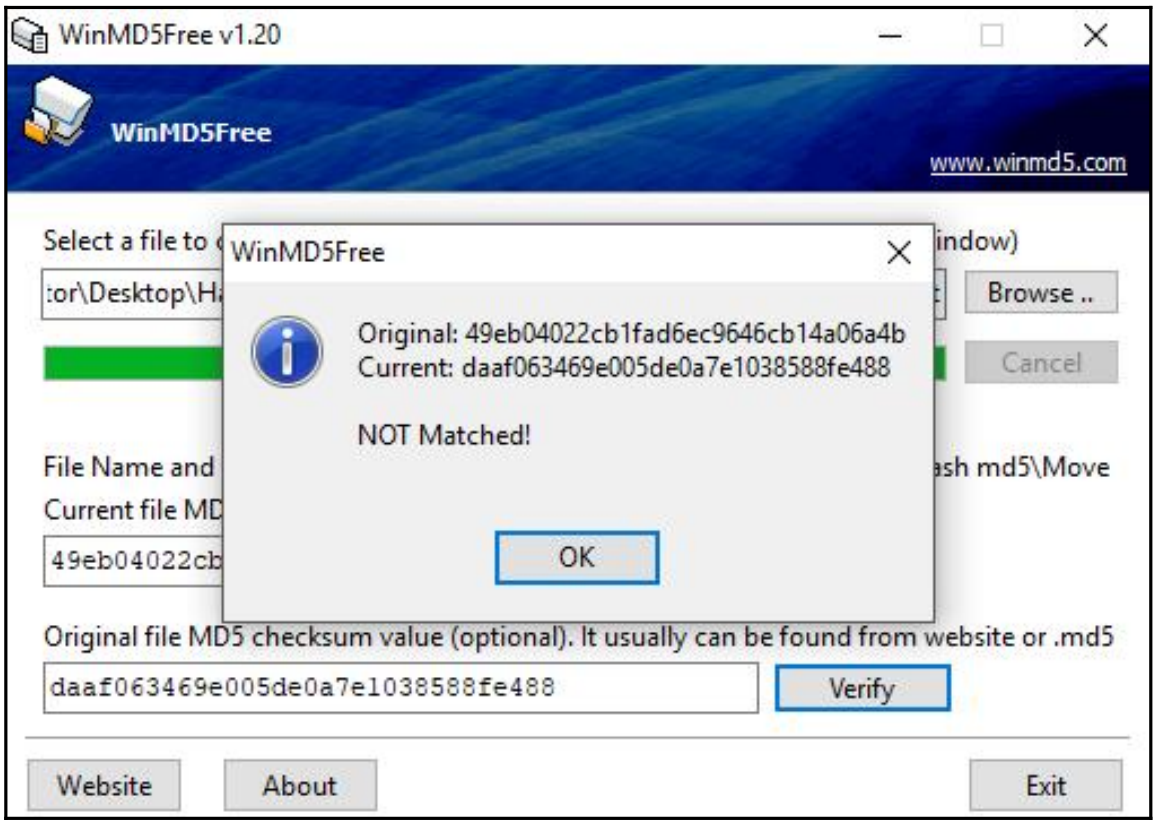

Smart Card

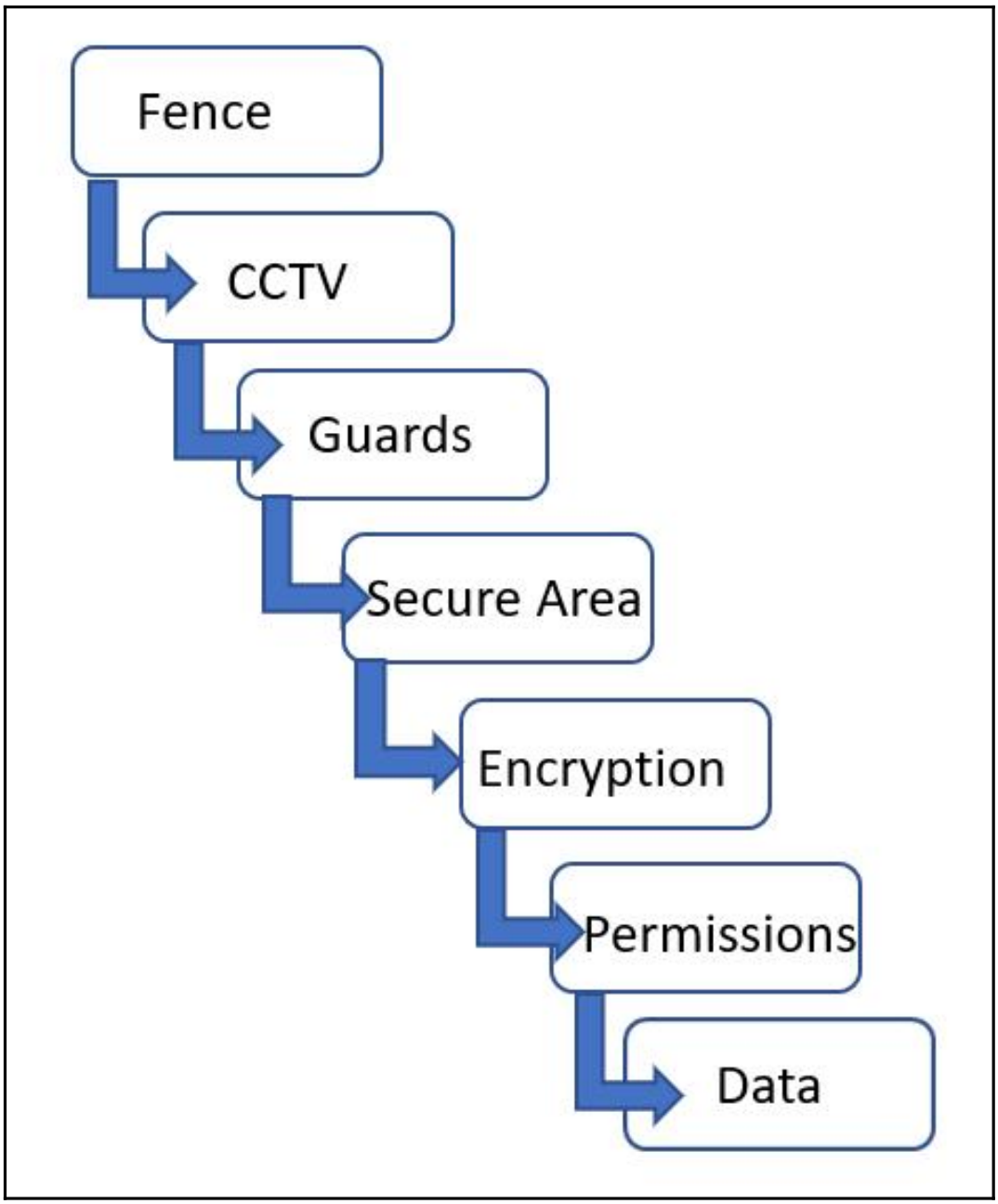

Permissions for 501 example.txt
Security
Object name: C:\Users\Administrator\Desktop\501\501 example
Group or user names:
Neil (DESKTOP-QR6R2DA\lan)
Add...
Remove
Permissions for Neil
Allow
Deny
Full control
Modify
Read & execute
Read
Write
OK
Cancel
Apply


Bill
Ben
Bill
Ben
IT Group
Information Technology
Data
Access: IT Group
Full Control

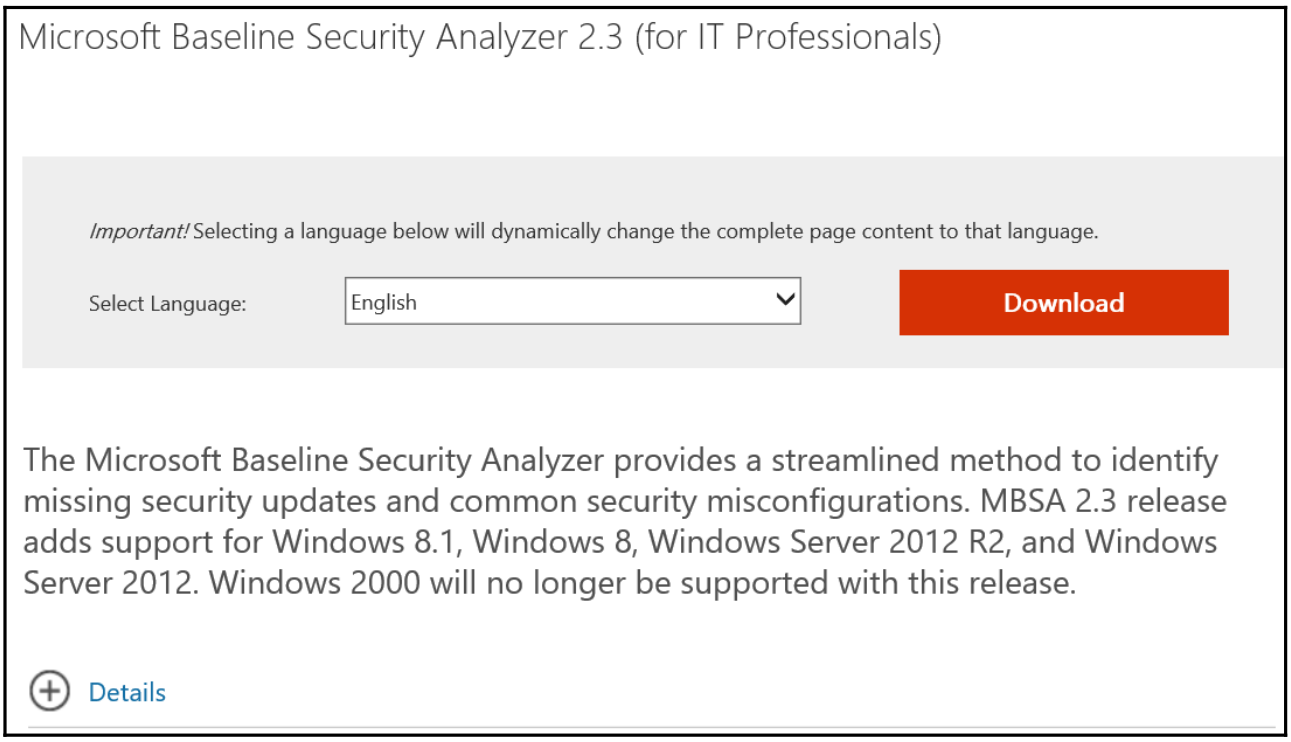

WinMD5Free v1.20
WinMD5Free
www.winmd5.com
Select a file to compute MD5 checksum (or drag and drop a file onto this window)
C:\Users\Administrator\Desktop\Hashing Example\hash md5\Data.txt
Browse ..
Cancel
File Name and Size: C:\Users\Administrator\Desktop\Hashing Example\hash md5\Data.txt
Current file MD5 checksum value:
daaf063469e005de0a7e1038588fe488
Original file MD5 checksum value (optional). It usually can be found from website or .md5 file
paste its original md5 value to verify
Verify
Website
About
Exit


WinMD5Free v1.20
WinMD5Free
www.winmd5.com
Select a file to c
indow)
C:\Users\Admi
Browse ..
Cancel
File Name and
ash md5\Data.txt (
Current file MD
daaf063469e
Original file MD5 checksum value (optional). It usually can be found from website or .md5 file
daaf063469e005de0a7e1038588fe488
Verify
Website
About
Exit
WinMD5Free
Original: daaf063469e005de0a7e1038588fe488
Current: daaf063469e005de0a7e1038588fe488
Matched!
OK

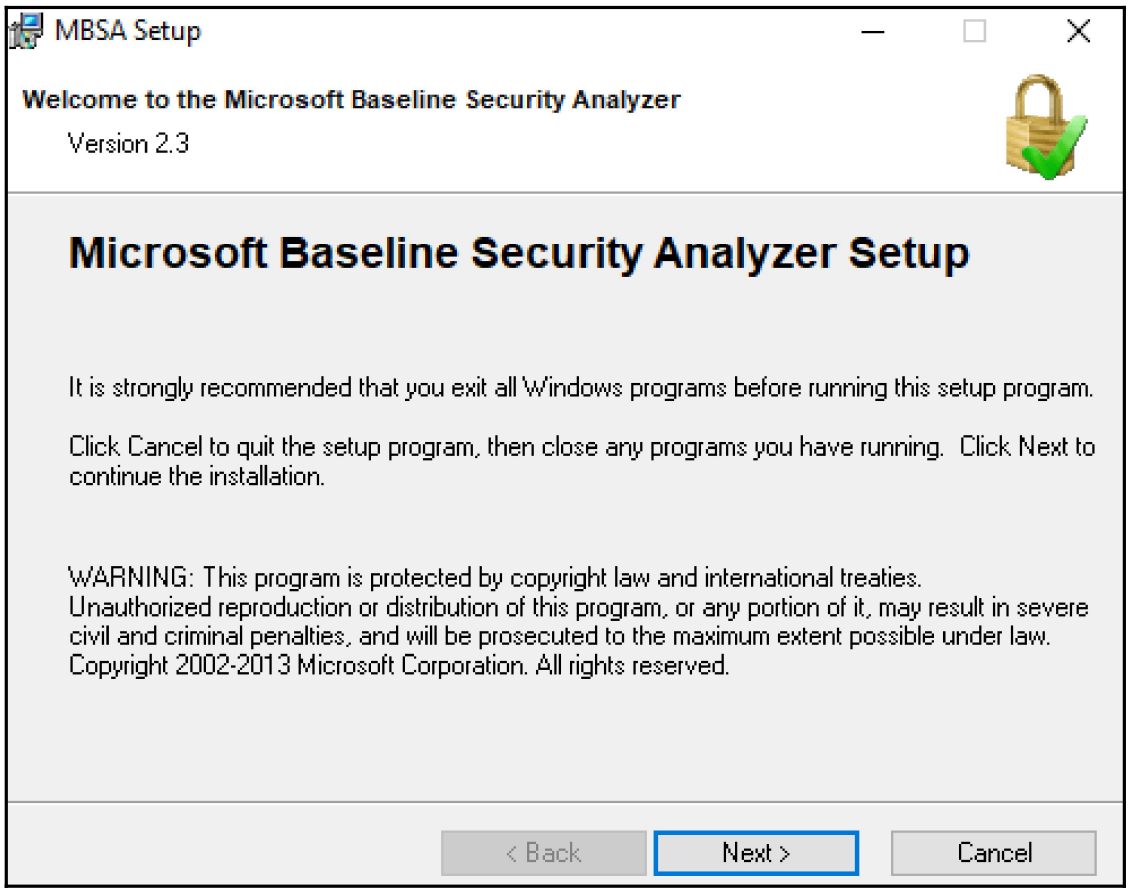

WinMD5Free v1.20
WinMD5Free
www.winmd5.com
Select a file to
indow)
Browse ..
Cancel
File Name and
ash md5\Move
Current file MD
49eb04022cb
Original file MD5 checksum value (optional). It usually can be found from website or .md5
daaf063469e005de0a7e1038588fe488
Verify
Website
About
Exit
WinMD5Free
Original: 49eb04022cb1fad6ec9646cb14a06a4b
Current: daaf063469e005de0a7e1038588fe488
NOT Matched!
OK

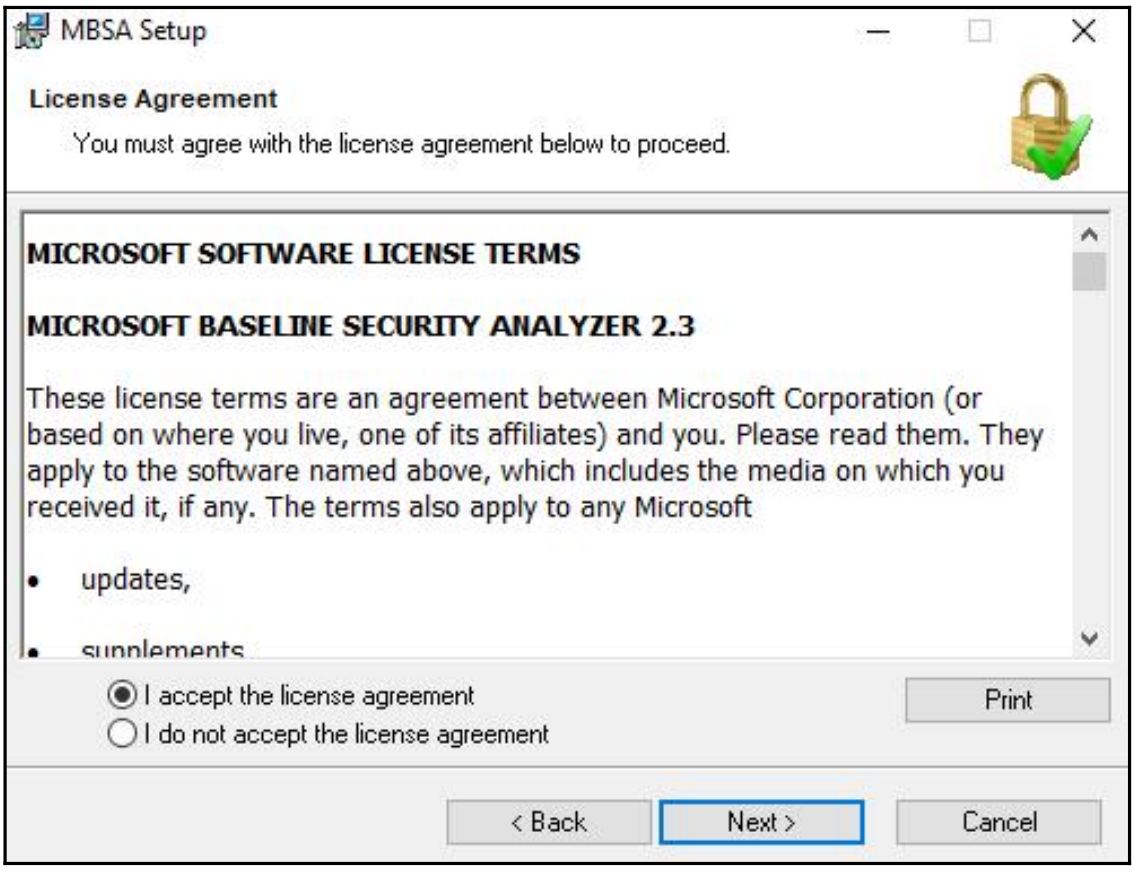

Fence
CCTV
Guards
Secure Area
Encryption
Permissions
Data

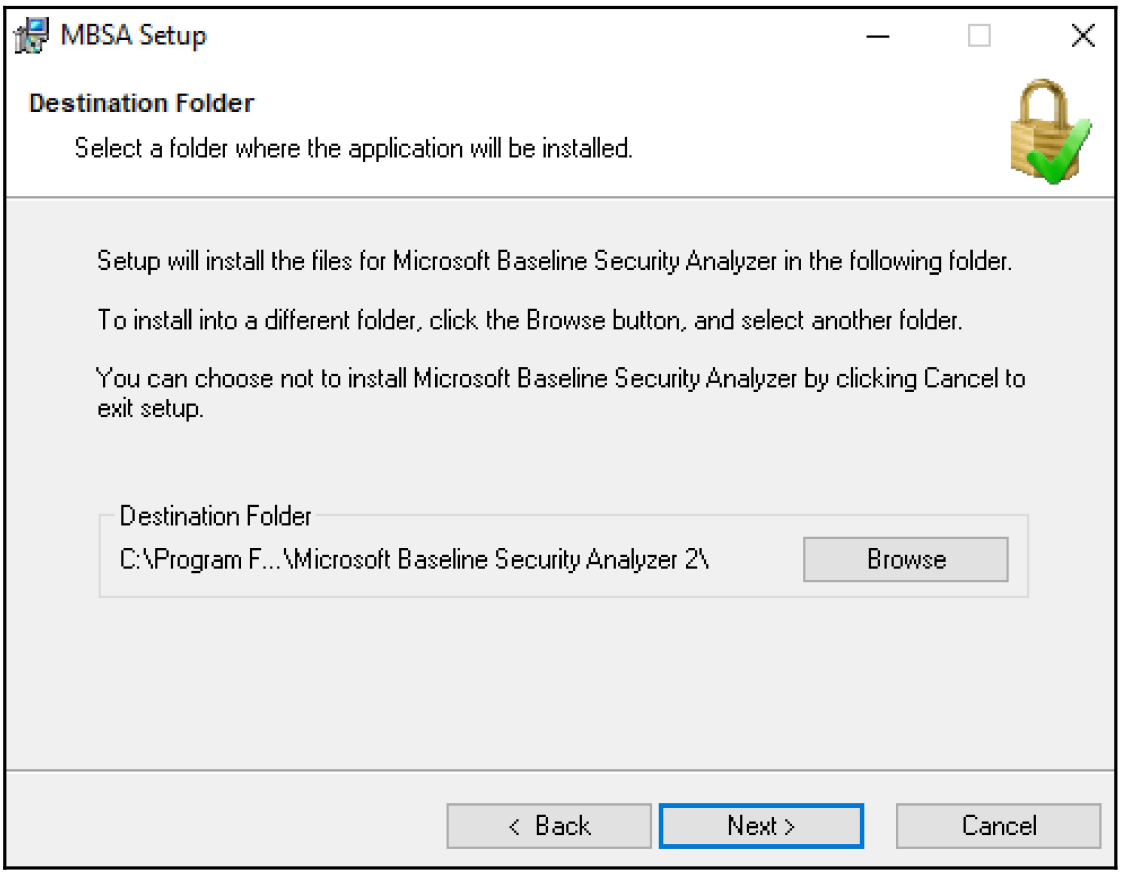
Chapter 03: Implementing Security Policies and Procedures

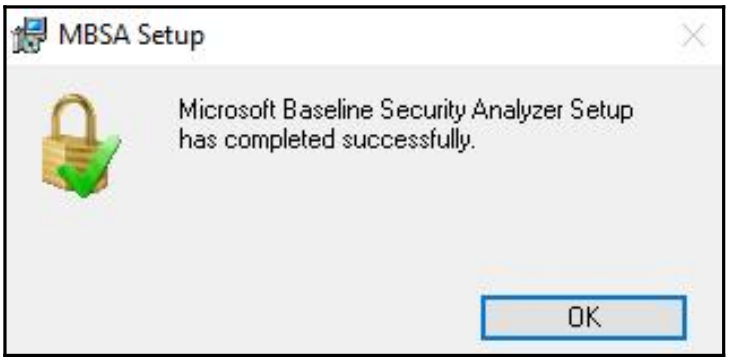

Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)
Important! Selecting a language below will dynamically change the complete page content to that language.
Select Language:
English
Download
The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations. MBSA 2.3 release adds support for Windows 8.1, Windows 8, Windows Server 2012 R2, and Windows Server 2012. Windows 2000 will no longer be supported with this release.
Details


Choose the download that you want
File Name
Size
MBSASetup-x64-EN.msi
1.7 MB
MBSASetup-x64-DE.msi
1.7 MB
MBSASetup-x64-FR.msi
1.7 MB
MBSASetup-x64-JA.msi
1.8 MB
MBSASetup-x86-DE.msi
1.6 MB
MBSASetup-x86-EN.msi
1.6 MB
Download Summary:
KBMBGB
1. MBSASetup-x64-EN.msi
Total Size: 1.7 MB
Next

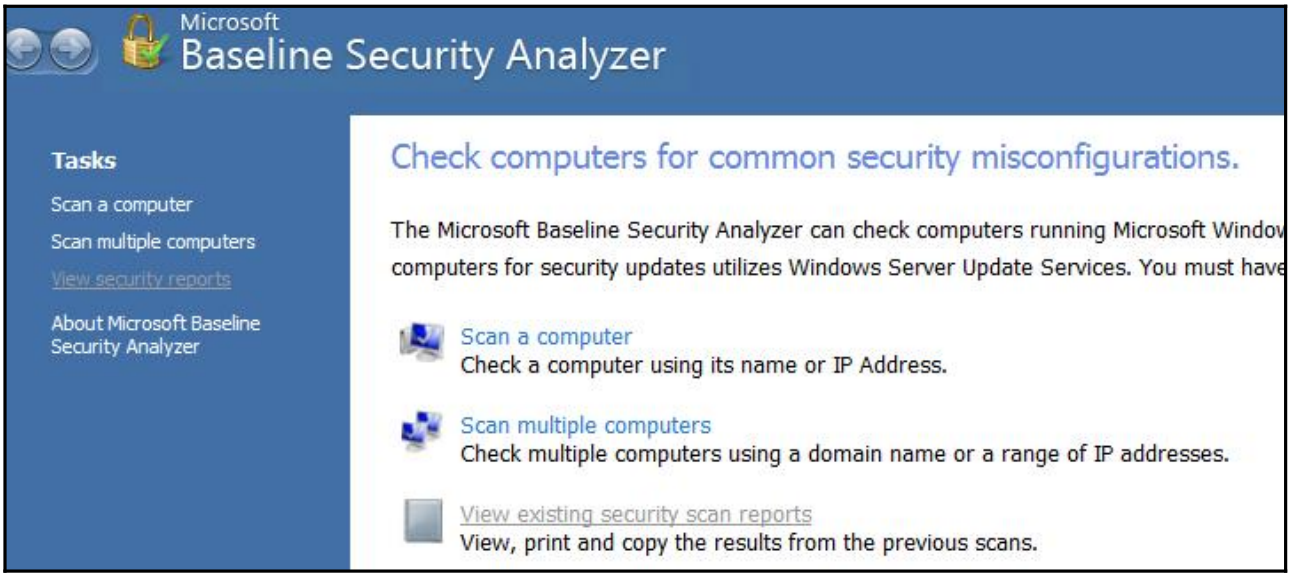

MBSA Setup
Welcome to the Microsoft Baseline Security Analyzer
Version 2.3
Microsoft Baseline Security Analyzer Setup
It is strongly recommended that you exit all Windows programs before running this setup program.
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Copyright 2002-2013 Microsoft Corporation. All rights reserved.
< Back
Next >
Cancel


MBSA Setup
License Agreement
You must agree with the license agreement below to proceed.
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT BASELINE SECURITY ANALYZER 2.3
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft
updates,
supplements
I accept the license agreement
I do not accept the license agreement
Print
< Back
Next >
Cancel

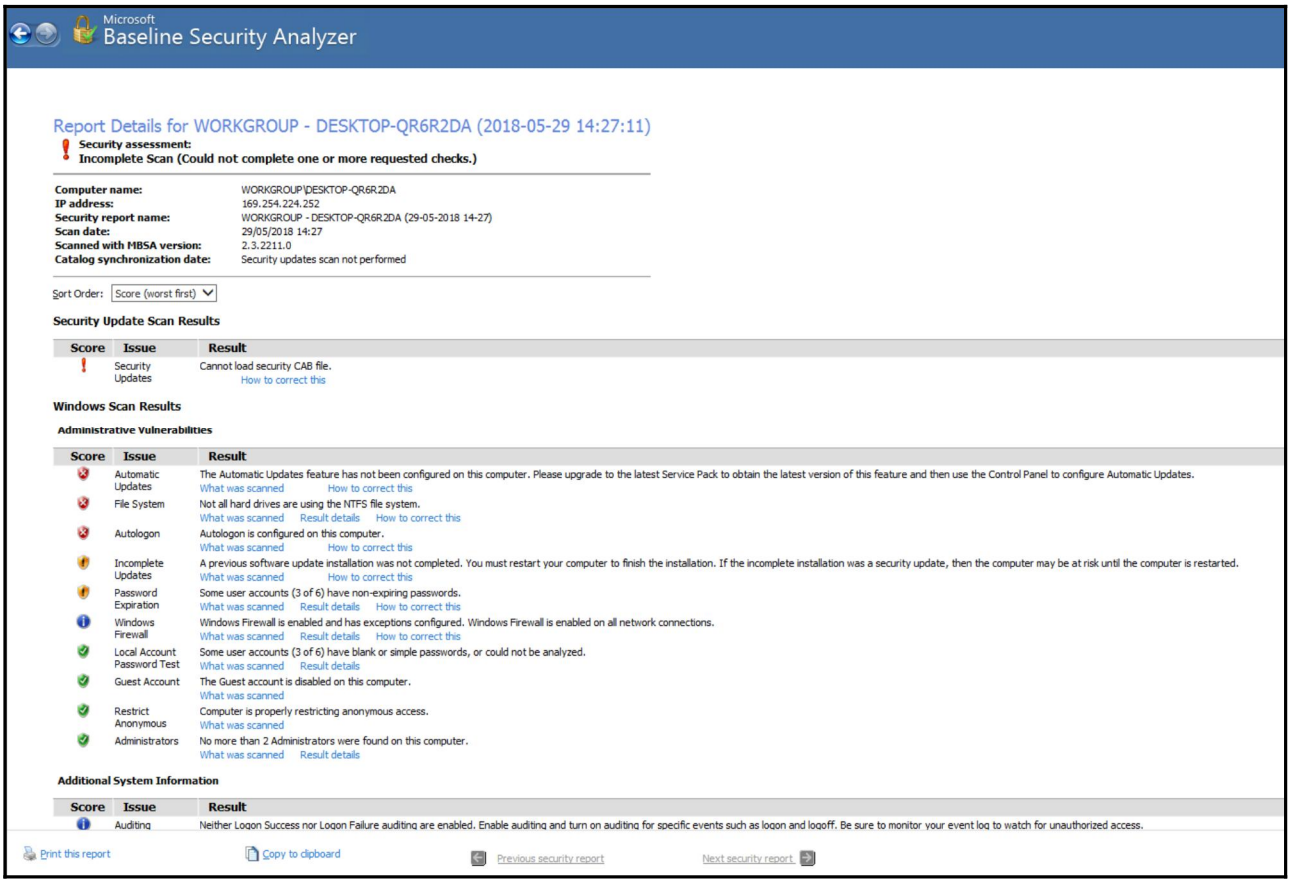

MBSA Setup
Destination Folder
Select a folder where the application will be installed.
Setup will install the files for Microsoft Baseline Security Analyzer in the following folder.
To install into a different folder, click the Browse button, and select another folder.
You can choose not to install Microsoft Baseline Security Analyzer by clicking Cancel to exit setup.
Destination Folder
C:\Program F...\Microsoft Baseline Security Analyzer 2\
Browse
< Back
Next >
Cancel


MBSA Setup
Microsoft Baseline Security Analyzer Setup has completed successfully.
OK


Microsoft
Baseline S...


Microsoft
Baseline Security Analyzer
Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer
Check computers for common security misconfigurations.
The Microsoft Baseline Security Analyzer can check computers running Microsoft Windov
computers for security updates utilizes Windows Server Update Services. You must have
Scan a computer
Check a computer using its name or IP Address.
Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.
View existing security scan reports
View, print and copy the results from the previous scans.


Microsoft
Baseline Security Analyzer
Scanning...
Downloading security update information from Microsoft...



Microsoft
Baseline Security Analyzer

Report Details for WORKGROUP - DESKTOP-QR6R2DA (2018-05-29 14:27:11)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	WORKGROUP\DESKTOP-QR6R2DA
IP address:	169.254.224.252
Security report name:	WORKGROUP - DESKTOP-QR6R2DA (29-05-2018 14-27)
Scan date:	29/05/2018 14:27
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	Security updates scan not performed

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot load security CAB file. How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
✗	File System	Not all hard drives are using the NTFS file system. What was scanned Result details How to correct this
✗	Autologon	Autologon is configured on this computer. What was scanned How to correct this
!	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
!	Password Expiration	Some user accounts (3 of 6) have non-expiring passwords. What was scanned Result details How to correct this
i	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. What was scanned Result details How to correct this
✓	Local Account Password Test	Some user accounts (3 of 6) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details

Additional System Information

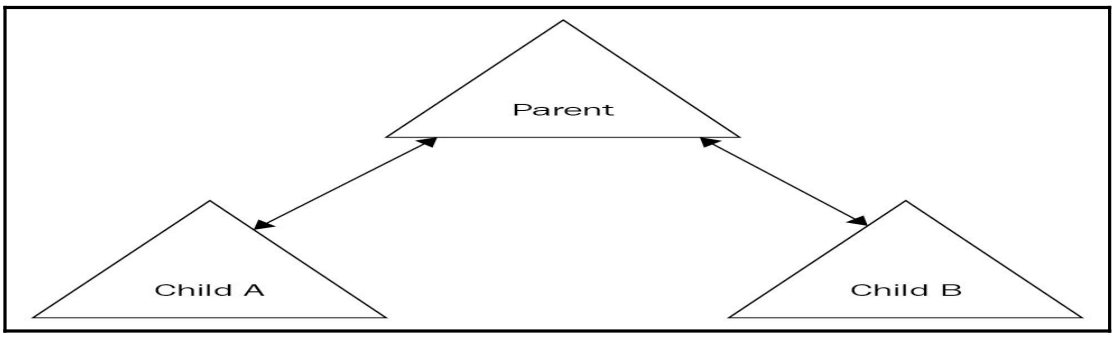
Score	Issue	Result
i	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.

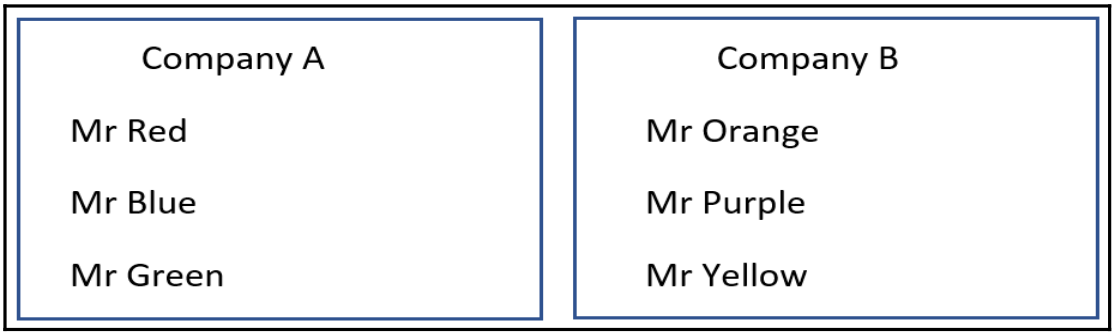
Print this report Copy to clipboard Previous security report Next security report

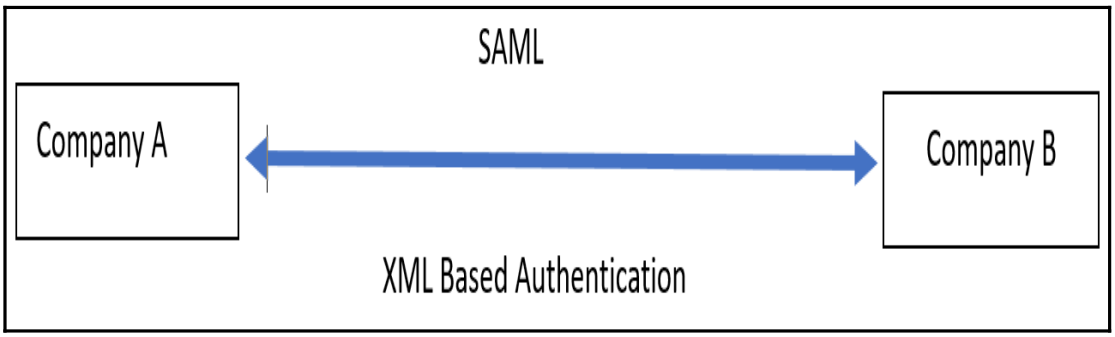
Chapter 04: Delving into Identity and Access Management

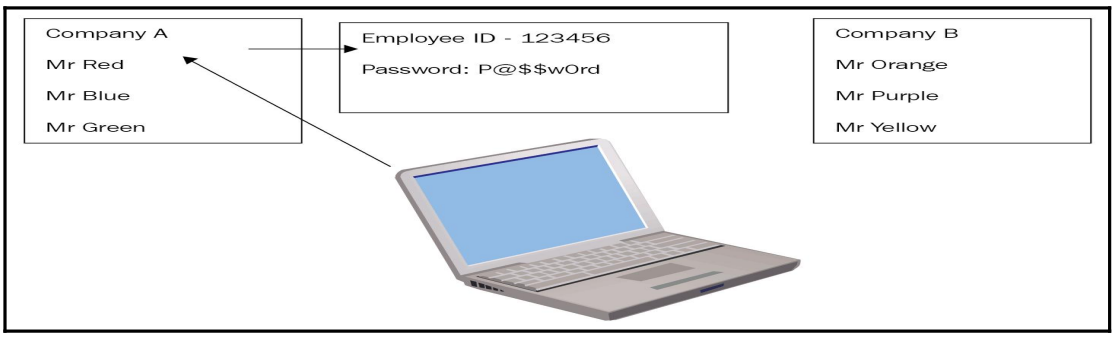
Policy	Security Setting
Enforce password history	24 passwords remember
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

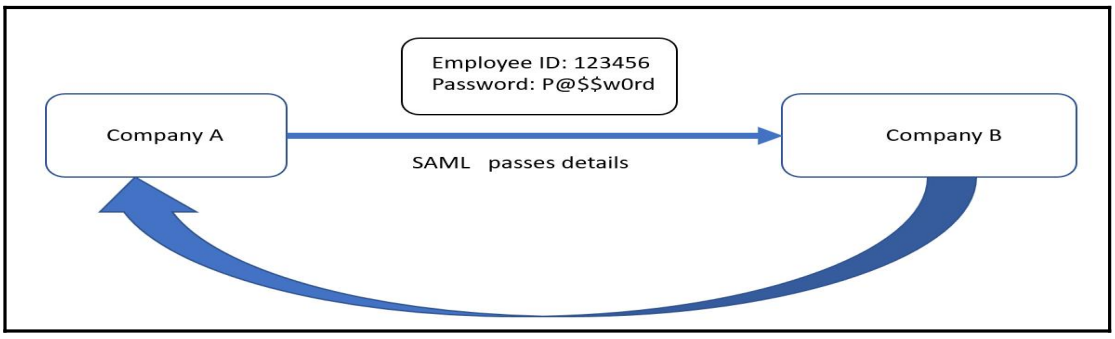
Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

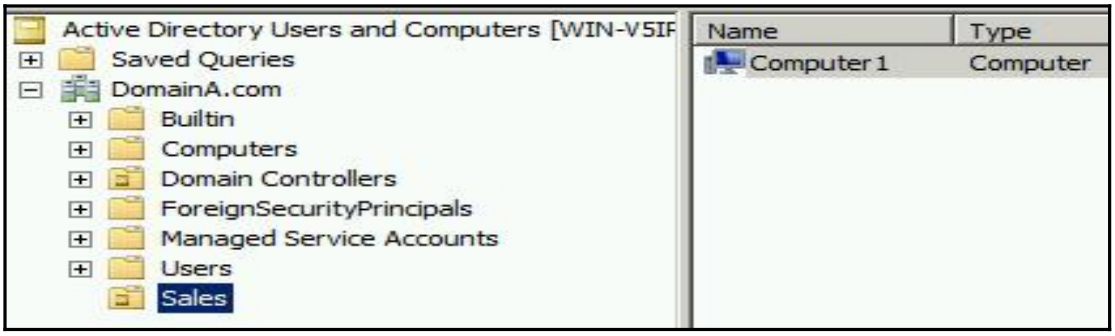

Parent
Child A
Child B

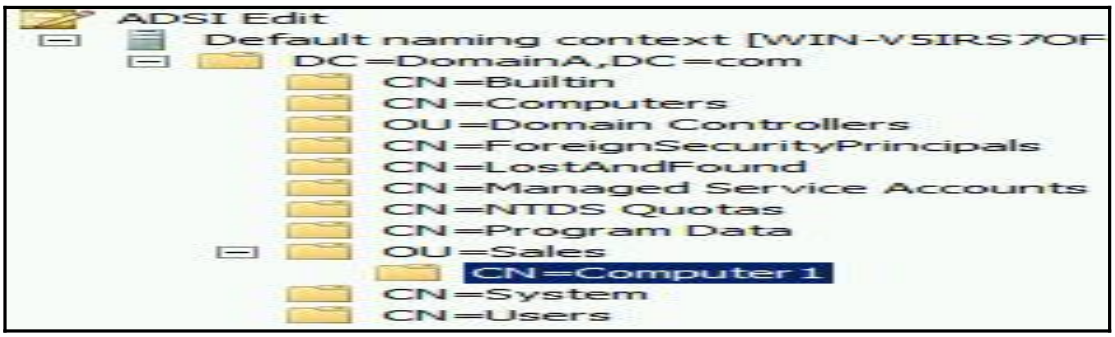

Company A
Mr Red
Mr Blue
Mr Green
Company B
Mr Orange
Mr Purple
Mr Yellow

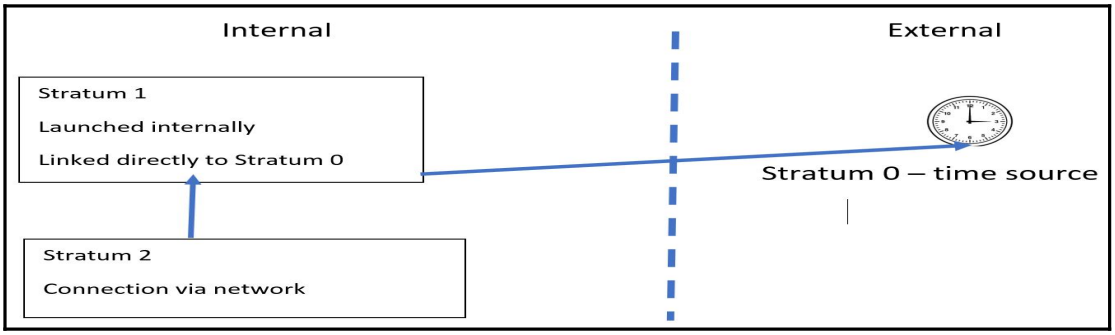

SAML
Company A
Company B
XML Based Authentication

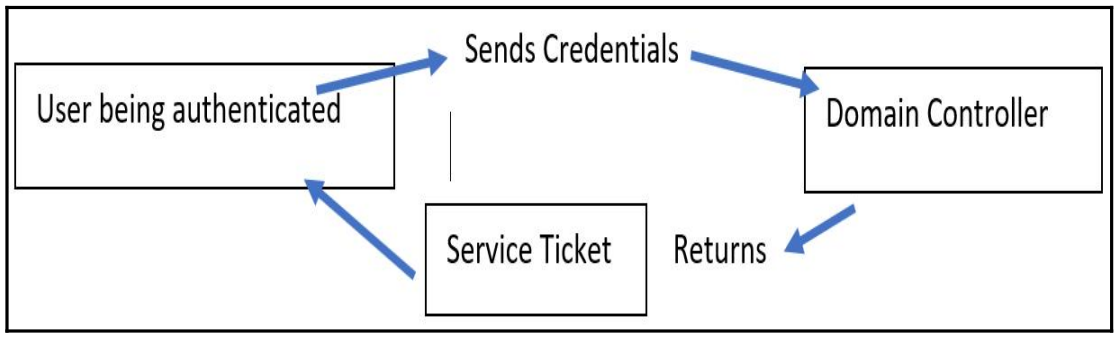

Company A
Mr Red
Mr Blue
Mr Green
Employee ID - 123456
Password: P@$$w0rd
Company B
Mr Orange
Mr Purple
Mr Yellow

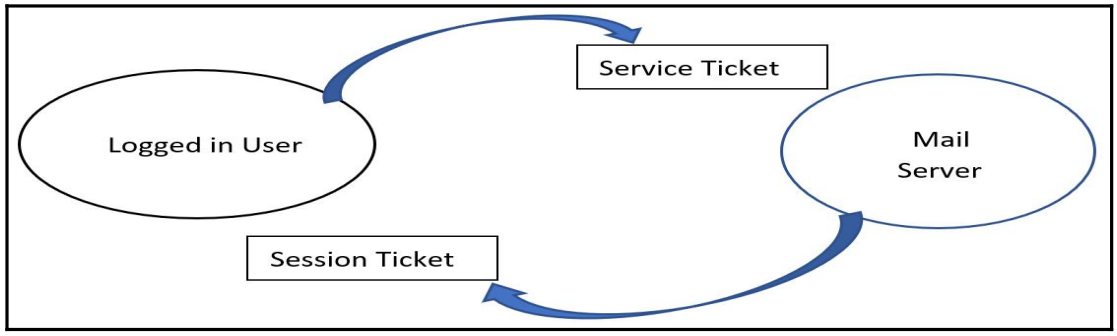

Employee ID: 123456
Password: P@$$w0rd
Company A
Company B
SAML passes details

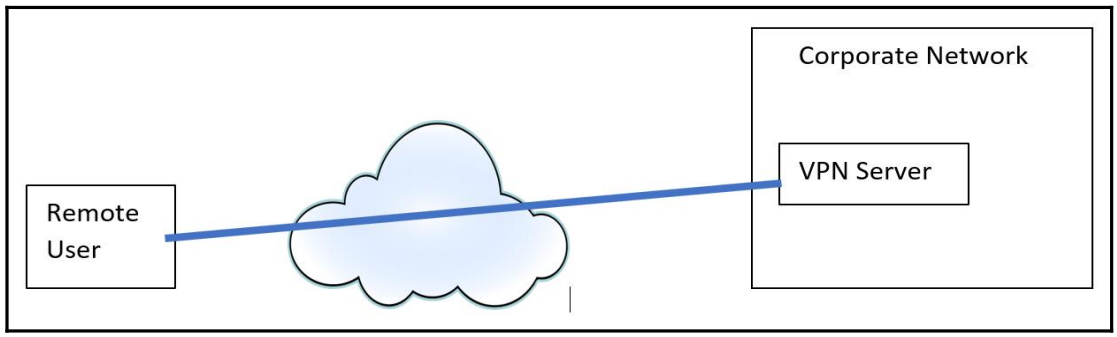

Active Directory Users and Computers [WIN-V5IF
Saved Queries
DomainA.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Sales
Name
Type
Computer 1
Computer


ADSI Edit
Default naming context [WIN-V5IRS7OF
DC=DomainA,DC=com
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=LostAndFound
CN=Managed Service Accounts
CN=NTDS Quotas
CN=Program Data
OU=Sales
CN=Computer 1
CN=System
CN=Users

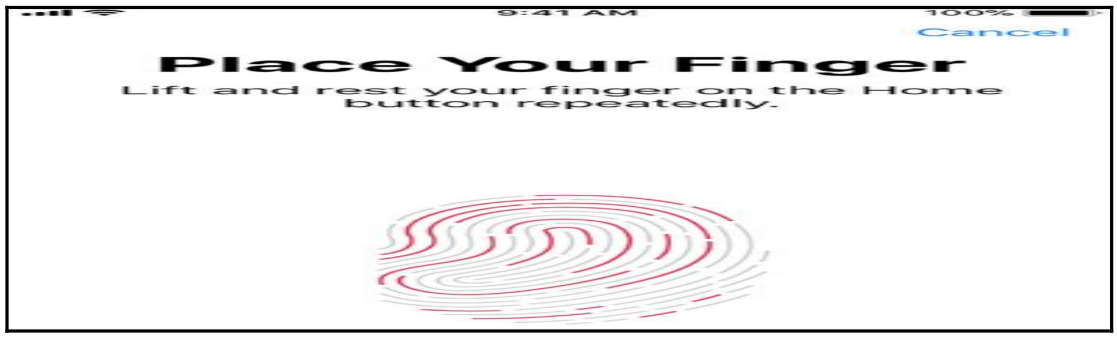

Internal
External
Stratum 1
Launched internally
Linked directly to Stratum 0
Stratum 0 – time source
Stratum 2
Connection via network

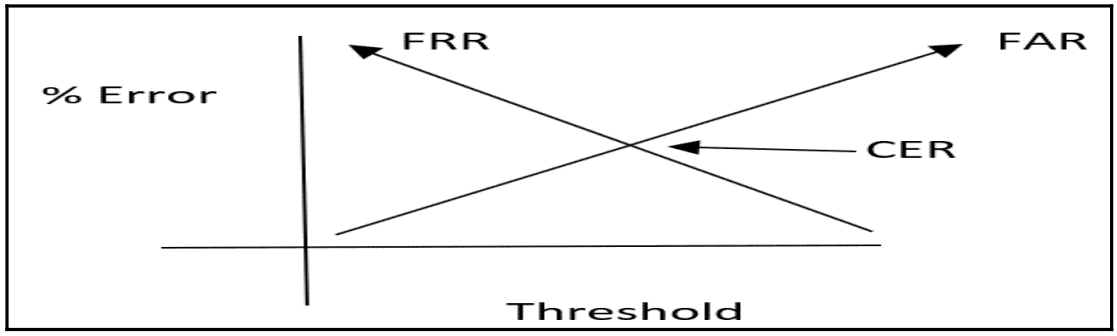

Sends Credentials
User being authenticated
Domain Controller
Service Ticket
Returns


Service Ticket
Logged in User
Mail
Server
Session Ticket

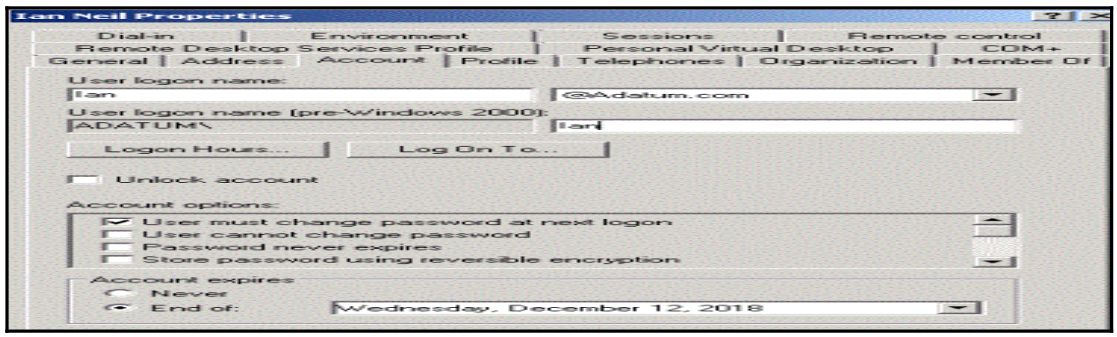

Corporate Network
VPN Server
Remote
User

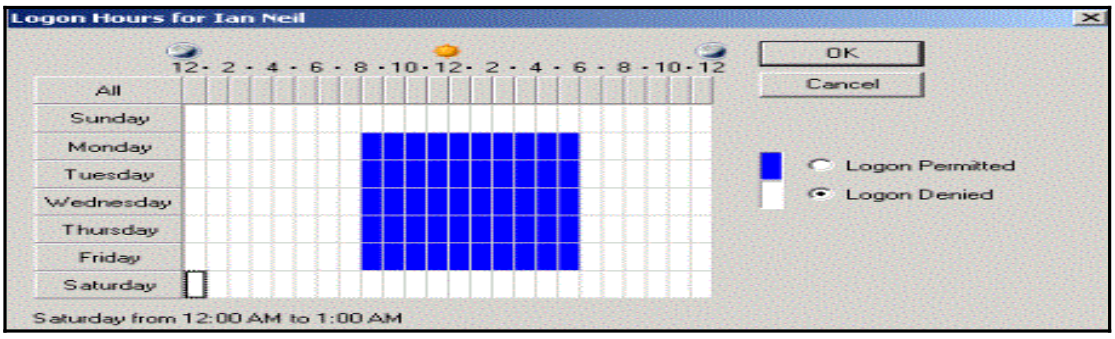

Connection Request
Random String sent as Challenge
Uses client's password to encrypt challenge
Logon allowed
Remote Client
RAS Server

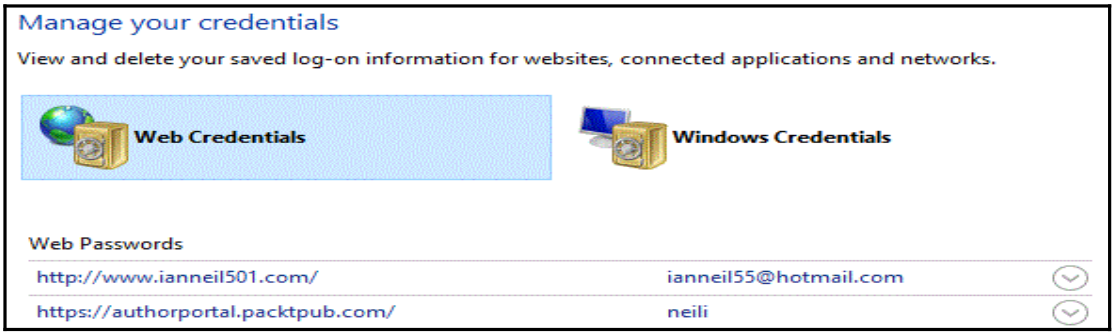

9:41 AM
100%
Cancel
Place Your Finger
Lift and rest your finger on the Home button repeatedly.


FRR
FAR
% Error
CER
Threshold


165323
Use with 30 seconds

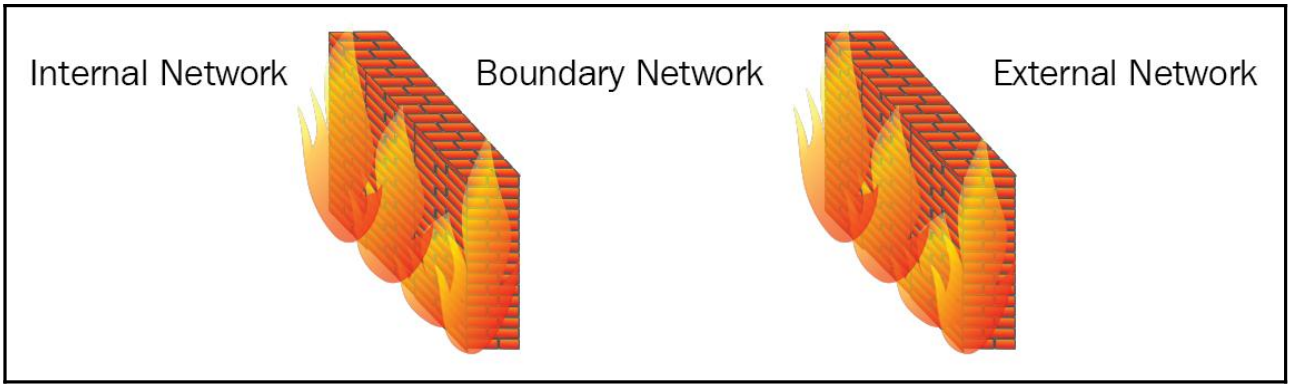

Ian Neil Properties
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
Personal Virtual Desktop
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
User logon name:
Ian
@Adatum.com
User logon name (pre-Windows 2000):
ADATUM\
Ian
Logon Hours...
Log On To...
Unlock account
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account expires
Never
End of:
Wednesday, December 12, 2018

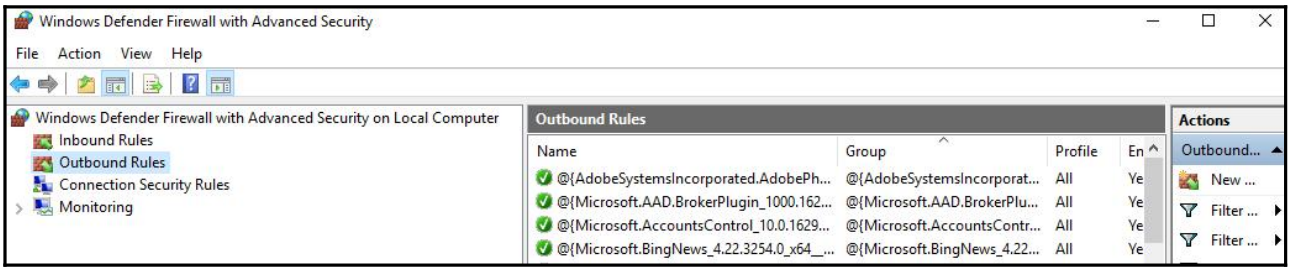

Logon Hours for Ian Neil
12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12
All
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
OK
Cancel
Logon Permitted
Logon Denied
Saturday from 12:00 AM to 1:00 AM

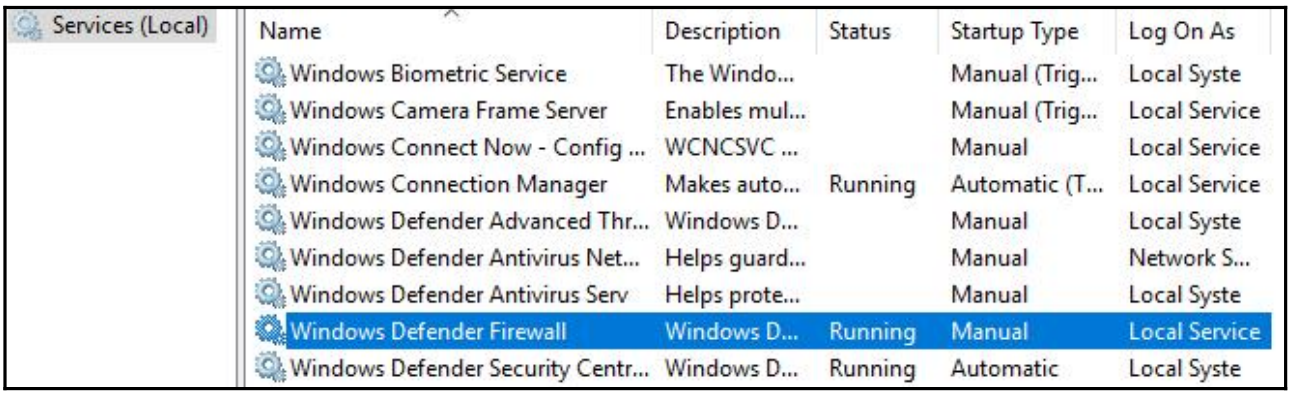

Manage your credentials
View and delete your saved log-on information for websites, connected applications and networks.
Web Credentials
Windows Credentials
Web Passwords
http://www.ianneil501.com/
ianneil55@hotmail.com
https://authorportal.packtpub.com/
neili

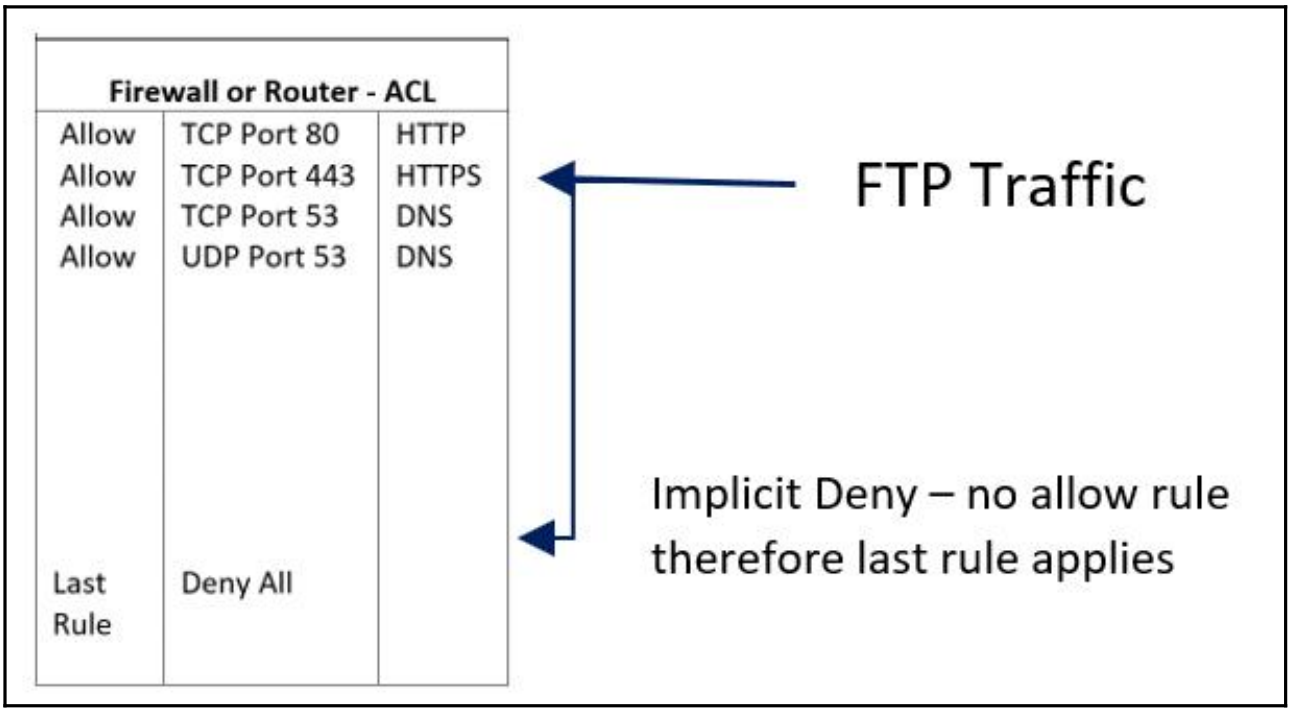
Chapter 05: Understanding Network Components

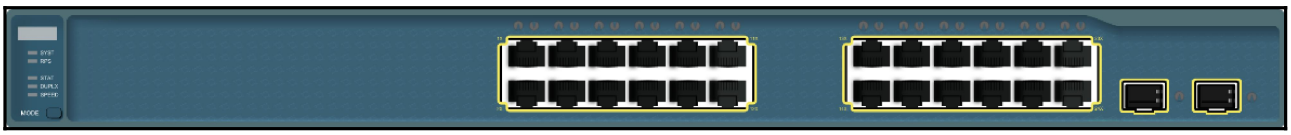
Layer	Description	Example	Devices	Packet Structure
7	Application	HTTP, SMTP		
6	Presentation	Encryption, Formatting		
5	Session	Logging On/Off		
4	Transport	TCP, UDP		Datagrams
3	Network	IP, ICMP	Router	Packets
2	Data Link	IP Sec, VLAN, ARP	Switch	Frames
1	Physical	Cables	Hub	Bits - 01010101

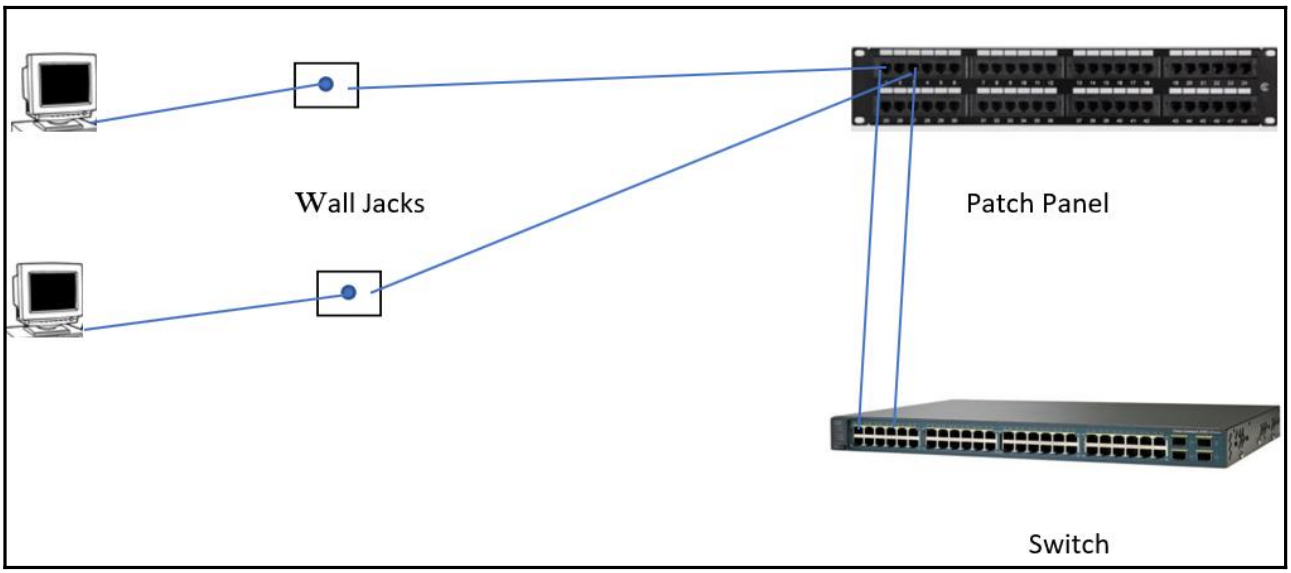


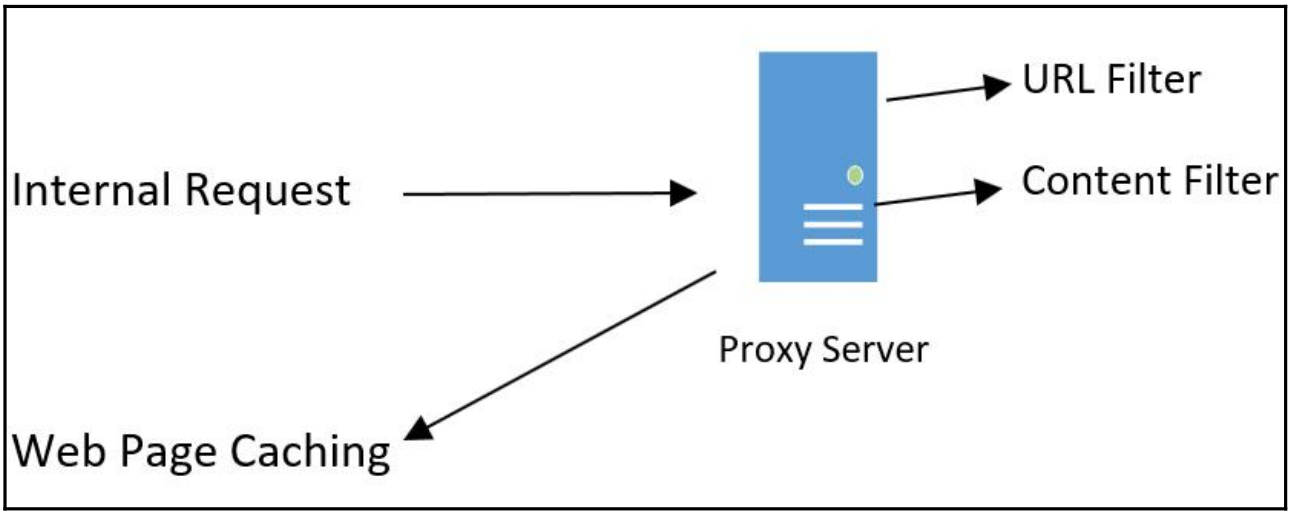


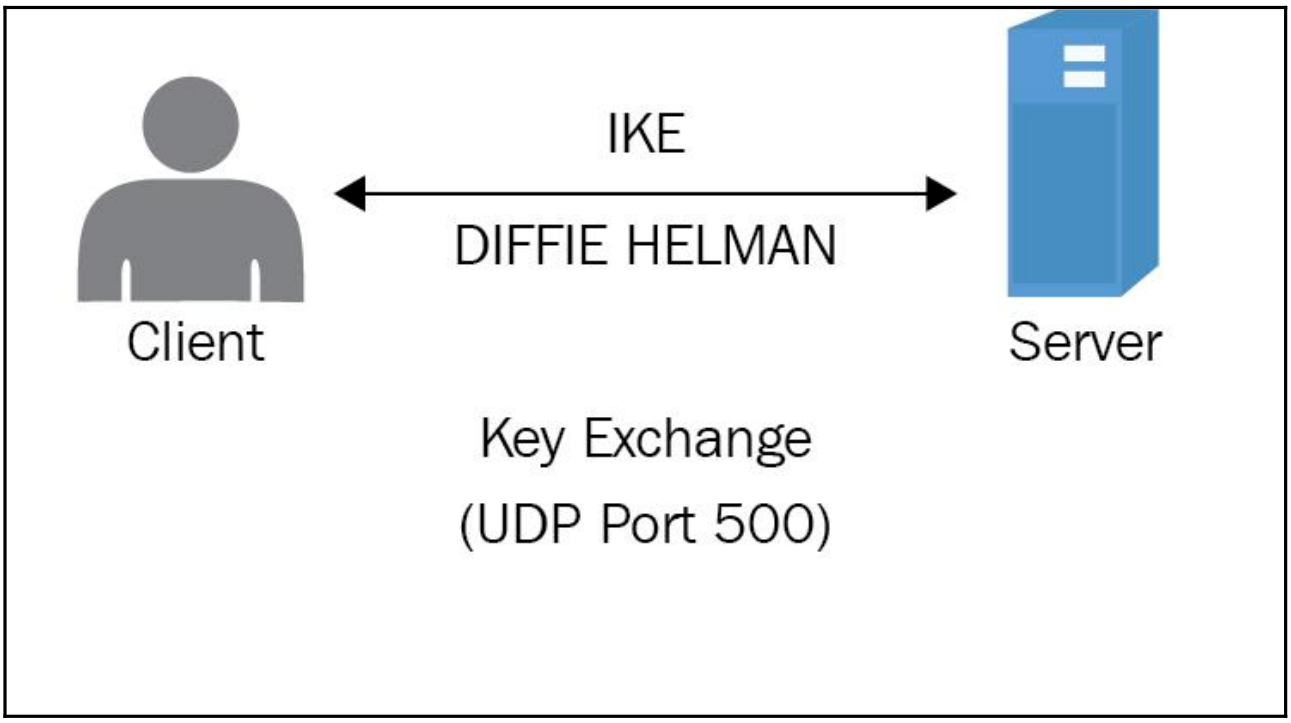

Services (Local)
Name
Description
Status
Startup Type
Log On As
Windows Biometric Service
The Windo...
Manual (Trig...
Local Syste
Windows Camera Frame Server
Enables mul...
Manual (Trig...
Local Service
Windows Connect Now - Config ...
WCNCSVC ...
Manual
Local Service
Windows Connection Manager
Makes auto...
Running
Automatic (T...
Local Service
Windows Defender Advanced Thr...
Windows D...
Manual
Local Syste
Windows Defender Antivirus Net...
Helps guard...
Manual
Network S...
Windows Defender Antivirus Serv
Helps prote...
Manual
Local Syste
Windows Defender Firewall
Windows D...
Running
Manual
Local Service
Windows Defender Security Centr...
Windows D...
Running
Automatic
Local Syste

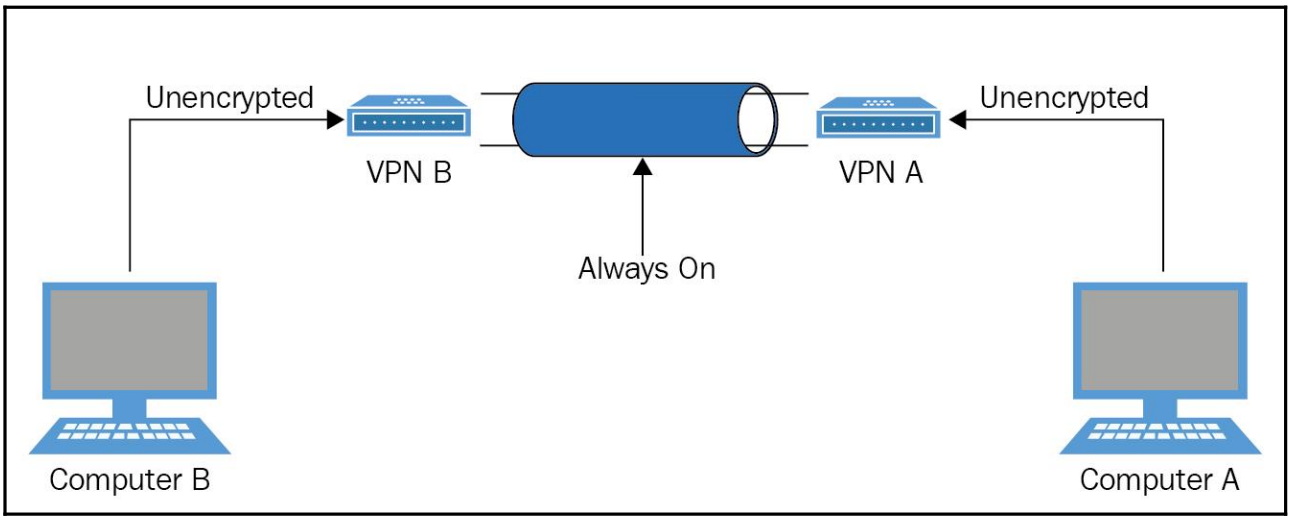

Firewall or Router - ACL
Allow
TCP Port 80
HTTP
Allow
TCP Port 443
HTTPS
Allow
TCP Port 53
DNS
Allow
UDP Port 53
DNS
Last Rule
Deny All
FTP Traffic
Implicit Deny – no allow rule therefore last rule applies

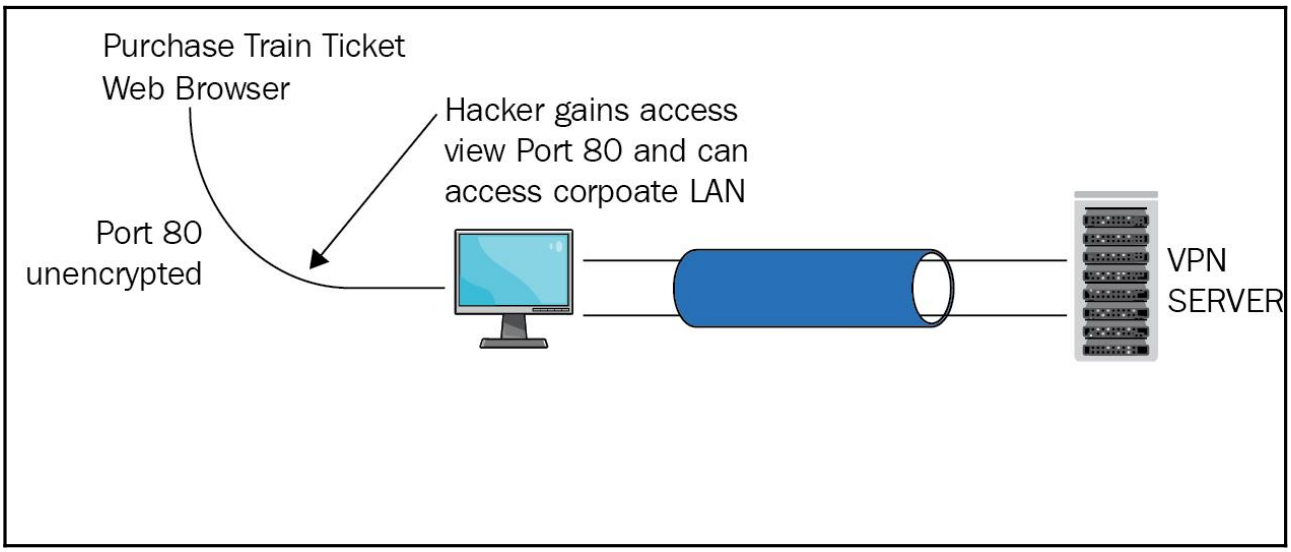


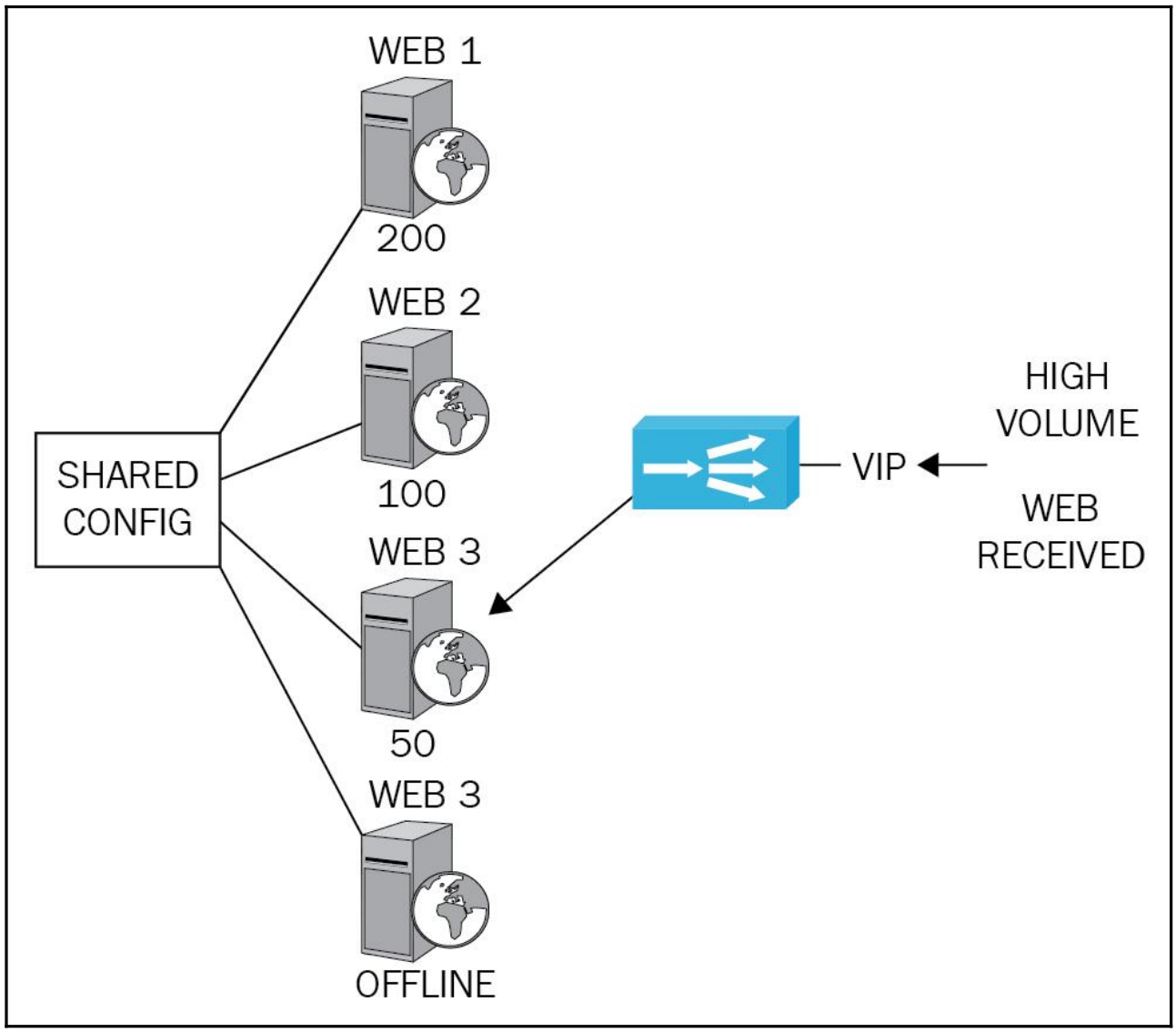

Wall Jacks
Patch Panel
Switch

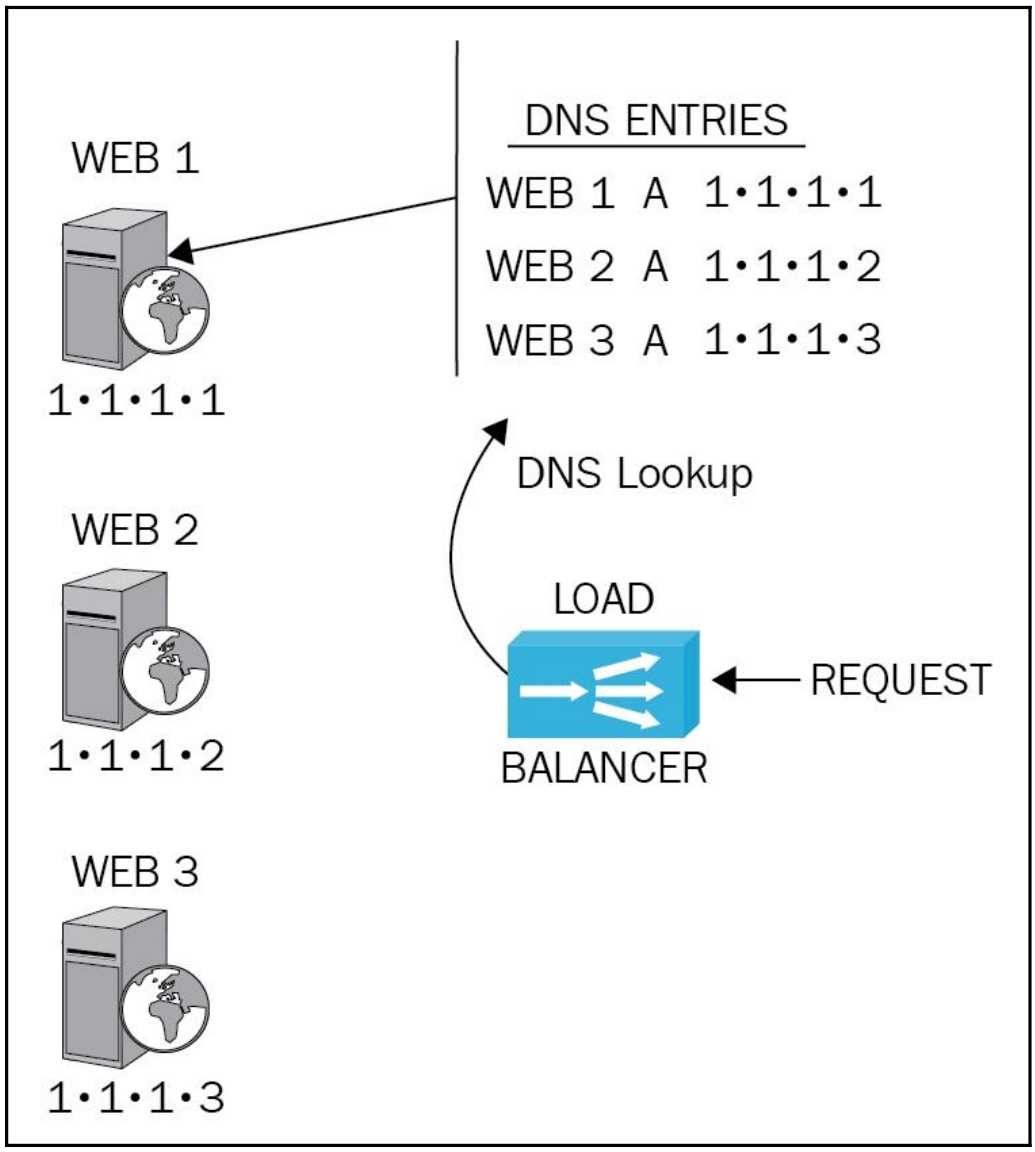

Internal Request
URL Filter
Content Filter
Proxy Server
Web Page Caching

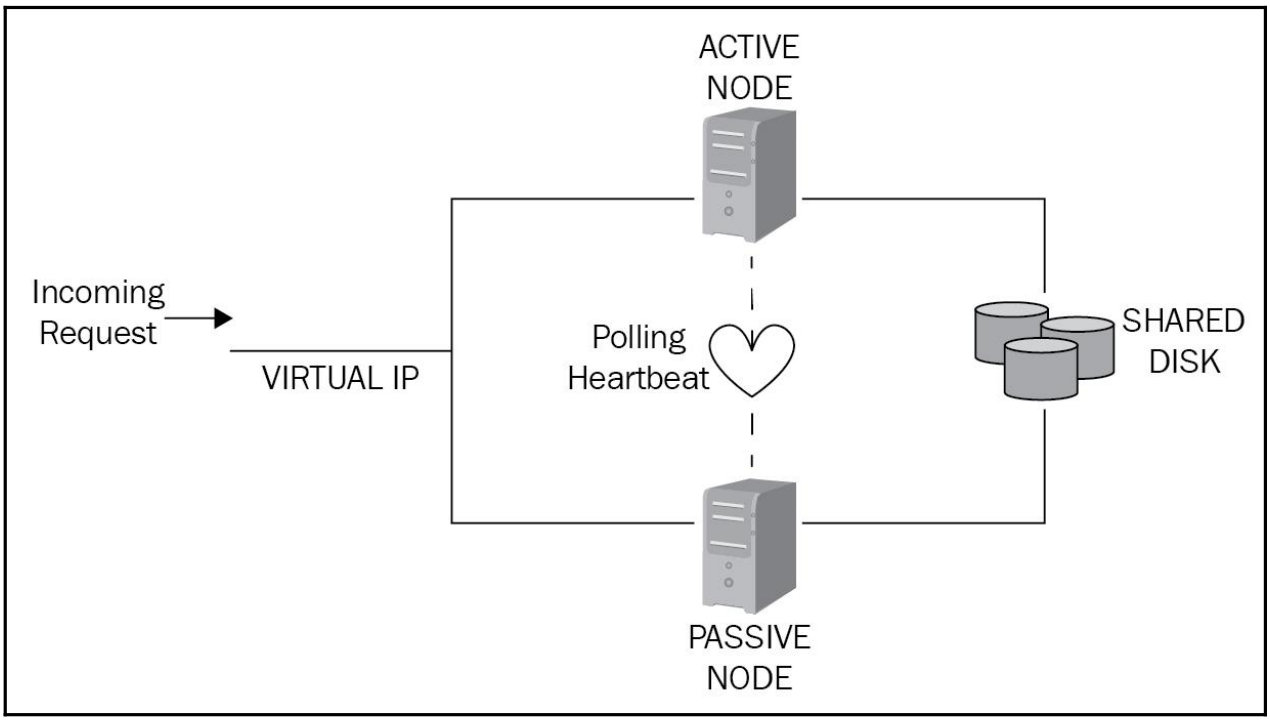

IKE
DIFFIE HELMAN
Client
Server
Key Exchange
(UDP Port 500)

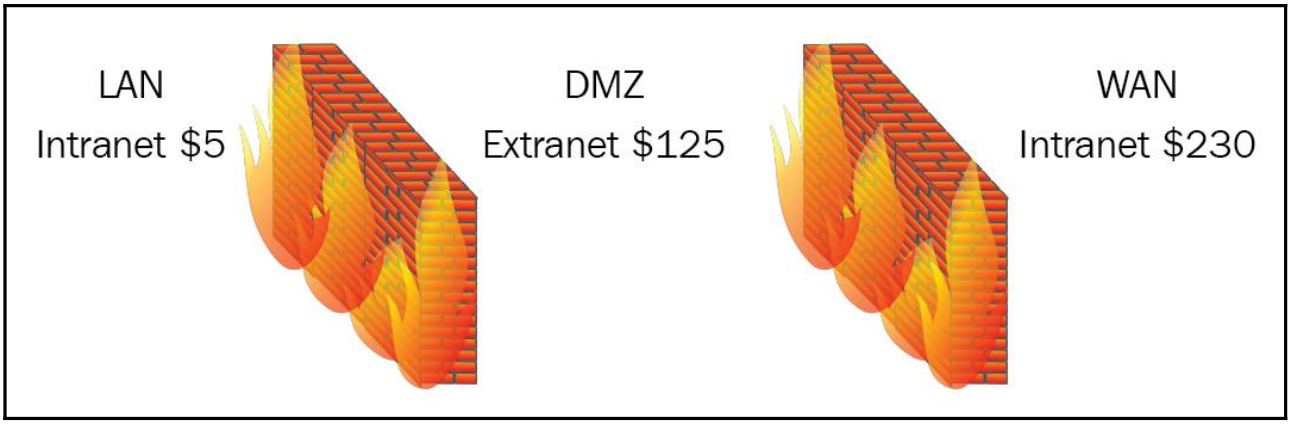

Unencrypted
VPN B
VPN A
Unencrypted
Always On
Computer B
Computer A

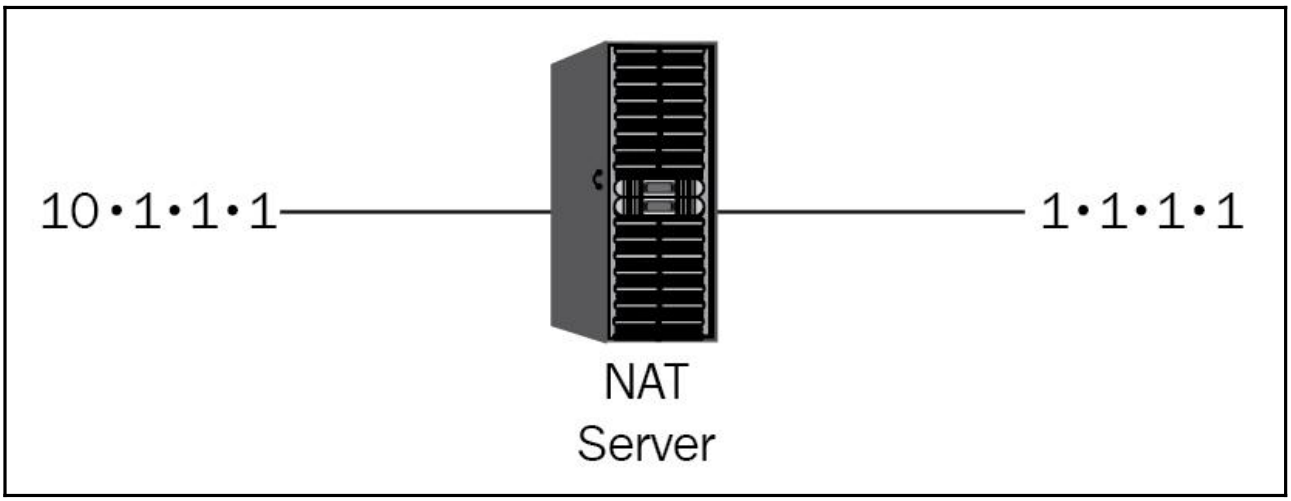

Purchase Train Ticket
Web Browser
Hacker gains access
view Port 80 and can
access corpoate LAN
Port 80
unencrypted
VPN
SERVER

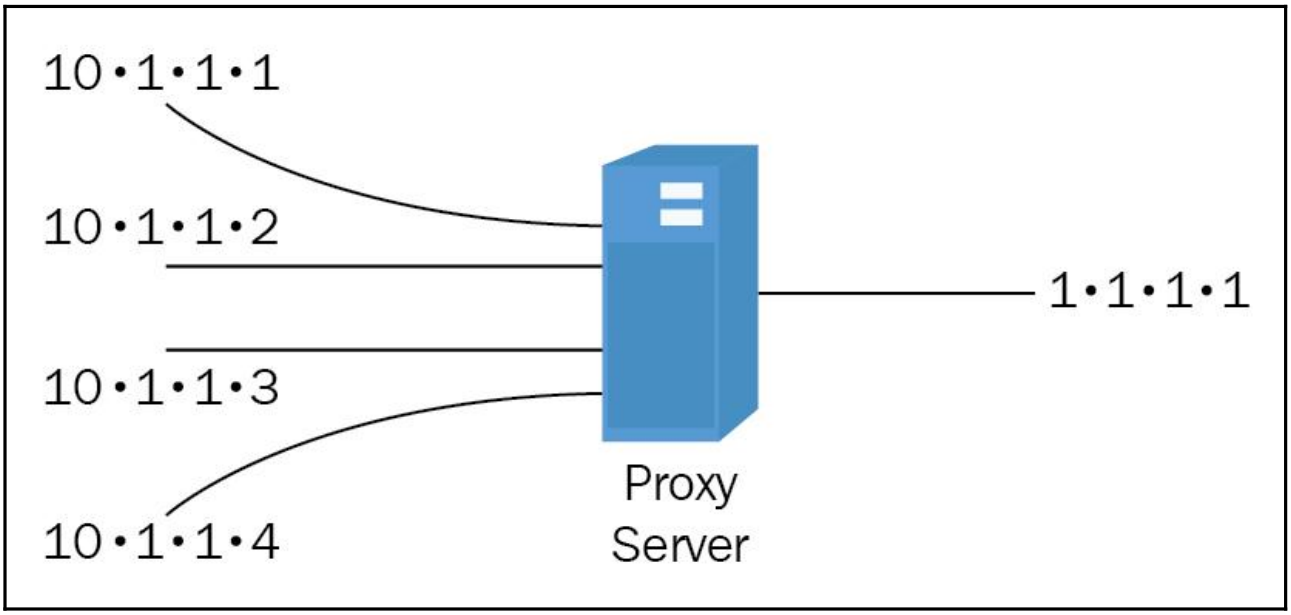

WEB 1
200
WEB 2
100
SHARED
CONFIG
HIGH
VOLUME
VIP
WEB
RECEIVED
WEB 3
50
WEB 3
OFFLINE

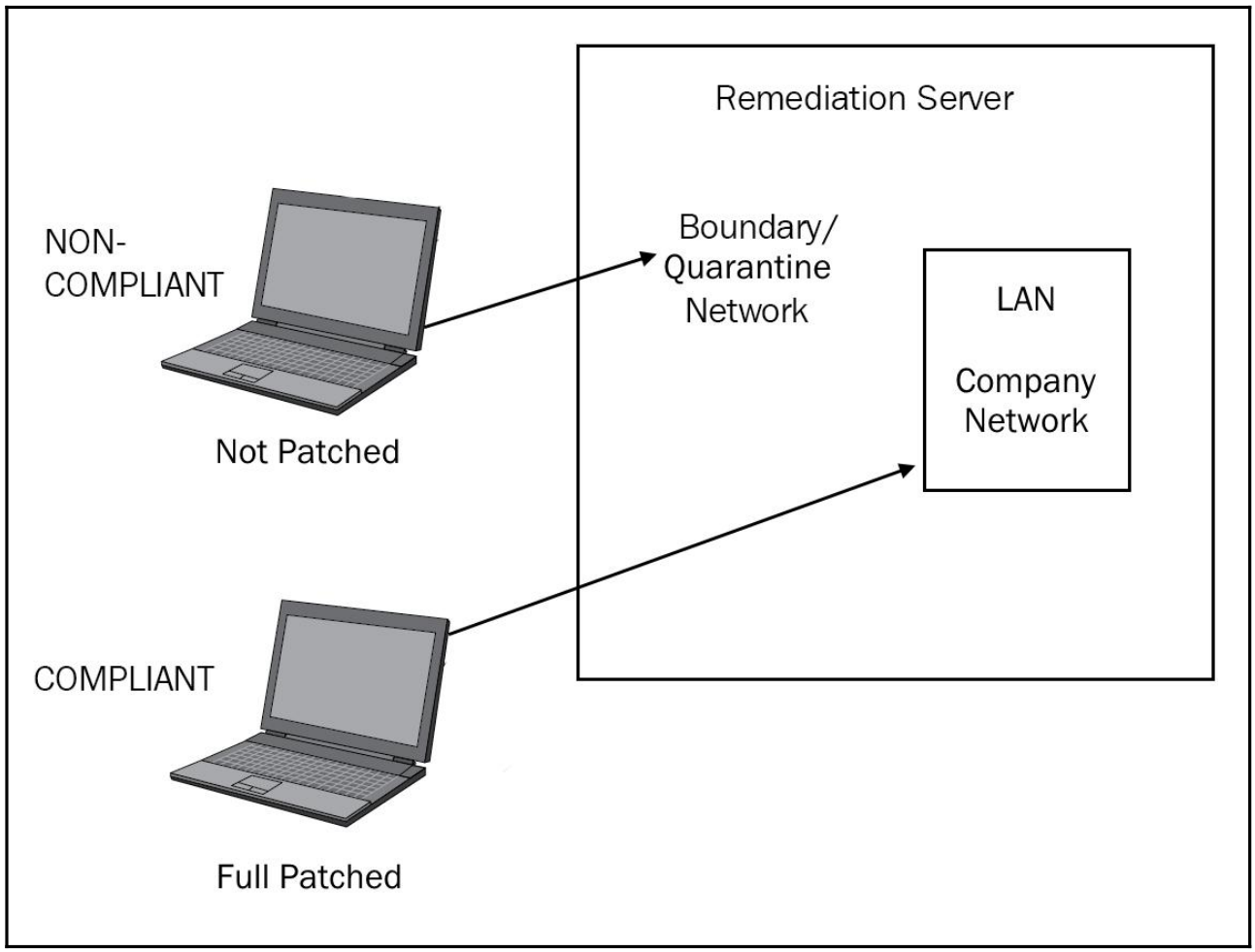

DNS ENTRIES
WEB 1 A 1•1•1•1
WEB 2 A 1•1•1•2
WEB 3 A 1•1•1•3
WEB 1
1•1•1•1
WEB 2
1•1•1•2
WEB 3
1•1•1•3
DNS Lookup
LOAD
REQUEST
BALANCER

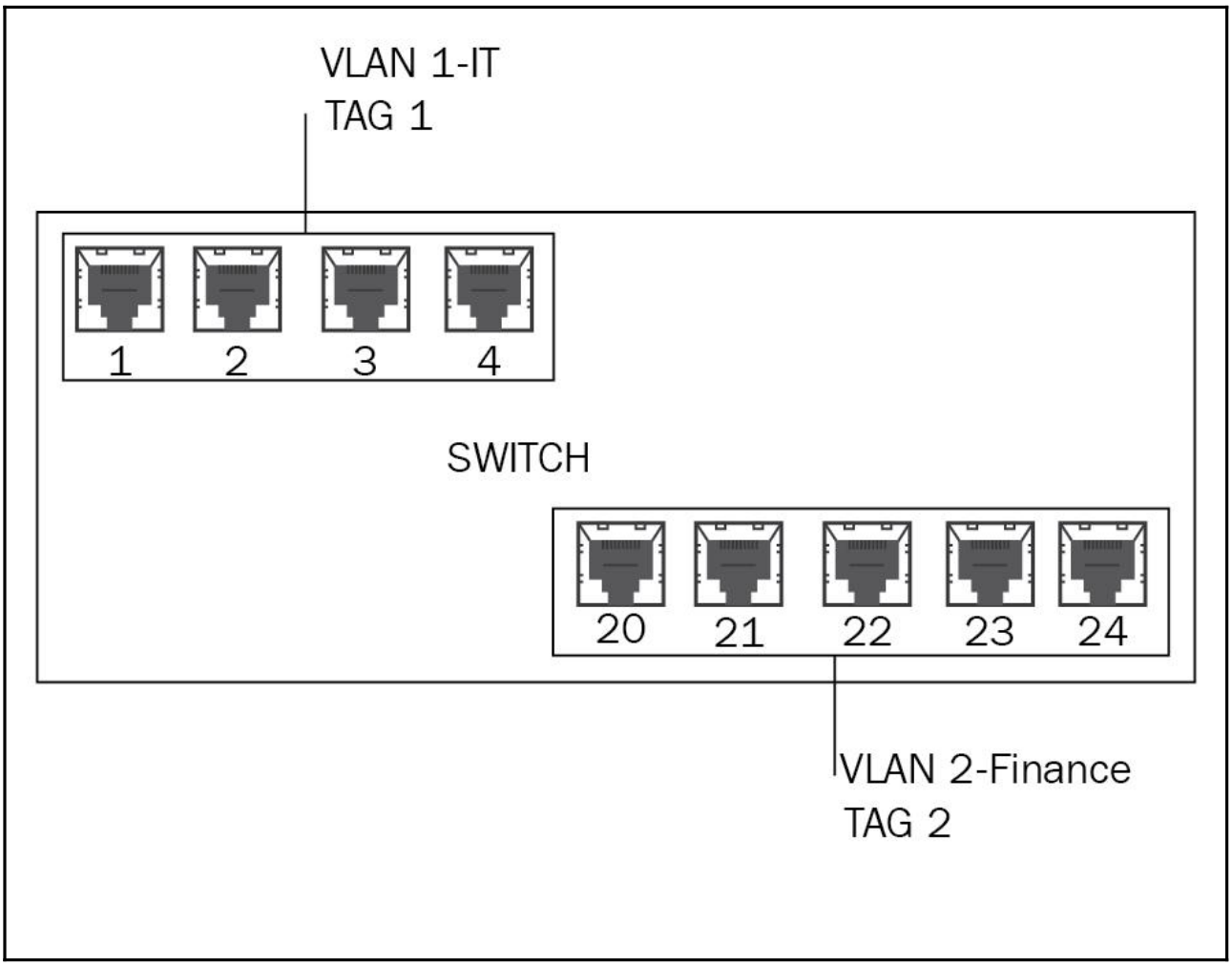

ACTIVE
NODE
Incoming
Request
VIRTUAL IP
Polling
Heartbeat
SHARED
DISK
PASSIVE
NODE

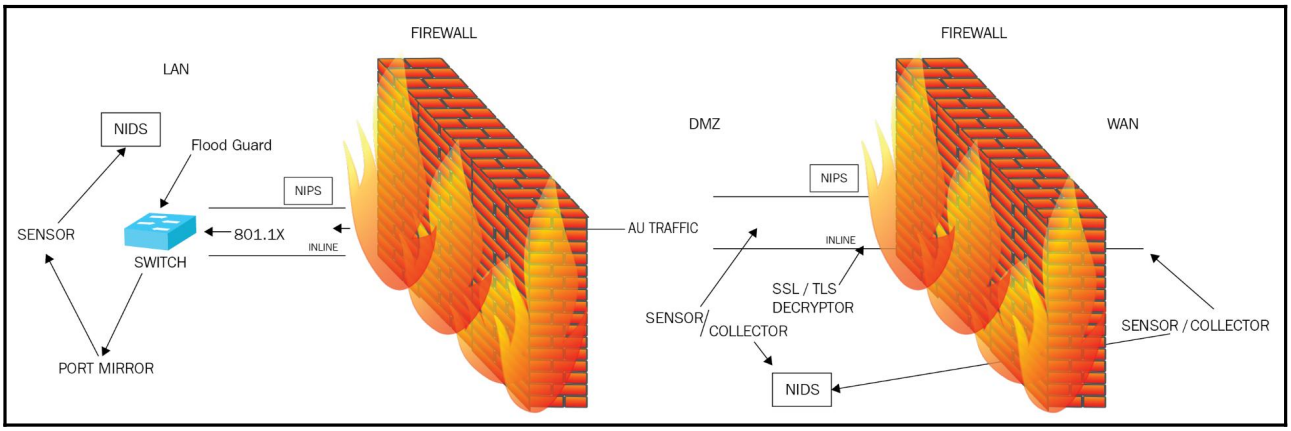

LAN
Intranet $5
DMZ
Extranet $125
WAN
Intranet $230

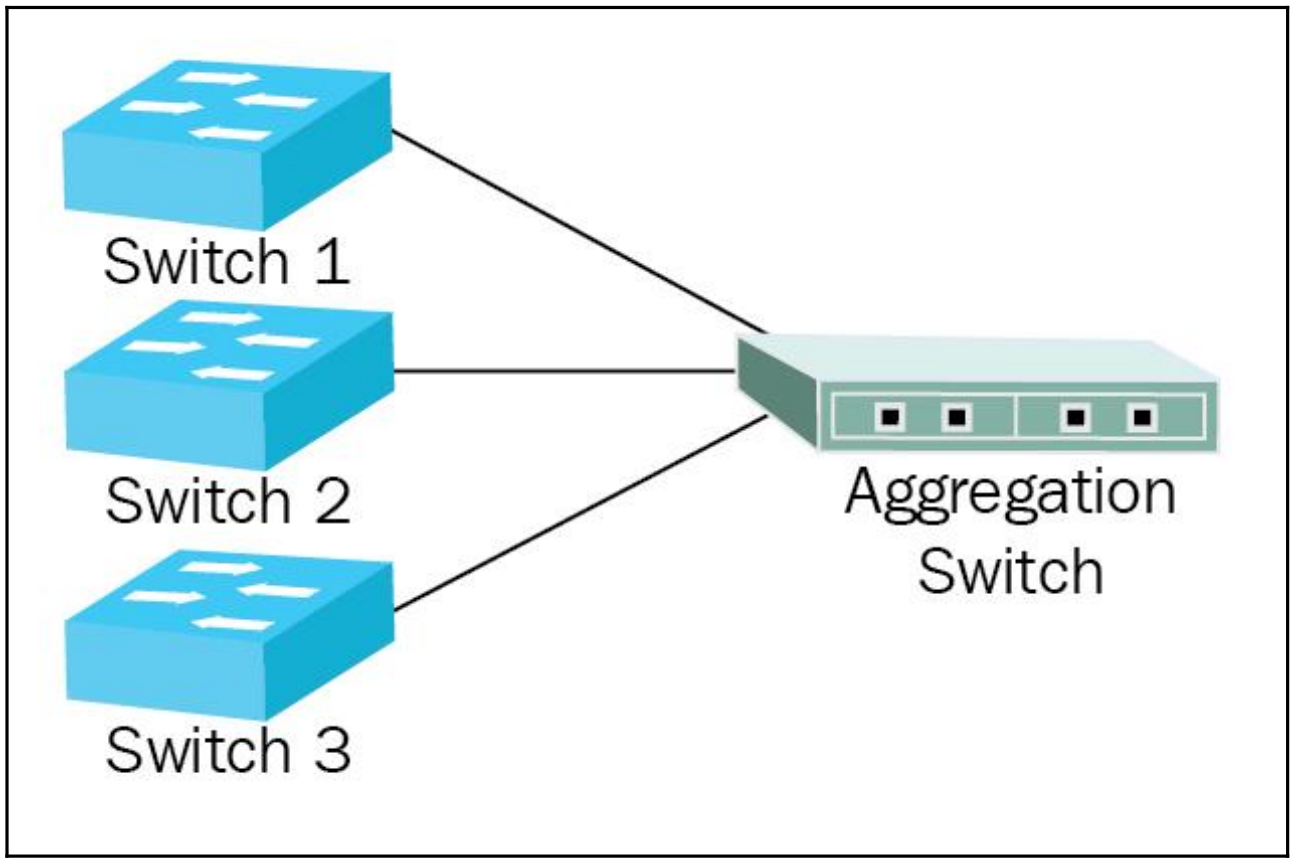

10•1•1•1
1•1•1•1
NAT
Server

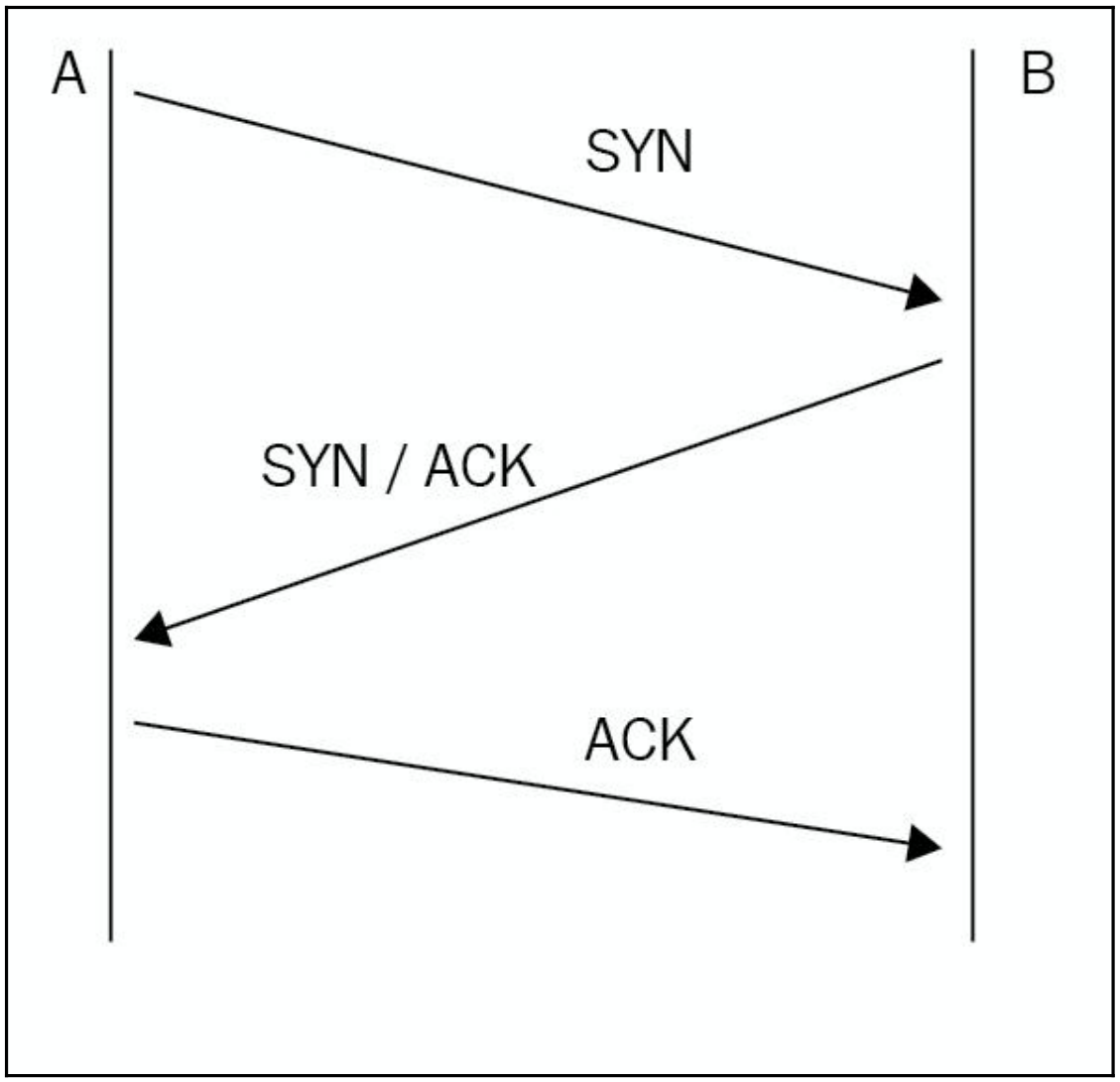

10•1•1•1
10•1•1•2
10•1•1•3
10•1•1•4
1•1•1•1
Proxy
Server

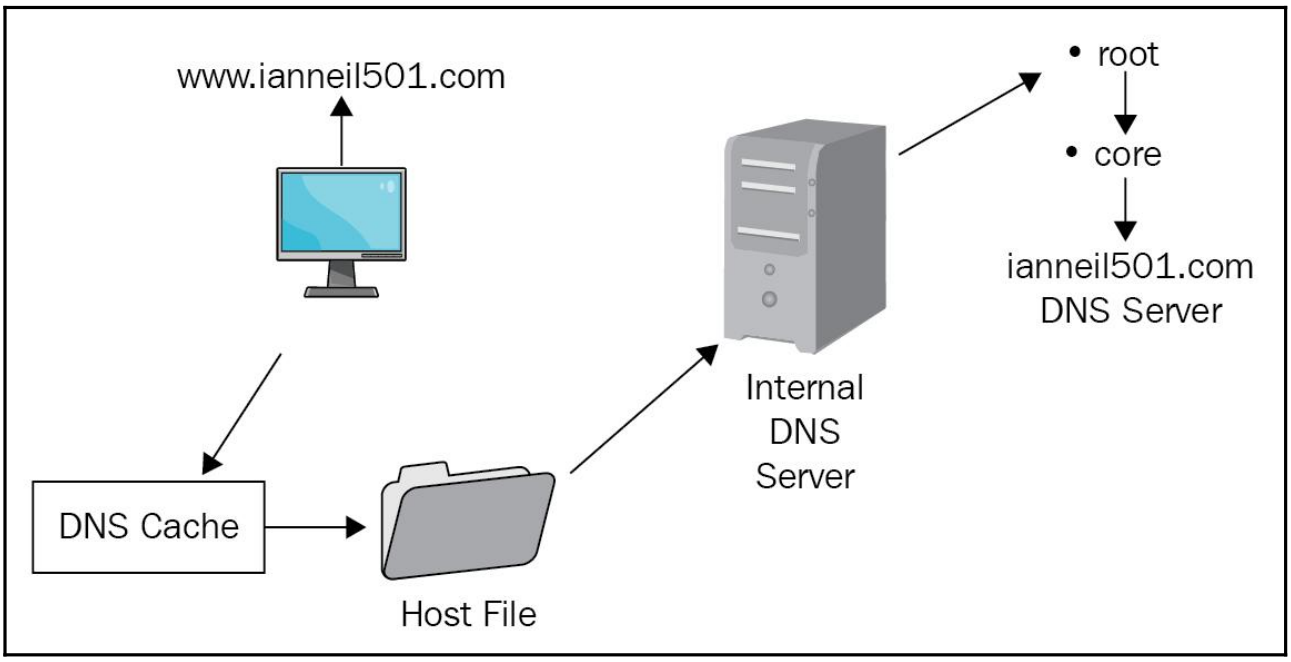

Remediation Server
NON-
COMPLIANT
Boundary/
Quarantine
Network
LAN
Company
Network
Not Patched
COMPLIANT
Full Patched

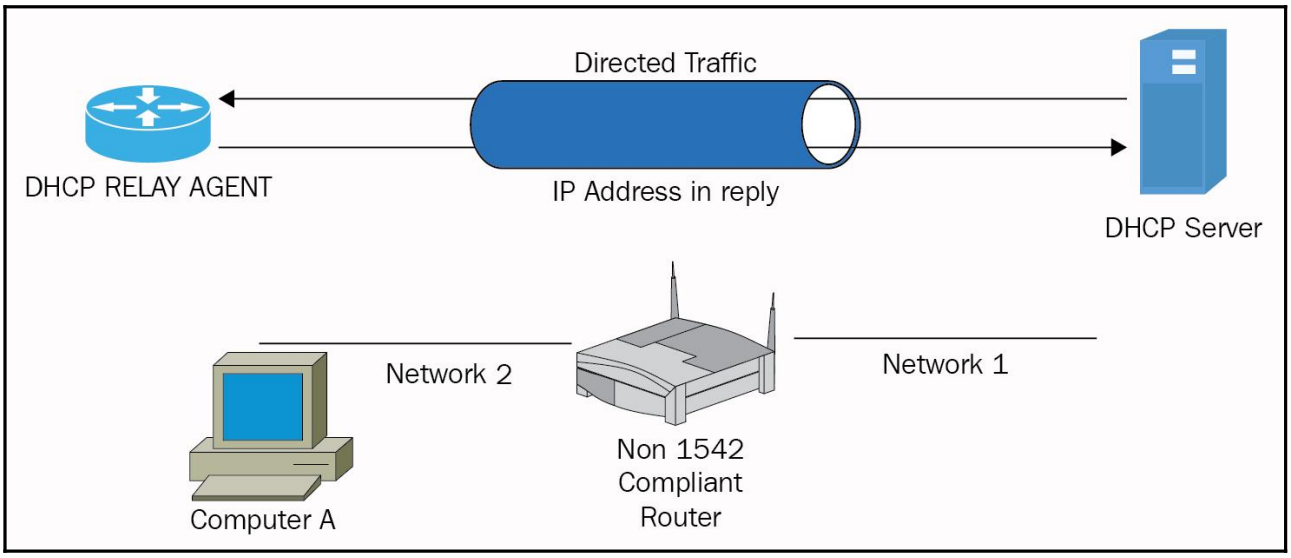

VLAN 1-IT
TAG 1
1
2
3
4
SWITCH
20
21
22
23
24
VLAN 2-Finance
TAG 2

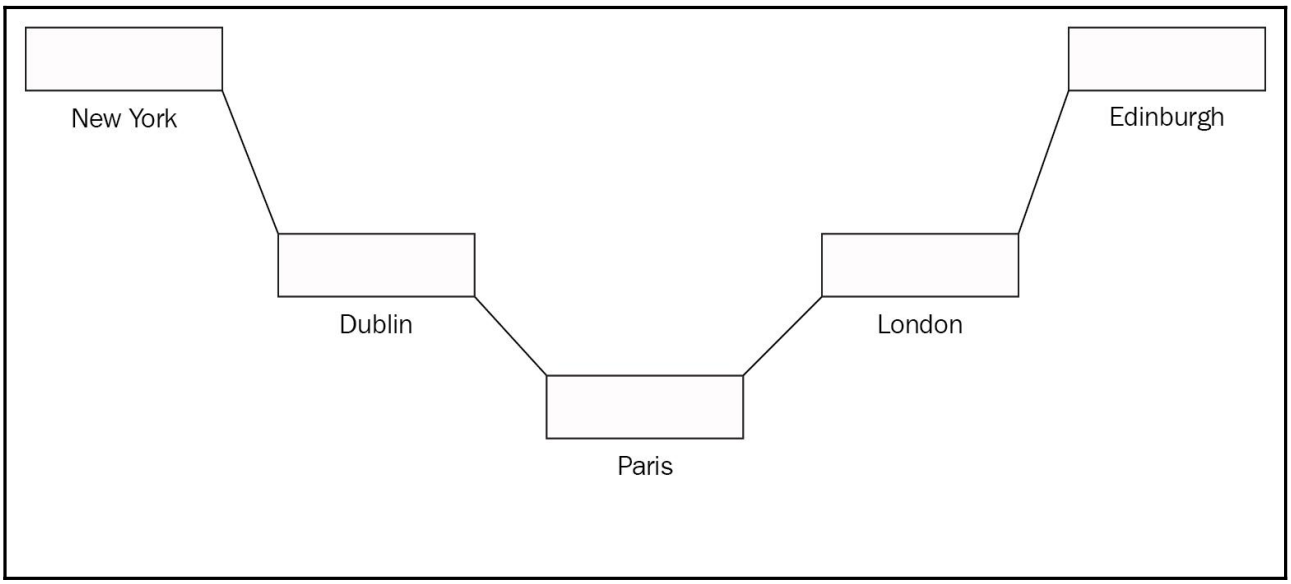

FIREWALL
LAN
NIDS
Flood Guard
NIPS
SENSOR
801.1X
INLINE
SWITCH
PORT MIRROR
AU TRAFFIC
FIREWALL
DMZ
WAN
NIPS
INLINE
SSL / TLS
DECRYPTOR
SENSOR
COLLECTOR
NIDS
SENSOR / COLLECTOR

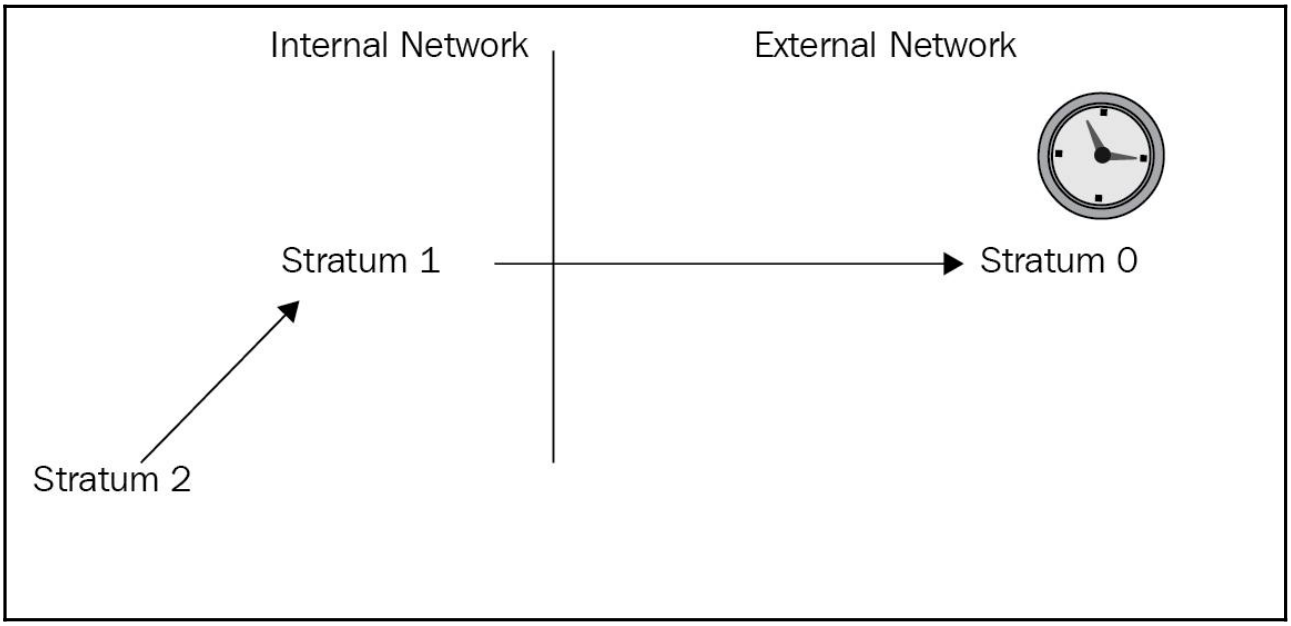

Switch 1
Switch 2
Switch 3
Aggregation
Switch

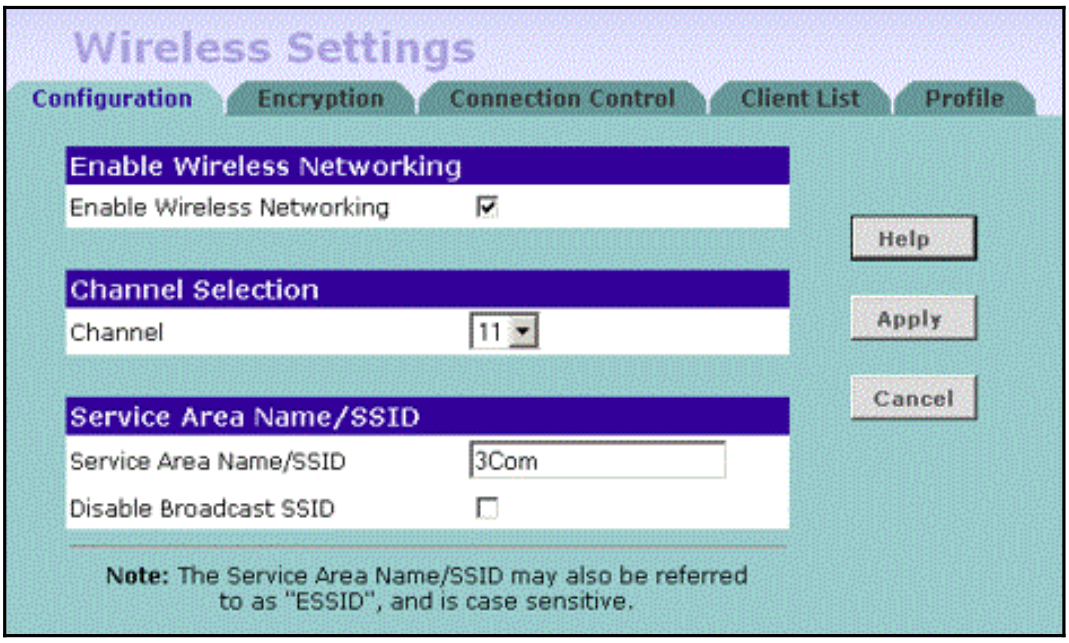

A
B
SYN
SYN / ACK
ACK


www.ianneil501.com
• root
• core
ianneil501.com
DNS Server
Internal
DNS
Server
DNS Cache
Host File

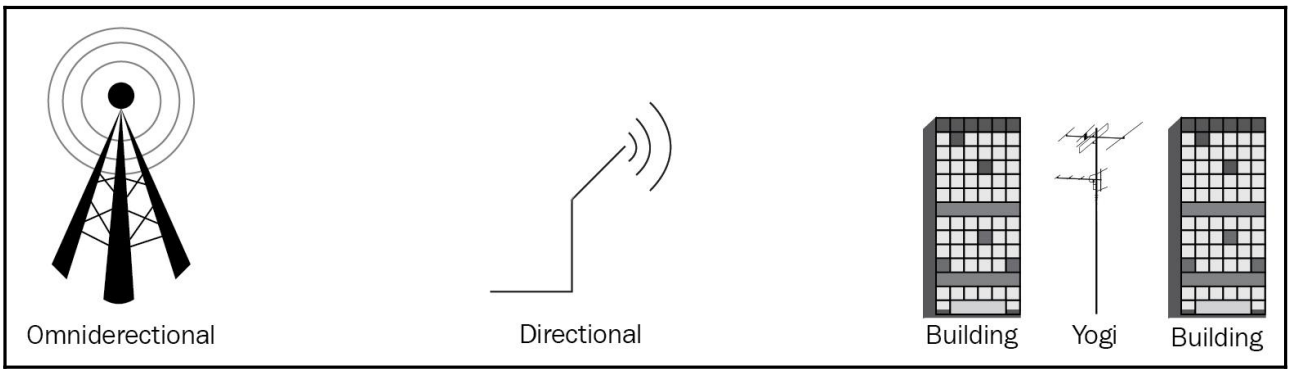

Directed Traffic
DHCP RELAY AGENT
IP Address in reply
DHCP Server
Network 2
Network 1
Non 1542
Compliant
Router
Computer A


New York
Edinburgh
Dublin
London
Paris

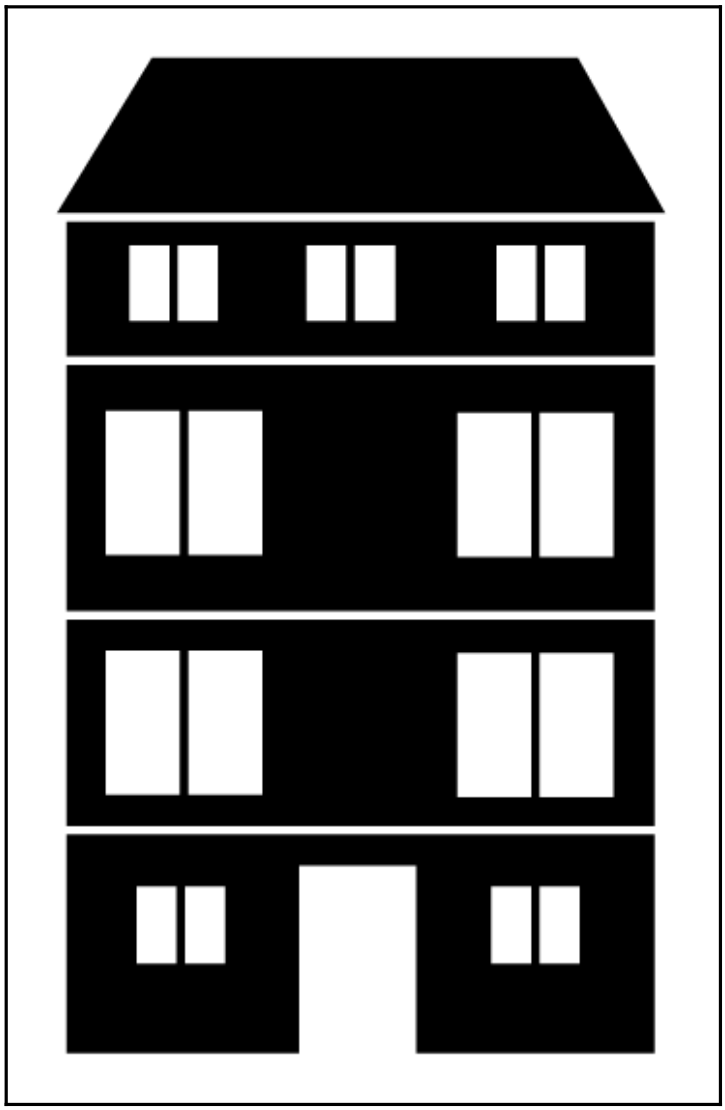

Internal Network
External Network
Stratum 1
Stratum 0
Stratum 2

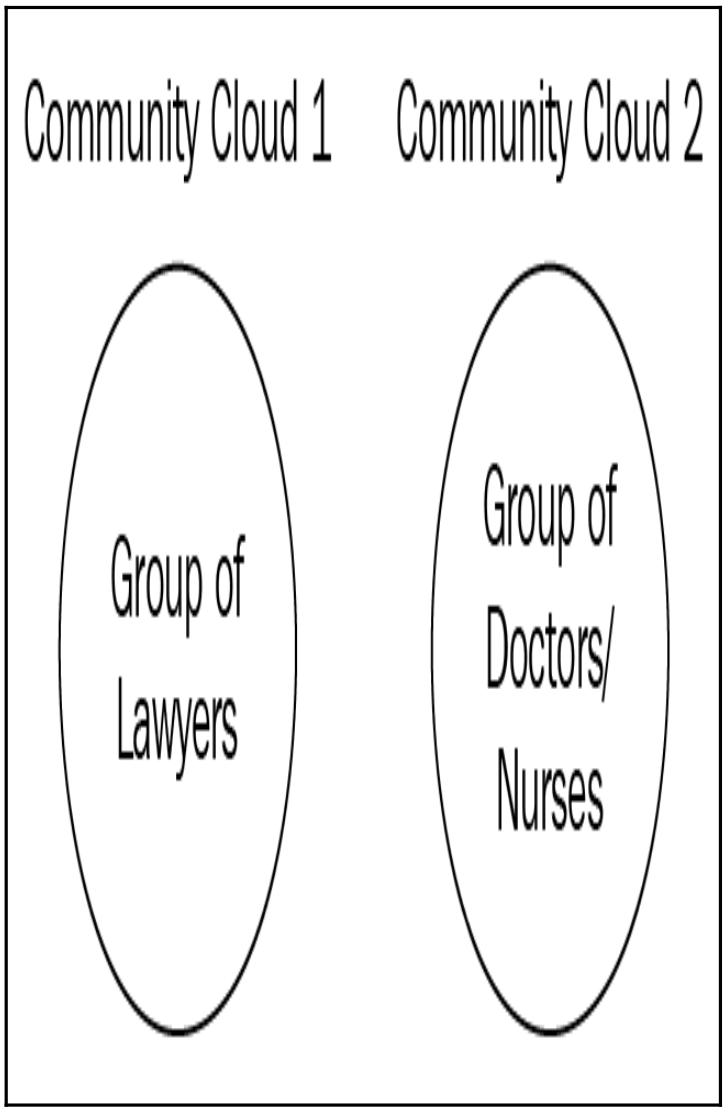

Wireless Settings
Configuration
Encryption
Connection Control
Client List
Profile
Enable Wireless Networking
Enable Wireless Networking
Channel Selection
Channel
11
Service Area Name/SSID
Service Area Name/SSID
3Com
Disable Broadcast SSID
Note: The Service Area Name/SSID may also be referred to as "ESSID", and is case sensitive.
Help
Apply
Cancel

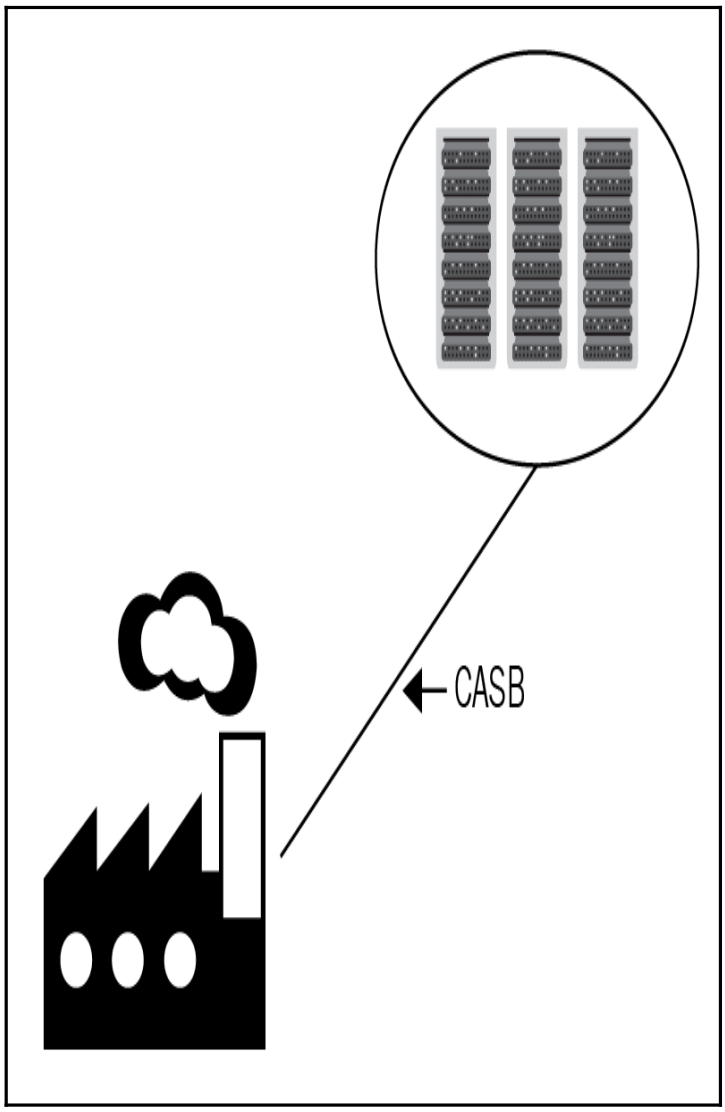

Wireless Settings
Configuration
Encryption
Connection Control
Client List
Profile
Enable Connection Control
All Wireless PCs can connect to the Gateway
Only authorised Wireless PCs can connect to the Gateway
Note: Enabling this feature will disconnect existing Wireless PCs.
Note: Use the PC Privileges feature on the Firewall page to restrict individual PCs access to the Internet.
Authorised Wireless PCs
delete
00-04-75-CC-3A-4B
Help
New

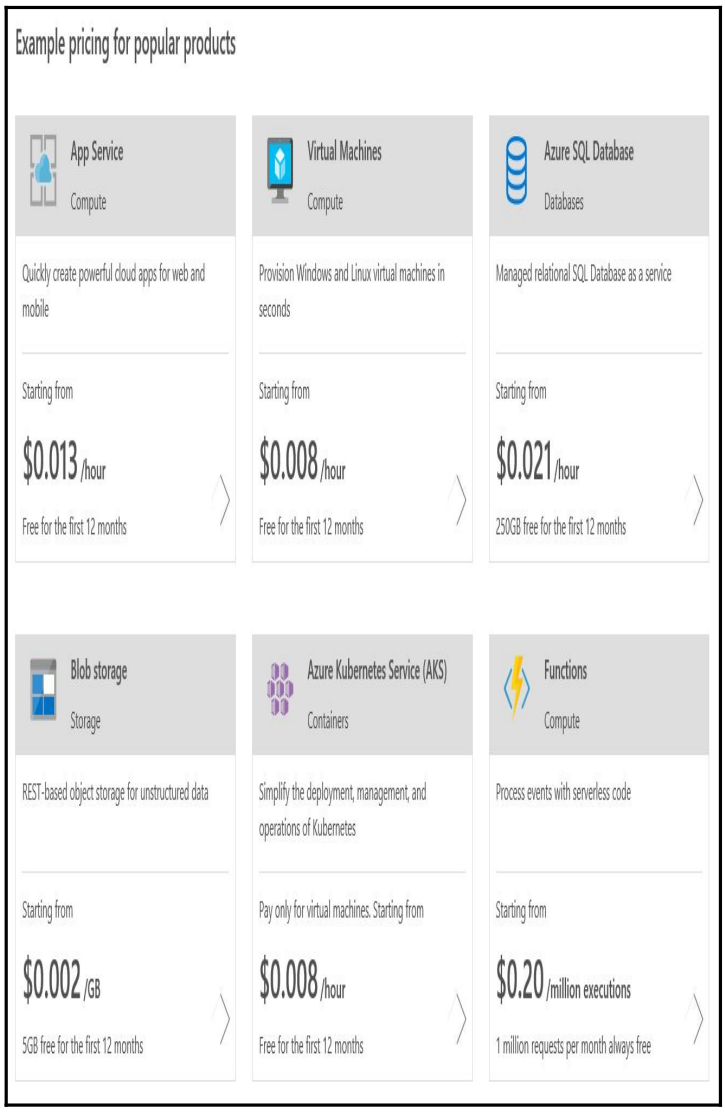

Omniderectional
Directional
Building
Yogi
Building

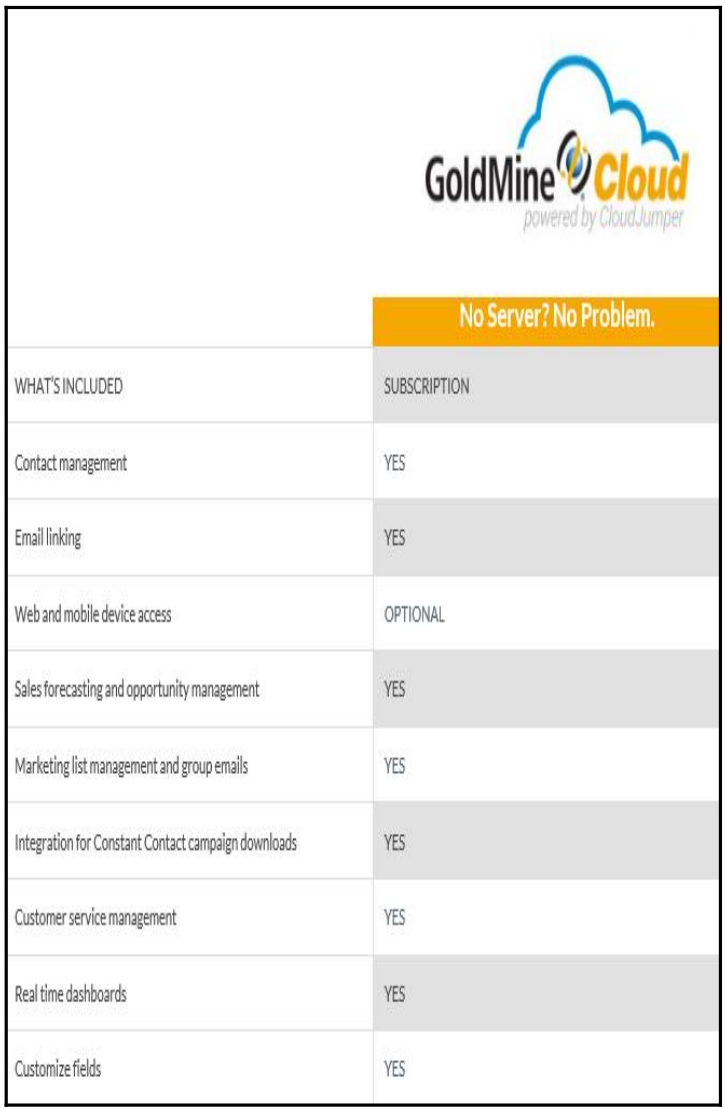
Chapter 06: Understanding Cloud Models and Virtualization



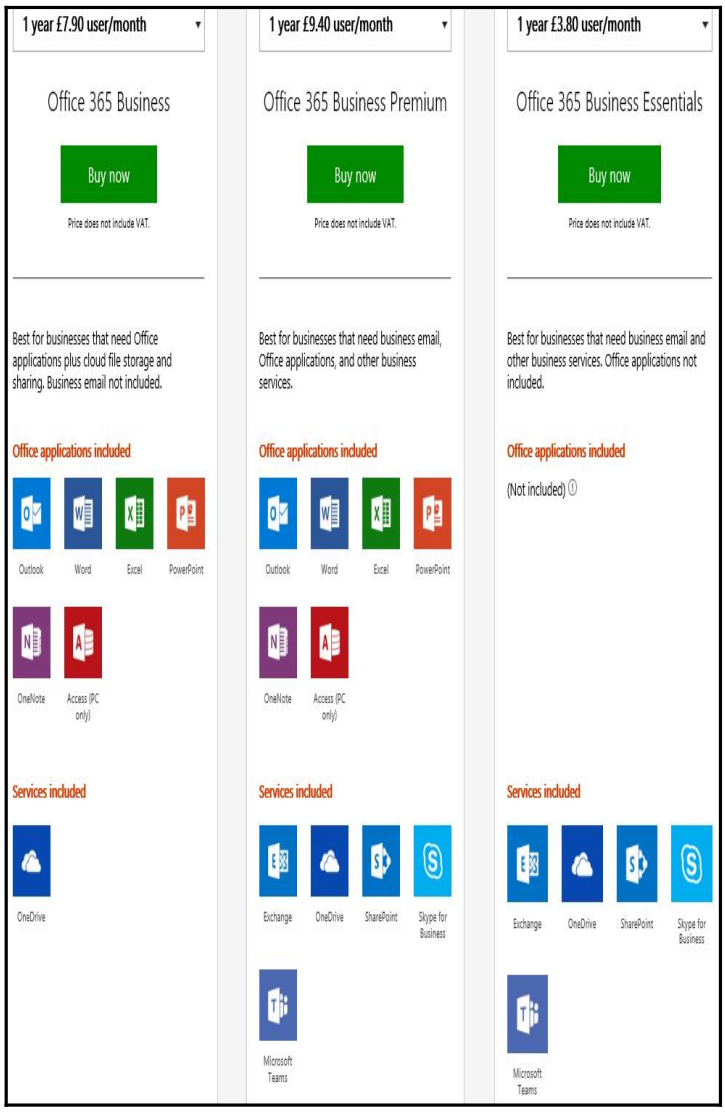

Community Cloud 1
Community Cloud 2
Group of Lawyers
Group of Doctors/ Nurses

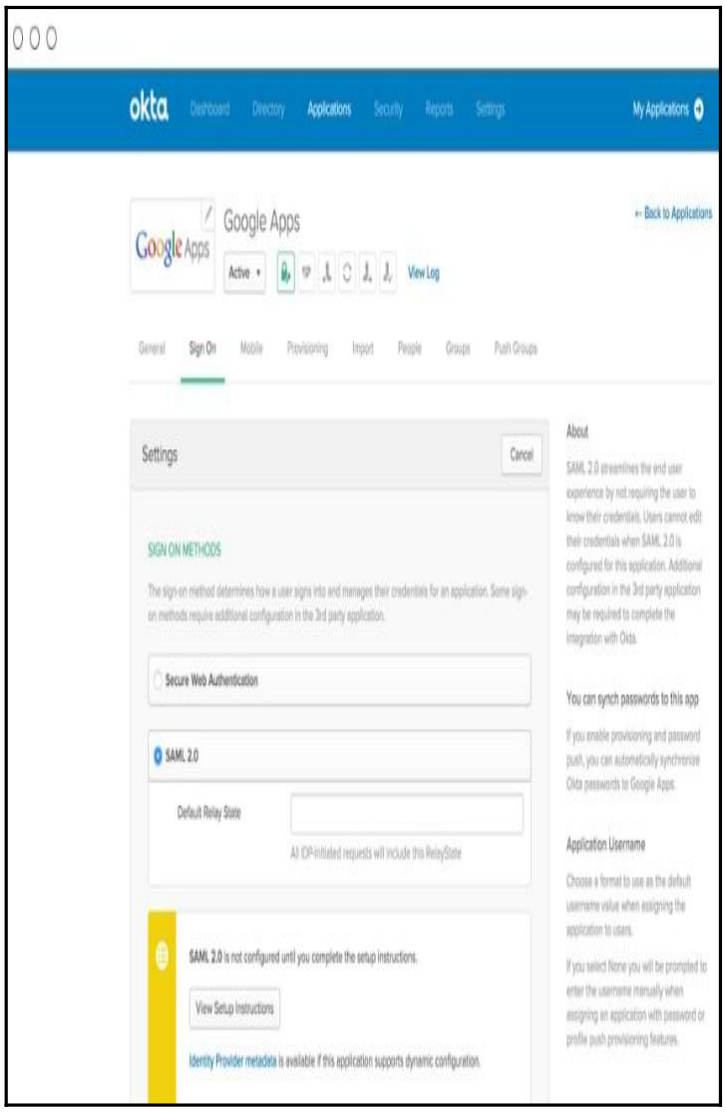

CASB

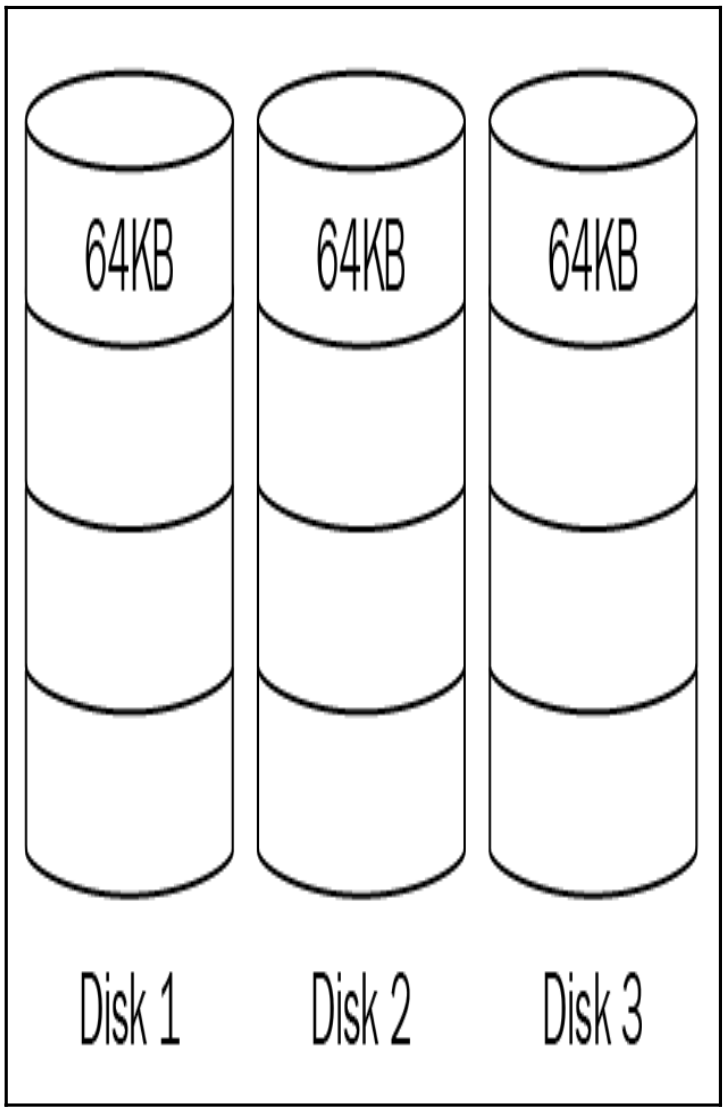

Example pricing for popular products
App Service
Compute
Quickly create powerful cloud apps for web and mobile
Starting from
$0.013 /hour
Free for the first 12 months
Virtual Machines
Compute
Provision Windows and Linux virtual machines in seconds
Starting from
$0.008 /hour
Free for the first 12 months
Azure SQL Database
Databases
Managed relational SQL Database as a service
Starting from
$0.021 /hour
250GB free for the first 12 months
Blob storage
Storage
REST-based object storage for unstructured data
Starting from
$0.002 /GB
5GB free for the first 12 months
Azure Kubernetes Service (AKS)
Containers
Simplify the deployment, management, and operations of Kubernetes
Pay only for virtual machines. Starting from
$0.008 /hour
Free for the first 12 months
Functions
Compute
Process events with serverless code
Starting from
$0.20 /million executions
1 million requests per month always free

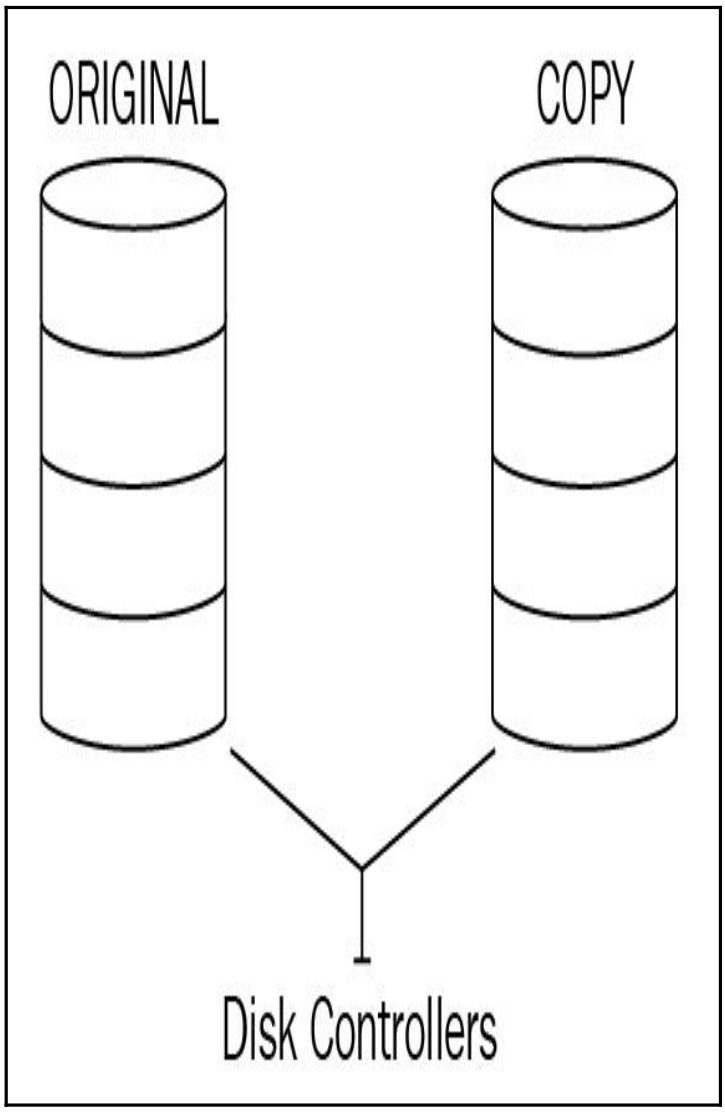

GoldMine Cloud
powered by CloudJumper
No Server? No Problem.
WHAT'S INCLUDED
SUBSCRIPTION
Contact management
YES
Email linking
YES
Web and mobile device access
OPTIONAL
Sales forecasting and opportunity management
YES
Marketing list management and group emails
YES
Integration for Constant Contact campaign downloads
YES
Customer service management
YES
Real time dashboards
YES
Customize fields
YES

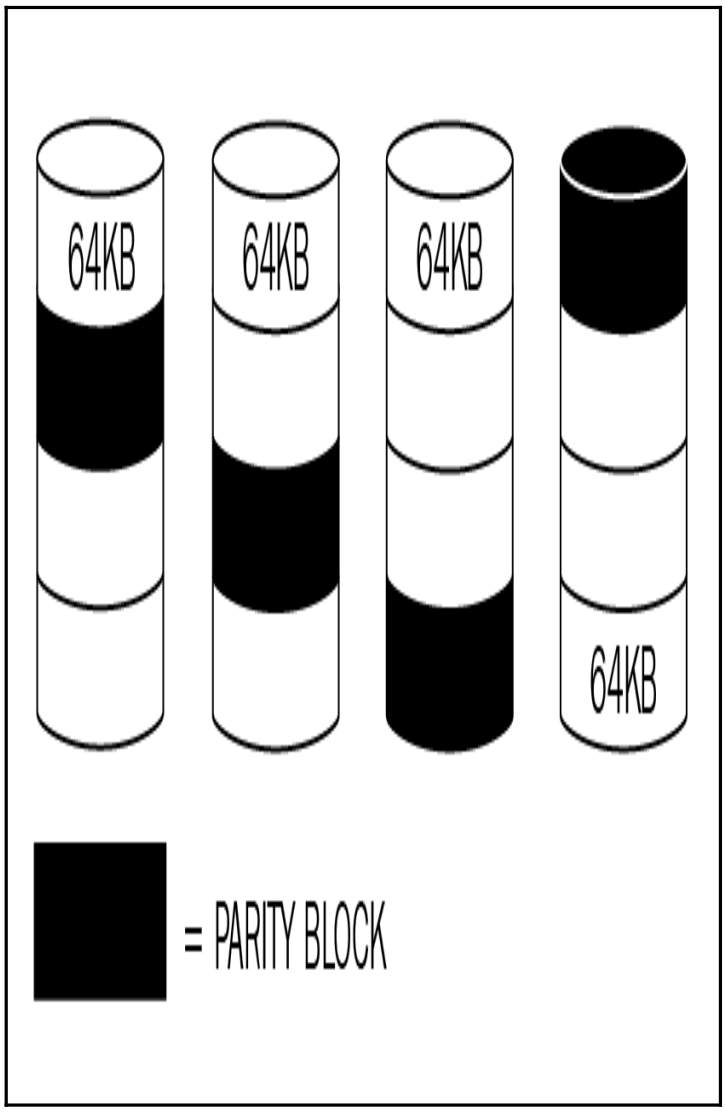

See Salesforce in action.
TAKE THE SALES CLOUD GUIDED TOUR
Lightning Sales Executive Dashboard


1 year £7.90 user/month
Office 365 Business
Buy now
Price does not include VAT.
Best for businesses that need Office applications plus cloud file storage and sharing. Business email not included.
Office applications included
Outlook
Word
Excel
PowerPoint
OneNote
Access (PC only)
Services included
OneDrive
1 year £9.40 user/month
Office 365 Business Premium
Buy now
Price does not include VAT.
Best for businesses that need business email, Office applications, and other business services.
Office applications included
Outlook
Word
Excel
PowerPoint
OneNote
Access (PC only)
Services included
Exchange
OneDrive
SharePoint
Skype for Business
Microsoft Teams
1 year £3.80 user/month
Office 365 Business Essentials
Buy now
Price does not include VAT.
Best for businesses that need business email and other business services. Office applications not included.
Office applications included
(Not included)
Services included
Exchange
OneDrive
SharePoint
Skype for Business
Microsoft Teams


okta
Dashboard
Directory
Applications
Security
Reports
Settings
My Applications
Google Apps
Google Apps
Active
View Log
← Back to Applications
General
Sign On
Mobile
Provisioning
Import
People
Groups
Push Groups
Settings
Cancel
SIGN ON METHODS
The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.
Secure Web Authentication
SAML 2.0
Default Relay State
All IDP-initiated requests will include this RelayState
SAML 2.0 is not configured until you complete the setup instructions.
View Setup Instructions
Identity Provider metadata is available if this application supports dynamic configuration.
About
SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.
You can synch passwords to this app
If you enable provisioning and password push, you can automatically synchronize Okta passwords to Google Apps.
Application Username
Choose a format to use as the default username value when assigning the application to users.
If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.


64KB
64KB
64KB
Disk 1
Disk 2
Disk 3


ORIGINAL
COPY
Disk Controllers


64KB
64KB
64KB
64KB
= PARITY BLOCK

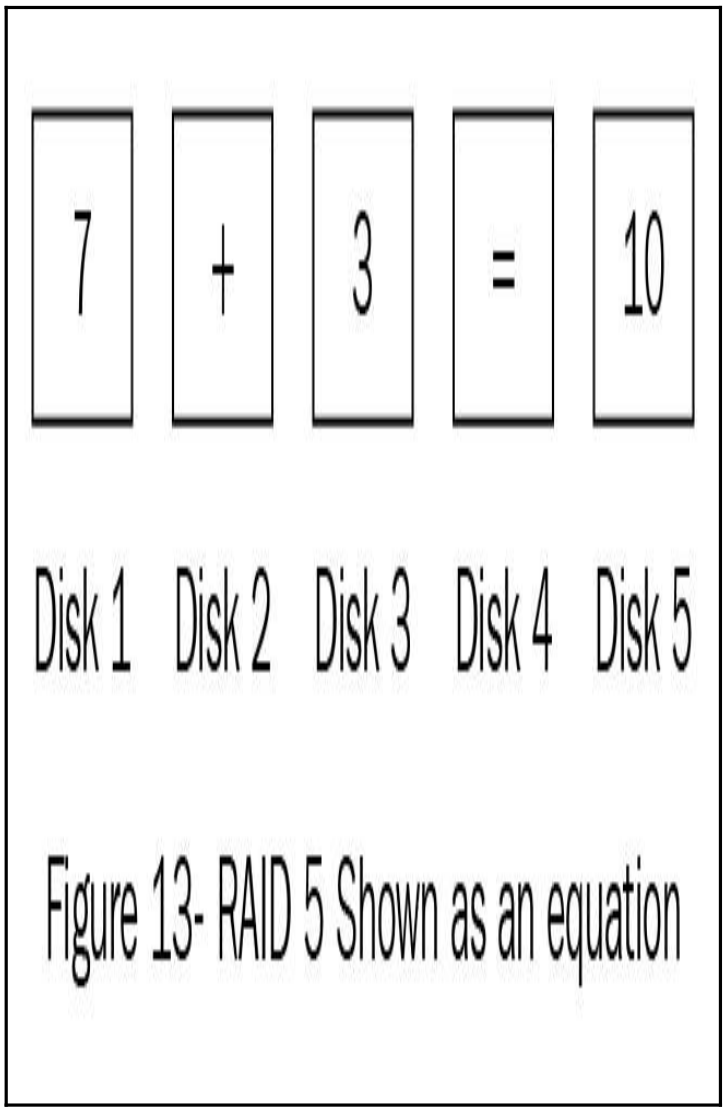
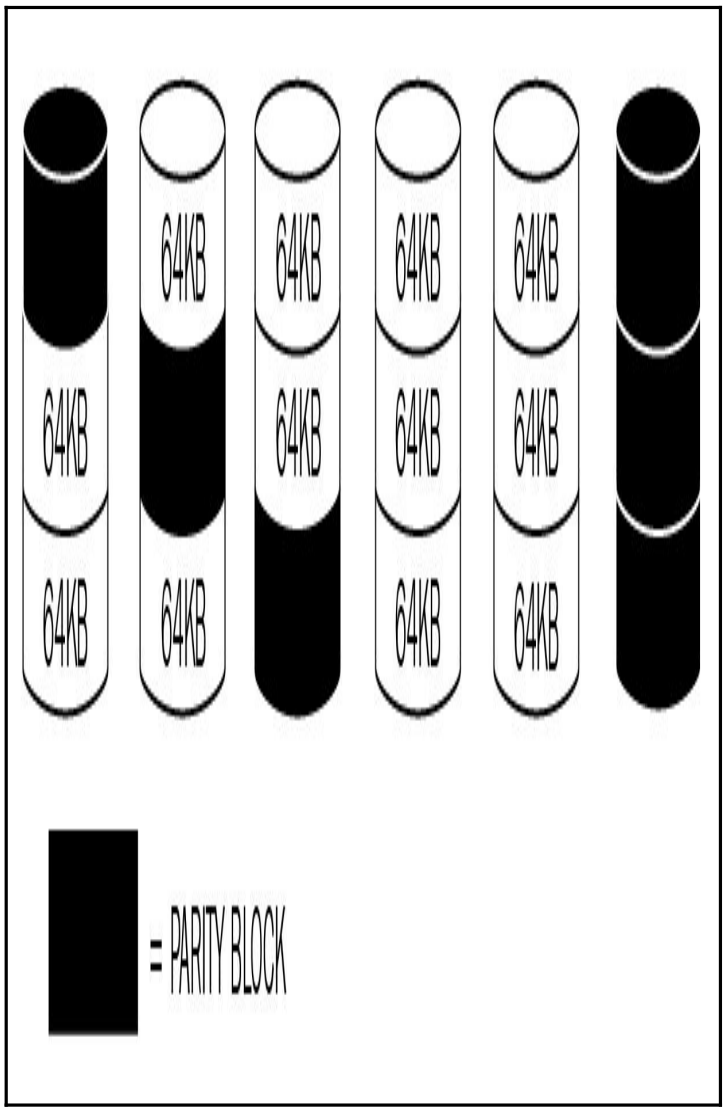
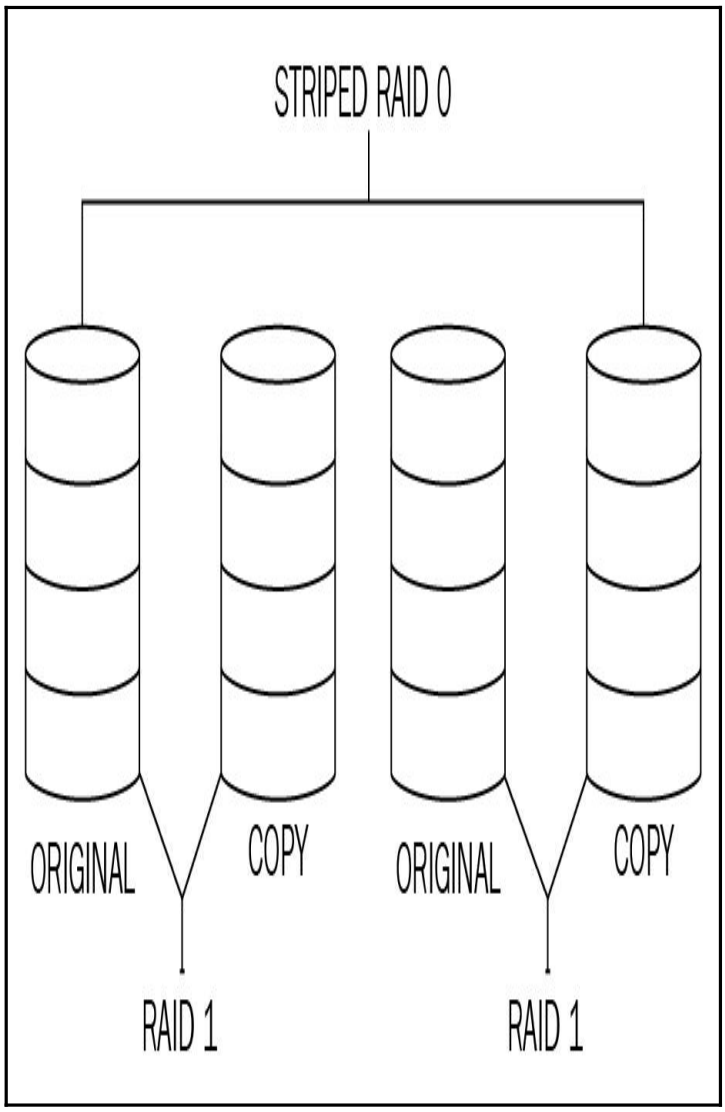
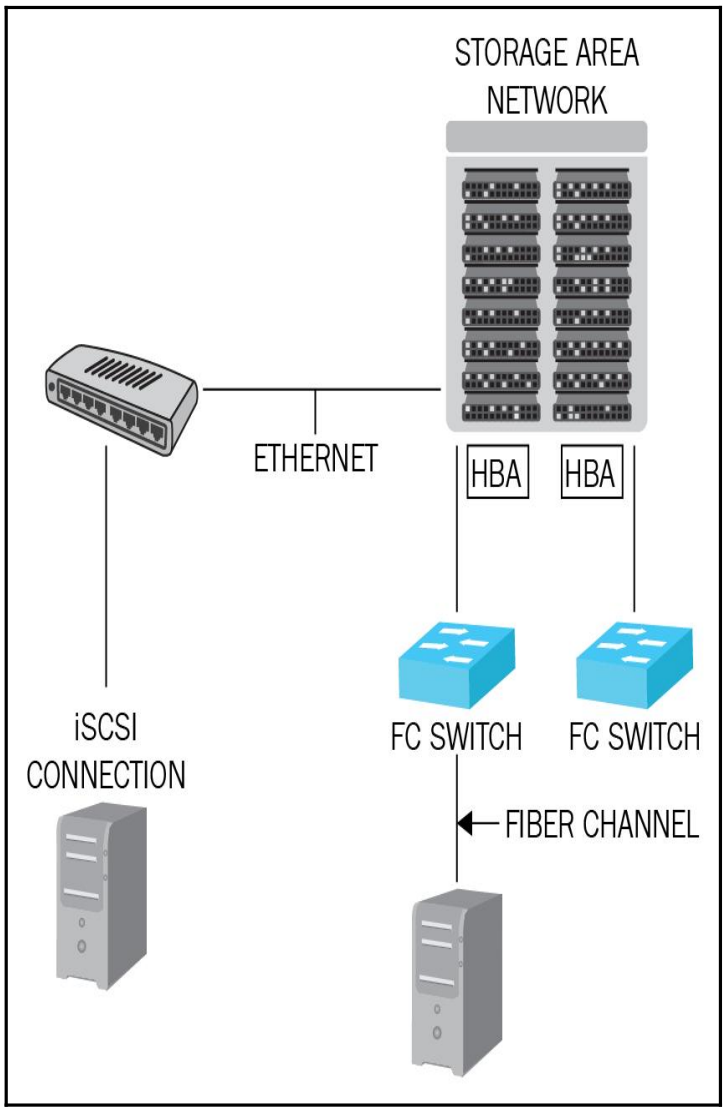
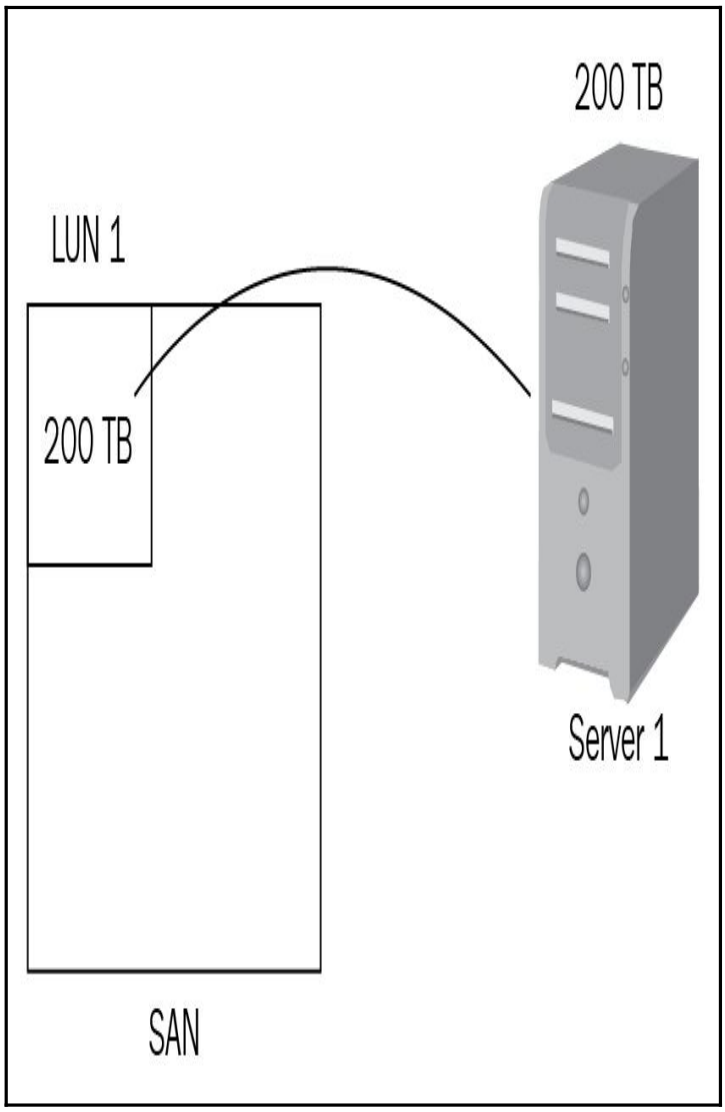


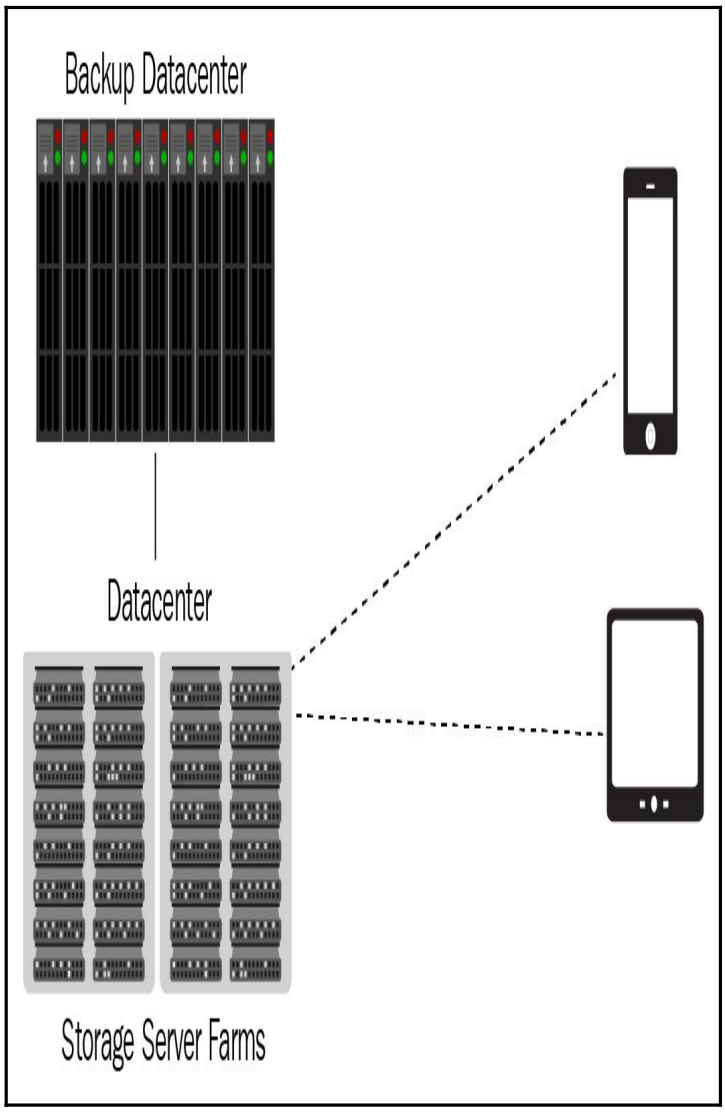
Figure 13- RAID 5 Shown as an equation

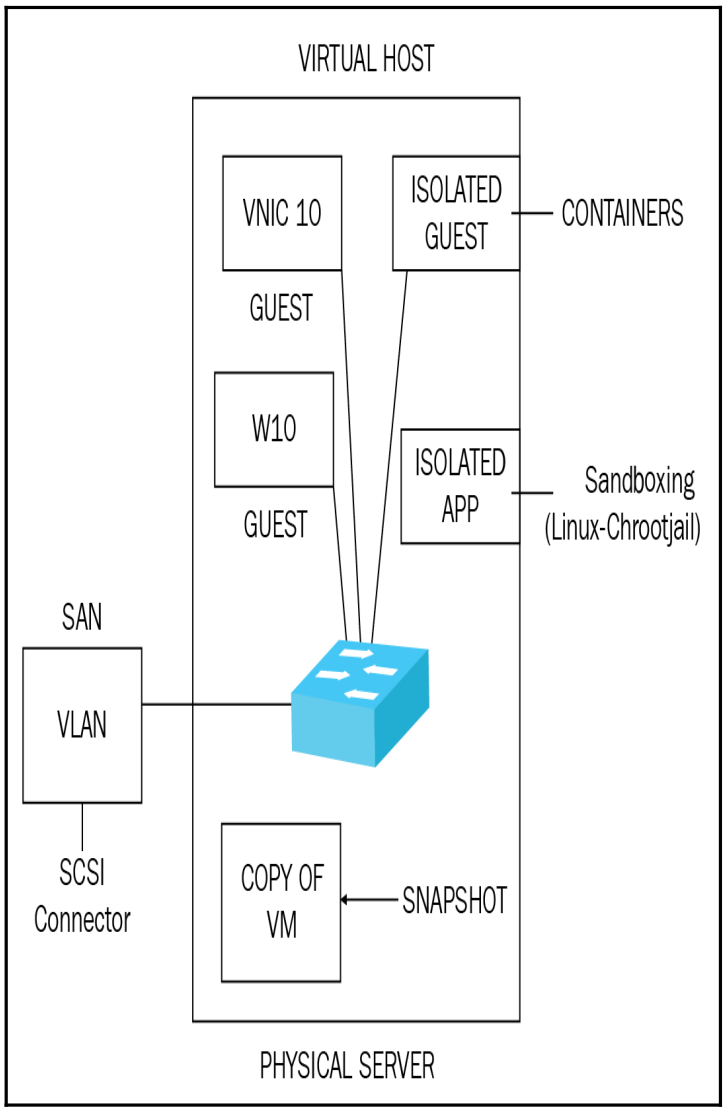

64KB
64KB
64KB
64KB
64KB
64KB
64KB
64KB
64KB
64KB
64KB
64KB
= PARITY BLOCK

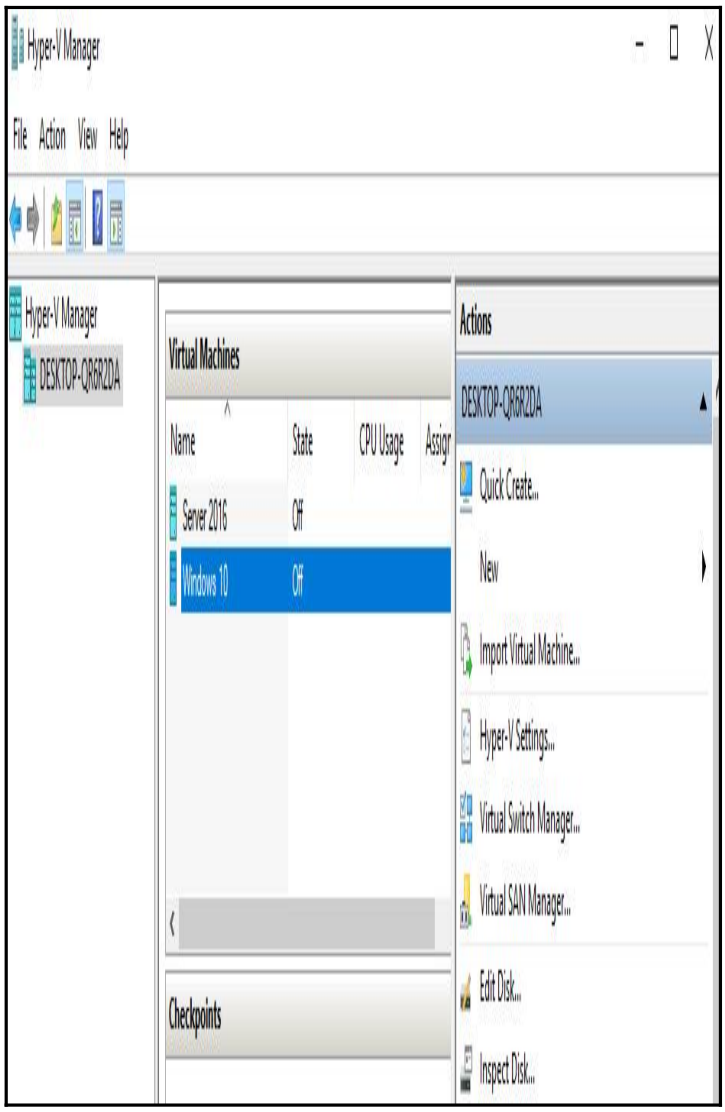

STRIPED RAID 0
ORIGINAL
COPY
ORIGINAL
COPY
RAID 1
RAID 1

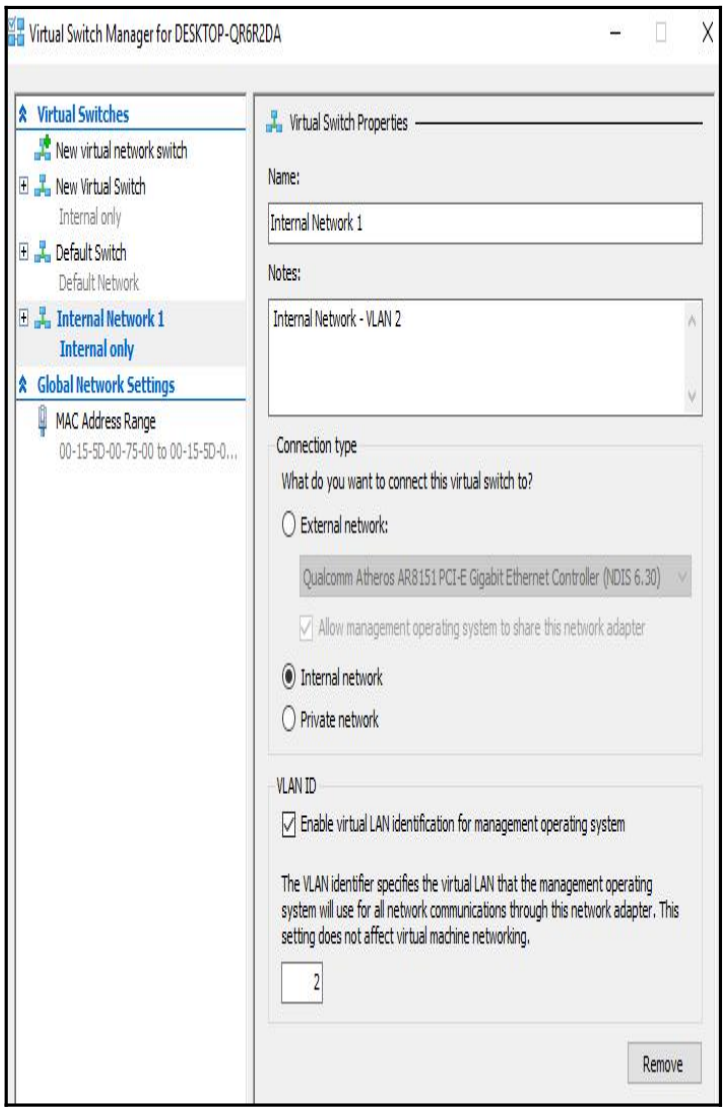

STORAGE AREA
NETWORK
ETHERNET
HBA
HBA
iSCSI
CONNECTION
FC SWITCH
FC SWITCH
FIBER CHANNEL

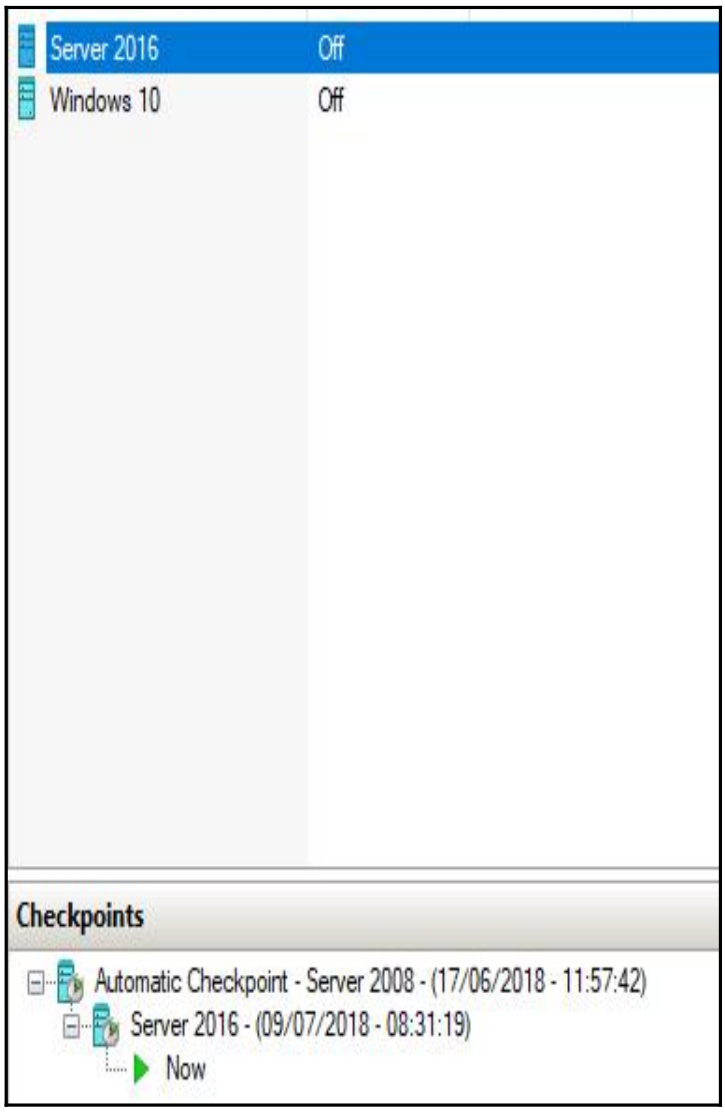

200 TB
LUN 1
200 TB
Server 1
SAN

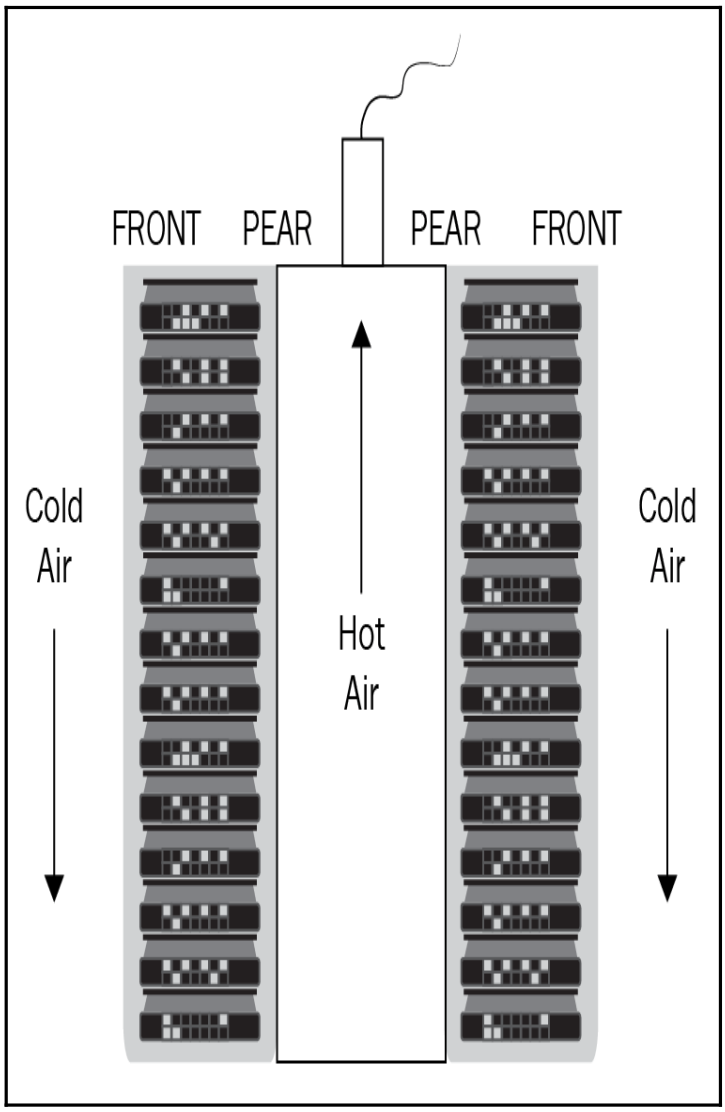

Backup Datacenter
Datacenter
Storage Server Farms


VIRTUAL HOST
VNIC 10
GUEST
ISOLATED GUEST
CONTAINERS
W10
GUEST
ISOLATED APP
Sandboxing (Linux-Chrootjail)
SAN
VLAN
SCSI Connector
COPY OF VM
SNAPSHOT
PHYSICAL SERVER

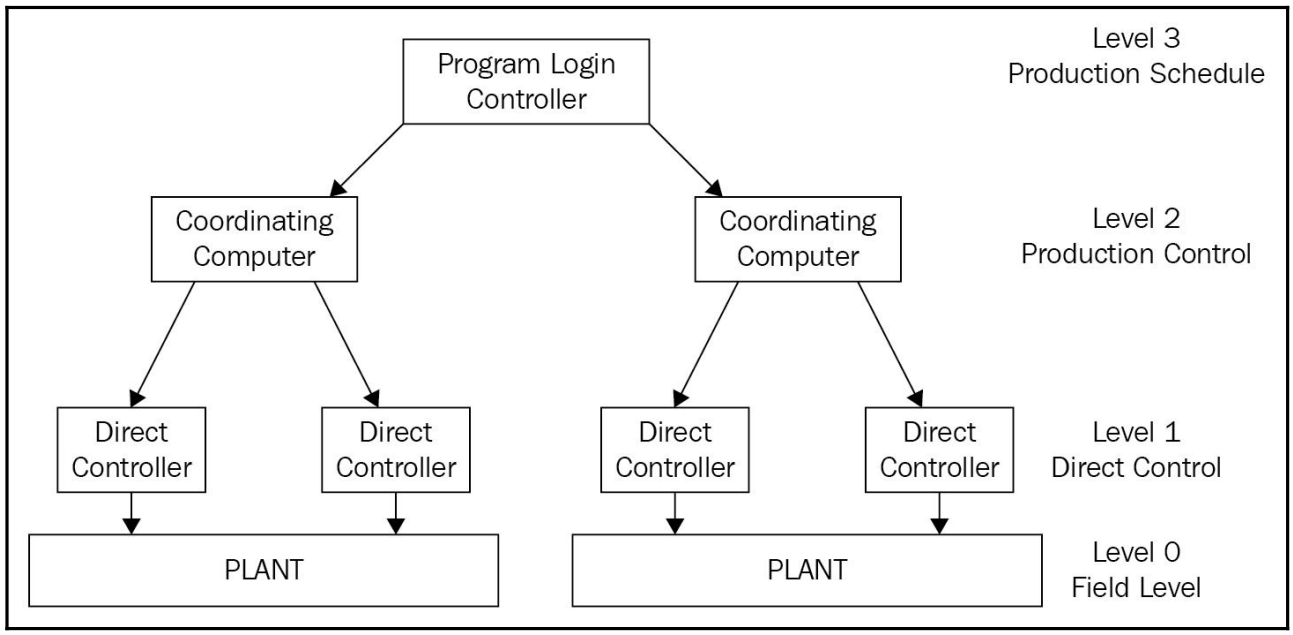

Hyper-V Manager
File Action View Help
Hyper-V Manager
DESKTOP-QR6R2DA
Virtual Machines
Name
State
CPU Usage
Assigr
Server 2016
Off
Windows 10
Off
Checkpoints
Actions
DESKTOP-QR6R2DA
Quick Create...
New
Import Virtual Machine...
Hyper-V Settings...
Virtual Switch Manager...
Virtual SAN Manager...
Edit Disk...
Inspect Disk...

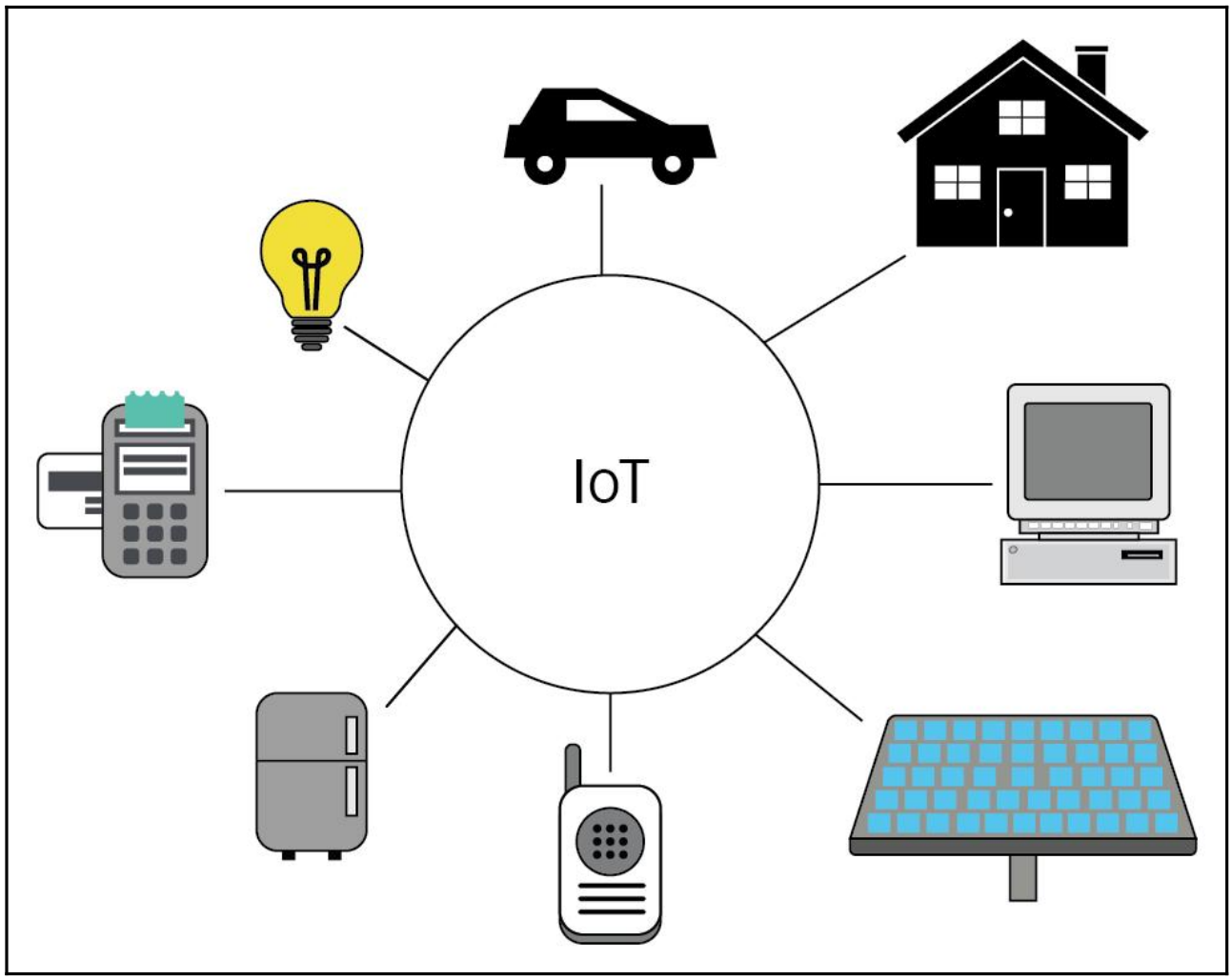

Virtual Switch Manager for DESKTOP-QR6R2DA
Virtual Switches
New virtual network switch
New Virtual Switch
Internal only
Default Switch
Default Network
Internal Network 1
Internal only
Global Network Settings
MAC Address Range
00-15-5D-00-75-00 to 00-15-5D-0...
Virtual Switch Properties
Name:
Internal Network 1
Notes:
Internal Network - VLAN 2
Connection type
What do you want to connect this virtual switch to?
External network:
Qualcomm Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6.30)
Allow management operating system to share this network adapter
Internal network
Private network
VLAN ID
Enable virtual LAN identification for management operating system
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2
Remove


Server 2016
Off
Windows 10
Off
Checkpoints
Automatic Checkpoint - Server 2008 - (17/06/2018 - 11:57:42)
Server 2016 - (09/07/2018 - 08:31:19)
Now

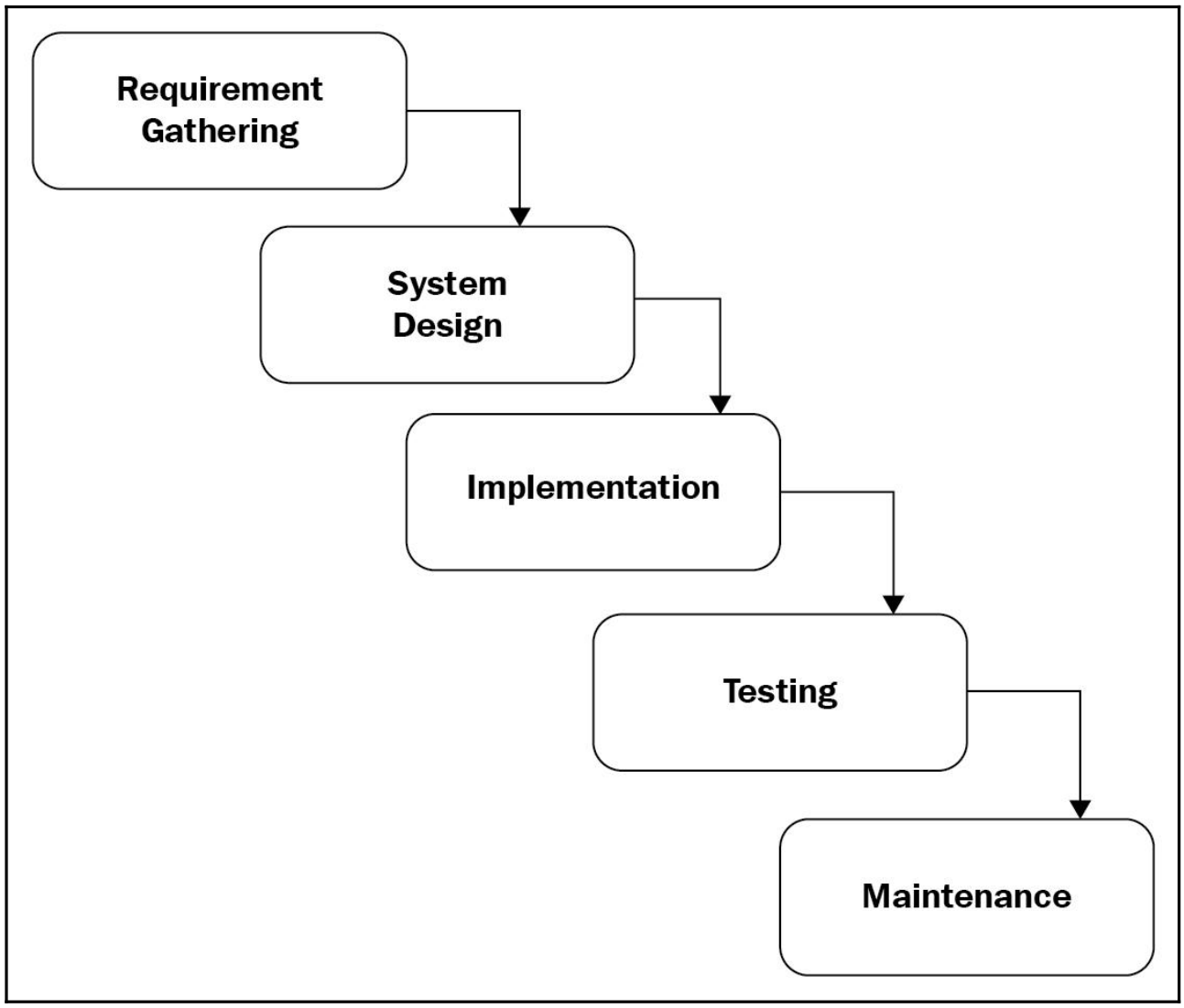

FRONT
PEAR
PEAR
FRONT
Cold
Air
Hot
Air
Cold
Air

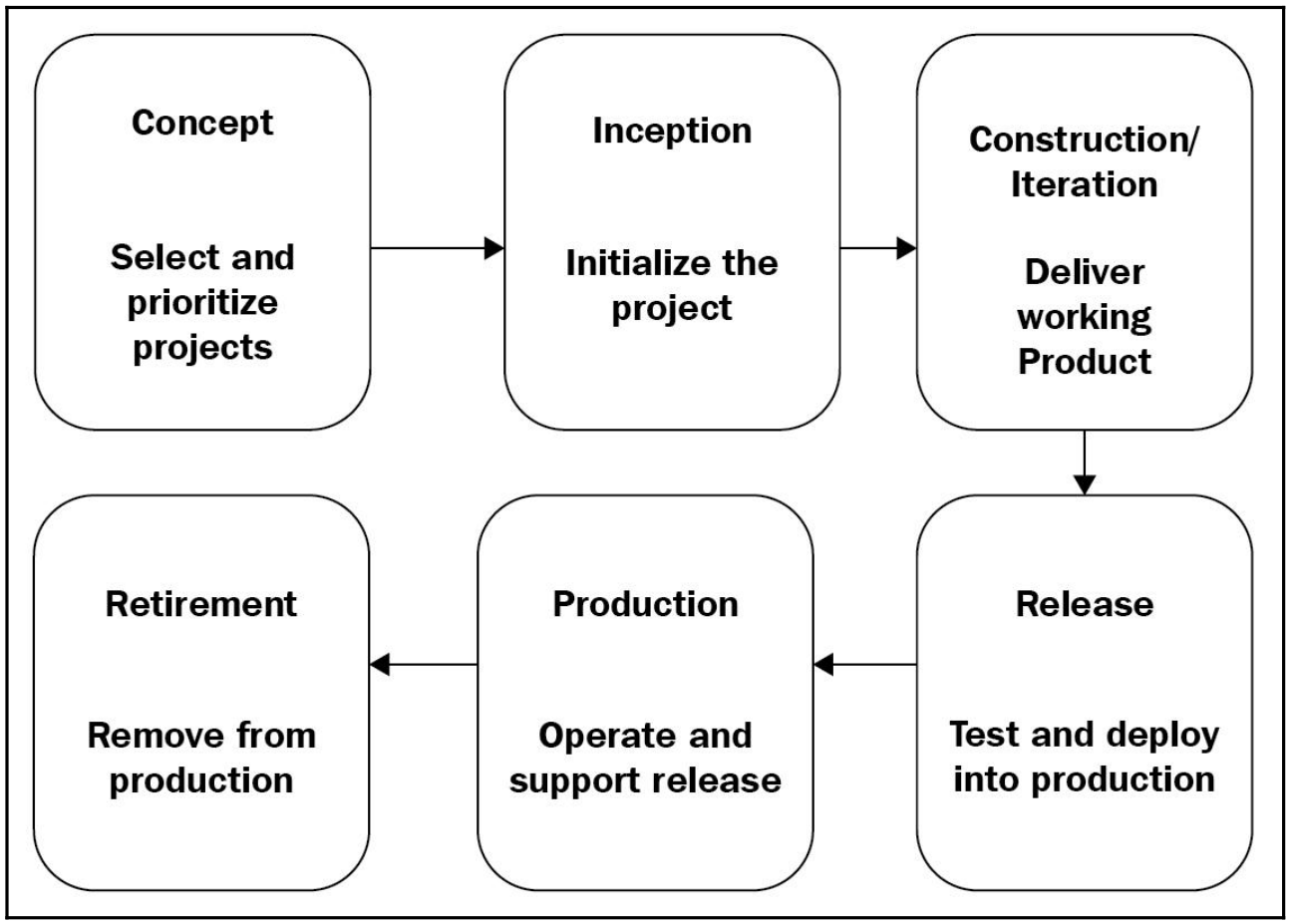
Chapter 07: Managing Hosts and Applications Deployment


Program Login Controller
Level 3
Production Schedule
Coordinating Computer
Coordinating Computer
Level 2
Production Control
Direct Controller
Direct Controller
Direct Controller
Direct Controller
Level 1
Direct Control
PLANT
PLANT
Level 0
Field Level

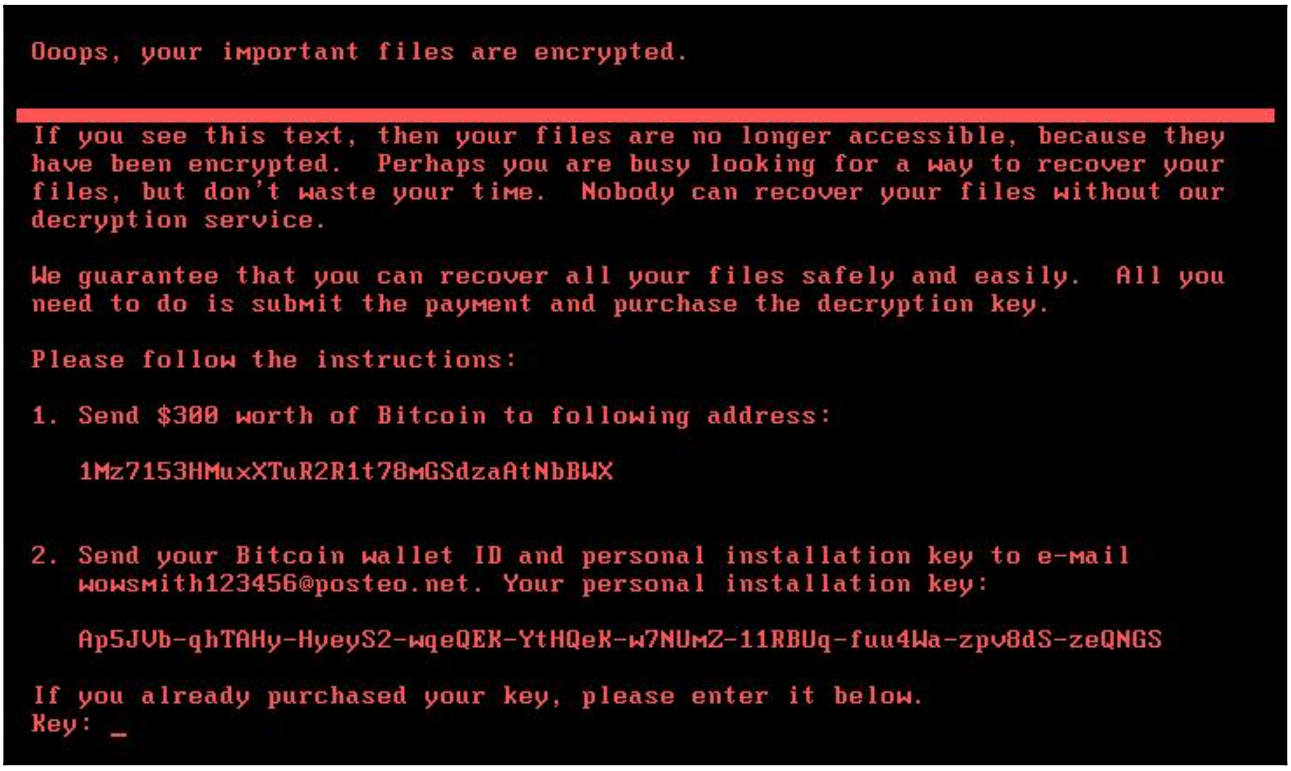

IoT

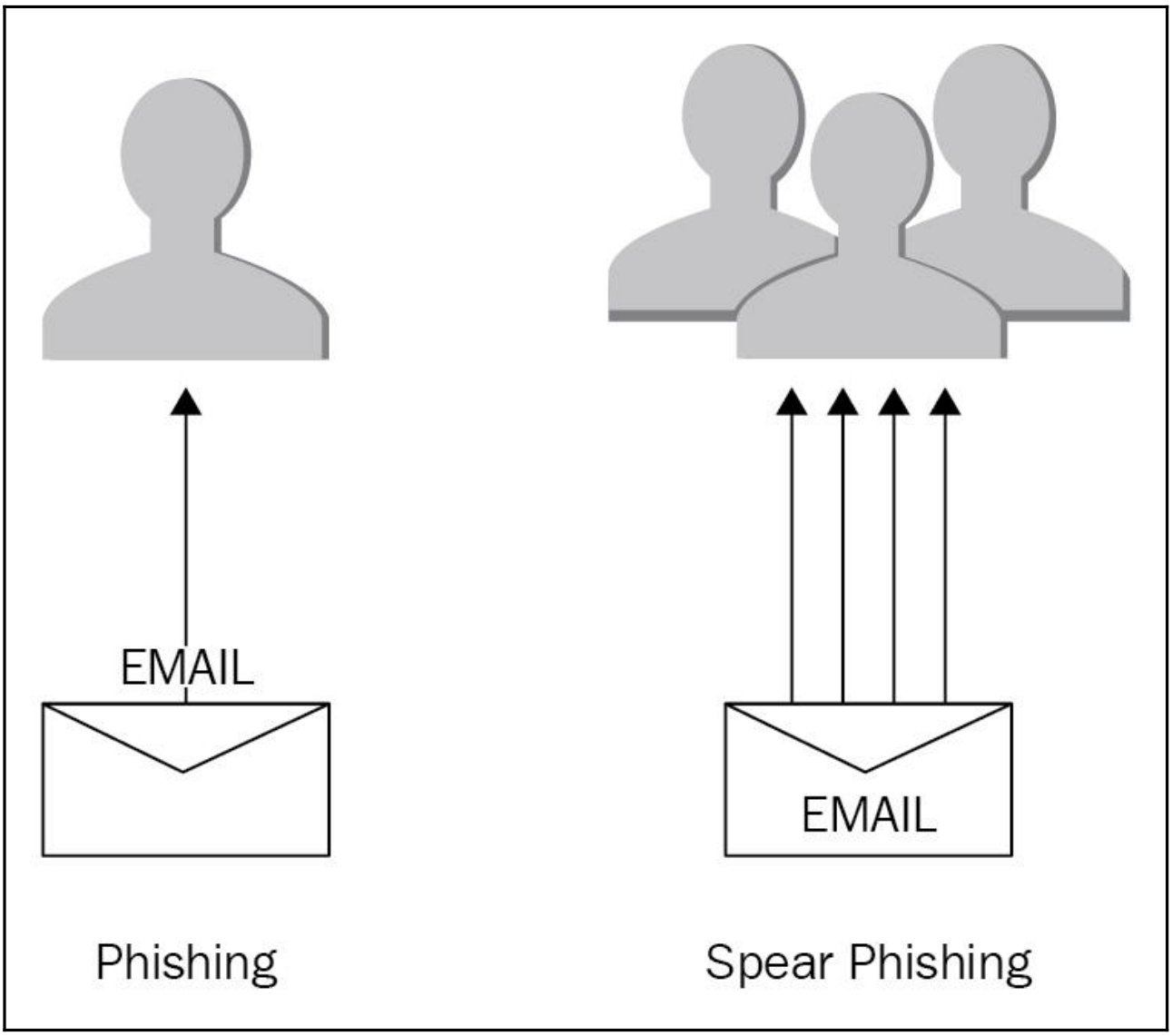

defibtech
Lifeline VIEW
Give 30 Compressions
SHOCK


Requirement Gathering
System Design
Implementation
Testing
Maintenance

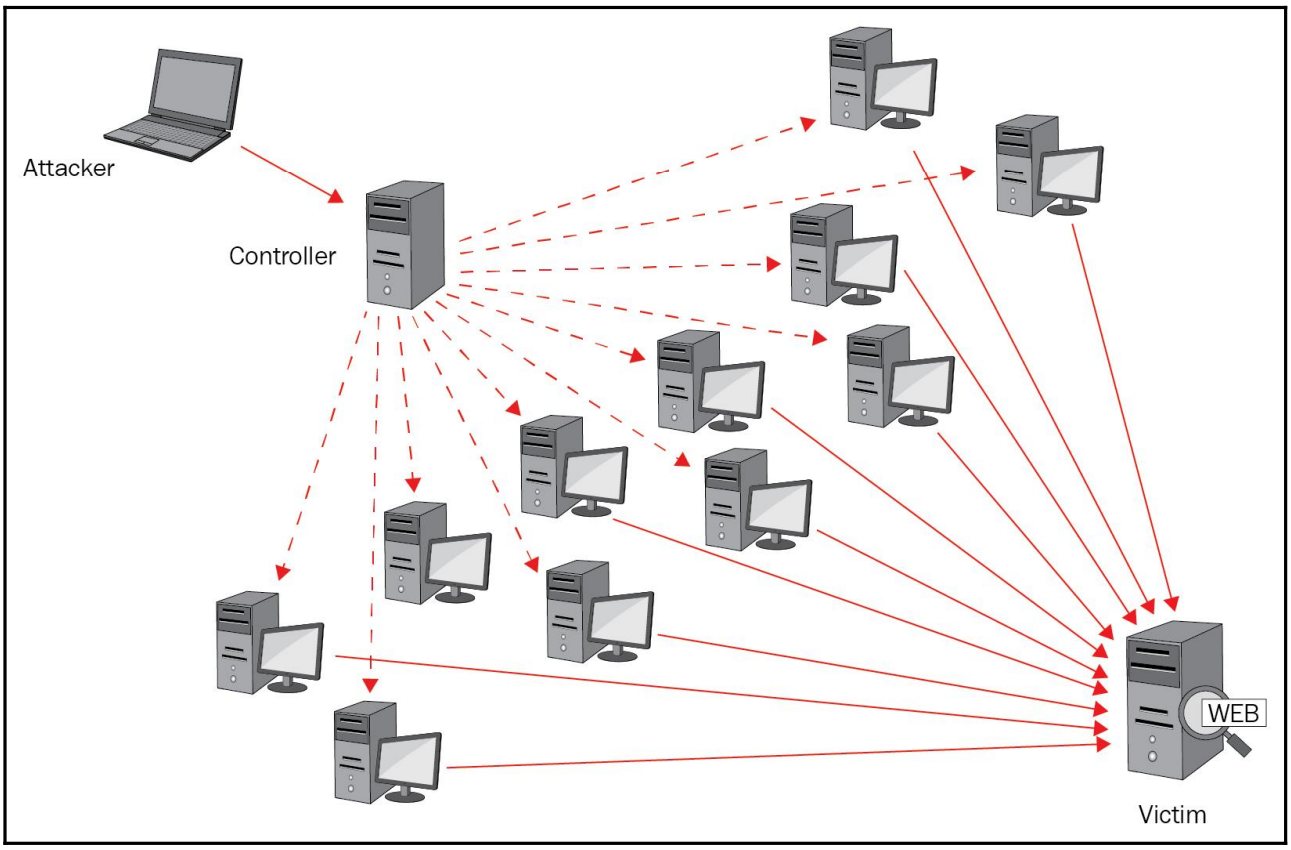

Concept
Select and prioritize projects
Inception
Initialize the project
Construction/ Iteration
Deliver working Product
Release
Test and deploy into production
Production
Operate and support release
Retirement
Remove from production

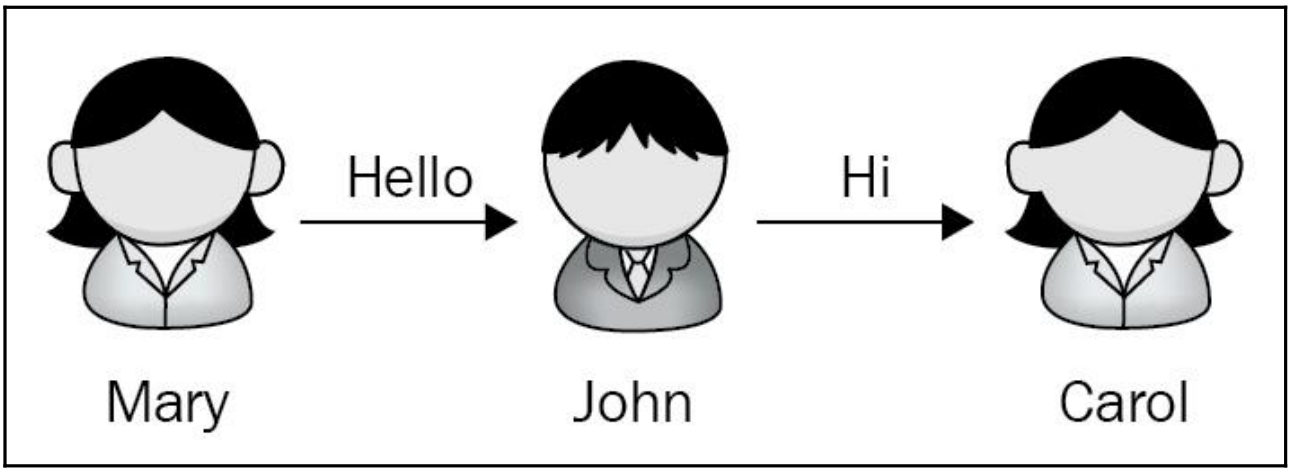
Chapter 08: Protecting Against Attacks and Vulnerabilities

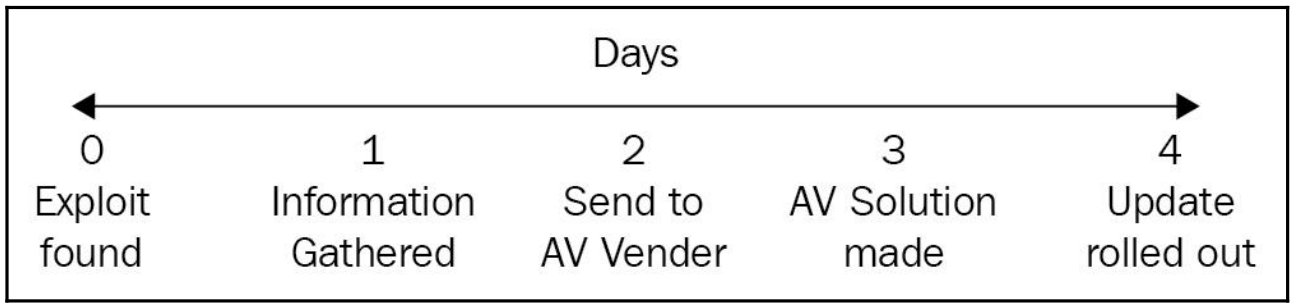


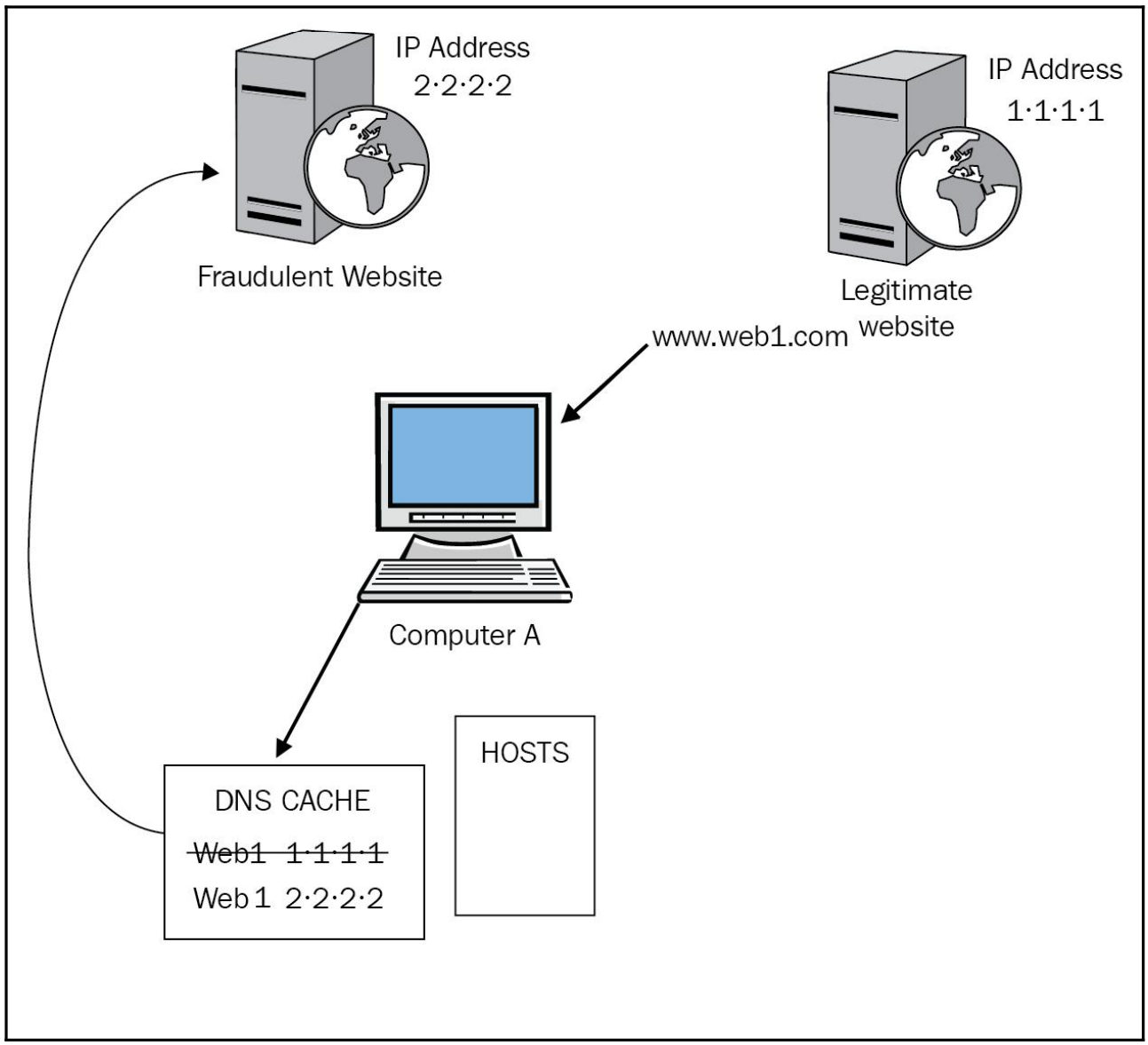

EMAIL
EMAIL
Phishing
Spear Phishing

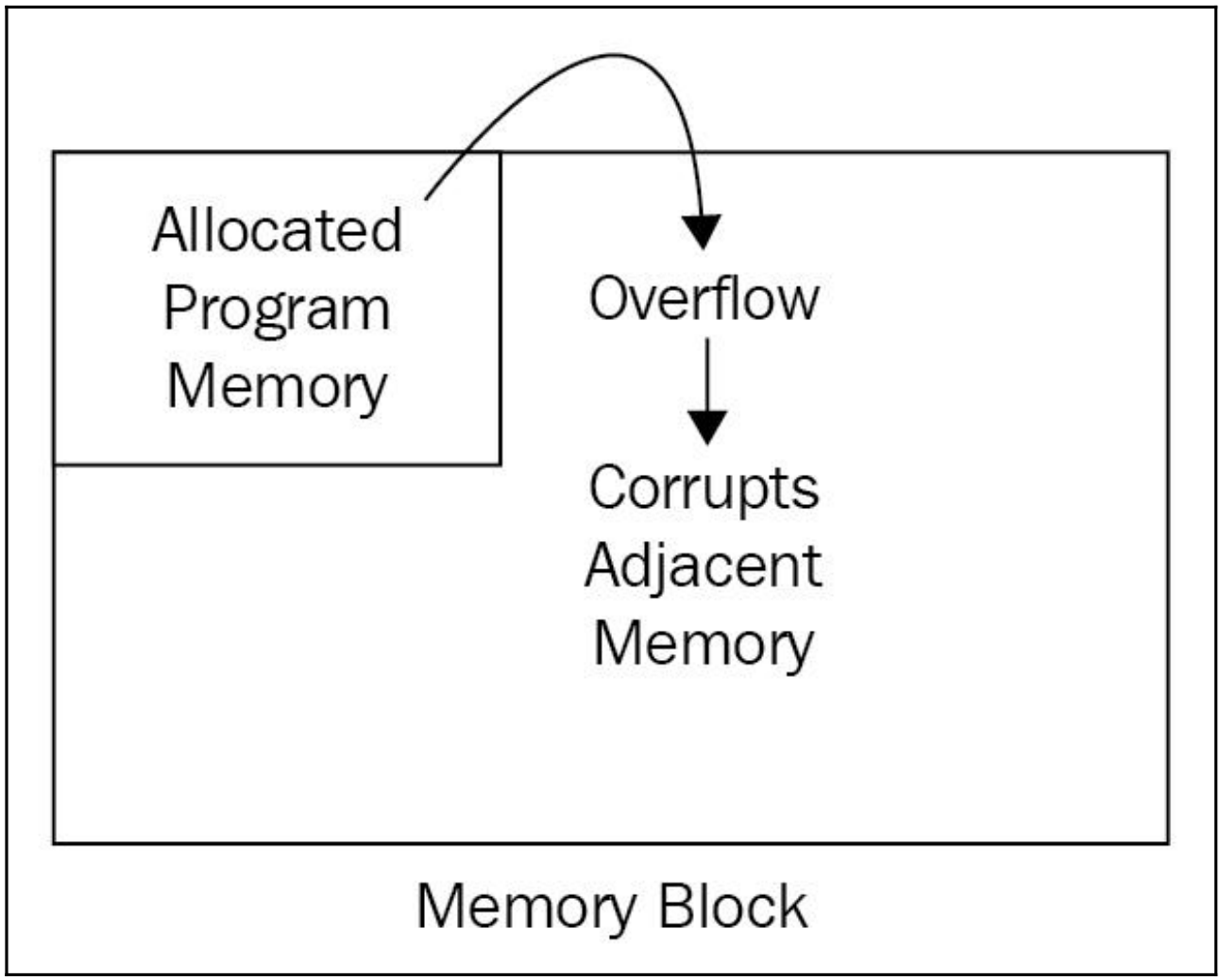

jdbgmgr.exe

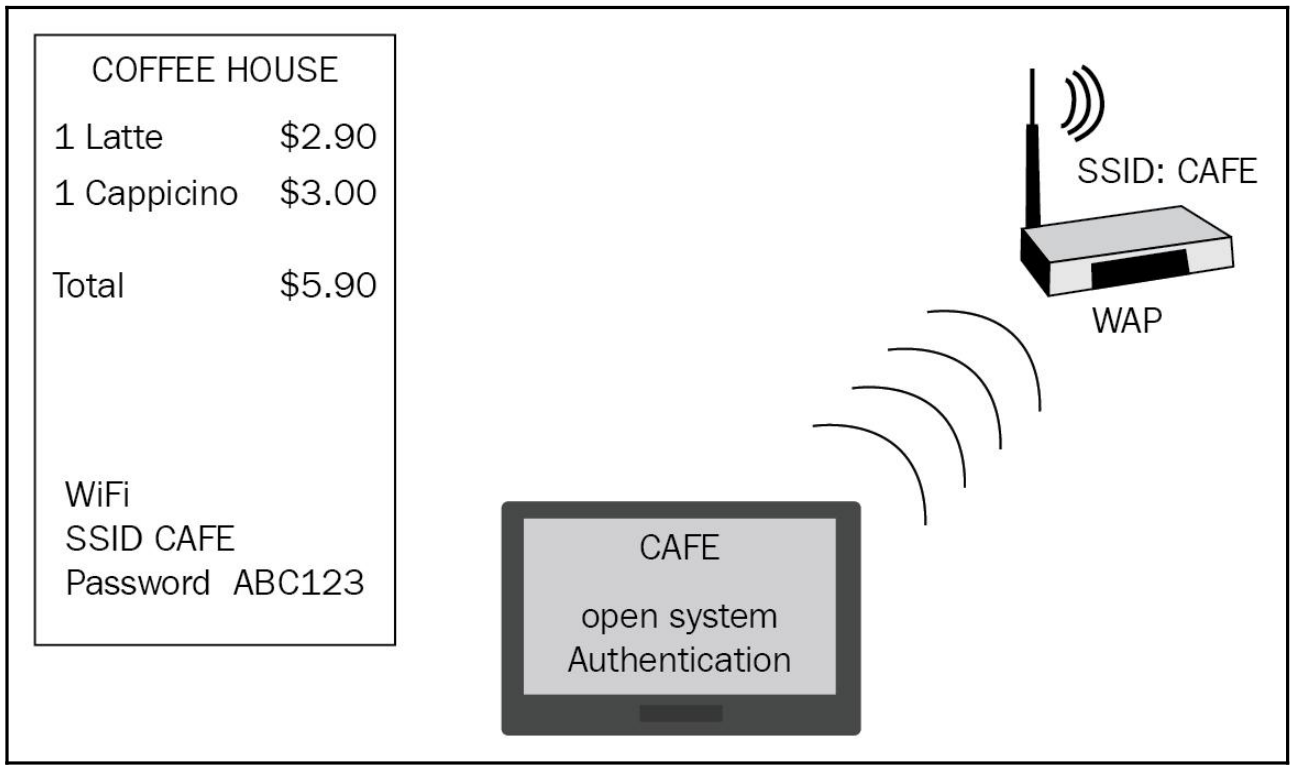

Attacker
Controller
WEB
Victim


Hello
Hi
Mary
John
Carol

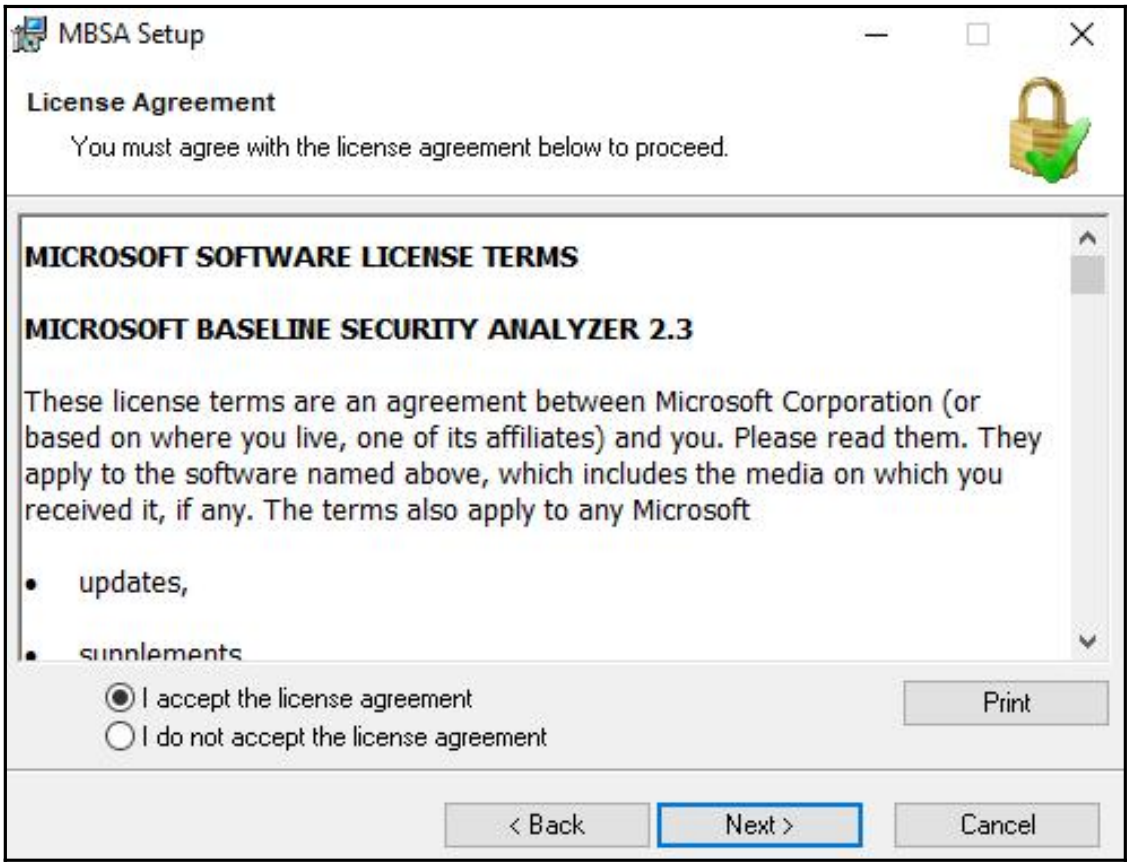

Days
0
Exploit found
1
Information Gathered
2
Send to AV Vender
3
AV Solution made
4
Update rolled out

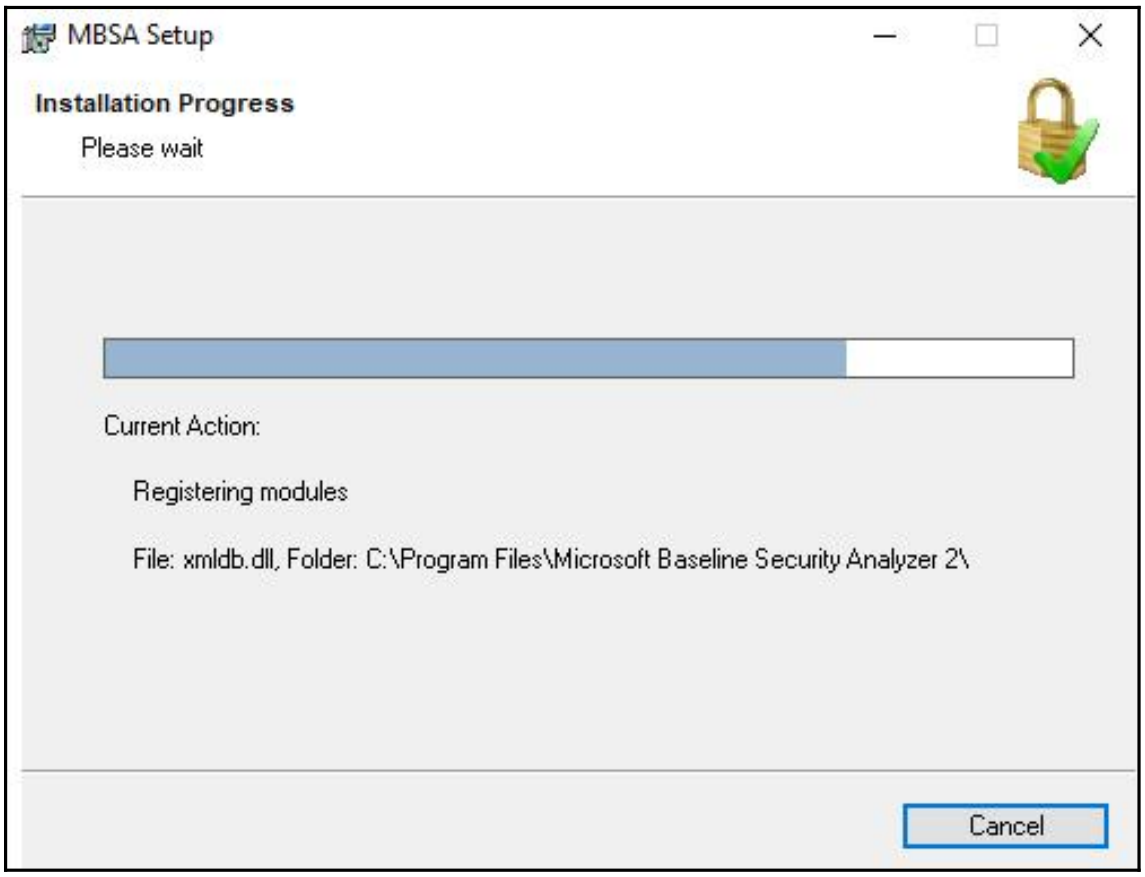

IP Address
2·2·2·2
Fraudulent Website
IP Address
1·1·1·1
Legitimate website
www.web1.com
Computer A
HOSTS
DNS CACHE
~~Web1 1·1·1·1~~
Web1 2·2·2·2

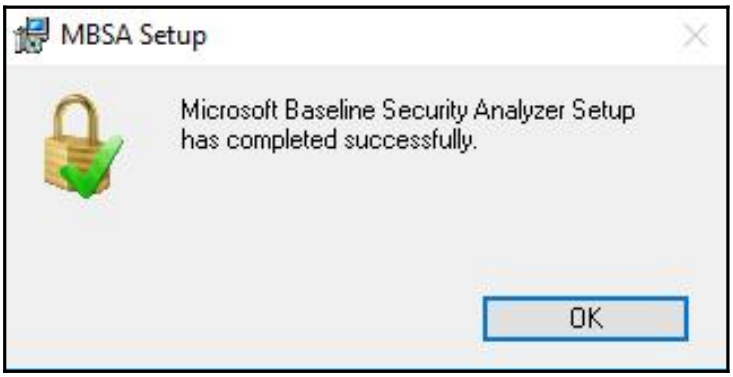

Allocated
Program
Memory
Overflow
Corrupts
Adjacent
Memory
Memory Block


COFFEE HOUSE
1 Latte $2.90
1 Cappicino $3.00
Total $5.90
WiFi
SSID CAFE
Password ABC123
SSID: CAFE
WAP
CAFE
open system
Authentication

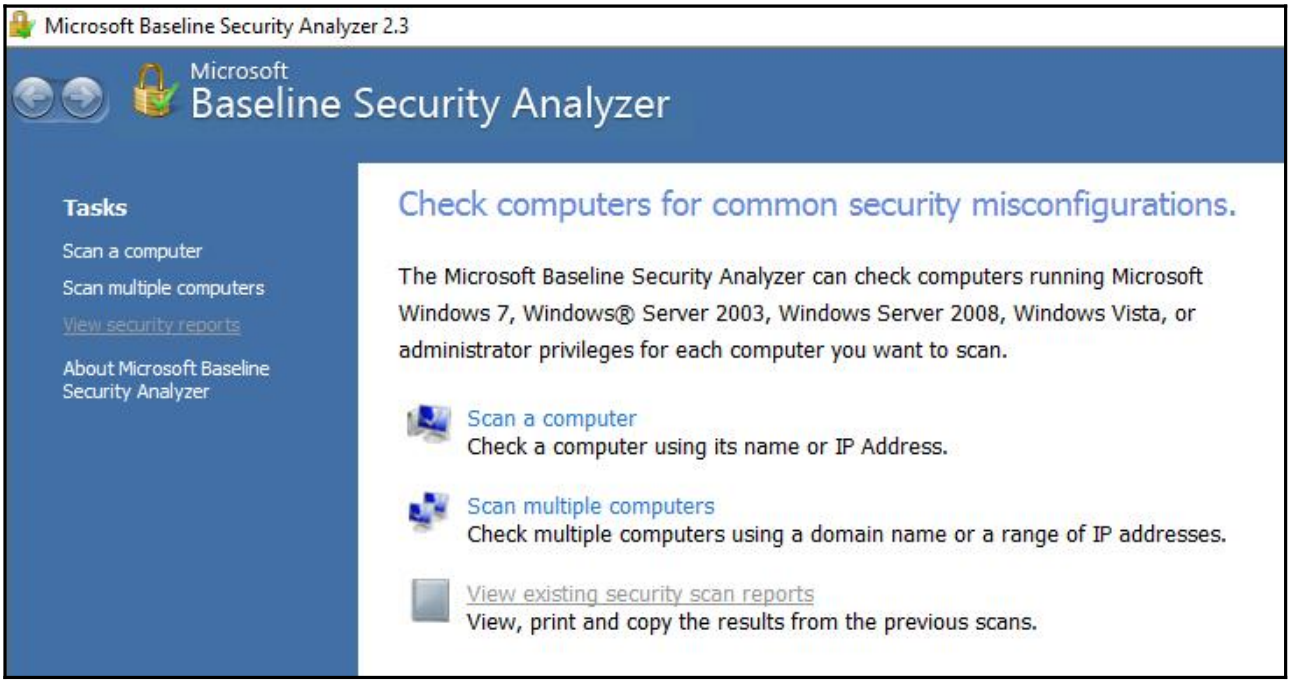

MBSA Setup
Welcome to the Microsoft Baseline Security Analyzer
Version 2.3
Microsoft Baseline Security Analyzer Setup
It is strongly recommended that you exit all Windows programs before running this setup program.
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Copyright 2002-2013 Microsoft Corporation. All rights reserved.
< Back
Next >
Cancel

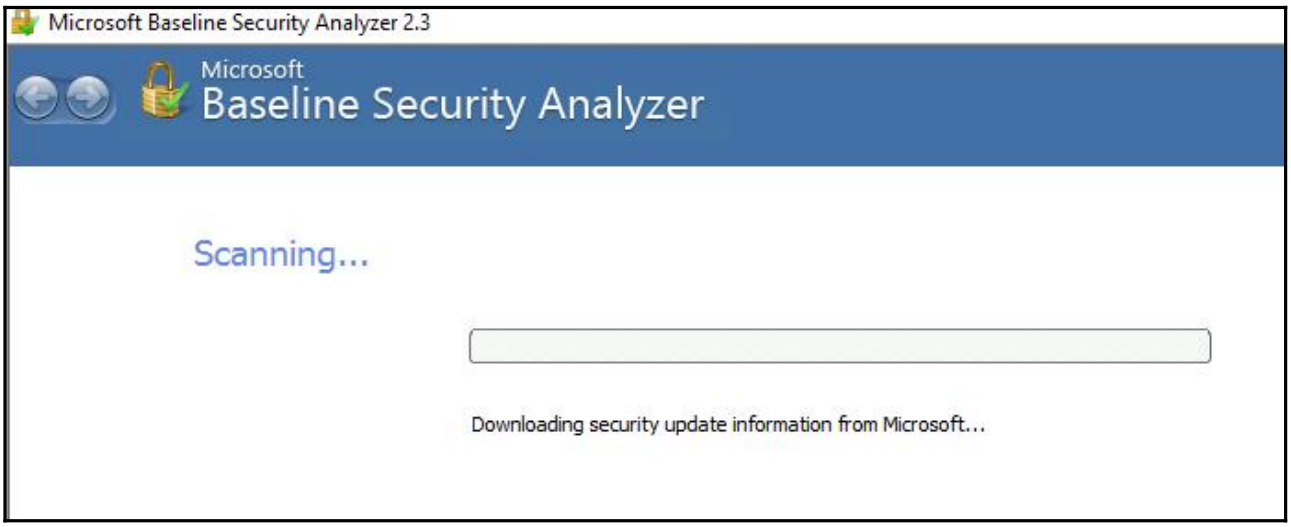

MBSA Setup
License Agreement
You must agree with the license agreement below to proceed.
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT BASELINE SECURITY ANALYZER 2.3
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft
updates,
supplements
I accept the license agreement
I do not accept the license agreement
Print
< Back
Next >
Cancel

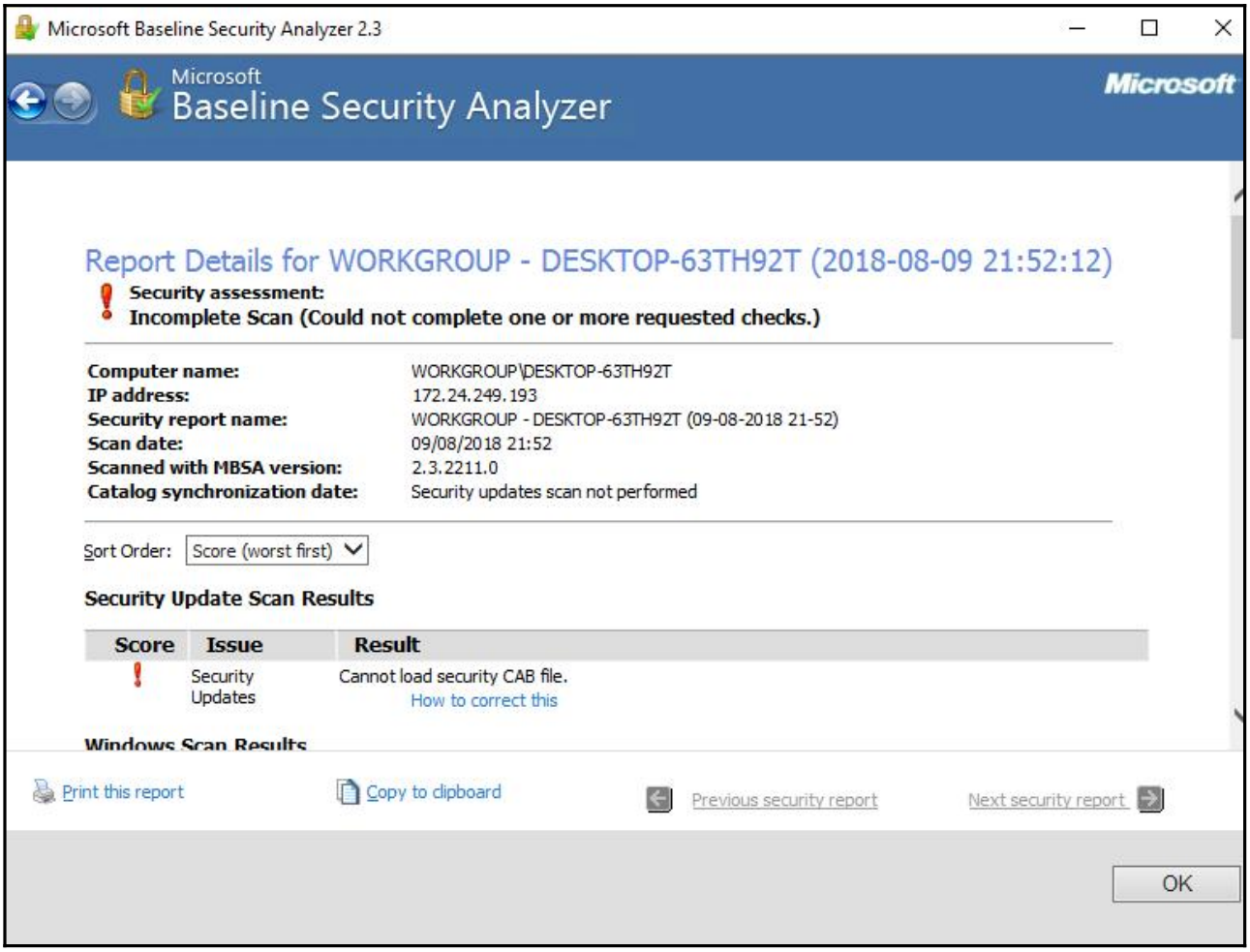

MBSA Setup
Installation Progress
Please wait
Current Action:
Registering modules
File: xmldb.dll, Folder: C:\Program Files\Microsoft Baseline Security Analyzer 2\
Cancel

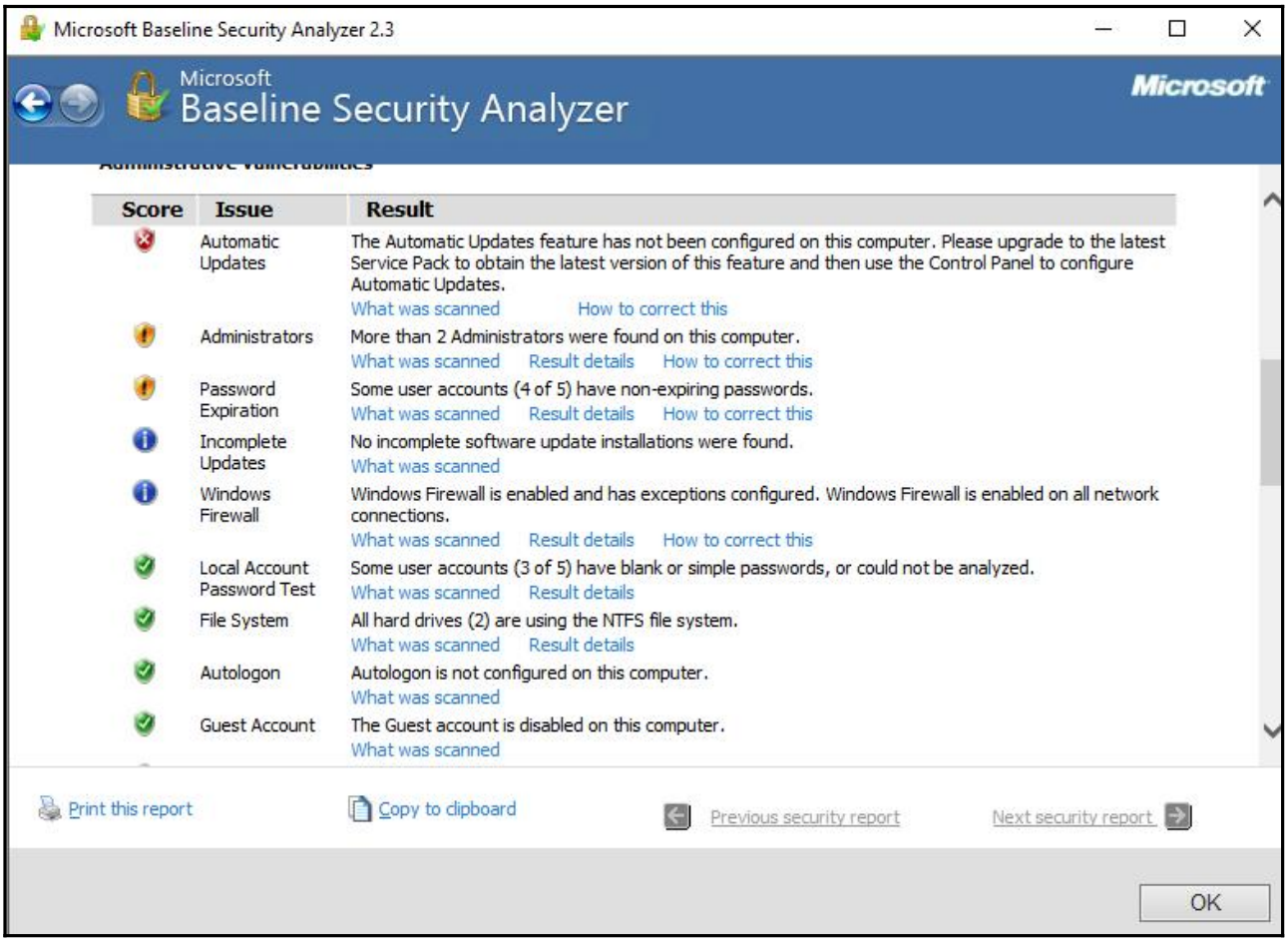

MBSA Setup
Microsoft Baseline Security Analyzer Setup
has completed successfully.
OK


Microsoft
Baseline S...

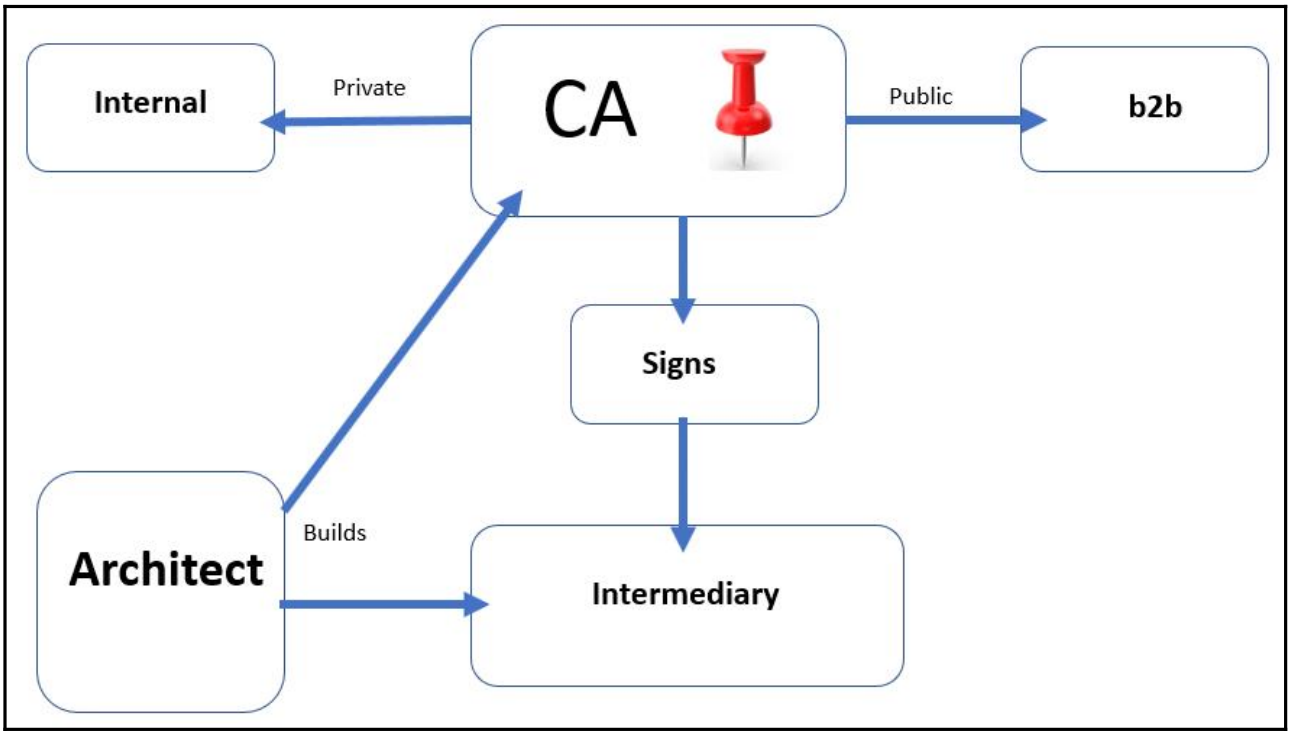

Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer
Check computers for common security misconfigurations.
The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or administrator privileges for each computer you want to scan.
Scan a computer
Check a computer using its name or IP Address.
Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.
View existing security scan reports
View, print and copy the results from the previous scans.

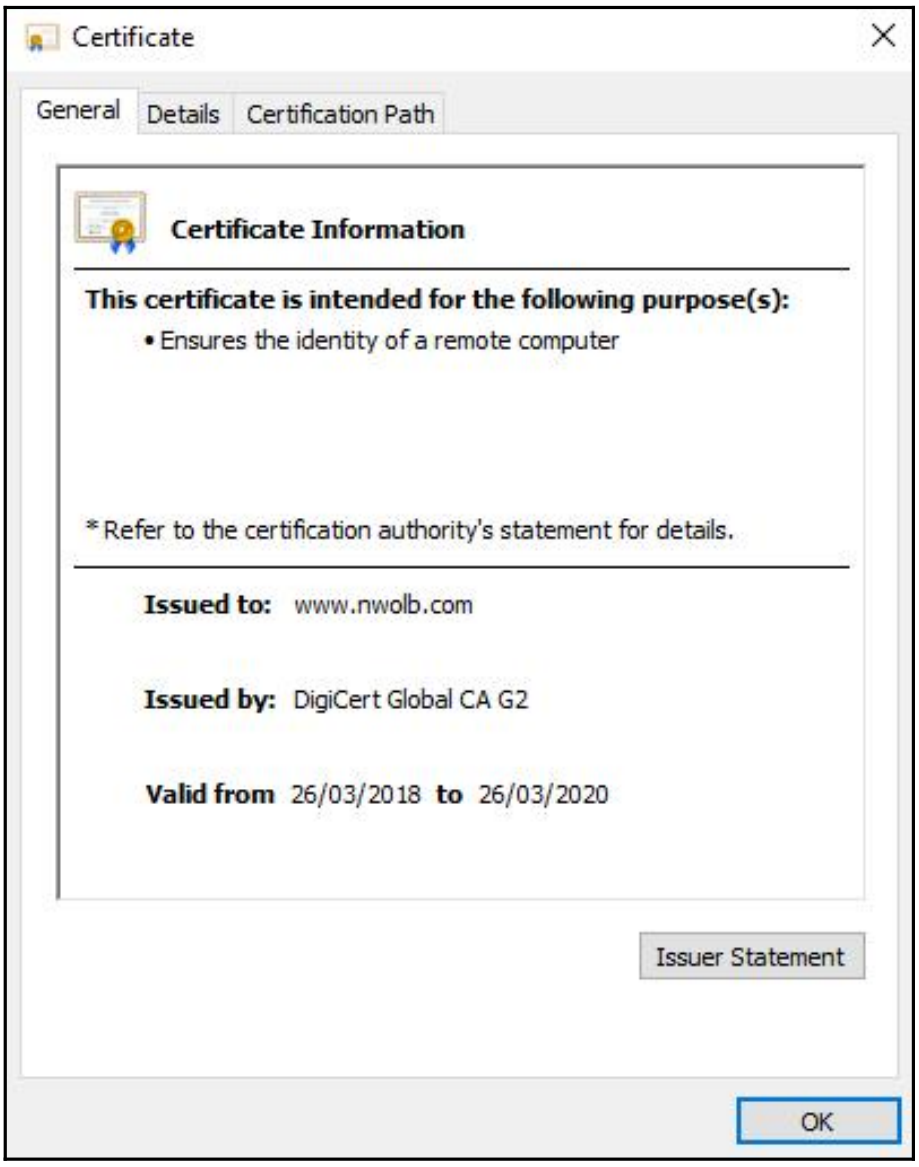

Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Scanning...
Downloading security update information from Microsoft...

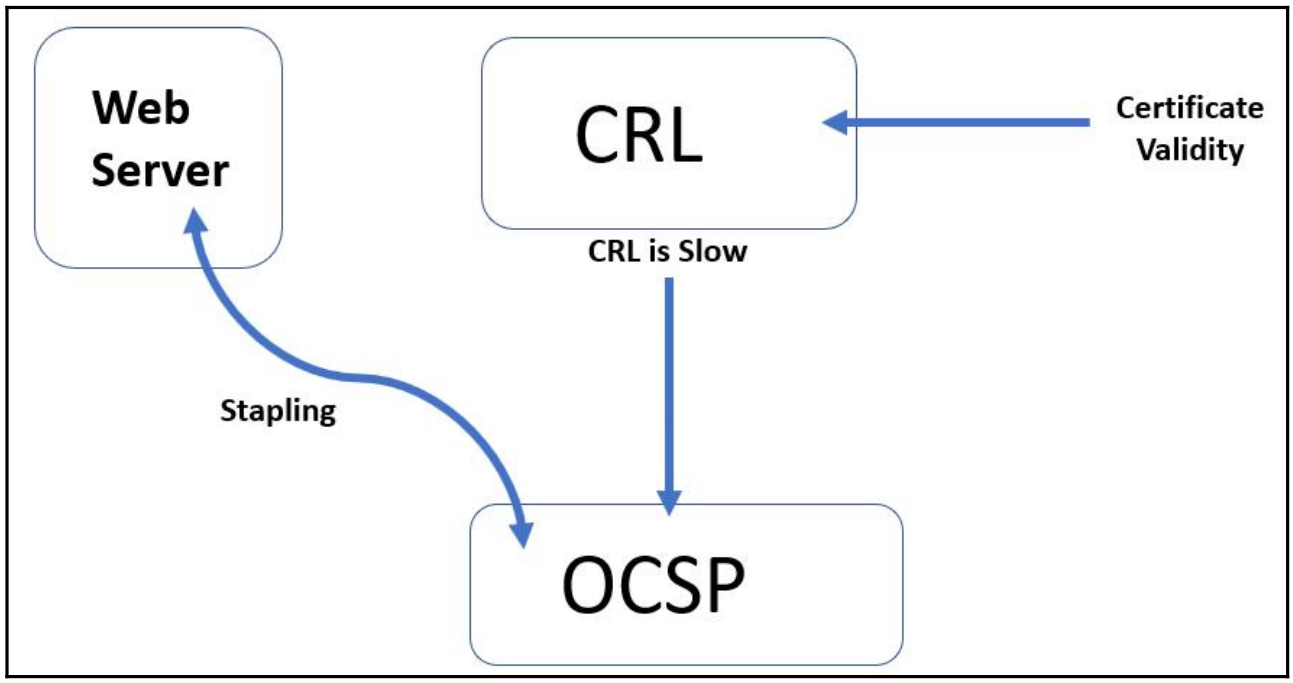

Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Report Details for WORKGROUP - DESKTOP-63TH92T (2018-08-09 21:52:12)
Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)
Computer name: WORKGROUP\DESKTOP-63TH92T
IP address: 172.24.249.193
Security report name: WORKGROUP - DESKTOP-63TH92T (09-08-2018 21-52)
Scan date: 09/08/2018 21:52
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date: Security updates scan not performed
Sort Order: Score (worst first)
Security Update Scan Results
Score
Issue
Result
Security Updates
Cannot load security CAB file.
How to correct this
Windows Scan Results
Print this report
Copy to clipboard
Previous security report
Next security report
OK

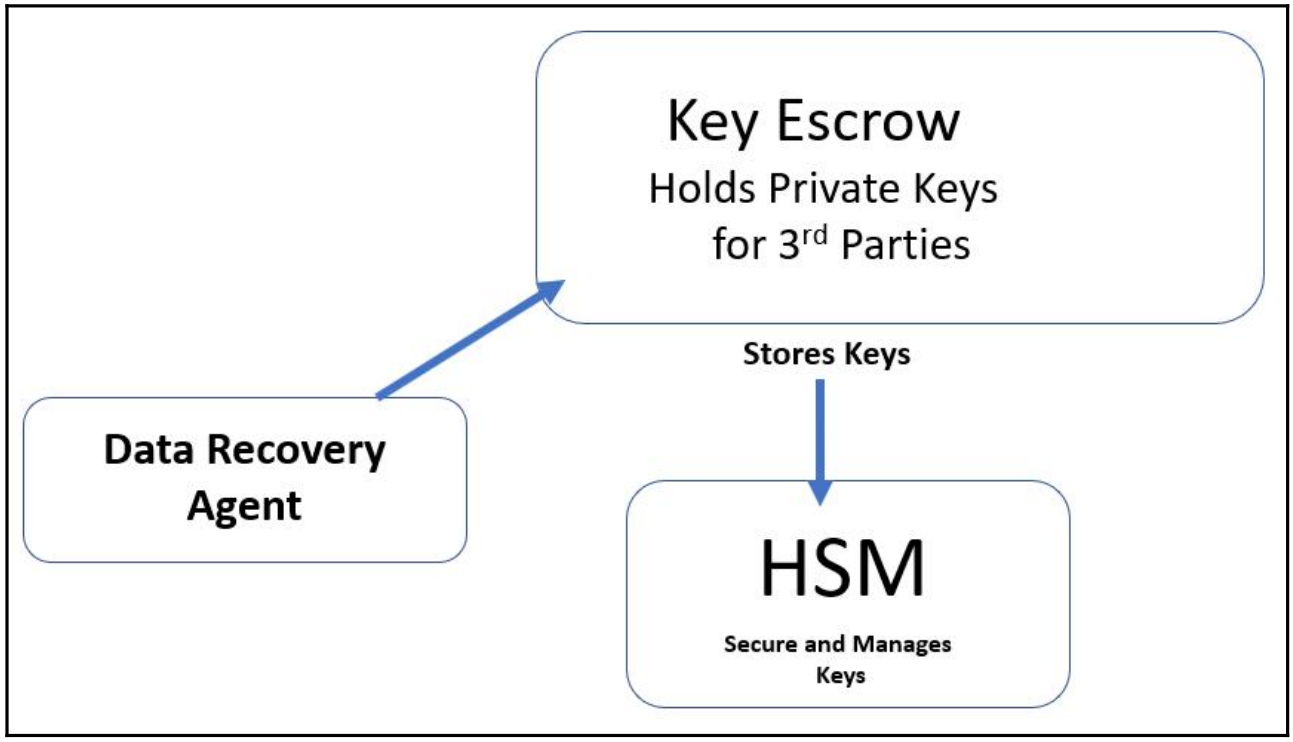

Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Score
Issue
Result
Automatic Updates
The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates.
What was scanned
How to correct this
Administrators
More than 2 Administrators were found on this computer.
What was scanned
Result details
How to correct this
Password Expiration
Some user accounts (4 of 5) have non-expiring passwords.
What was scanned
Result details
How to correct this
Incomplete Updates
No incomplete software update installations were found.
What was scanned
Windows Firewall
Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections.
What was scanned
Result details
How to correct this
Local Account Password Test
Some user accounts (3 of 5) have blank or simple passwords, or could not be analyzed.
What was scanned
Result details
File System
All hard drives (2) are using the NTFS file system.
What was scanned
Result details
Autologon
Autologon is not configured on this computer.
What was scanned
Guest Account
The Guest account is disabled on this computer.
What was scanned
Print this report
Copy to clipboard
Previous security report
Next security report
OK

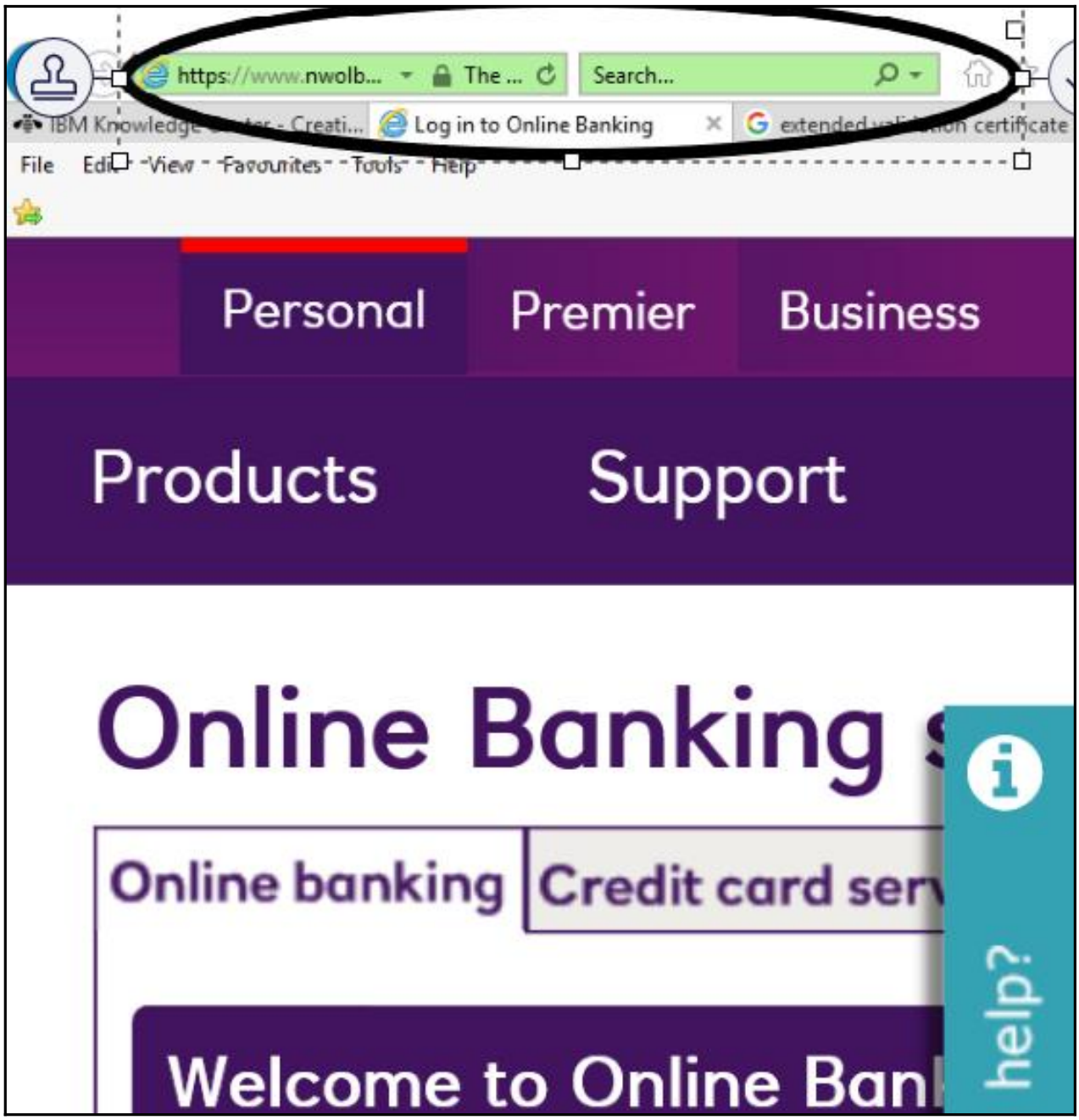
Chapter 09: Implementing Public Key Infrastructure

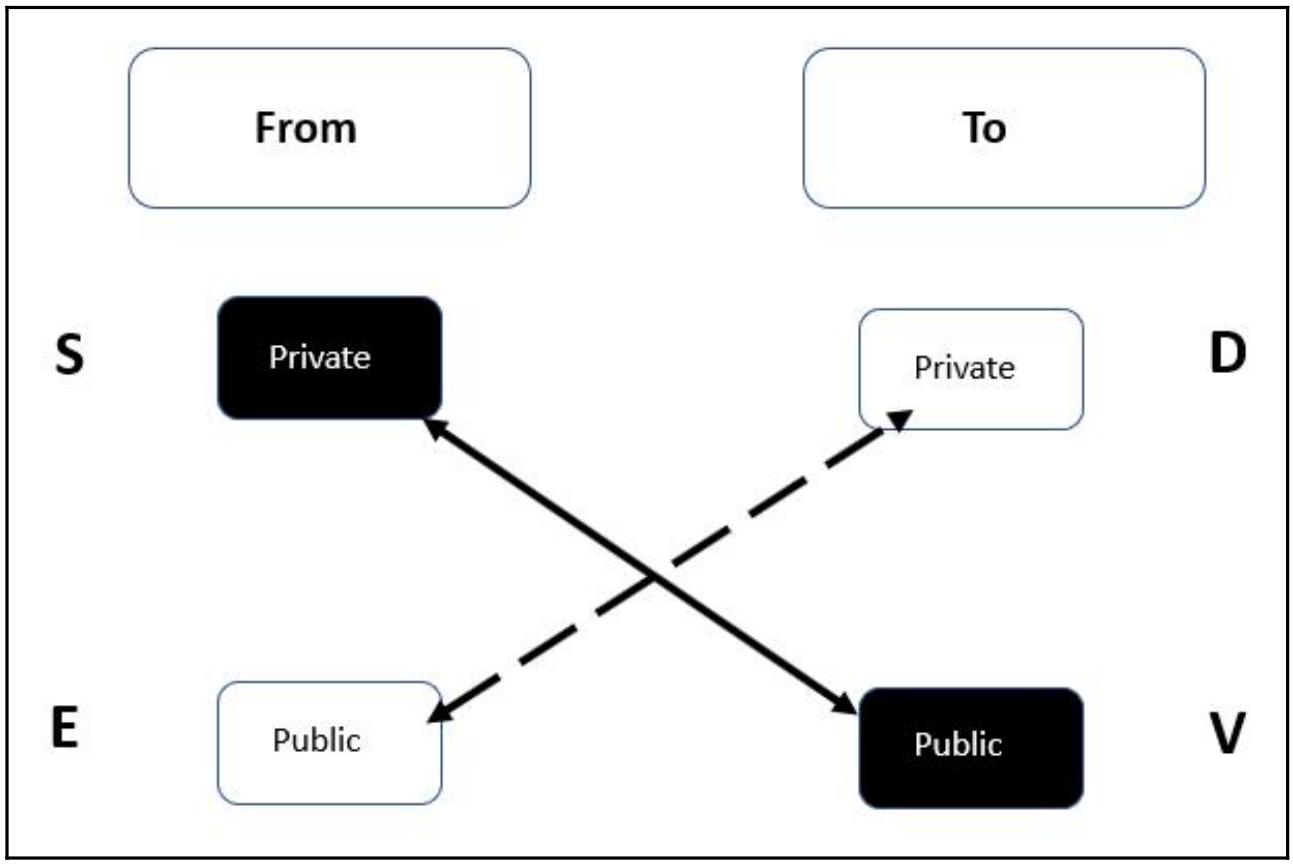


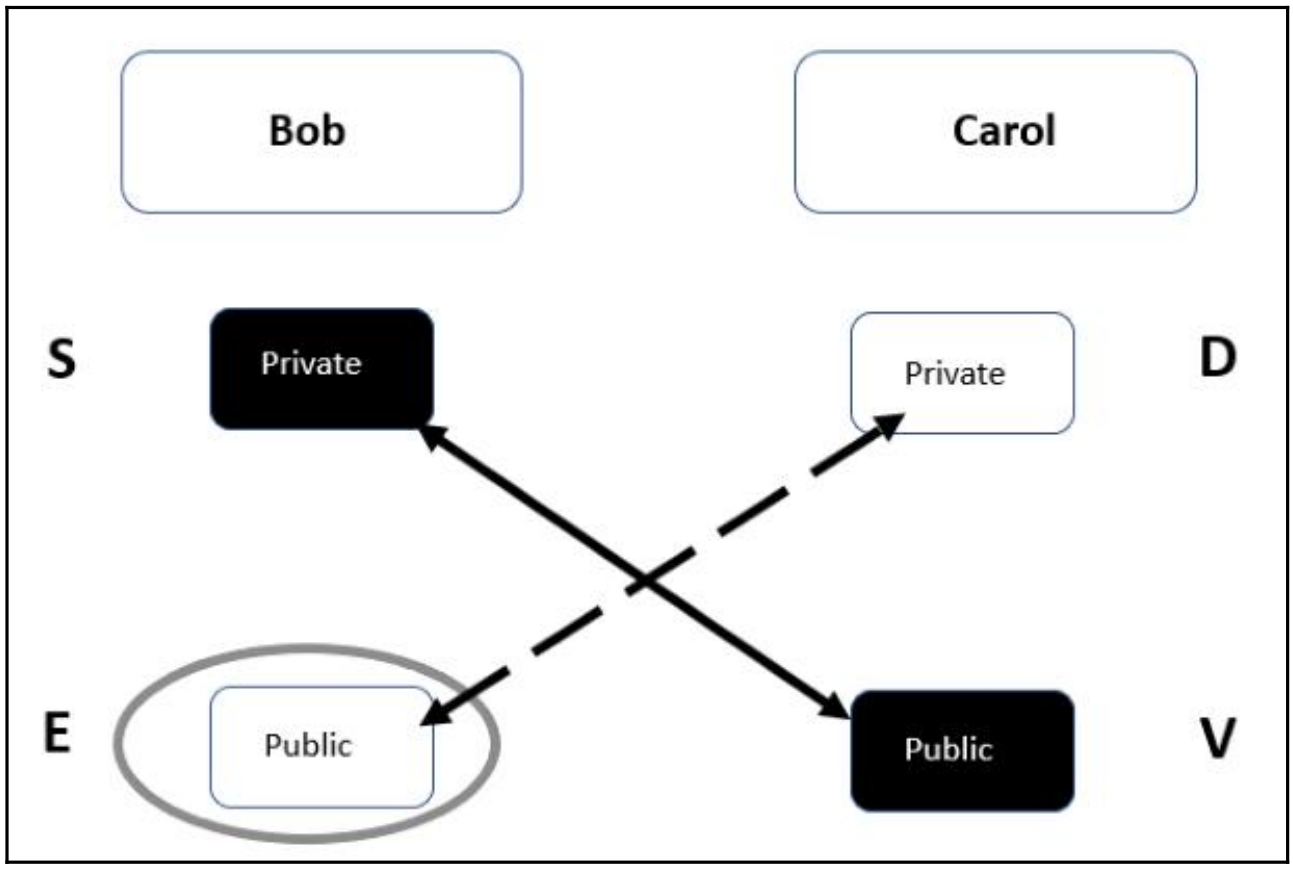

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: www.nwolb.com
Issued by: DigiCert Global CA G2
Valid from 26/03/2018 to 26/03/2020
Issuer Statement
OK

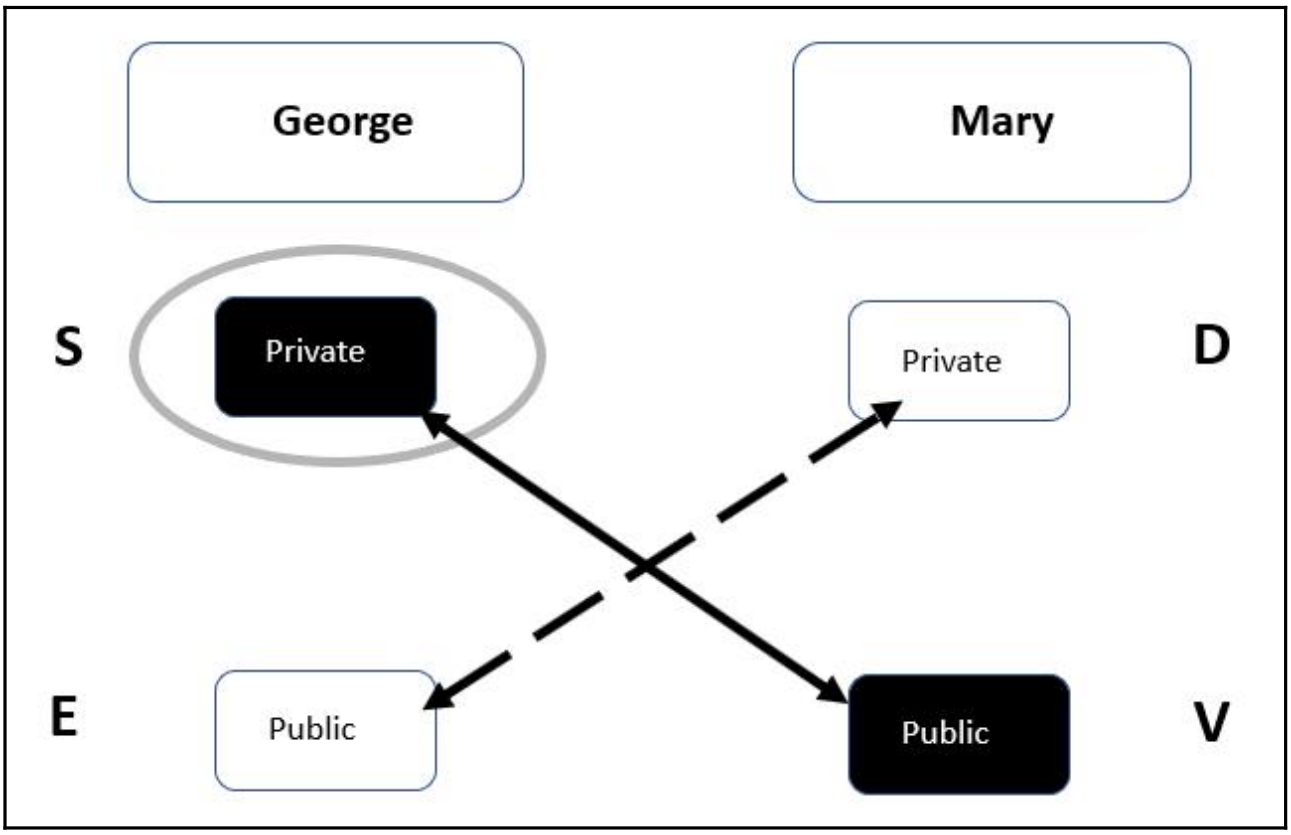

Web Server
CRL
Certificate Validity
CRL is Slow
Stapling
OCSP

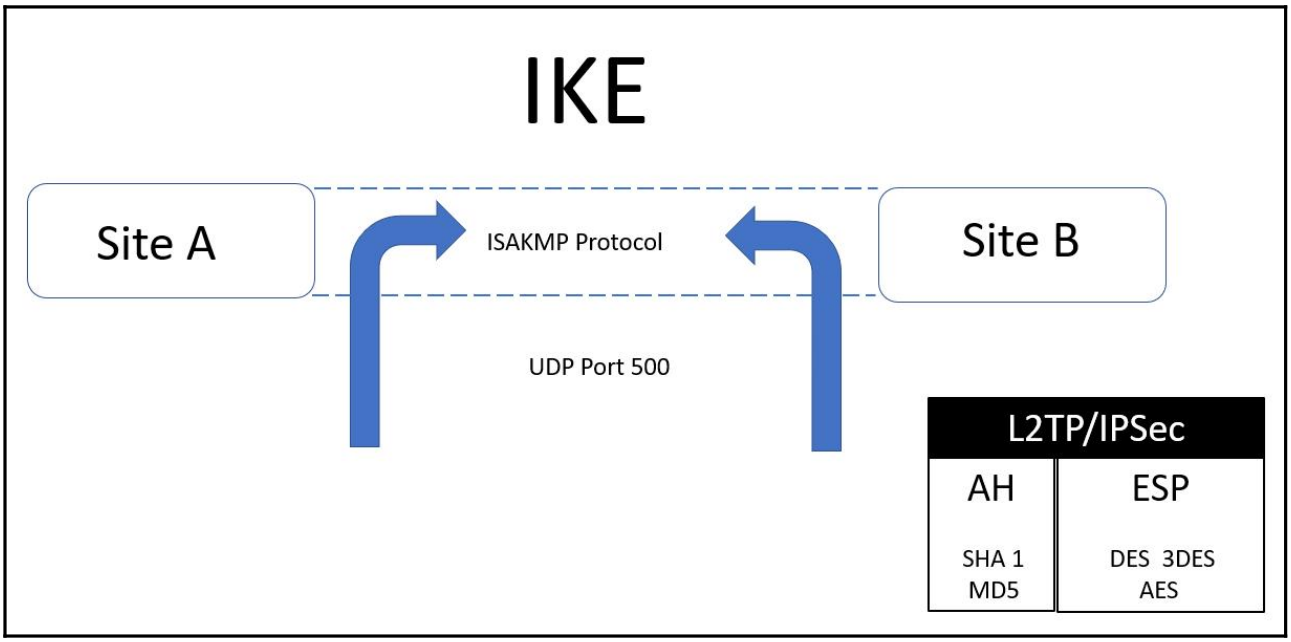

Key Escrow
Holds Private Keys for 3rd Parties
Stores Keys
Data Recovery Agent
HSM
Secure and Manages Keys


https://www.nwolb...
The ...
Search...
Log in to Online Banking
File
Edit
View
Favourites
Tools
Help
Personal
Premier
Business
Products
Support
Online Banking
Online banking
Credit card serv
help?
Welcome to Online Ban

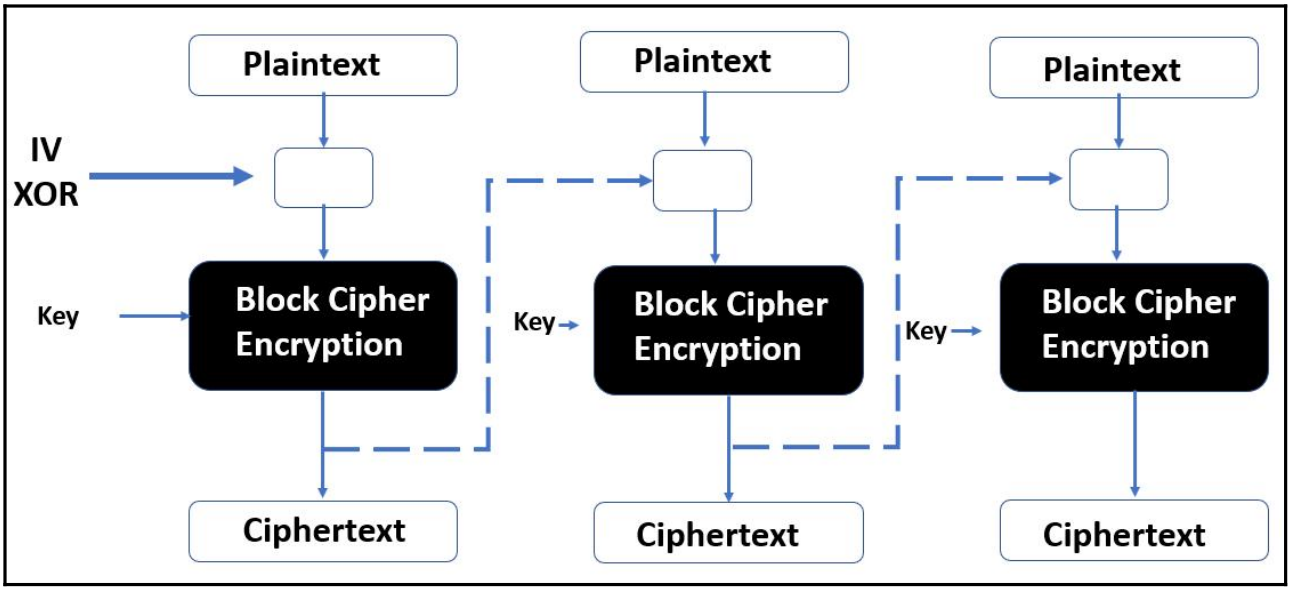

From
To
S
Private
Private
D
E
Public
Public
V

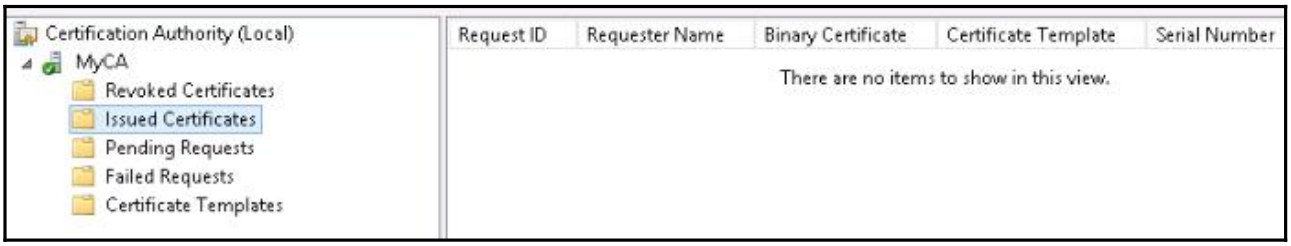

Bob
Carol
S
Private
Private
D
E
Public
Public
V


George
Mary
S
Private
Private
D
E
Public
Public
V

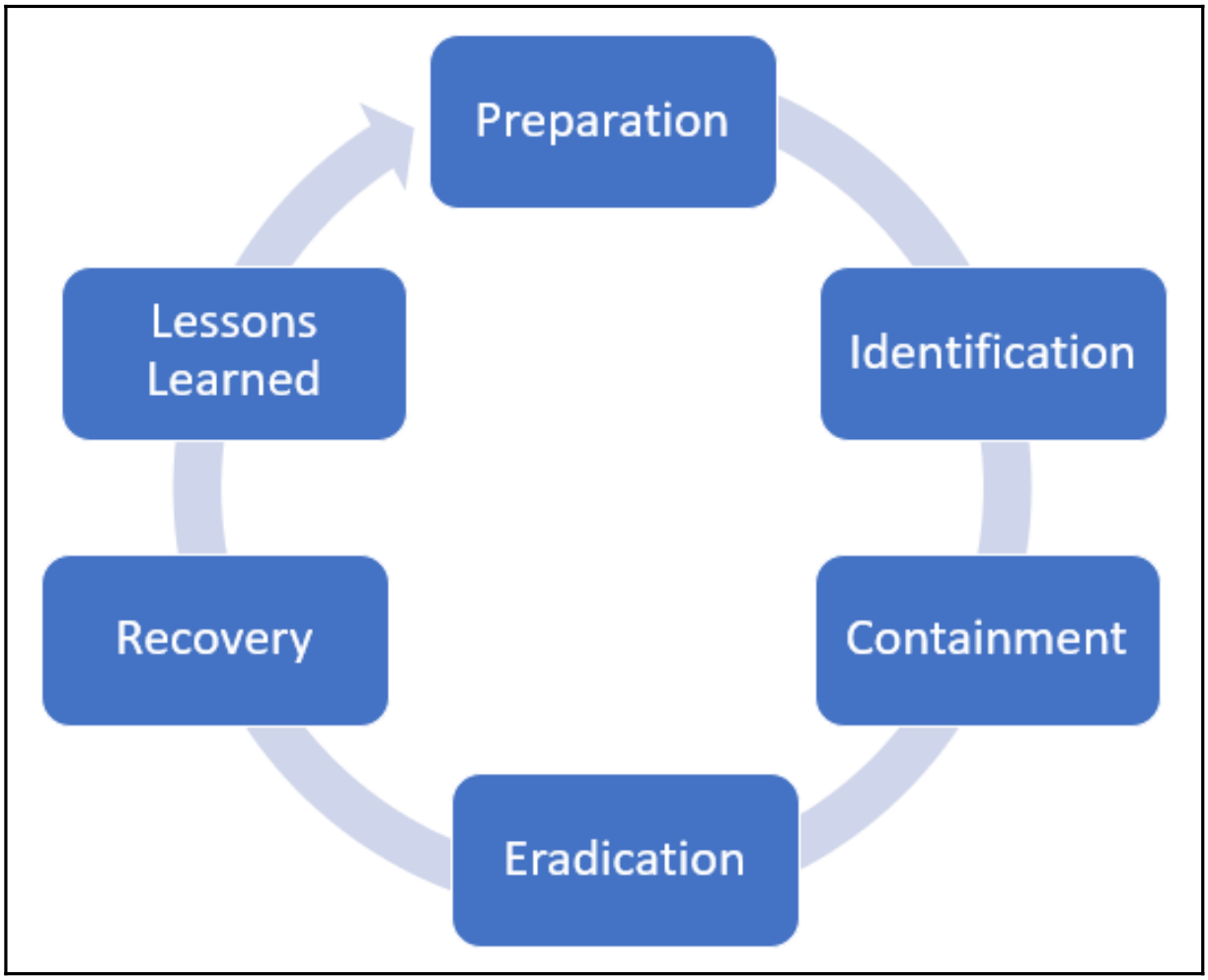

IKE
Site A
ISAKMP Protocol
Site B
UDP Port 500
L2TP/IPSec
AH
SHA 1
MD5
ESP
DES 3DES
AES

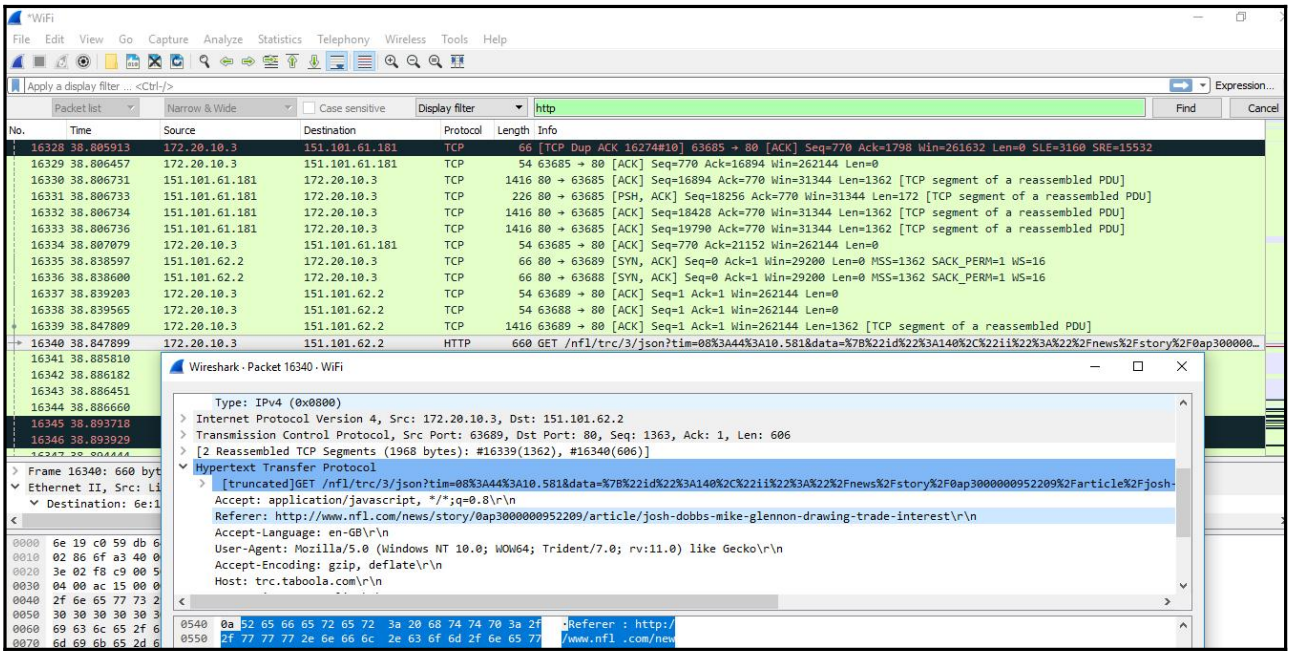
	T	R	E	A	D
XOR (Original Input)	01010100	01110010	01100101	01100001	01100100
Key	01101000	01100101	01101100	01101100	01101111
Output	00111100	00010111	00001001	00001101	00001011

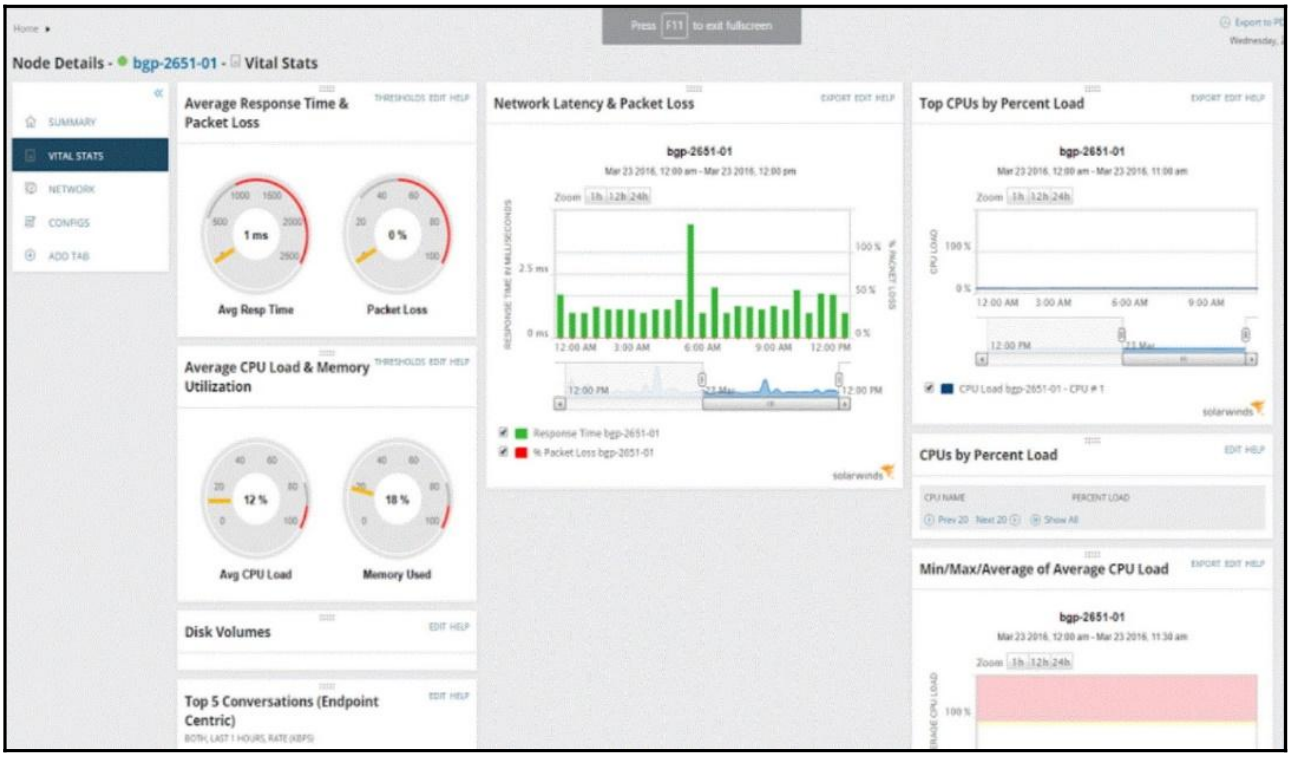


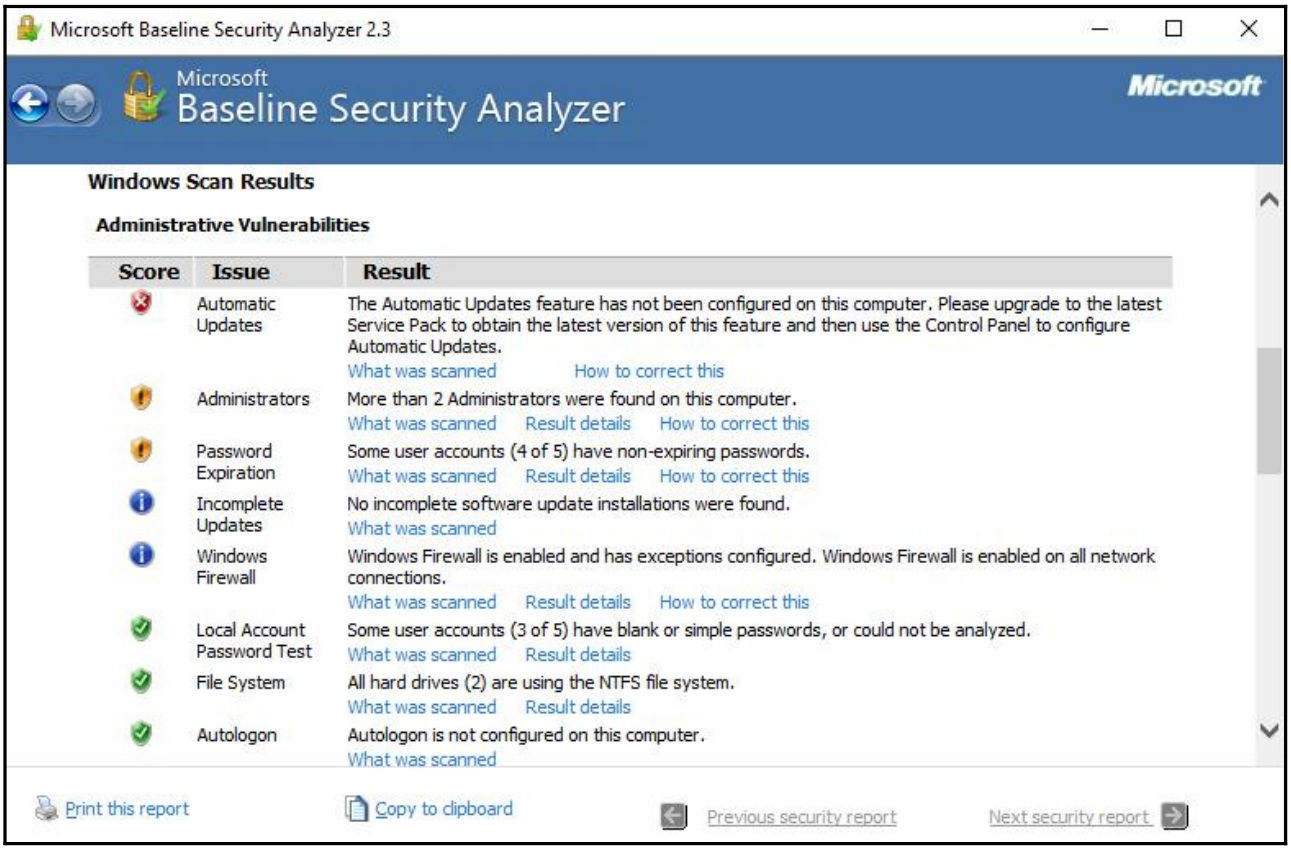


Chapter 10: Responding to Security Incidents




*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Packet list
Narrow & Wide
Case sensitive
Display filter
http
Find
Cancel
No. Time Source Destination Protocol Length Info
16328 38.805913 172.20.10.3 151.101.61.181 TCP 66 [TCP Dup ACK 16274#10] 63685 → 80 [ACK] Seq=770 Ack=1798 Win=261632 Len=0 SLE=3160 SRE=15532
16329 38.806457 172.20.10.3 151.101.61.181 TCP 54 63685 → 80 [ACK] Seq=770 Ack=16894 Win=262144 Len=0
16330 38.806731 151.101.61.181 172.20.10.3 TCP 1416 80 → 63685 [ACK] Seq=16894 Ack=770 Win=31344 Len=1362 [TCP segment of a reassembled PDU]
16331 38.806733 151.101.61.181 172.20.10.3 TCP 226 80 → 63685 [PSH, ACK] Seq=18256 Ack=770 Win=31344 Len=172 [TCP segment of a reassembled PDU]
16332 38.806734 151.101.61.181 172.20.10.3 TCP 1416 80 → 63685 [ACK] Seq=18428 Ack=770 Win=31344 Len=1362 [TCP segment of a reassembled PDU]
16333 38.806736 151.101.61.181 172.20.10.3 TCP 1416 80 → 63685 [ACK] Seq=19790 Ack=770 Win=31344 Len=1362 [TCP segment of a reassembled PDU]
16334 38.807079 172.20.10.3 151.101.61.181 TCP 54 63685 → 80 [ACK] Seq=770 Ack=21152 Win=262144 Len=0
16335 38.838597 151.101.62.2 172.20.10.3 TCP 66 80 → 63689 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1362 SACK_PERM=1 WS=16
16336 38.838600 151.101.62.2 172.20.10.3 TCP 66 80 → 63688 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1362 SACK_PERM=1 WS=16
16337 38.839203 172.20.10.3 151.101.62.2 TCP 54 63689 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
16338 38.839565 172.20.10.3 151.101.62.2 TCP 54 63688 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
16339 38.847809 172.20.10.3 151.101.62.2 TCP 1416 63689 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=1362 [TCP segment of a reassembled PDU]
16340 38.847899 172.20.10.3 151.101.62.2 HTTP 660 GET /nfl/trc/3/json?tim=08%3A44%3A10.581&data=%7B%22id%22%3A140%2C%22ii%22%3A%22%2Fnews%2Fstory%2F0ap300000...
16341 38.885810
16342 38.886182
16343 38.886451
16344 38.886660
16345 38.893718
16346 38.893929
Wireshark · Packet 16340 · WiFi
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.20.10.3, Dst: 151.101.62.2
Transmission Control Protocol, Src Port: 63689, Dst Port: 80, Seq: 1363, Ack: 1, Len: 606
[2 Reassembled TCP Segments (1968 bytes): #16339(1362), #16340(606)]
Hypertext Transfer Protocol
[truncated]GET /nfl/trc/3/json?tim=08%3A44%3A10.581&data=%7B%22id%22%3A140%2C%22ii%22%3A%22%2Fnews%2Fstory%2F0ap3000000952209%2Farticle%2Fjosh-
Accept: application/javascript, */*;q=0.8\r\n
Referer: http://www.nfl.com/news/story/0ap3000000952209/article/josh-dobbs-mike-glennon-drawing-trade-interest\r\n
Accept-Language: en-GB\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: trc.taboola.com\r\n
0540 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f ·Referer : http:/
0550 2f 77 77 77 2e 6e 66 6c 2e 63 6f 6d 2f 6e 65 77 /www.nfl .com/new


Node Details - bgp-2651-01 - Vital Stats
SUMMARY
VITAL STATS
NETWORK
CONFIGS
ADD TAB
Average Response Time & Packet Loss
1 ms
0 %
Avg Resp Time
Packet Loss
Average CPU Load & Memory Utilization
12 %
18 %
Avg CPU Load
Memory Used
Disk Volumes
Top 5 Conversations (Endpoint Centric)
Network Latency & Packet Loss
bgp-2651-01
Top CPUs by Percent Load
bgp-2651-01
CPUs by Percent Load
Min/Max/Average of Average CPU Load
bgp-2651-01




```
C:\WINDOWS\system32>ping ianneil501.com

Pinging ianneil501.com [46.30.213.45] with 32 bytes of data:
Reply from 46.30.213.45: bytes=32 time=42ms TTL=47
Reply from 46.30.213.45: bytes=32 time=44ms TTL=47
Reply from 46.30.213.45: bytes=32 time=42ms TTL=47
Reply from 46.30.213.45: bytes=32 time=43ms TTL=47

Ping statistics for 46.30.213.45:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 44ms, Average = 42ms
```

```
C:\WINDOWS\system32>ping -t www.ianneil501.com

Pinging www.ianneil501.com [46.30.213.45] with 32 bytes of data:
Reply from 46.30.213.45: bytes=32 time=42ms TTL=47
Reply from 46.30.213.45: bytes=32 time=43ms TTL=47
Reply from 46.30.213.45: bytes=32 time=41ms TTL=47
Reply from 46.30.213.45: bytes=32 time=41ms TTL=47
Reply from 46.30.213.45: bytes=32 time=47ms TTL=47
Reply from 46.30.213.45: bytes=32 time=49ms TTL=47
Reply from 46.30.213.45: bytes=32 time=45ms TTL=47
Reply from 46.30.213.45: bytes=32 time=43ms TTL=47
Reply from 46.30.213.45: bytes=32 time=44ms TTL=47
Reply from 46.30.213.45: bytes=32 time=46ms TTL=47
Reply from 46.30.213.45: bytes=32 time=42ms TTL=47
Reply from 46.30.213.45: bytes=32 time=43ms TTL=47
Reply from 46.30.213.45: bytes=32 time=42ms TTL=47
Reply from 46.30.213.45: bytes=32 time=43ms TTL=47
Reply from 46.30.213.45: bytes=32 time=43ms TTL=47
Reply from 46.30.213.45: bytes=32 time=41ms TTL=47
Reply from 46.30.213.45: bytes=32 time=46ms TTL=47
```

```
C:\WINDOWS\system32>NETSTAT

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:5939         DESKTOP-QR6R2DA:49758  ESTABLISHED
  TCP    127.0.0.1:7778         DESKTOP-QR6R2DA:49793  ESTABLISHED
  TCP    127.0.0.1:49669        DESKTOP-QR6R2DA:49670  ESTABLISHED
  TCP    127.0.0.1:49670        DESKTOP-QR6R2DA:49669  ESTABLISHED
  TCP    127.0.0.1:49758        DESKTOP-QR6R2DA:5939   ESTABLISHED
  TCP    127.0.0.1:49793        DESKTOP-QR6R2DA:7778   ESTABLISHED
  TCP    127.0.0.1:49794        DESKTOP-QR6R2DA:49795  ESTABLISHED
  TCP    127.0.0.1:49795        DESKTOP-QR6R2DA:49794  ESTABLISHED
  TCP    192.168.0.118:49672    r-54-45-234-77:https   CLOSE_WAIT
  TCP    192.168.0.118:49677    DE-HAM-PLS-R012:5938   ESTABLISHED
  TCP    192.168.0.118:49748    ams10-004:http         ESTABLISHED
  TCP    192.168.0.118:49753    40.67.255.199:https    ESTABLISHED
```

```
C:\WINDOWS\system32>tracert www.ianneil501.com

Tracing route to www.ianneil501.com [46.30.213.45]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.254
  2     1 ms     1 ms     1 ms  209.134-31-62.static.virginmediabusiness.co.uk [62.31.134.209]
  3     *        *        *     Request timed out.
  4    20 ms    19 ms    17 ms  perr-core-2a-ae16-0.network.virginmedia.net [62.253.138.245]
  5     *        *        *     Request timed out.
  6    29 ms    26 ms    26 ms  86.85-254-62.static.virginmediabusiness.co.uk [62.254.85.86]
  7    34 ms    33 ms    32 ms  ldn-b1-link.telia.net [213.248.84.25]
  8    30 ms    27 ms    26 ms  ldn-bb4-link.telia.net [62.115.143.26]
  9    42 ms    41 ms    37 ms  hbg-bb4-link.telia.net [62.115.122.160]
 10    46 ms    42 ms    49 ms  kbn-bb4-link.telia.net [213.155.135.121]
 11    53 ms    52 ms    45 ms  kbn-b3-link.telia.net [62.115.114.69]
 12    43 ms    43 ms    43 ms  onecom-ic-307407-kbn-horsk-i1.c.telia.net [62.115.47.242]
 13    43 ms    42 ms    44 ms  ae1-200.dr3-cph3.pub.network.one.com [46.30.210.17]
 14    43 ms    50 ms    43 ms  xe-0-2-0-200.ar1.pub.webpod1-cph3.one.com [46.30.210.31]
 15    41 ms    41 ms    41 ms  webcluster46.webpod1-cph3.one.com [46.30.213.45]
```

```
C:\Users\Administrator>nslookup wwww.ianneil501.com
Server:  cache2.service.virginmedia.net
Address:  194.168.8.100

Non-authoritative answer:
Name:    wwww.ianneil501.com
Addresses:  2a02:2350:5:100:8b40:0:7611:8566
          46.30.213.45
```

```
[root@centos7 ~]# dig google.com

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.3 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32702
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4000
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             5       IN      A       216.58.220.110

;; Query time: 27 msec
;; SERVER: 192.168.12.2#53(192.168.220.2)
;; WHEN: Tue Sep 04 11:18:22 AEST 2018
;; MSG SIZE  rcvd: 55
```

```
C:\Users\Administrator>arp -a

Interface: 172.18.27.177 --- 0x7
  Internet Address      Physical Address      Type
  172.18.27.191         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.118 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.134         20-47-ed-97-3b-3a     dynamic
  192.168.0.158         20-47-ed-c9-54-1a     dynamic
  192.168.0.159         20-47-ed-2a-27-42     dynamic
  192.168.0.163         30-59-b7-7e-c3-23     dynamic
  192.168.0.250         d0-bf-9c-45-b2-be     dynamic
  192.168.0.254         64-12-25-5a-06-c1     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

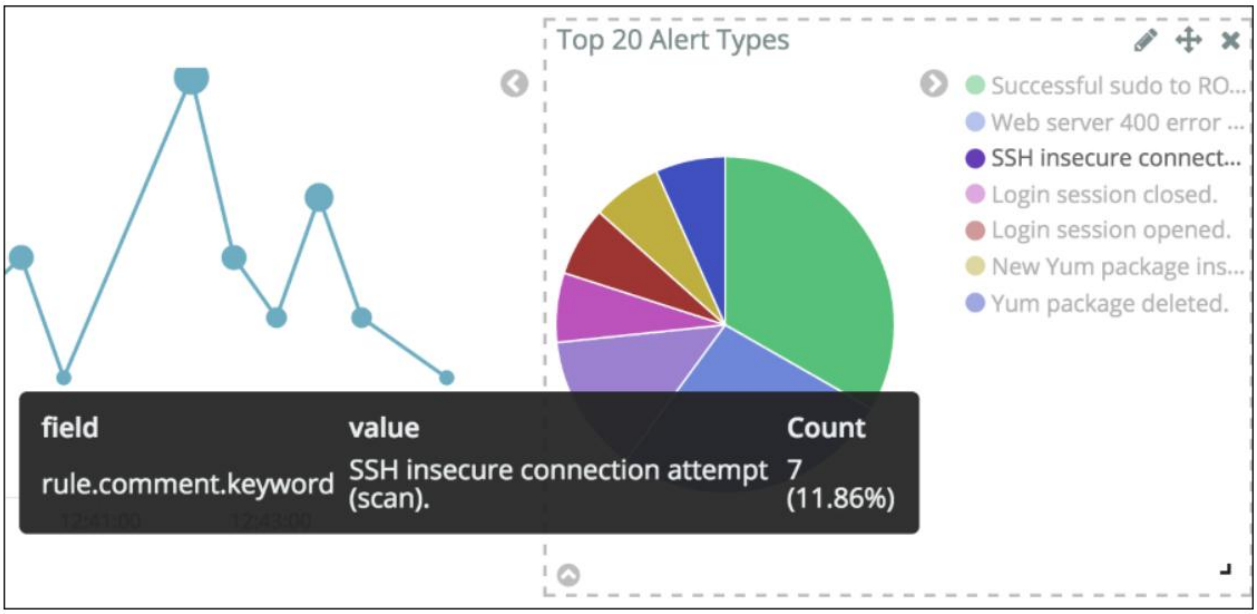
```
C:\Users\Administrator>ipconfig /displaydns

Windows IP Configuration

    177.27.18.172.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 177.27.18.172.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 86400
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : DESKTOP-QR6R2DA.mshome.net


    mssplus.mcafee.com
    ----------------------------------------
    No records of type AAAA


    mssplus.mcafee.com
    ----------------------------------------
    Record Name . . . . . : mssplus.mcafee.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 86400
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 0.0.0.1
```

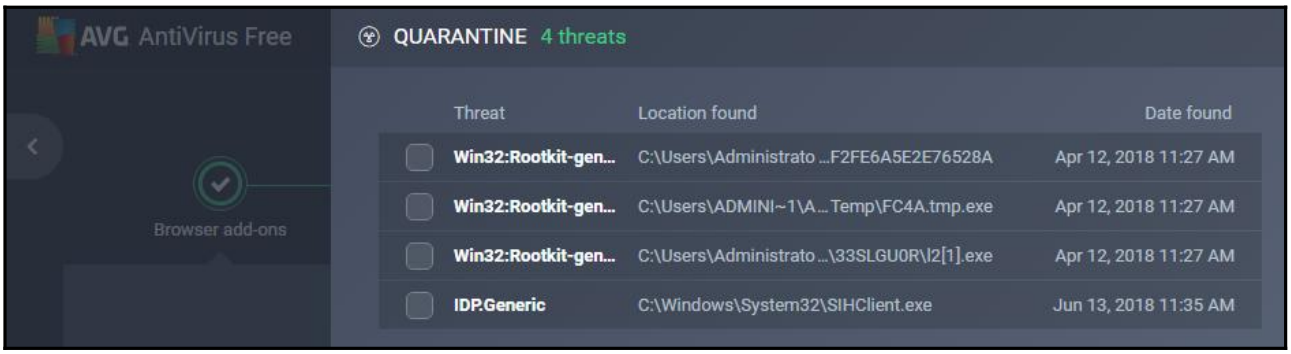
```
C:\Users\Administrator>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Administrator>
```

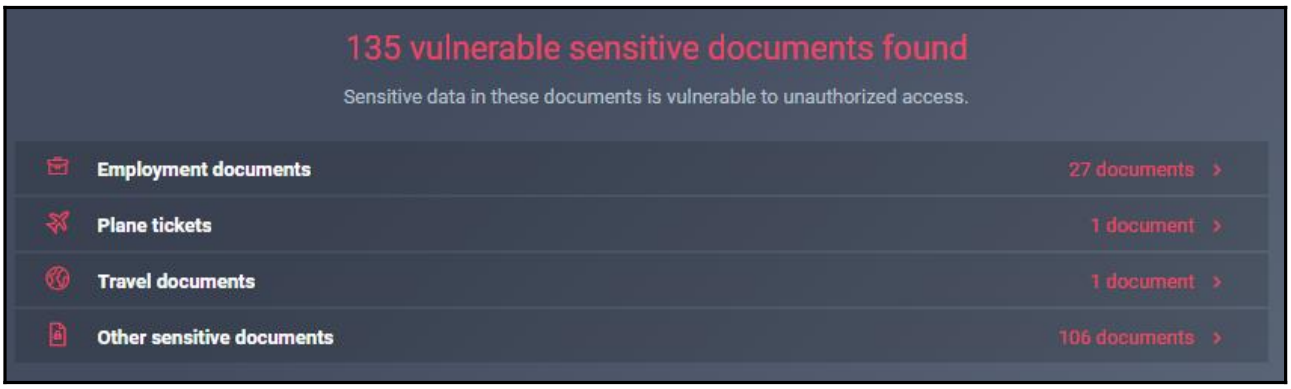
```
# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:33:31.976358 IP 172.16.25.126.ssh > 172.16.25.125.apwi-rxspooler: Flags [P.], seq 3500440357
:3500440553, ack 3652628334, win 18760, length 196
11:33:31.976603 IP 172.16.25.125.apwi-rxspooler > 172.16.25.126.ssh: Flags [.], ack 196, win 64
487, length 0
11:33:31.977243 ARP, Request who-has tecmint.com tell 172.16.25.126, length 28
11:33:31.977359 ARP, Reply tecmint.com is-at 00:14:5e:67:26:1d (oui Unknown), length 46
11:33:31.977367 IP 172.16.25.126.54807 > tecmint.com: 4240+ PTR? 125.25.16.172.in-addr.arpa. (4
4)
11:33:31.977599 IP tecmint.com > 172.16.25.126.54807: 4240 NXDomain 0/1/0 (121)
11:33:31.977742 IP 172.16.25.126.44519 > tecmint.com: 40988+ PTR? 126.25.16.172.in-addr.arpa. (
44)
11:33:32.028747 IP 172.16.20.33.netbios-ns > 172.16.31.255.netbios-ns: NBT UDP PACKET(137): QUE
RY; REQUEST; BROADCAST
11:33:32.112045 IP 172.16.21.153.netbios-ns > 172.16.31.255.netbios-ns: NBT UDP PACKET(137): QU
ERY; REQUEST; BROADCAST
11:33:32.115606 IP 172.16.21.144.netbios-ns > 172.16.31.255.netbios-ns: NBT UDP PACKET(137): QU
ERY; REQUEST; BROADCAST
```

```
$  netcat -z -v ianneil501.com 78-80

nc: connect to ianneil501.com port 78 (tcp) failed: connection refused
nc: connect to ianneil501.com port 79 (tcp) failed: connection refused

Connection to ianneil501.com port 80 (tcp/html) succeeded!
```

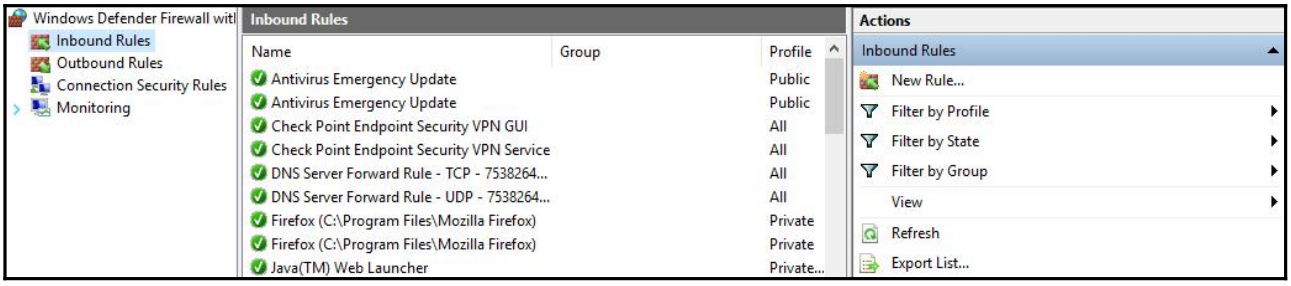
To explore the alert data in more detail, you can choose an alert type on which to filter, as shown in the following two screenshots.



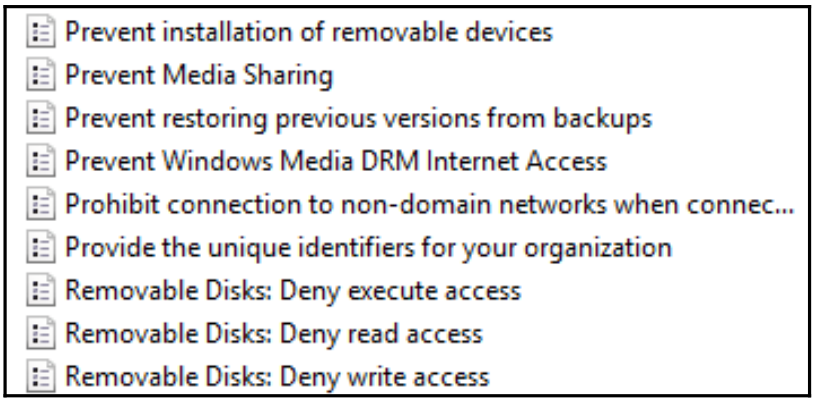


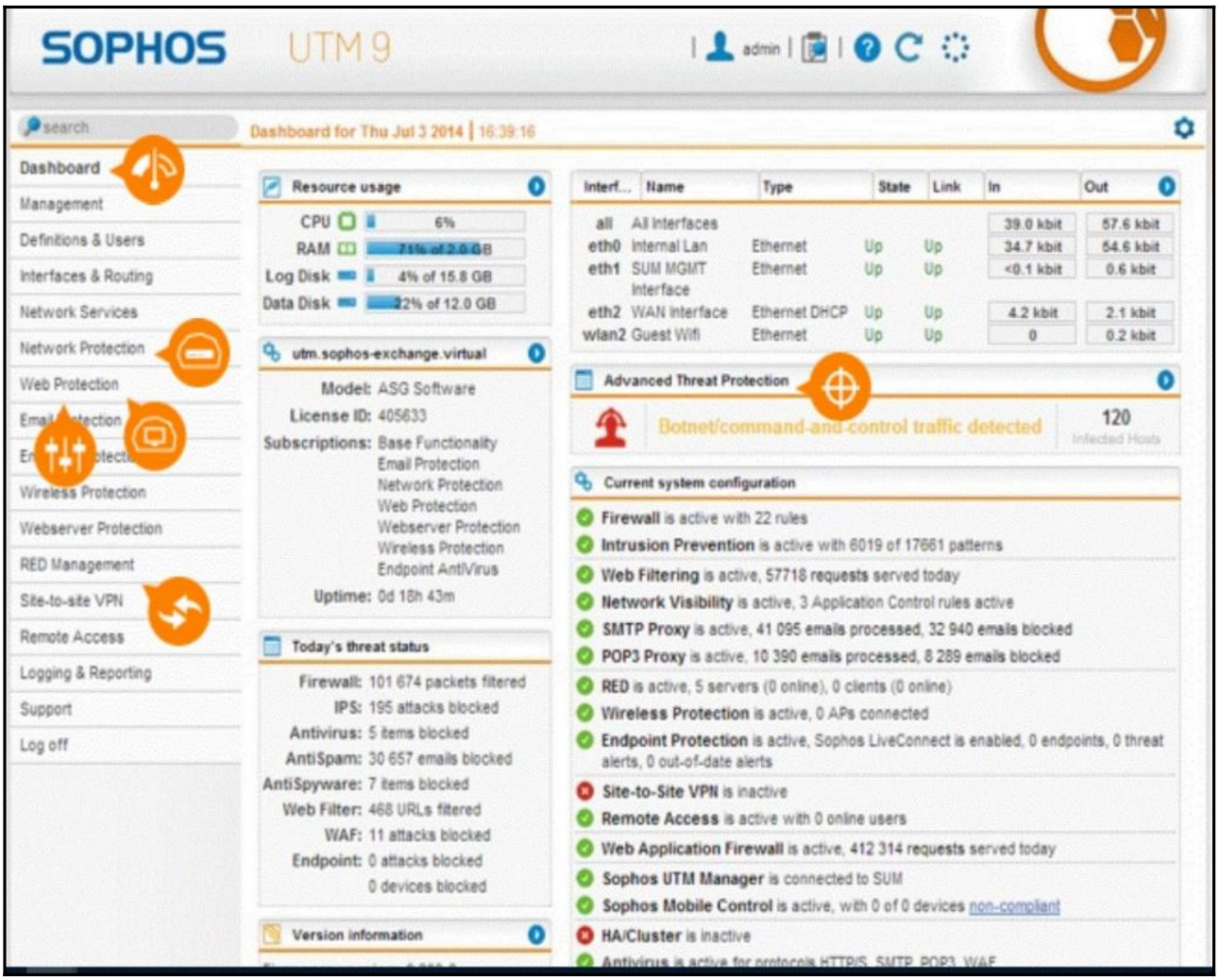



```
C:\WINDOWS\system32>sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection found corrupt files and successfully repaired them.
For online repairs, details are included in the CBS log file located at
windir\Logs\CBS\CBS.log. For example C:\Windows\Logs\CBS\CBS.log. For offline
repairs, details are included in the log file provided by the /OFFLOGFILE flag.
```



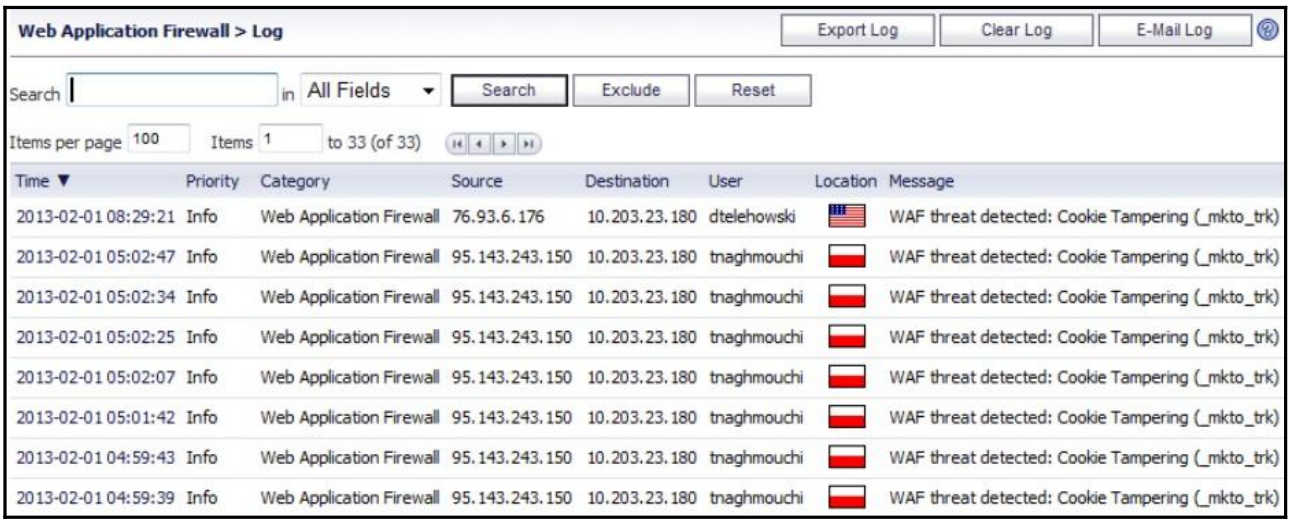
Action	User	Name	Condition
Allow	Everyone	Microsoft Office 2016	Publisher
Allow	Everyone	McAfee Security Scan	Publisher
Allow	Everyone	Mozilla Firefox	Publisher
Allow	Everyone	Internet Explorer	Publisher
Allow	Everyone	Wireshark	Publisher
Allow	Everyone	Adobe Acrobat Pro	Publisher



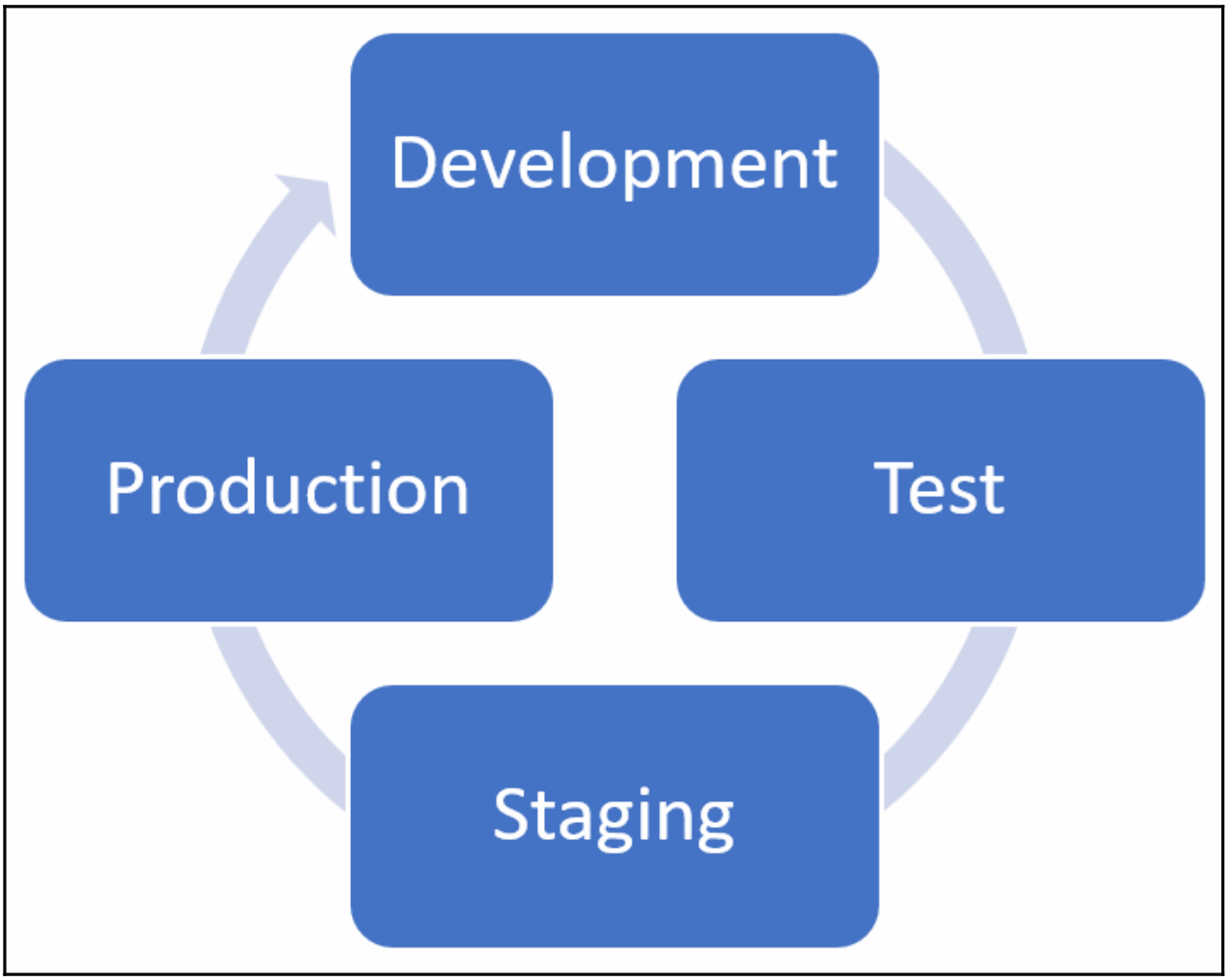



```
^(?:4[0-9]{12}(?:[0-9]{3})?|[25][1-7][0-9]{14}|6(?:011|5[0-9][0-9])[0-9]{12}|3[47][0-9]{13}|3(?:0[0-5]|[68][0-9])[0-9]{11}|(?:2131|1800|35\d{3})\d{11})$
```

```
C:\WINDOWS\system32>wmic OS Get DataExecutionPrevention_SupportPolicy
DataExecutionPrevention_SupportPolicy
2
```


Web Application Firewall > Log
Export Log
Clear Log
E-Mail Log
Search
in
All Fields
Search
Exclude
Reset
Items per page 100
Items 1 to 33 (of 33)
Time ▼ Priority Category Source Destination User Location Message
2013-02-01 08:29:21 Info Web Application Firewall 76.93.6.176 10.203.23.180 dtelehowski WAF threat detected: Cookie Tampering (_mkto_trk)
2013-02-01 05:02:47 Info Web Application Firewall 95.143.243.150 10.203.23.180 tnaghmouchi WAF threat detected: Cookie Tampering (_mkto_trk)
2013-02-01 05:02:34 Info Web Application Firewall 95.143.243.150 10.203.23.180 tnaghmouchi WAF threat detected: Cookie Tampering (_mkto_trk)
2013-02-01 05:02:25 Info Web Application Firewall 95.143.243.150 10.203.23.180 tnaghmouchi WAF threat detected: Cookie Tampering (_mkto_trk)
2013-02-01 05:02:07 Info Web Application Firewall 95.143.243.150 10.203.23.180 tnaghmouchi WAF threat detected: Cookie Tampering (_mkto_trk)
2013-02-01 05:01:42 Info Web Application Firewall 95.143.243.150 10.203.23.180 tnaghmouchi WAF threat detected: Cookie Tampering (_mkto_trk)
2013-02-01 04:59:43 Info Web Application Firewall 95.143.243.150 10.203.23.180 tnaghmouchi WAF threat detected: Cookie Tampering (_mkto_trk)
2013-02-01 04:59:39 Info Web Application Firewall 95.143.243.150 10.203.23.180 tnaghmouchi WAF threat detected: Cookie Tampering (_mkto_trk)

Chapter 11: Managing Business Continuity




Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Other People
Smart Card Trusted Roots
Issued To | Issued By | Expiration Date | Intended Purposes | Friendly Name | Status
Actalis Authentication Root CA | Actalis Authentication Root CA | 22/09/2030 | Server Authenticati... | Actalis Authenticati...
AddTrust External CA Root | AddTrust External CA Root | 30/05/2020 | Server Authenticati... | The USERTrust Net...
Baltimore CyberTrust Root | Baltimore CyberTrust Root | 13/05/2025 | Server Authenticati... | DigiCert Baltimore ...
Certum CA | Certum CA | 11/06/2027 | Server Authenticati... | Certum
Certum Trusted Network CA | Certum Trusted Network CA | 31/12/2029 | Server Authenticati... | Certum Trusted Net...
Class 3 Public Primary Certificat... | Class 3 Public Primary Certificatio... | 02/08/2028 | Server Authenticati... | VeriSign Class 3 Pu...
COMODO RSA Certification Au... | COMODO RSA Certification Auth... | 19/01/2038 | Server Authenticati... | COMODO SECURE™
Copyright (c) 1997 Microsoft C... | Copyright (c) 1997 Microsoft Corp. | 31/12/1999 | Time Stamping | Microsoft Timesta...
DESKTOP-QR6R2DA | DESKTOP-QR6R2DA | 23/08/3017 | Server Authenticati | <None>
DESKTOP-QR6R2DA | DESKTOP-QR6R2DA | 24/09/3017 | Server Authenticati | <None>
DigiCert Assured ID Root CA | DigiCert Assured ID Root CA | 10/11/2031 | Server Authenticati... | DigiCert
DigiCert Global Root CA | DigiCert Global Root CA | 10/11/2031 | Server Authenticati... | DigiCert
DigiCert Global Root G2 | DigiCert Global Root G2 | 15/01/2038 | Server Authenticati... | DigiCert Global Roo...
DigiCert High Assurance EV Ro... | DigiCert High Assurance EV Root | 10/11/2031 | Server Authenticati... | DigiCert
DigiCert Trusted Root G4 | DigiCert Trusted Root G4 | 15/01/2038 | Server Authenticati... | DigiCert Trusted Ro...
DST Root CA X3 | DST Root CA X3 | 30/09/2021 | Secure Email, Serve... | DST Root CA X3
D-TRUST Root Class 3 CA 2 2009 | D-TRUST Root Class 3 CA 2 2009 | 05/11/2029 | Server Authenticati... | D-TRUST Root Clas...
Entrust Root Certification Auth... | Entrust Root Certification Authority | 27/11/2026 | Server Authenticati... | Entrust
Entrust Root Certification Auth... | Entrust Root Certification Authori... | 07/12/2030 | Server Authenticati... | Entrust.net
Entrust.net Certification Author... | Entrust.net Certification Authority... | 24/07/2029 | Server Authenticati... | Entrust (2048)
Equifax Secure Certificate Auth... | Equifax Secure Certificate Authority | 22/08/2018 | Secure Email, Serve... | GeoTrust
GeoTrust Global CA | GeoTrust Global CA | 21/05/2022 | Server Authenticati... | GeoTrust Global CA

END