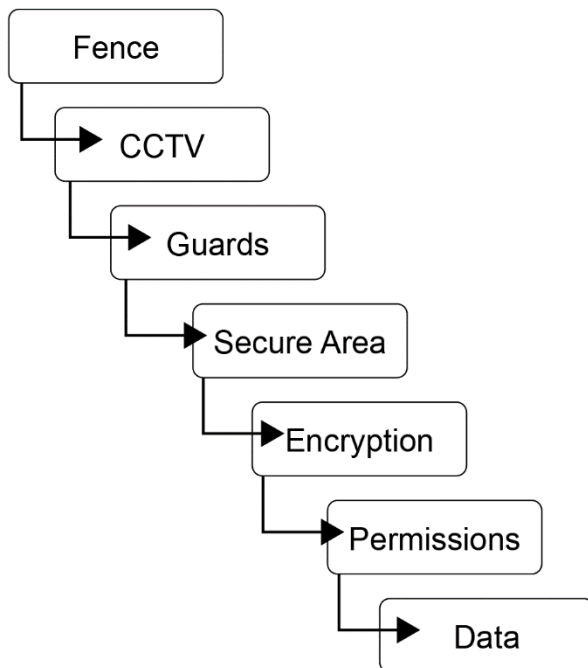
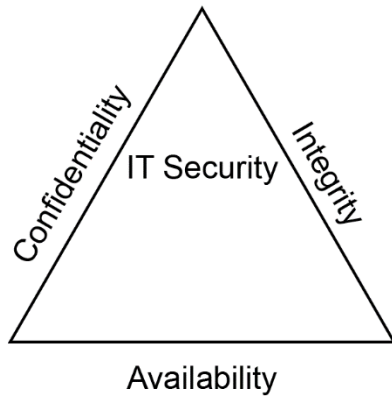
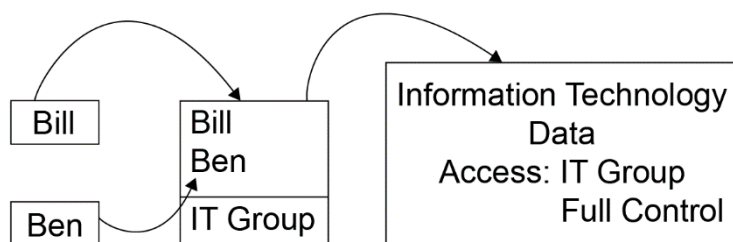
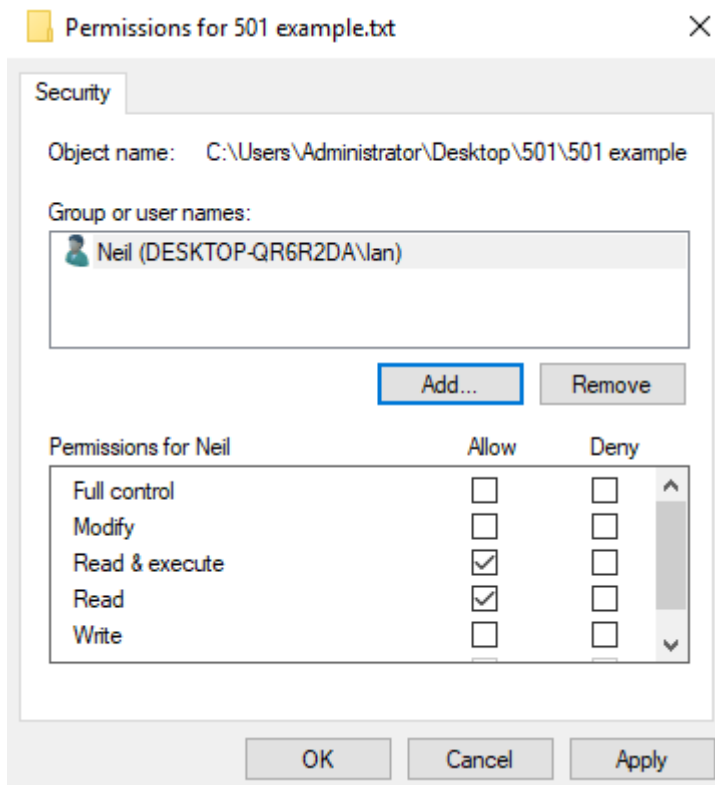
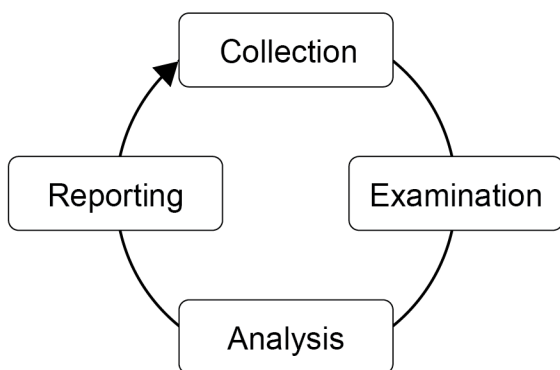


Chapter 1: Understanding Security Fundamentals







Virtual Sec +.zip Properties



General Security Details Previous Versions



Virtual Sec +.zip

Type of file: Compressed (zipped) Folder (.zip)

Opens with: Windows Explorer

Change...

Location: C:\Users\Administrator.WIN-HB5RLG5VD60\Desktop

Size: 3.68 MB (3,869,293 bytes)

Size on disk: 3.69 MB (3,870,720 bytes)

Created: 28 May 2020, 16:07:04

Modified: 28 May 2020, 16:07:04

Accessed: 28 May 2020, 16:07:04

Attributes: ☐ Read-only ☐ Hidden

Advanced...

OK

Cancel

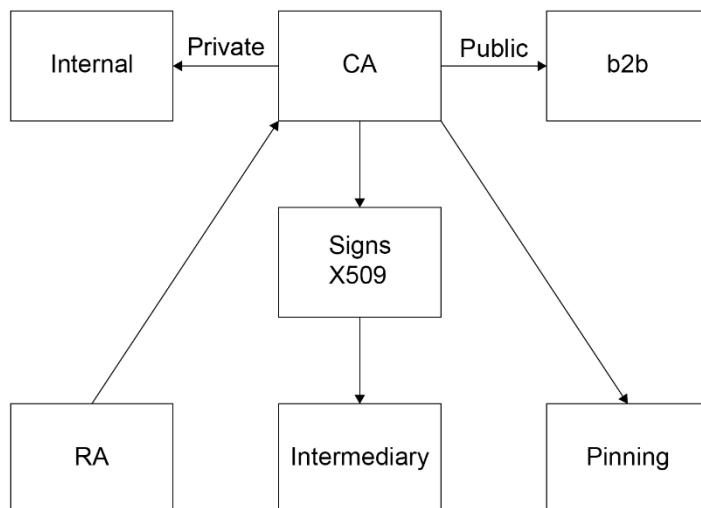
Apply

Chapter 2: Implementing Public Key Infrastructure

Certification Authority (Local)

- MyCA
 - Revoked Certificates
 - Issued Certificates
 - Pending Requests
 - Failed Requests
 - Certificate Templates

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number
There are no items to show in this view.				



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.

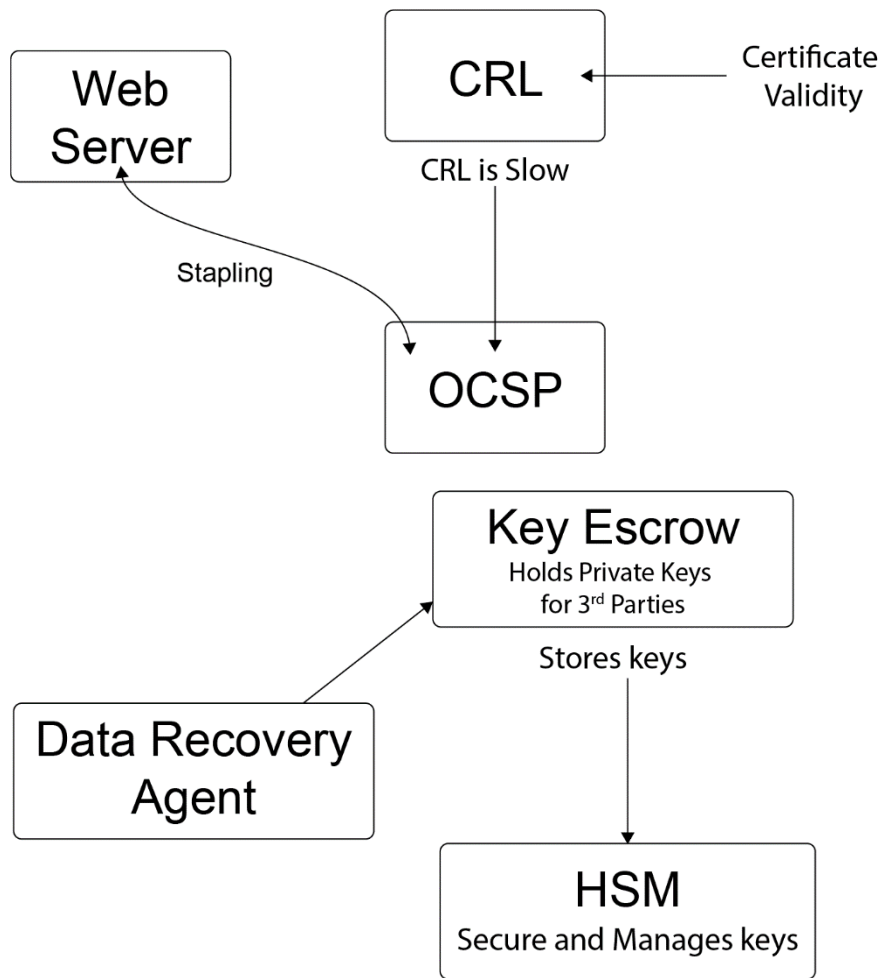
Issued to: www.nwolb.com

Issued by: DigiCert Global CA G2

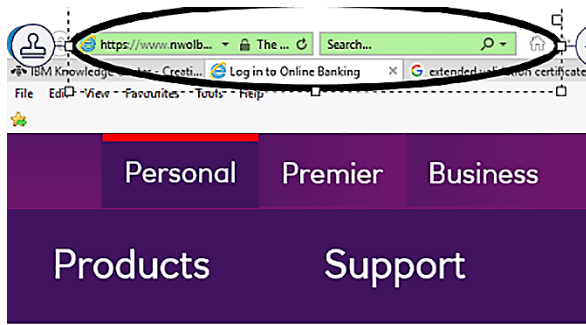
Valid from: 26/03/2018 **to:** 26/03/2020

Issuer Statement

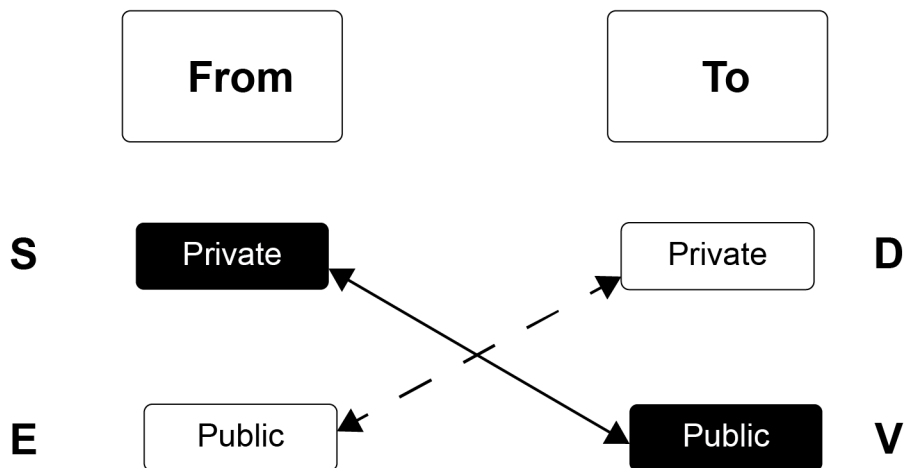
OK

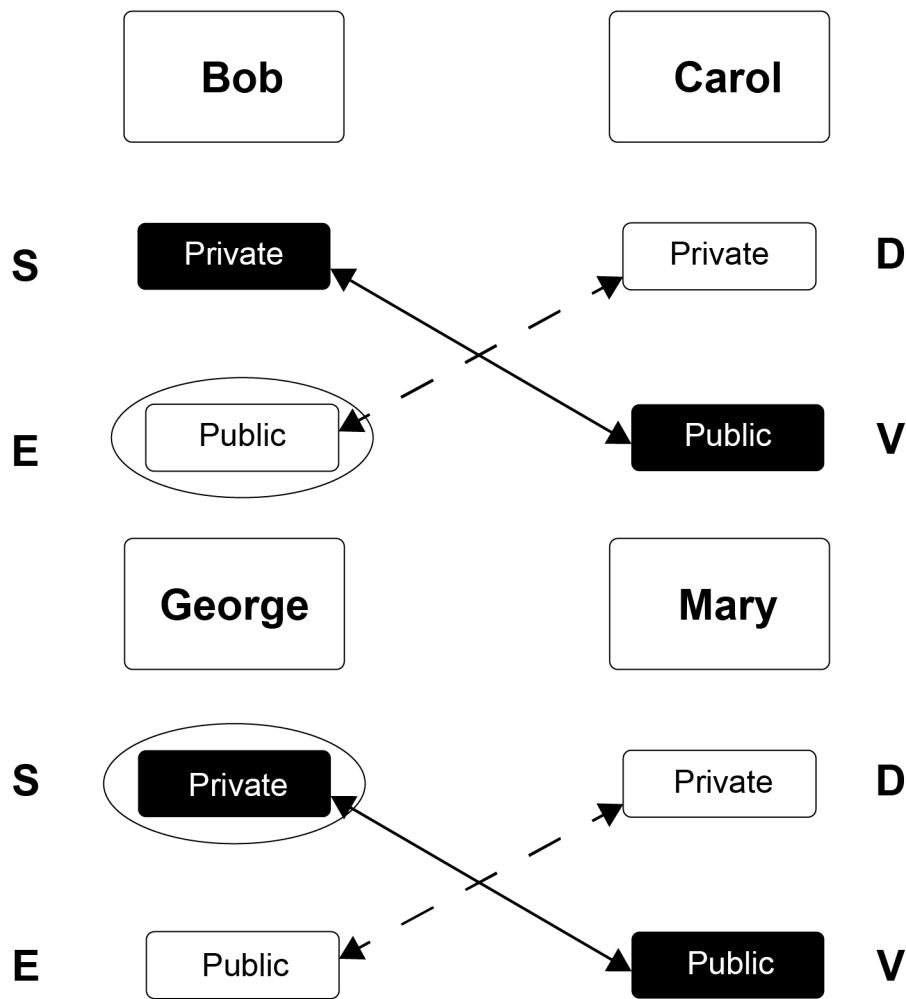


Certificate type	Format	File Extension
Private	P12	.pfx
Public	P7B	.cer
PREM	Base64 format	.pem
DER	Extension for PEM	.der

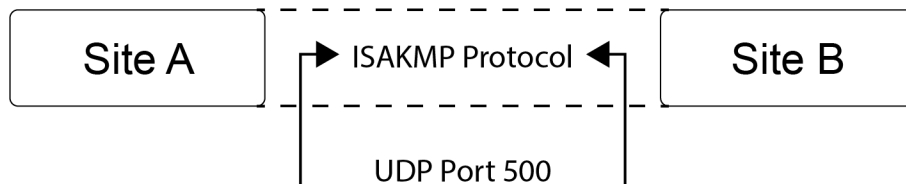


Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
ROT 13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ROT 13	A	B	C	D	E	F	G	H	I	J	K	L	M



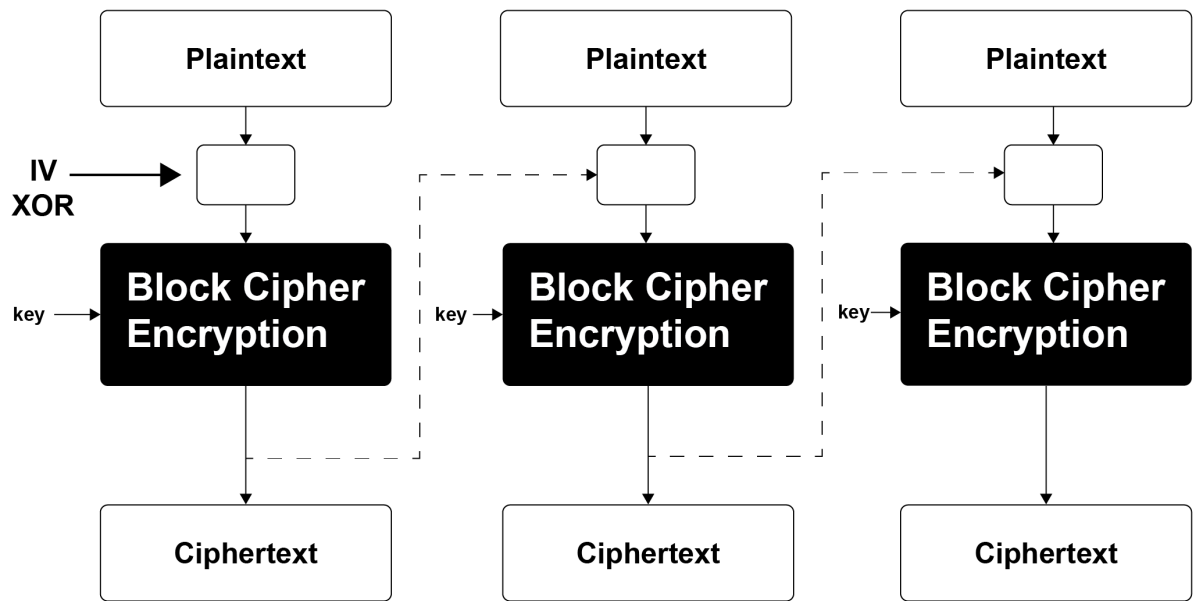


IKE



L2TP/IPSec	
AH	ESP
SHA 1	DES 3DES
MD5	AES

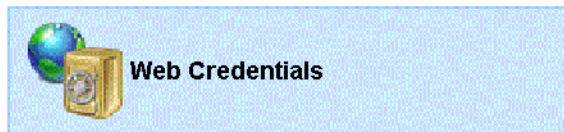
	T	R	E	A	D
XOR (Original Input)	01010100	01110010	01100101	01100001	01100100
Key	01101000	01100101	01101100	01101100	01101111
Output	00111100	00010111	00001001	00001101	00001011



Chapter 3: Investigating Identity and Access Management

Manage your credentials

View and delete your saved log-on information for websites, connected applications and networks.



Windows Credentials

Web Passwords

<http://www.ianneil501.com/>

ianneil55@hotmail.com



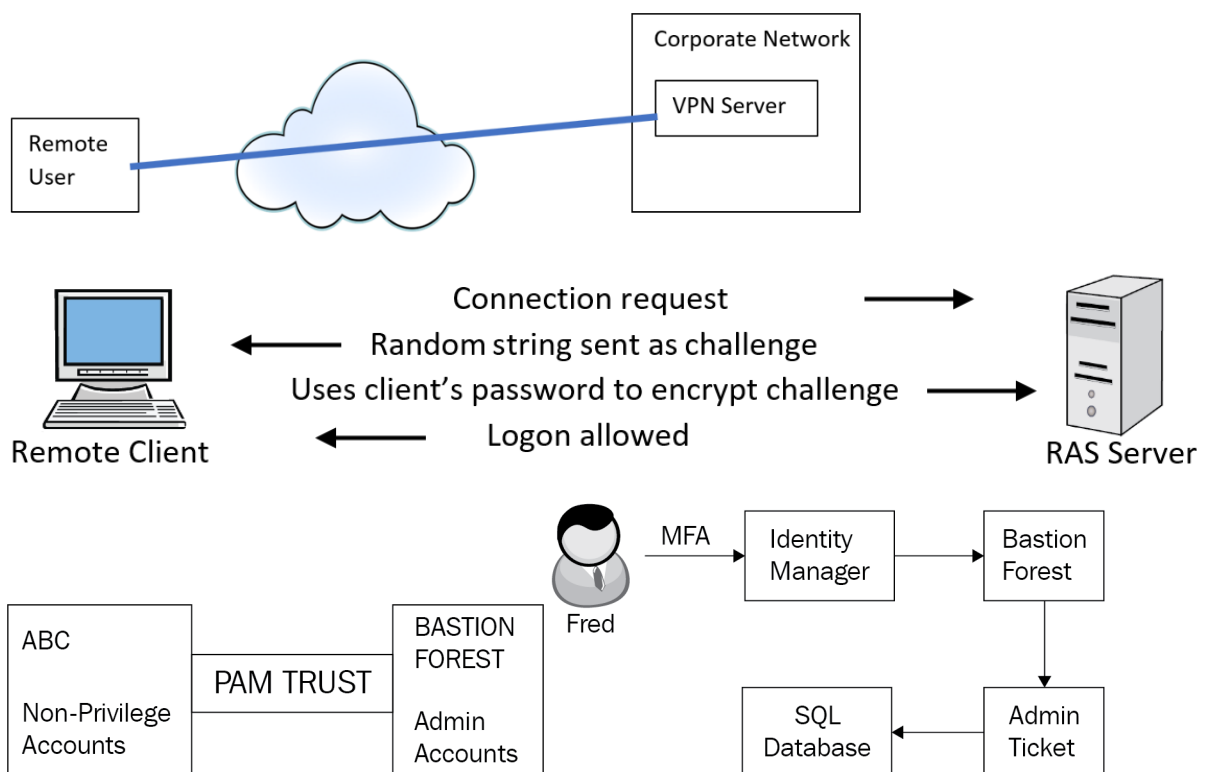
<https://authorportal.packtpub.com/>

neili

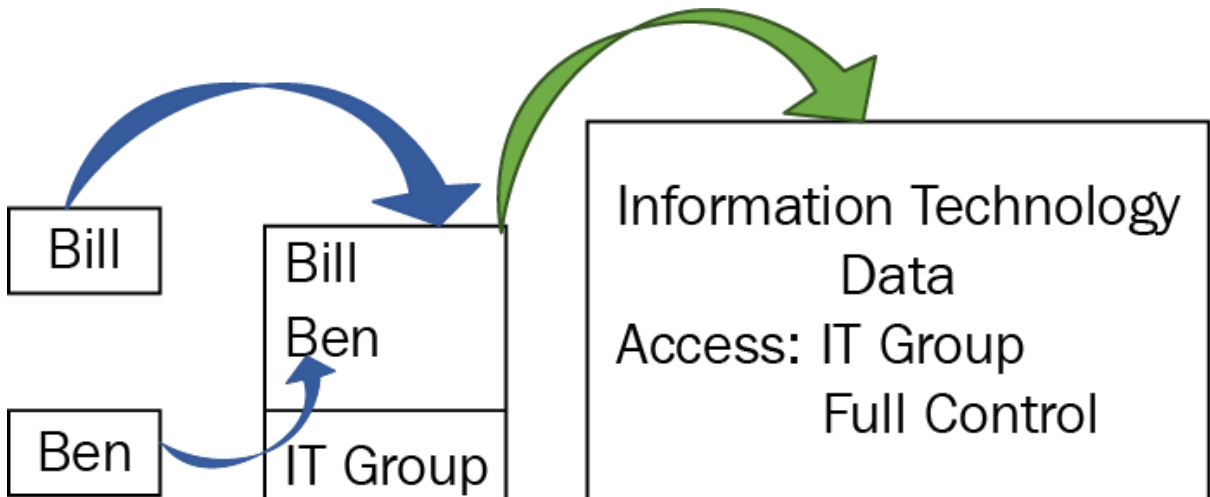
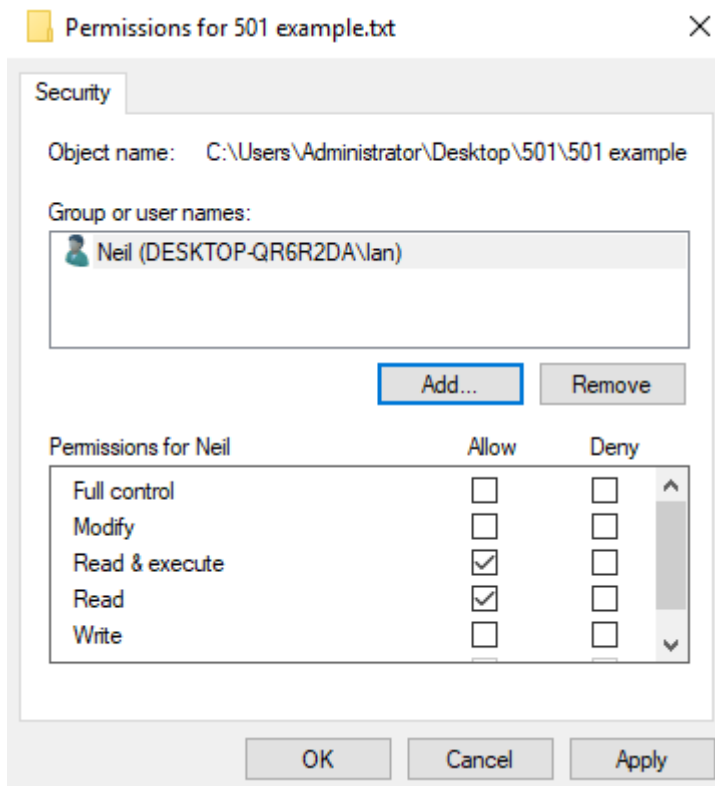


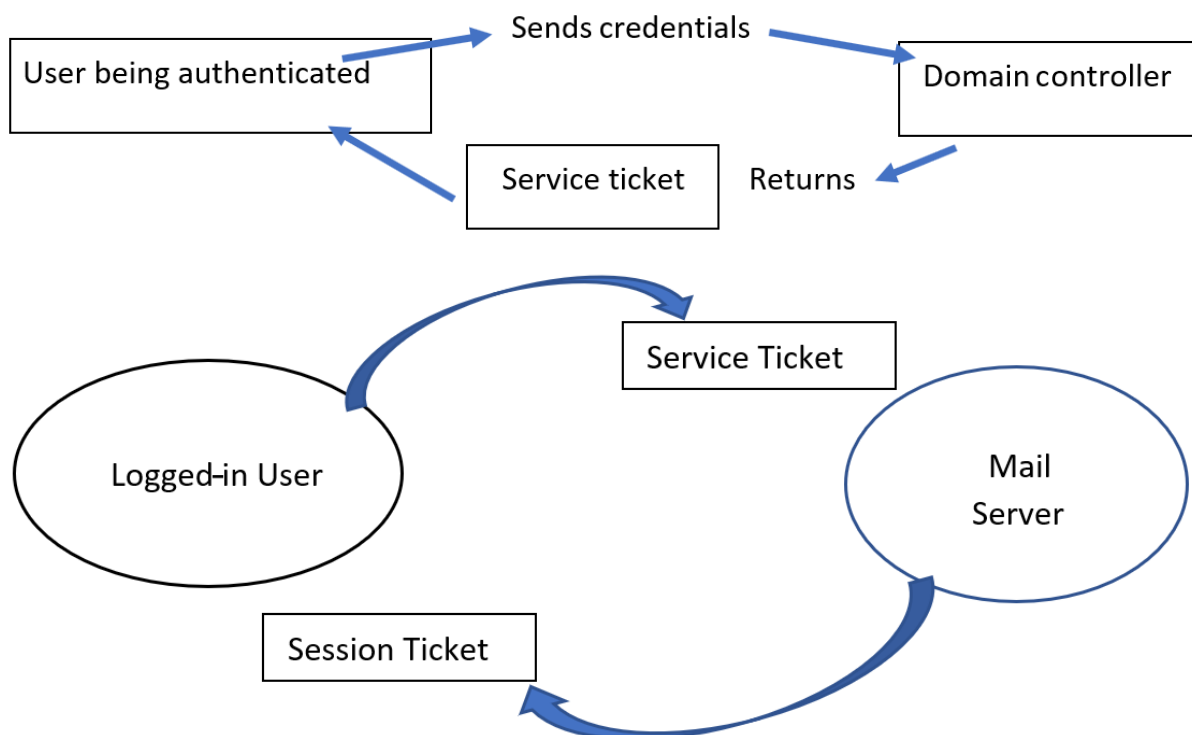
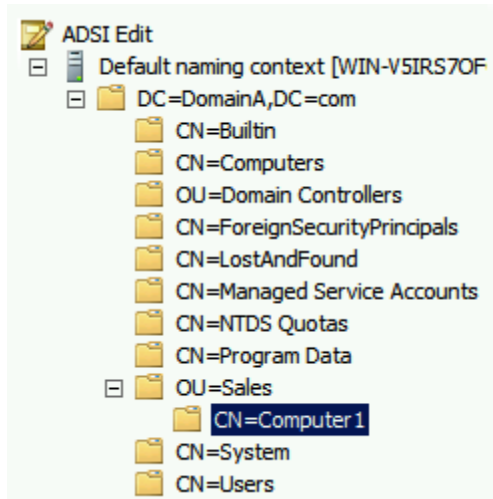
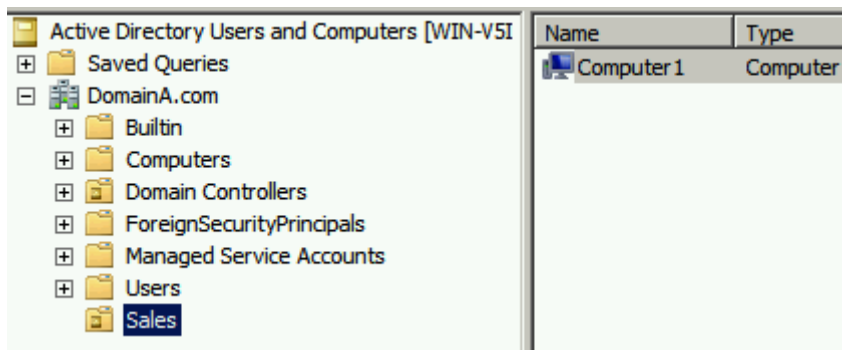
165323

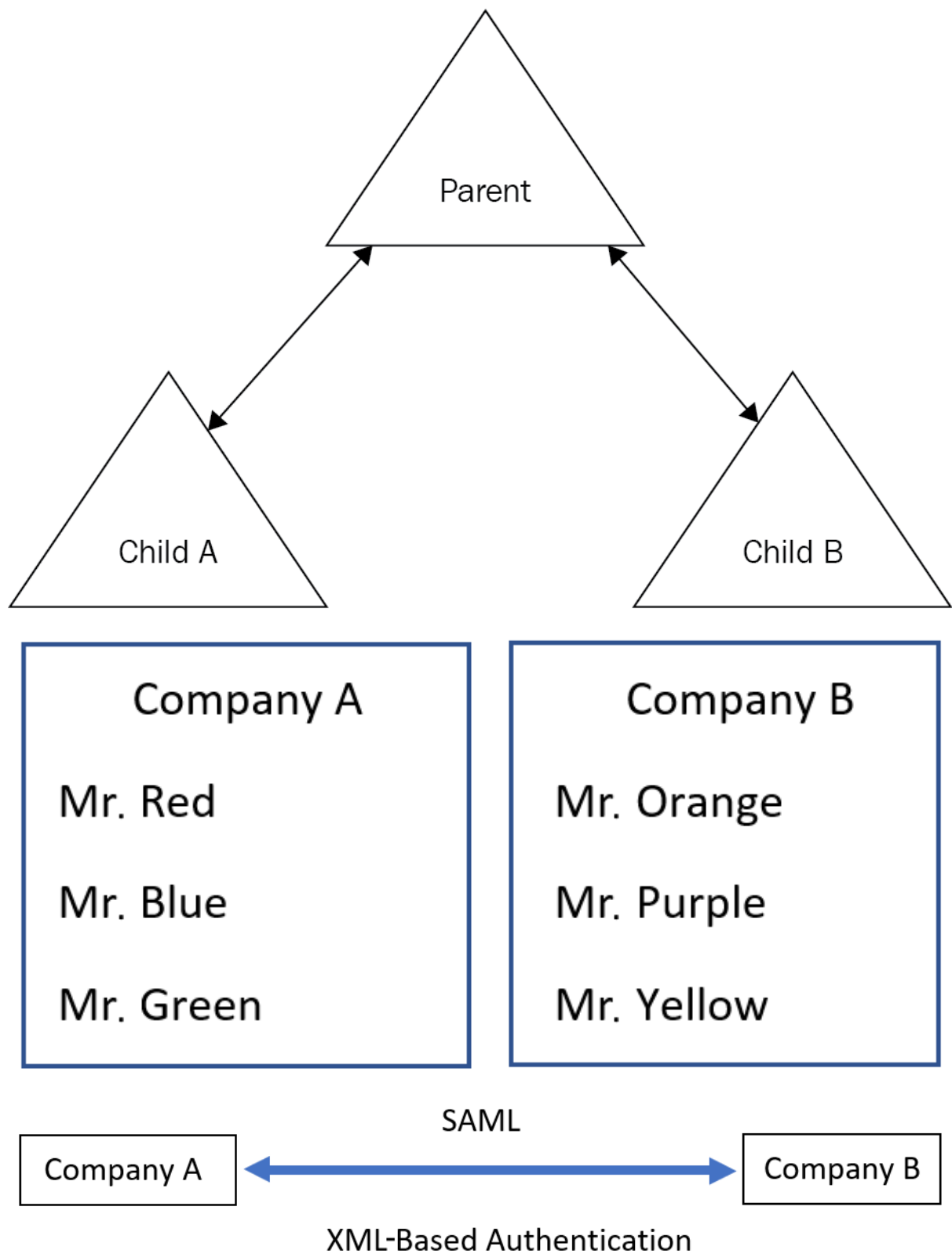
Use with 30 seconds

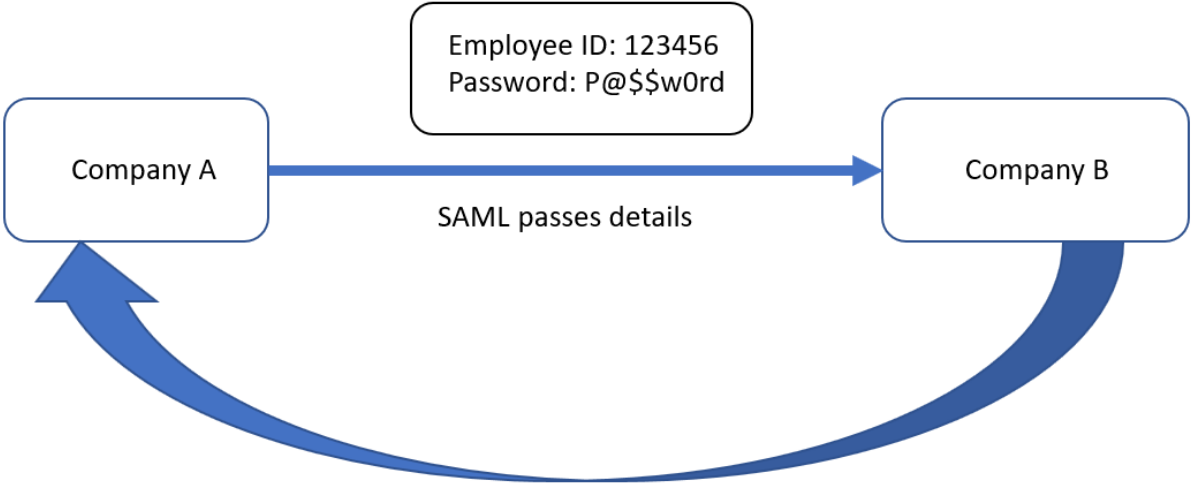
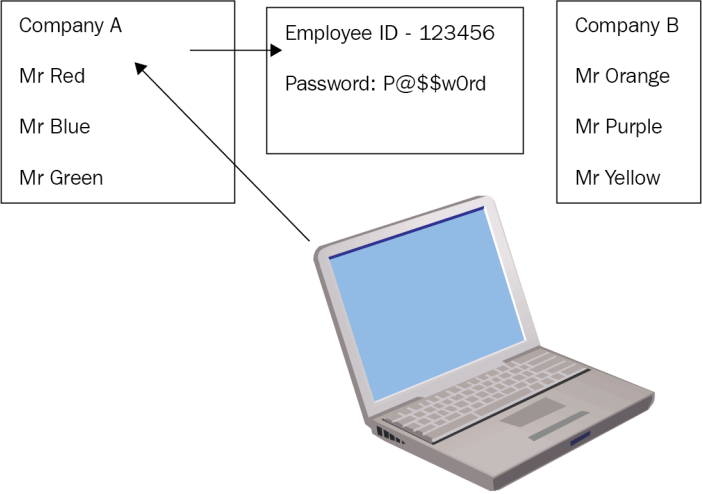


Data types	Classification
Nuclear energy project	Top secret
Research and development	Secret
Ongoing legal issues	Confidential
Government payroll	Restricted











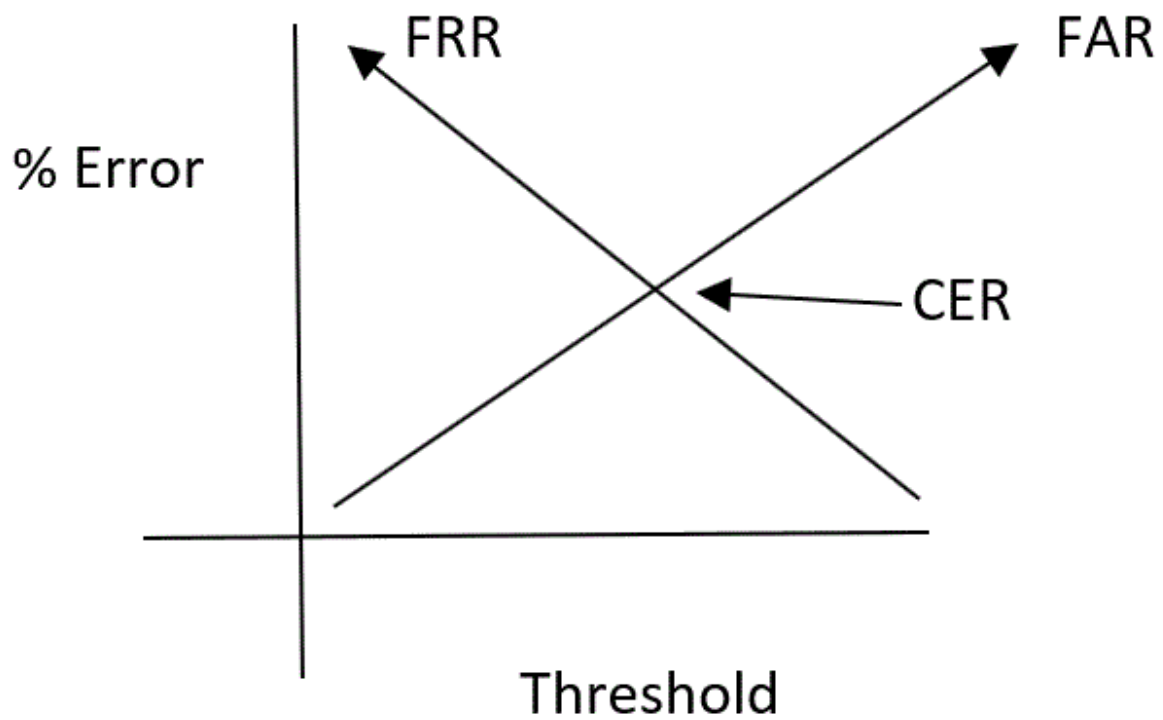
9:41 AM

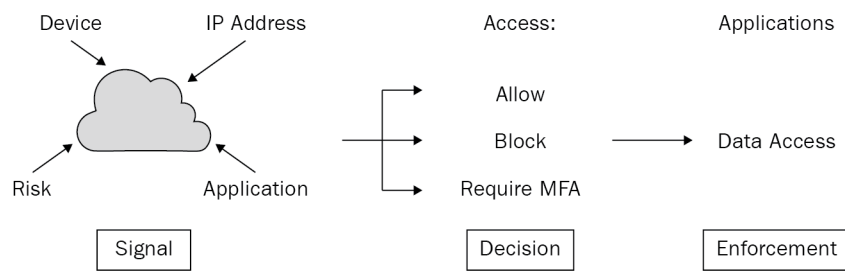
100%

[Cancel](#)

Place Your Finger

Lift and rest your finger on the Home button repeatedly.





Ian Neil Properties

Member Of

Dial-in

Environment

Sessions

Remote control

Remote Desktop Services Profile

COM+

General

Address

Account

Profile

Telephones

Organization

User logon name:

ianneil

@Adatum.com

User logon name (pre-Windows 2000):

ADATUM\

ianneil

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, January 13, 2021

OK

Cancel

Apply

Help

Logon Hours for Ian Neil

12 • 2 • 4 • 6 • 8 • 10 • 12 • 2 • 4 • 6 • 8 • 10 • 12

OK

Cancel

All	12	2	4	6	8	10	12	2	4	6	8	10	12
Sunday													
Monday													
Tuesday													
Wednesday													
Thursday													
Friday													
Saturday													

☒ Logon Permitted
☐ Logon Denied

Monday through Friday from 7:00 AM to 6:00 PM

Policy

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirements
- Store passwords using reversible encryption

Security Setting

- 24 passwords remember
- 42 days
- 0 days
- 0 characters
- Disabled
- Disabled

Policy

- Account lockout duration
- Account lockout threshold
- Reset account lockout counter after

Security Setting

- 30 minutes
- 3 invalid logon attempts
- 30 minutes

Chapter 4: Exploring Virtualization and Cloud Concepts

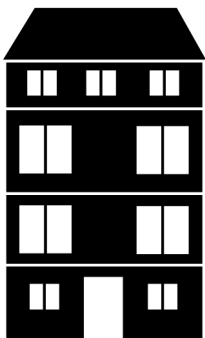
Server 2016	Off
Windows 10	Off

Checkpoints

Automatic Checkpoint - Server 2008 - (17/06/2018 - 11:57:42)

Server 2016 - (09/07/2018 - 08:31:19)

Now









Community Cloud 1

Community Cloud 2



← CASB

Example pricing for popular products

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



	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



1 year £7.90 user/month

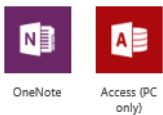
Office 365 Business

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



Services included



OneDrive

1 year £9.40 user/month

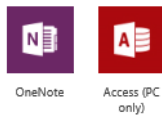
Office 365 Business Premium

Buy now

Price does not include VAT.

Best for businesses that need business email, Office applications, and other business services.

Office applications included



Services included



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



Microsoft Teams

← Back to Applications



Google Apps

Active View Logs

General Sign On Mobile Import Assignments

Settings

Edit

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.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State



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.

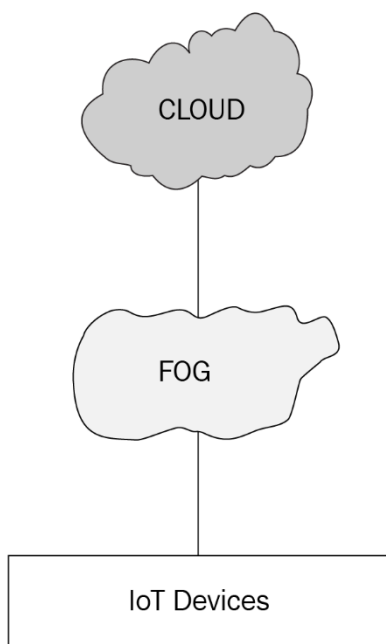
About

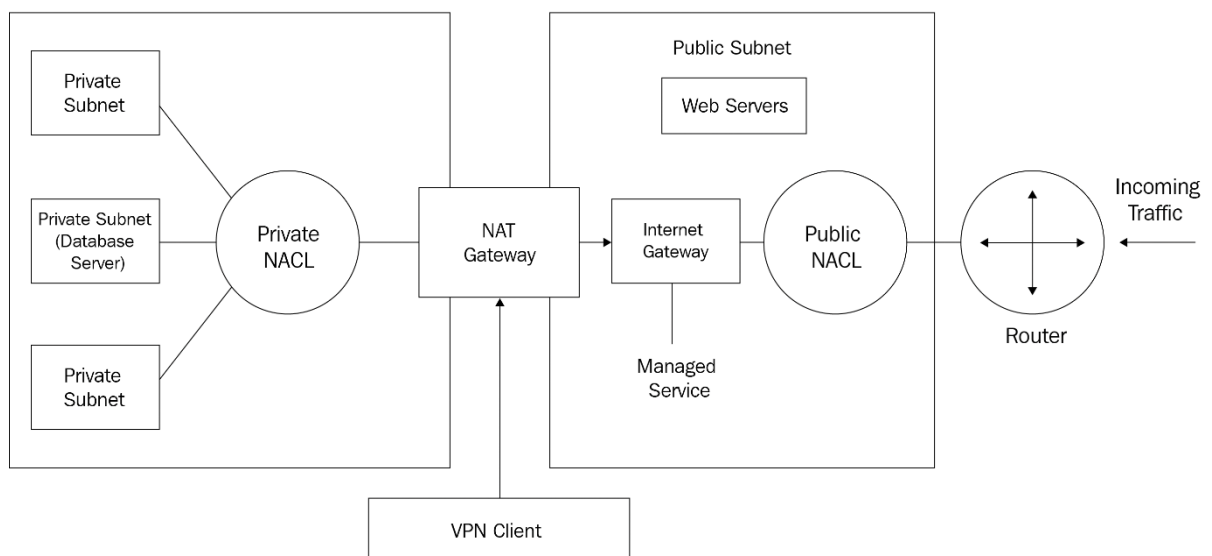
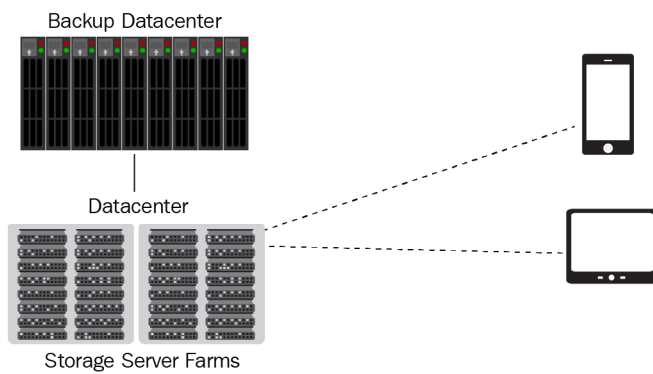
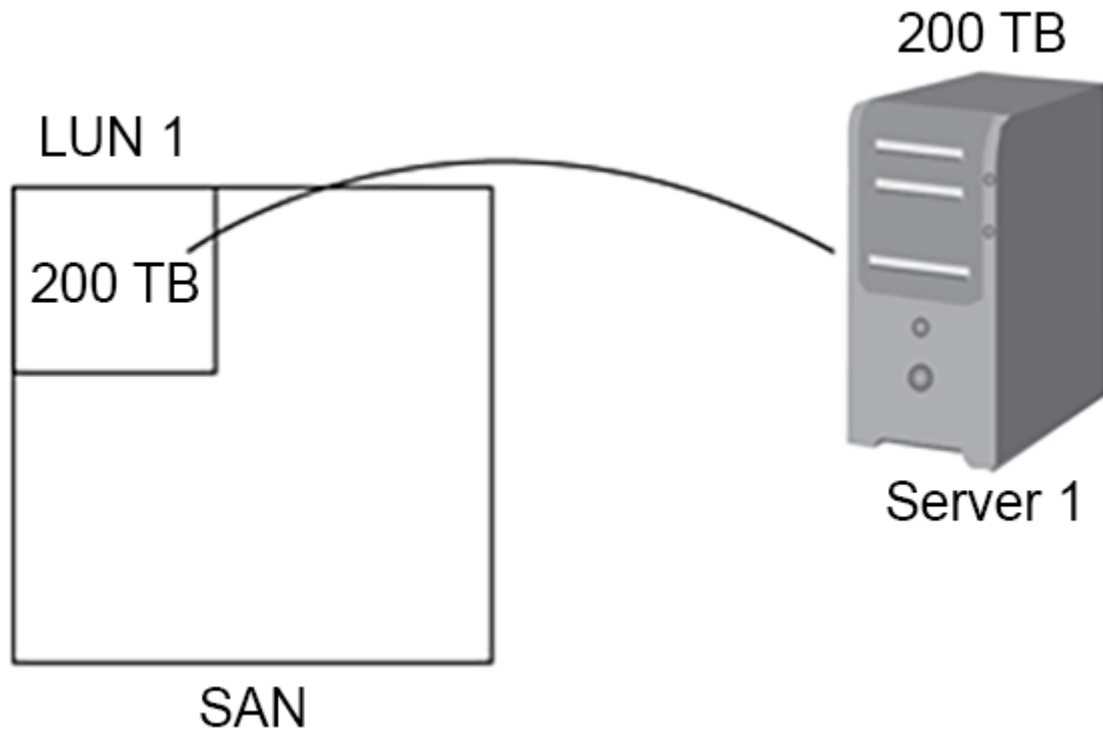
SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

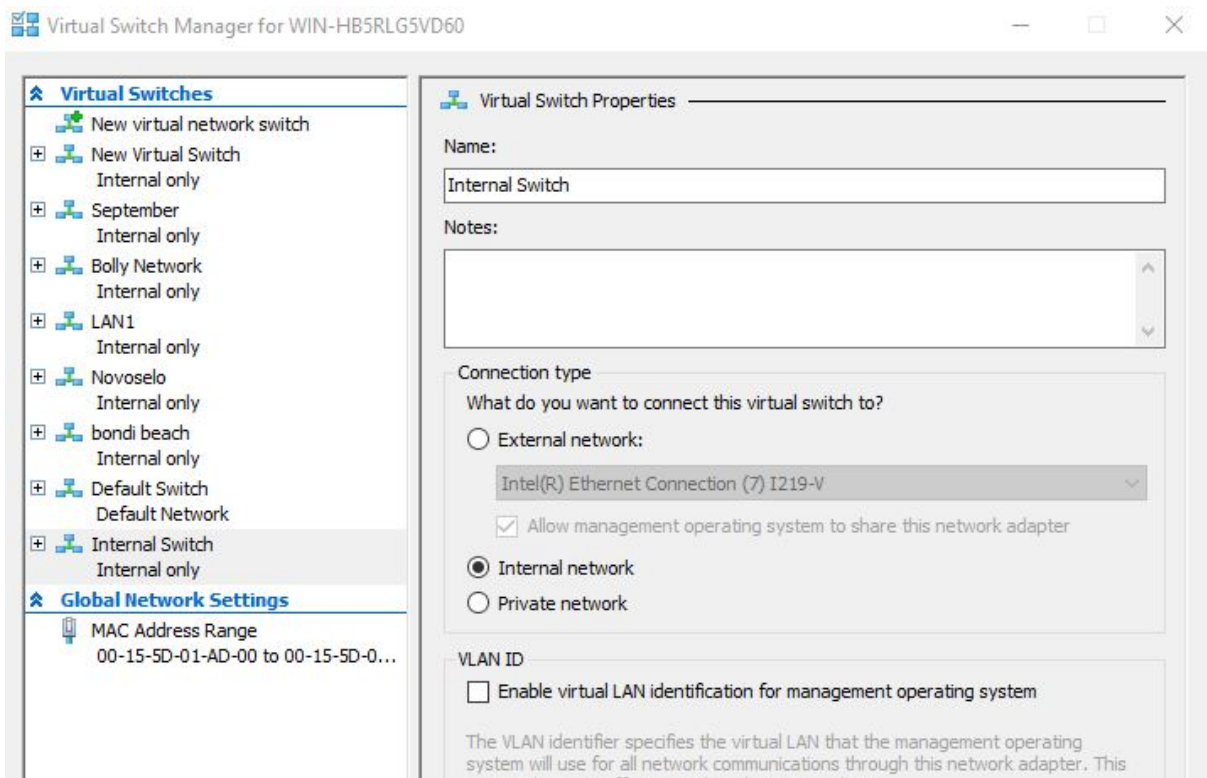
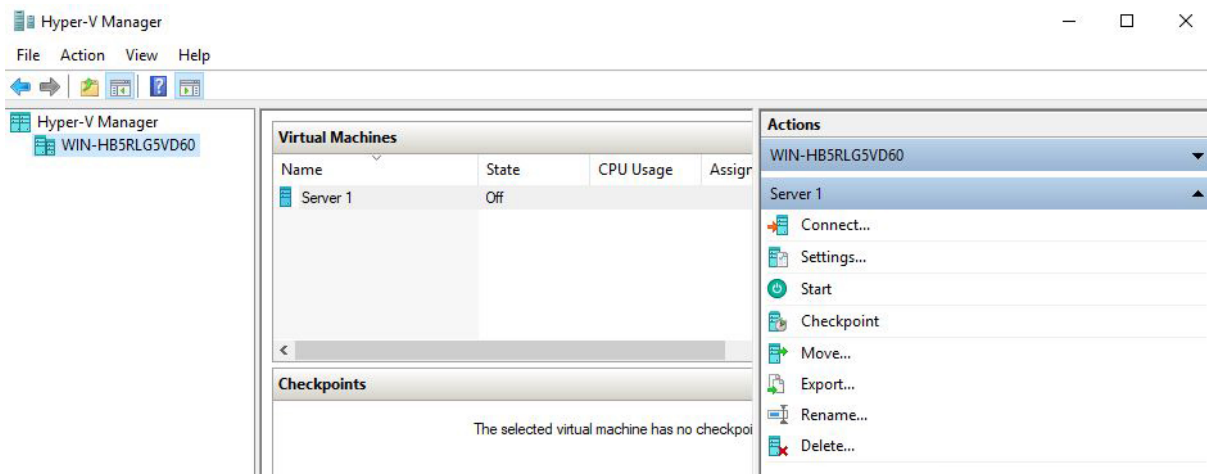
Application Username

Choose a format to use as the default username value when assigning the application to users.

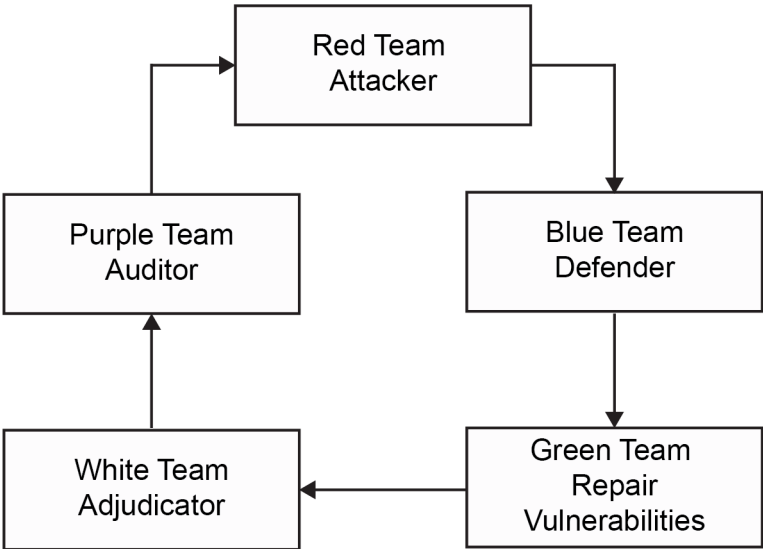
If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.



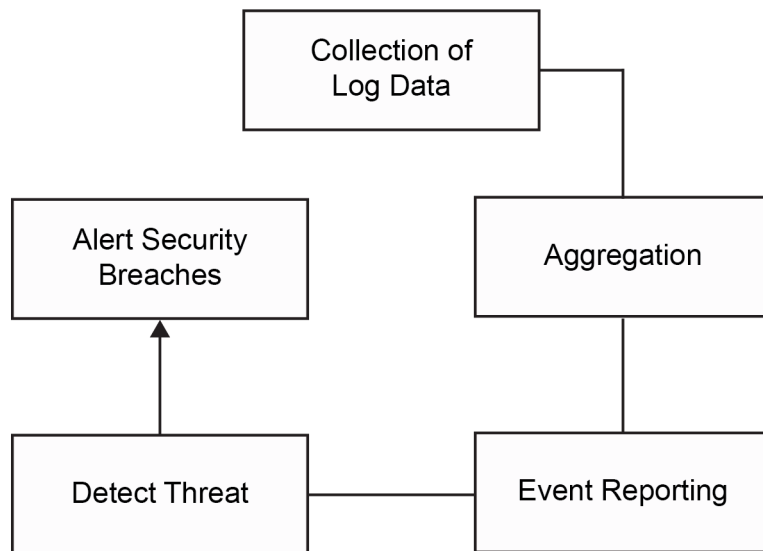




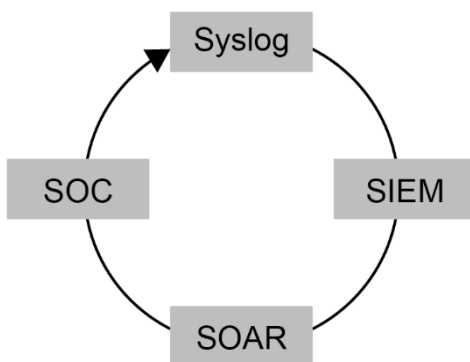
Chapter 5: Monitoring, Scanning, and Penetration Testing



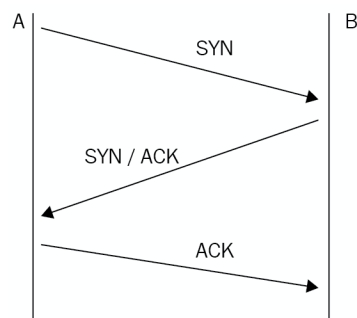
Score	Rating
Critical	9.0-10.0
High	7.0-8.9
Medium	4.0-6.9
Low	0.1-3.9



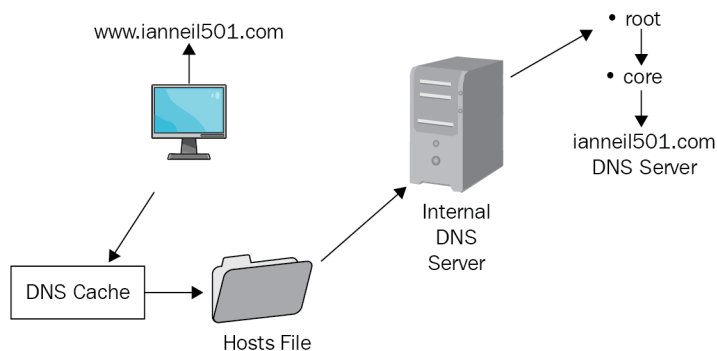
Intrusion detection systems	Desktop events
Firewall logs	Server events
Network packets	Antivirus events
Application servers	Database logs
Switches logs	Router logs



Chapter 6: Understanding Secure and Insecure Protocols

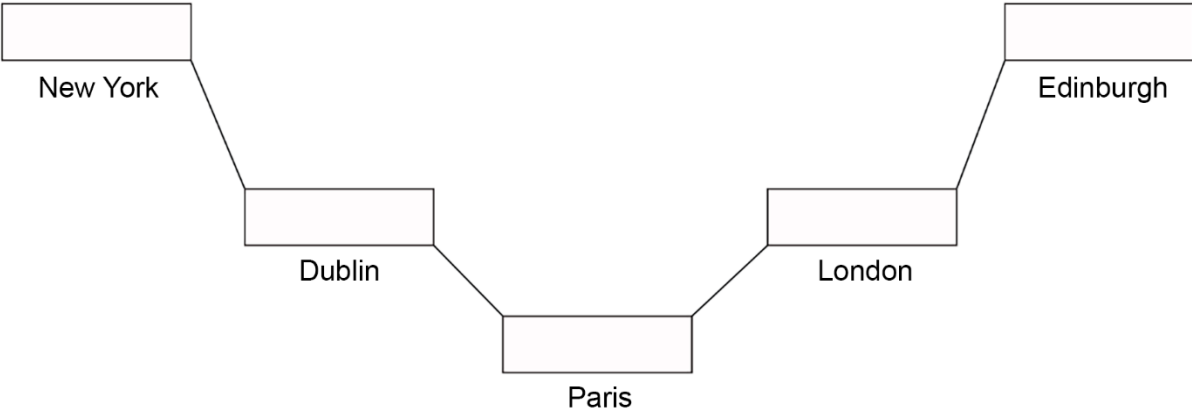


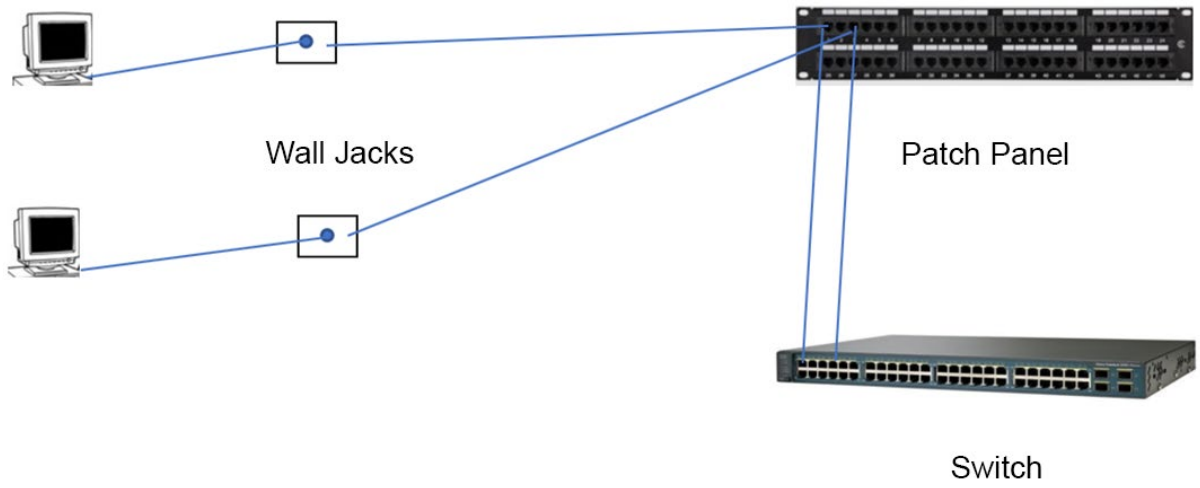
Insecure Protocols			
Protocol	UDP	Port	Use Case
File Transfer Protocol (FTP)		21	File transfer – passive FTP
Telnet		23	Run commands on remote hosts
Simple Mail Transport Protocol (SMTP)		25	Transport mail between Mail Servers
Domain Name System (DNS)	UDP	53	Host name resolution
		53	Zone transfer
	UDP	53	Name queries
Dynamic Host Configuration Protocol (DHCP)	UDP	67/68	Automatic IP address allocation
Trivial File Transfer Protocol (TFTP)	UDP	69	File transfer using UDP
Hypertext Transport Protocol (HTTP)		80	Web browser
Post Office Protocol 3		110	Pull mail from mail server, no copy left on mail server
Network Time Protocol (NTP)		123	Time synchronization
NETBIOS	UDP	137-139	NETBIOS to IP address resolution
Internet Message Access Protocol (IMAP 4)		143	Pulls mail from mail server
Simple Network Management Protocol (SNMP)	UDP	161	Notifies the status and creates reports on network devices
Lightweight Directory Access Protocol (LDAP)		389	Stores X500 objects, searches Directory services for users and groups and other information



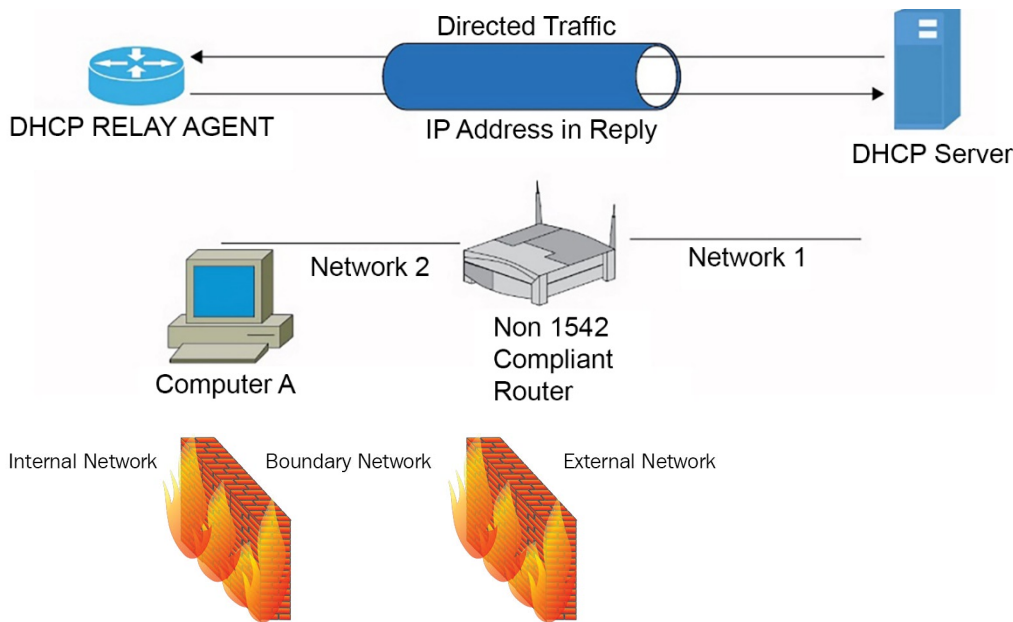
Secure Protocols			
Protocol	UDP	Port	Use Cases
Secure Shell (SSH)		22	Secure remote access
Secure Copy Protocol (SCP)		22	Secure copy to UNIX/LINUX
SSH File Transfer Protocol (SFTP)		22	Secure FTP download
DNSSEC	TCP/UDP	53	Secure DNS Traffic
Kerberos		88	Secure authentication
Simple Network Management Protocol Version 3 (SNMP v3)	UDP	162	Secure status and reports of network devices
Lightweight Directory Access Protocol Secure (LDAPS)		636	Manages directory service information securely
Hypertext Transport Protocol Secure (HTTPS)		443	Secure Web Browser
Transport Layer Security (TLS)/Secure Socket Layer (SSL)		443	Secure Data in Transit
Internet Protocol Security (IPSec)	UDP	500	Secure session for VPN or between two hosts
Secure Simple Mail Transfer Protocol (SMTPS)		587	Secure SMTP
Secure Internet Message Access Protocol (IMAP4)		993	Secure IMAP4
Secure Post Office Protocol 3		995	Secure POP3
Secure/Multipurpose Internet Mail Extensions (S/MIME)		993	Encrypt or digitally sign email
File Transfer Protocol Secure (FTPS)		989/990	Download large files securely
Remote Desktop Protocol (RDP)		3389	Microsoft remote access
Session Initiated Protocol (SIP)		5060/61	Connects internet-based calls
Secure Real Time Protocol (SRTP)		5061	Secure voice traffic

Authenticated Header (AH)	Encapsulated Security Payload (ESP)
SHA 1 MD5	DES – 56 bit 3DES – 168 bit AES – 256 bit





Chapter 7: Delving into Network and Security Concepts



Windows Defender Firewall with Advanced Security

File Action View Help

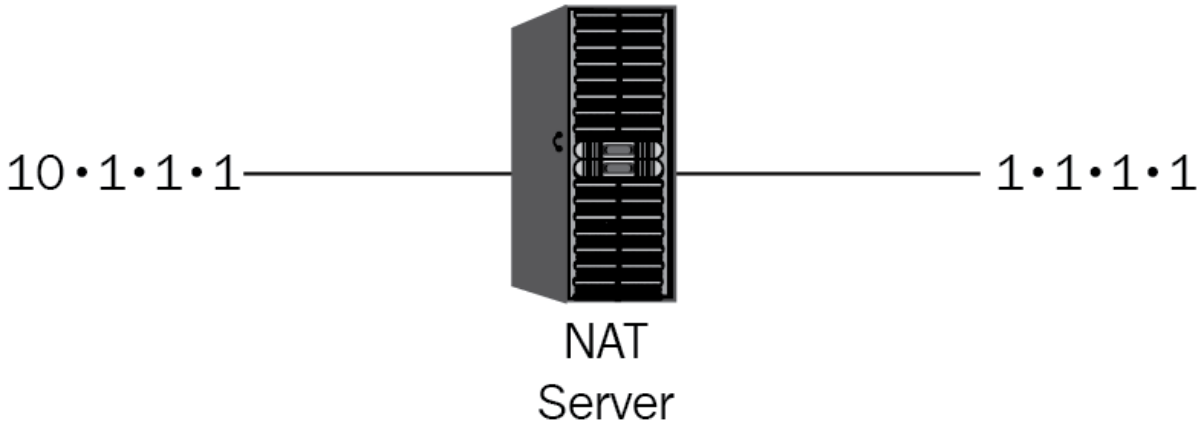
Windows Defender Firewall with Advanced Security on Local Computer

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Name	Group	Profile	Enabled
@{AdobeSystemsIncorporated.AdobePh...	@{AdobeSystemsIncorporat...	All	Yes
@{Microsoft.AAD.BrokerPlugin_1000.162...	@{Microsoft.AAD.BrokerPlu...	All	Yes
@{Microsoft.AccountsControl_10.0.1629...	@{Microsoft.AccountsContr...	All	Yes
@{Microsoft.BingNews_4.22.3254.0_x64_...	@{Microsoft.BingNews_4.22...	All	Yes

Services (Local)

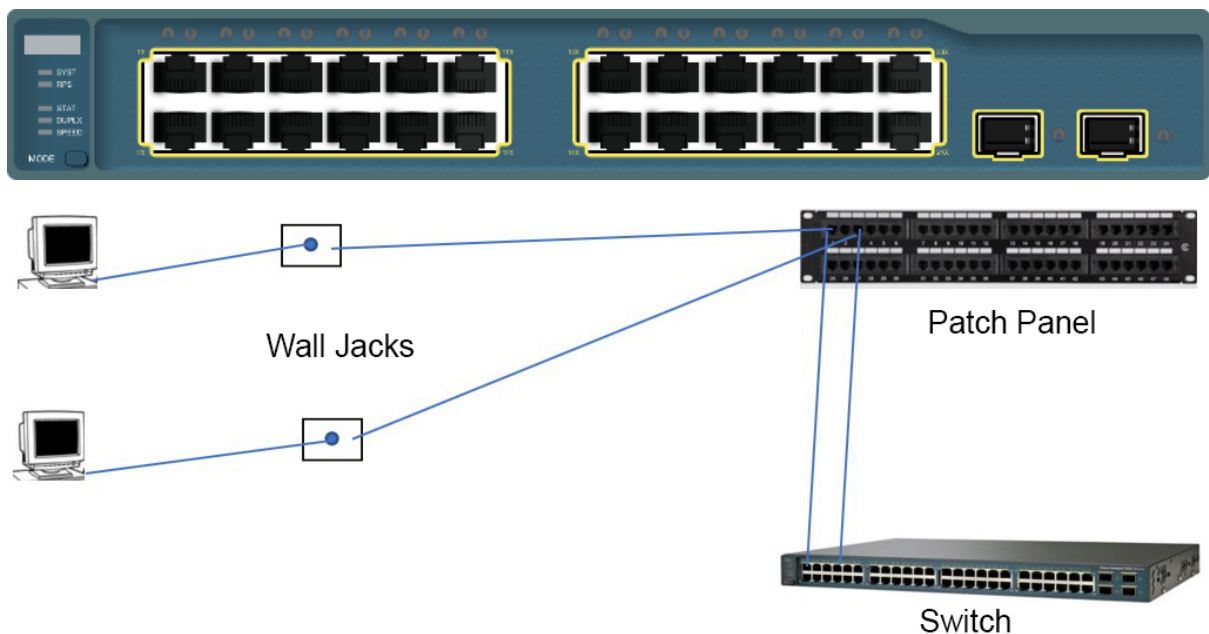
Name	Description	Status	Startup Type	Log On As
Windows Biometric Service	The Windo...		Manual (Trig...	Local Syste
Windows Camera Frame Server	Enables mul...		Manual (Trig...	Local Service
Windows Connect Now - Config ...	WCNCSVC ...		Manual	Local Service
Windows Connection Manager	Makes auto...	Running	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, so the last rule therefore applied



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.

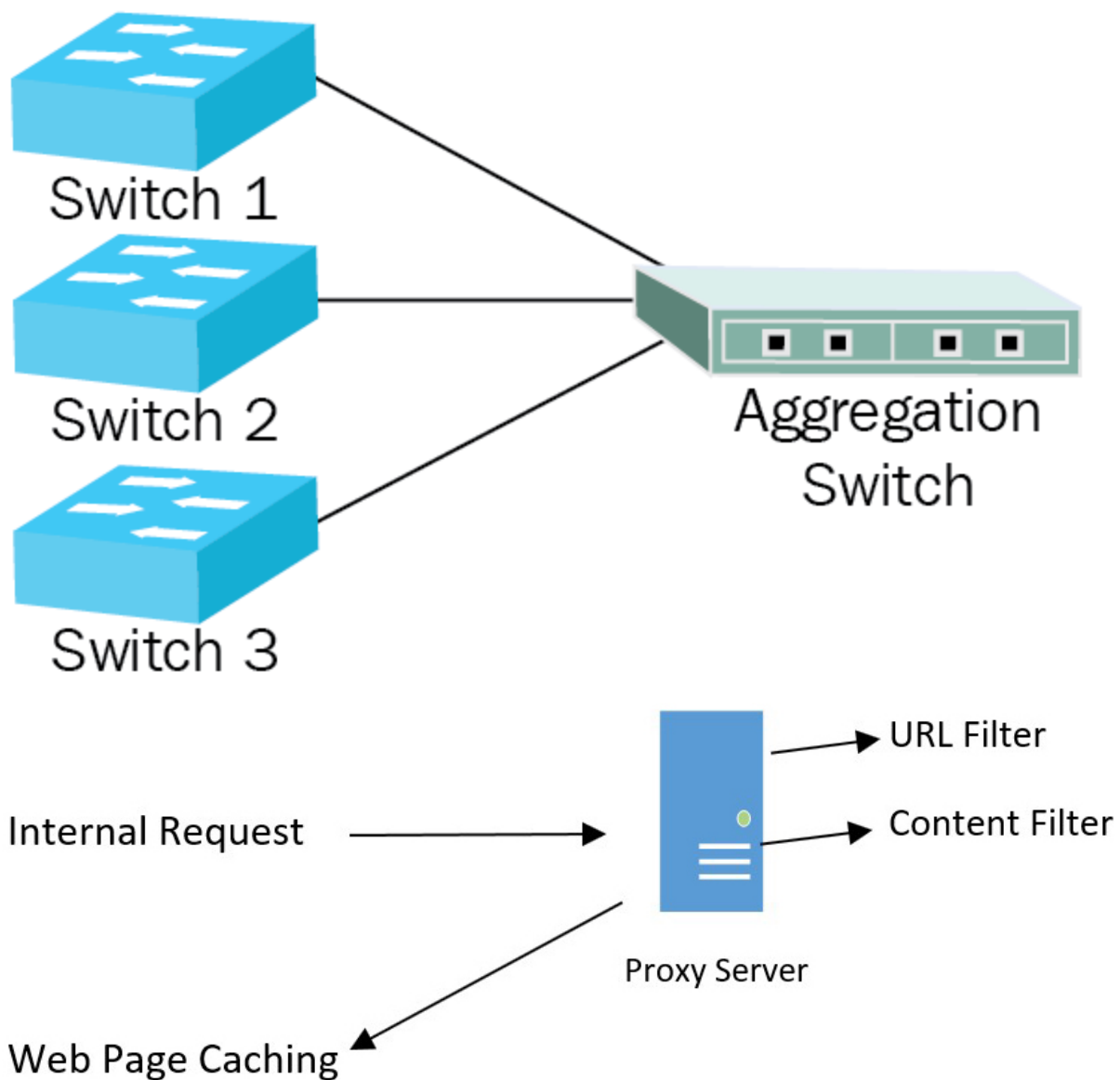
Note: Use the PC Privileges feature on the Firewall page to restrict individual PCs access to the Internet.

Authorised Wireless PCs

delete 00-04-75-CC-3A-4B

Help

New

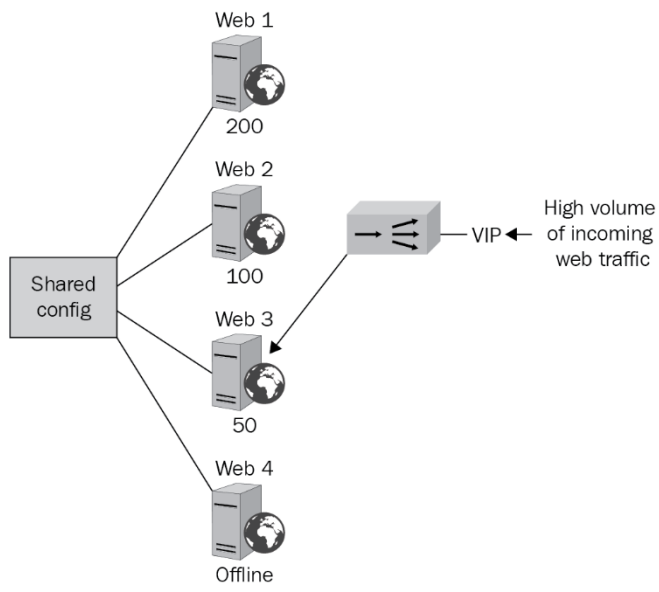


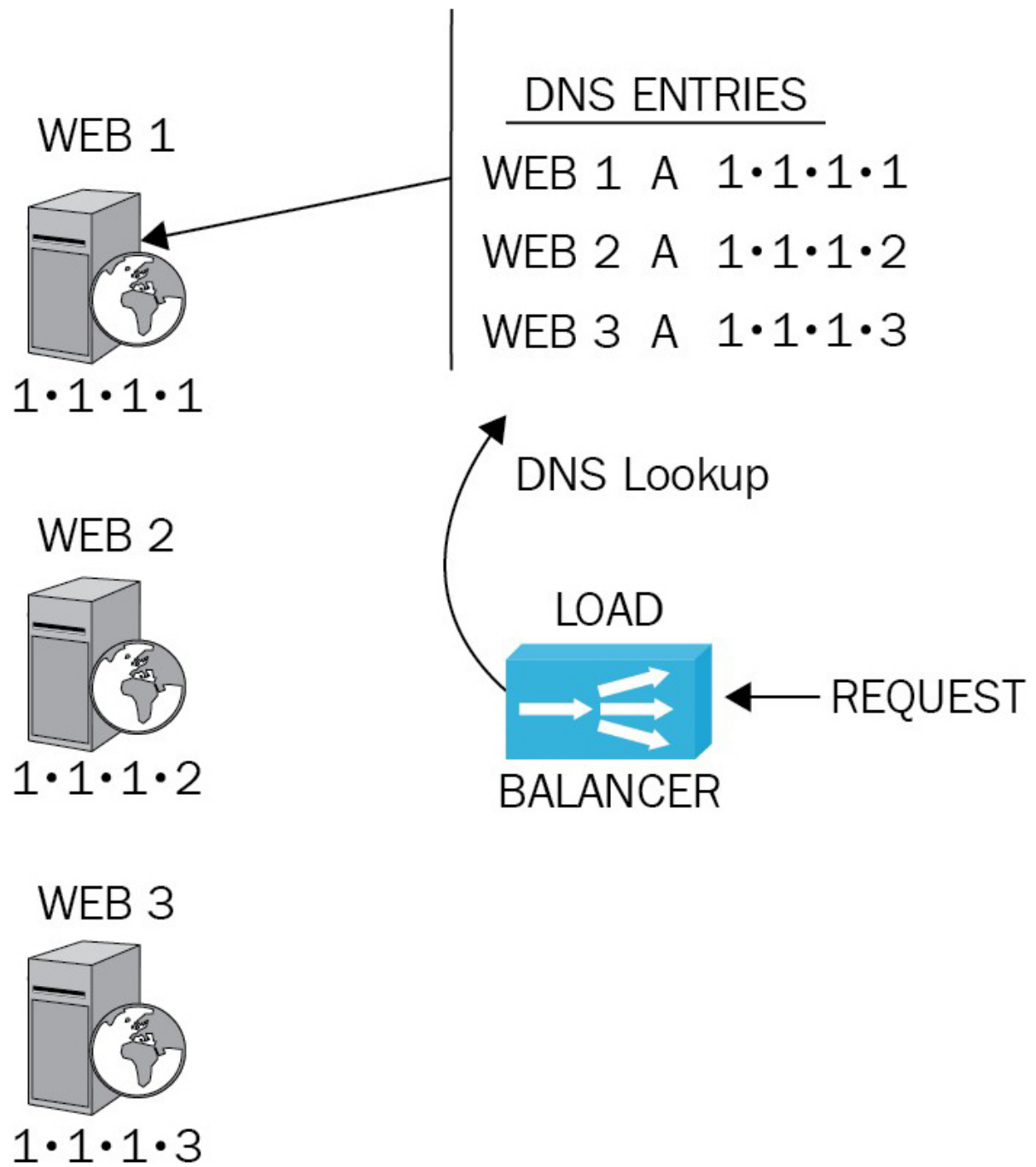
Transparent Proxy

Transparent HTTP Proxy ☒ Enable transport mode to forward all requests for destination Port 80 to the proxy server.

Transparent proxy mode works without an additional configuration being necessary on clients.

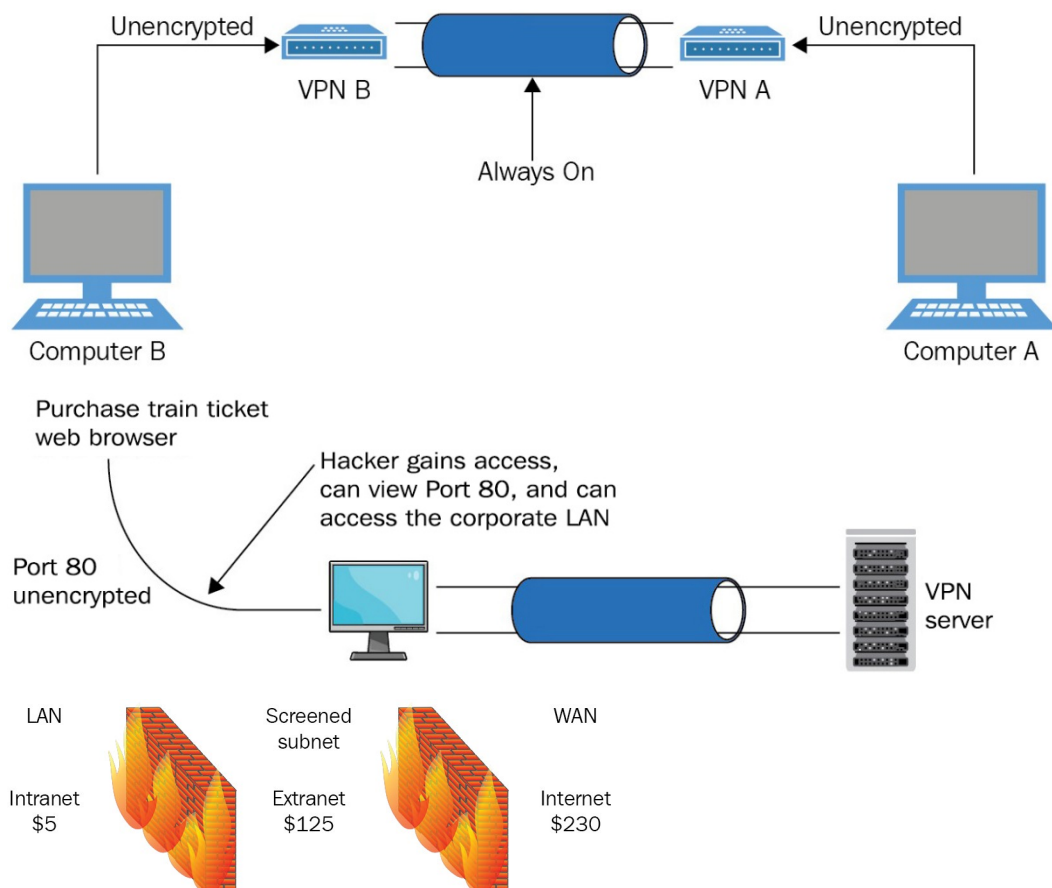
Address		
Proxy server		
<input checked="" type="checkbox"/> Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).		
Address:	192.168.2.2	Port: 8080
		Advanced
<input type="checkbox"/> Bypass proxy server for local addresses		
OK		Cancel

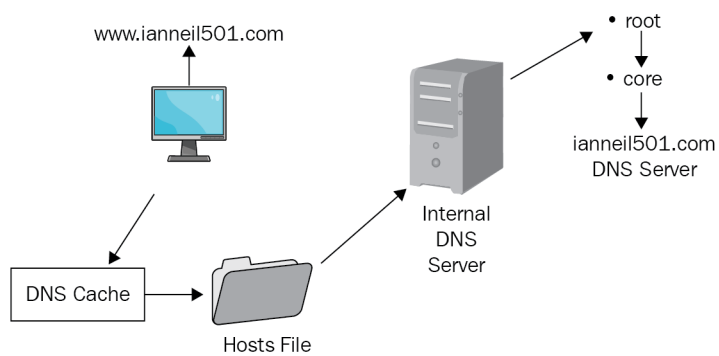
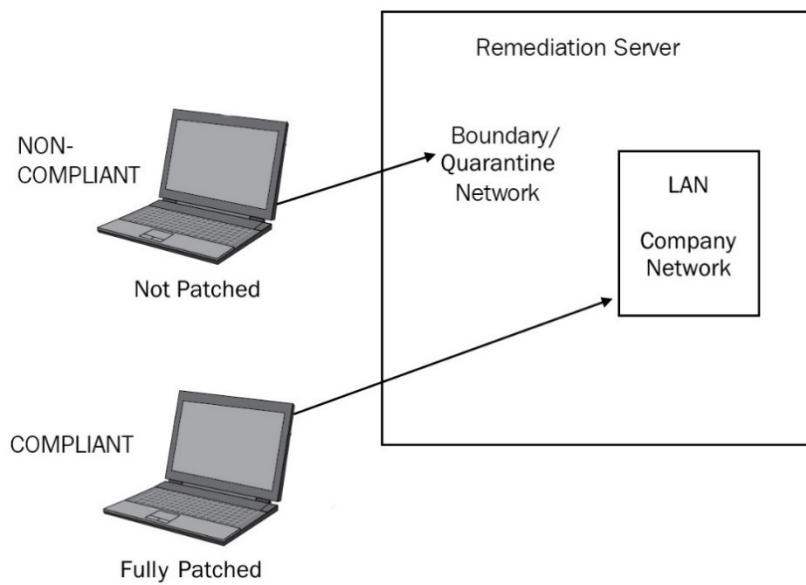
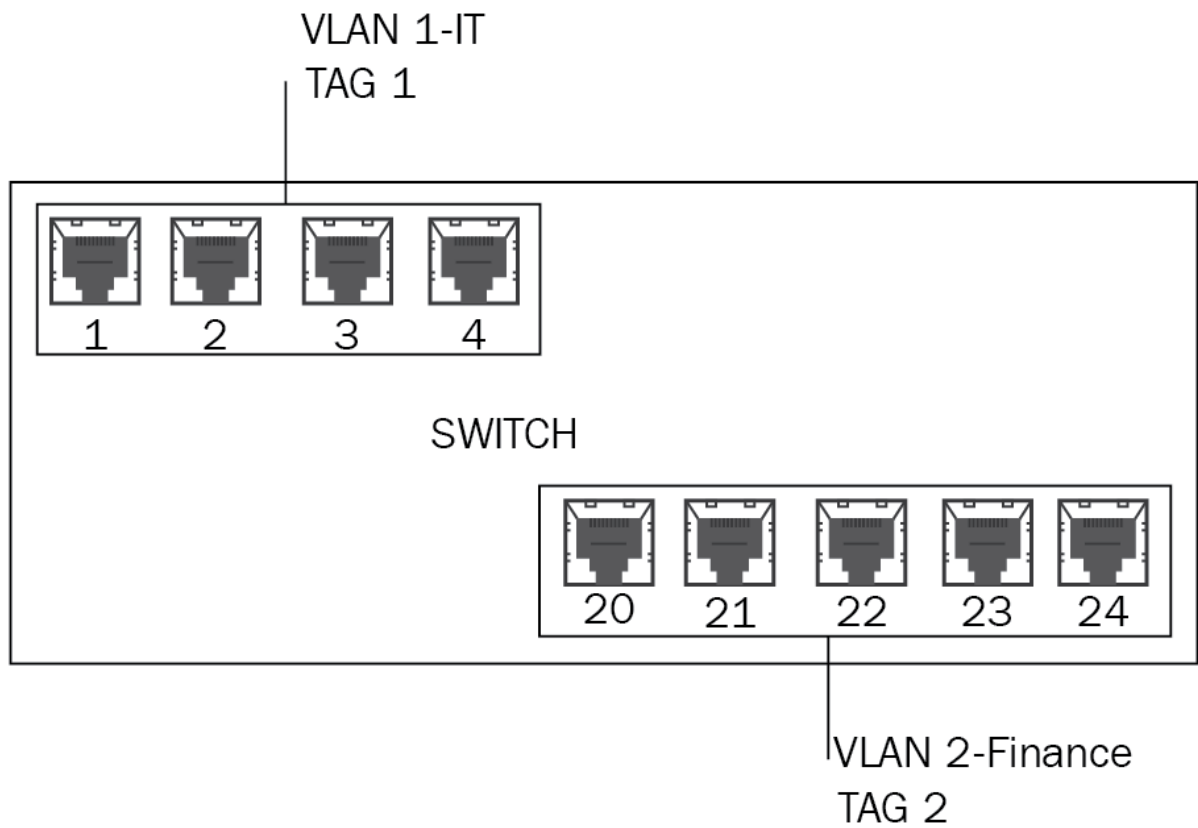


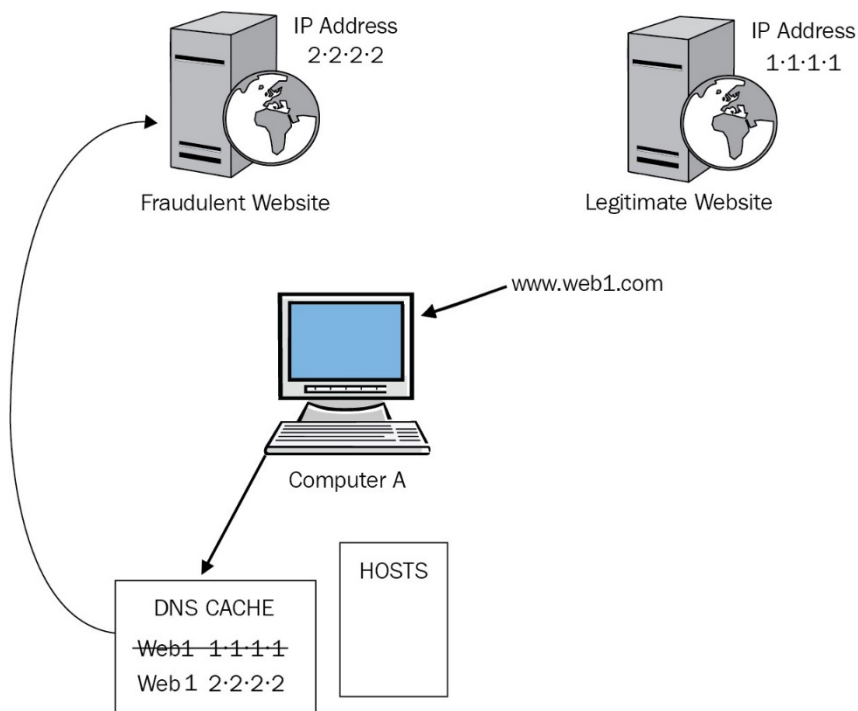




Key Exchange (UDP Port 500)







```
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=41ms TTL=47
Reply from 46.30.213.45: bytes=32 time=46ms TTL=47
```

```
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.telial.net [213.248.84.25]
  8  30 ms     27 ms     26 ms     ldn-bb4-link.telial.net [62.115.143.26]
  9  42 ms     41 ms     37 ms     hbg-bb4-link.telial.net [62.115.122.160]
 10  46 ms     42 ms     49 ms     kbn-bb4-link.telial.net [213.155.135.121]
 11  53 ms     52 ms     45 ms     kbn-b3-link.telial.net [62.115.114.69]
 12  43 ms     43 ms     43 ms     onecom-ic-307407-kbn-horsk-i1.c.telial.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]
```

```
0  WIN-HB5RLG5VD60.Domain.local [100.120.39.46]
1  100.120.39.1
2  r-1-43-234-77.ff.avast.com [77.234.43.1]
3  10.27.0.18
4  border4.ae15.avast-30.lon007.pnap.net [212.118.253.133]
5  core3.tge0-3-0-3-bbnet2.lon003.pnap.net [212.118.240.102]
6  107.6.86.150
7  173.231.129.66
8  195.66.226.81
9  a184-28-198-144.deploy.static.akamaitechnologies.com [184.28.198.144]

Computing statistics for 225 seconds...
      Source to Here   This Node/Link
Hop  RTT   Lost/Sent = Pct  Lost/Sent = Pct  Address
  0
    |
  1  21ms    0/ 100 = 0%      0/ 100 = 0%      100.120.39.1
    |
  2  23ms    0/ 100 = 0%      0/ 100 = 0%      r-1-43-234-77.ff.avast.com [77.234.43.1]
    |
  3  ---    100/ 100 =100%  100/ 100 =100%  10.27.0.18
    |
  4  ---    100/ 100 =100%  100/ 100 =100%  border4.ae15.avast-30.lon007.pnap.net [212.118.253.133]
    |
  5  23ms    0/ 100 = 0%      0/ 100 = 0%      core3.tge0-3-0-3-bbnet2.lon003.pnap.net [212.118.240.102]
    |
  6  23ms    0/ 100 = 0%      0/ 100 = 0%      107.6.86.150
    |
  7  ---    100/ 100 =100%  100/ 100 =100%  173.231.129.66
    |
  8  ---    100/ 100 =100%  100/ 100 =100%  195.66.226.81
    |
  9  23ms    0/ 100 = 0%      0/ 100 = 0%      a184-28-198-144.deploy.static.akamaitechnologies.com [184.28.198.144]
```

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

Non-authoritative answer:
Name: www.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!
```

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

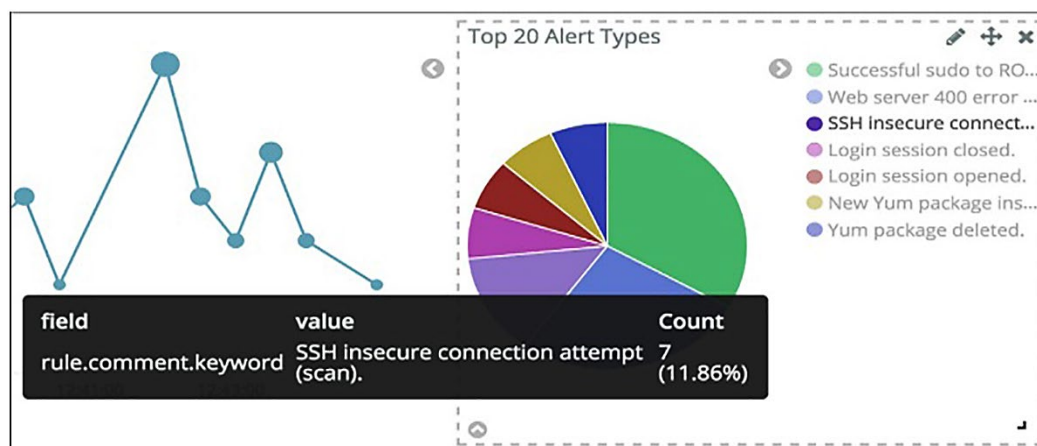
IP Range: 195.80.116.0 to 195.80.116.255

Hostname: e-estonia.com IP↑ /24

IP	Ping	Hostname
195.80.116.226	[n/a]	[n/s]
195.80.116.227	9 ms	[n/a]
195.80.116.228	10 ms	[n/a]
195.80.116.229	9 ms	[n/a]
195.80.116.230	13 ms	mx3.rm.k.ee
195.80.116.231	10 ms	mx4.rm.k.ee
195.80.116.232	[n/a]	[n/s]
195.80.116.233	[n/a]	[n/s]
195.80.116.234	[n/a]	[n/s]
195.80.116.235	9 ms	[n/a]
195.80.116.236	[n/a]	[n/s]

Ready

Display: All



AVG AntiVirus Free

QUARANTINE 4 threats

Threat	Location found	Date found
<input type="checkbox"/> Win32:Rootkit-gen...	C:\Users\Administrato ...F2FE6A5E2E76528A	Apr 12, 2018 11:27 AM
<input type="checkbox"/> Win32:Rootkit-gen...	C:\Users\ADMINI~1\A...Temp\FC4A.tmp.exe	Apr 12, 2018 11:27 AM
<input type="checkbox"/> Win32:Rootkit-gen...	C:\Users\Administrato ...33SLGU0R\2[1].exe	Apr 12, 2018 11:27 AM
<input type="checkbox"/> IDP.Generic	C:\Windows\System32\SIHClient.exe	Jun 13, 2018 11:35 AM

Browser add-ons

```

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.
  
```

*WiFi
 File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-/>
 Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
16329	38.895913	172.20.10.3	151.101.61.181	TCP	60	60 [TCP] Seq=770 Ack=16894 Win=262144 Len=0
16329	38.896457	172.20.10.3	151.101.61.181	TCP	54	54 [ACK] Seq=770 Ack=16894 Win=262144 Len=0
16330	38.896731	151.101.61.181	172.20.10.3	TCP	1416	1416 80 → 63685 [ACK] Seq=16894 Ack=770 Win=31344 Len=1362 [TCP segment of a reassembled PDU]
16331	38.896733	151.101.61.181	172.20.10.3	TCP	226	226 80 → 63685 [PSH, ACK] Seq=18256 Ack=770 Win=31344 Len=172 [TCP segment of a reassembled PDU]
16332	38.896734	151.101.61.181	172.20.10.3	TCP	1416	1416 80 → 63685 [ACK] Seq=18428 Ack=770 Win=31344 Len=1362 [TCP segment of a reassembled PDU]
16333	38.896736	151.101.61.181	172.20.10.3	TCP	1416	1416 80 → 63685 [ACK] Seq=19790 Ack=770 Win=31344 Len=1362 [TCP segment of a reassembled PDU]
16334	38.897079	172.20.10.3	151.101.61.181	TCP	54	54 [ACK] Seq=770 Ack=21152 Win=262144 Len=0
16335	38.838597	151.101.62.2	172.20.10.3	TCP	66	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	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	54 [ACK] Seq=1 Ack=1 Win=262144 Len=0
16338	38.839565	172.20.10.3	151.101.62.2	TCP	54	54 [ACK] Seq=1 Ack=1 Win=262144 Len=0
16339	38.847809	172.20.10.3	151.101.62.2	TCP	1416	1416 [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	660 GET /nfl/trc/3/json?tim=08%3A44%3A10.581&data=78%22id%22%3A140%2C%22i%22%3A%22%2Fnews%2Fstory%2F0ap3000000952209%2Farticle%2Fjosh...
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=78%22id%22%3A140%2C%22i%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

Chapter 8: Securing Wireless and Mobile Solutions

Wireless Settings

Configuration Encryption Connection Control Client List Profile

Enable Wireless Networking

Enable Wireless Networking ☒

Channel Selection

Channel

Service Area Name/SSID

Service Area Name/SSID

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.

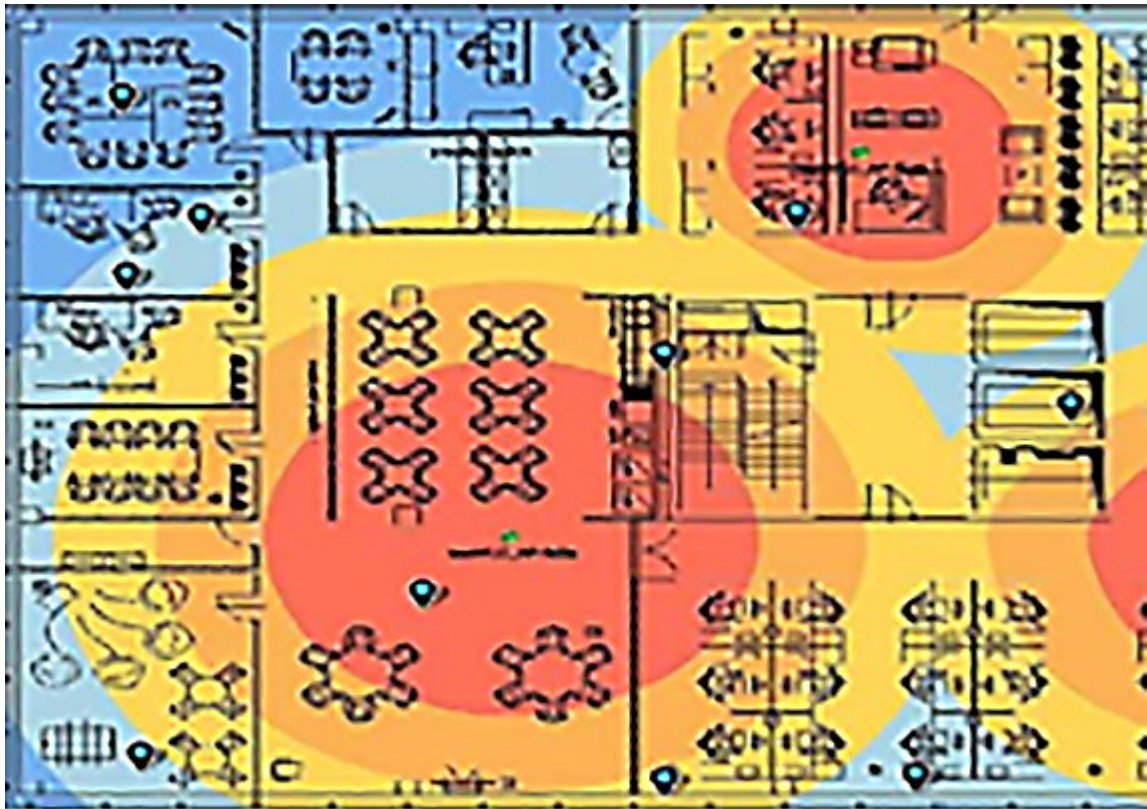
Note: Use the PC Privileges feature on the Firewall page to restrict individual PCs access to the Internet.

Authorised Wireless PCs

delete

Help New

Standard	Frequency	Speed	Remarks
802.11 a	5 GHz	54 Mbps	5 GHz channel bandwidth is 40 MHz
802.11 b	2.4 GHz	11 Mbps	2.4 GHz channel bandwidth is 20 MHz
802.11 g	2.4 GHz	54 Mbps	
802.11 n	2.4 GHz/5 GHz	150 Mbps	MIMO – multiple input multiple output and travels the furthest distance



Wireless Signal Strength



Chapter 9: Identifying Threats, Attacks, and Vulnerabilities

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

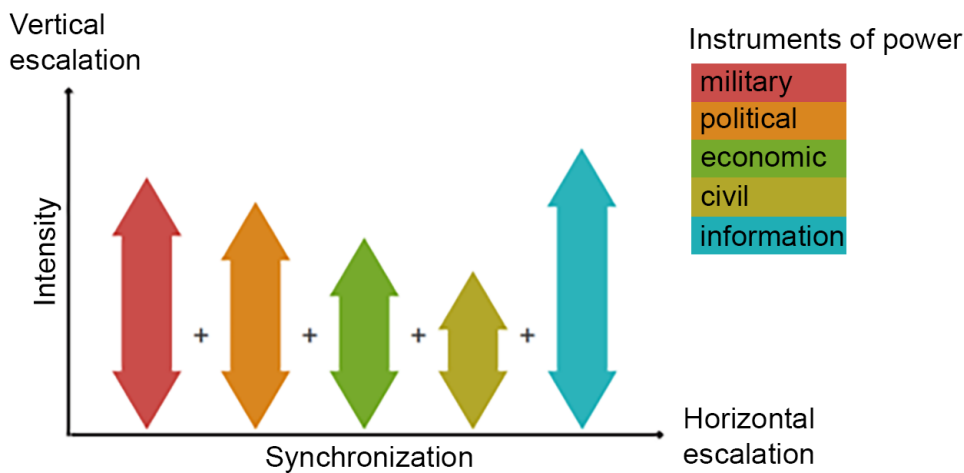
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

Ap5JUv-qhTAHy-HyeyS2-wqeQEK-YtHQeK-w7NUMZ-11RBUq-fuu4Wa-zpv8dS-zeQNGS

If you already purchased your key, please enter it below.

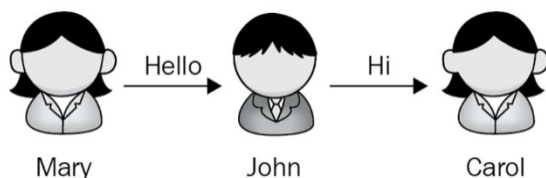
Key: _

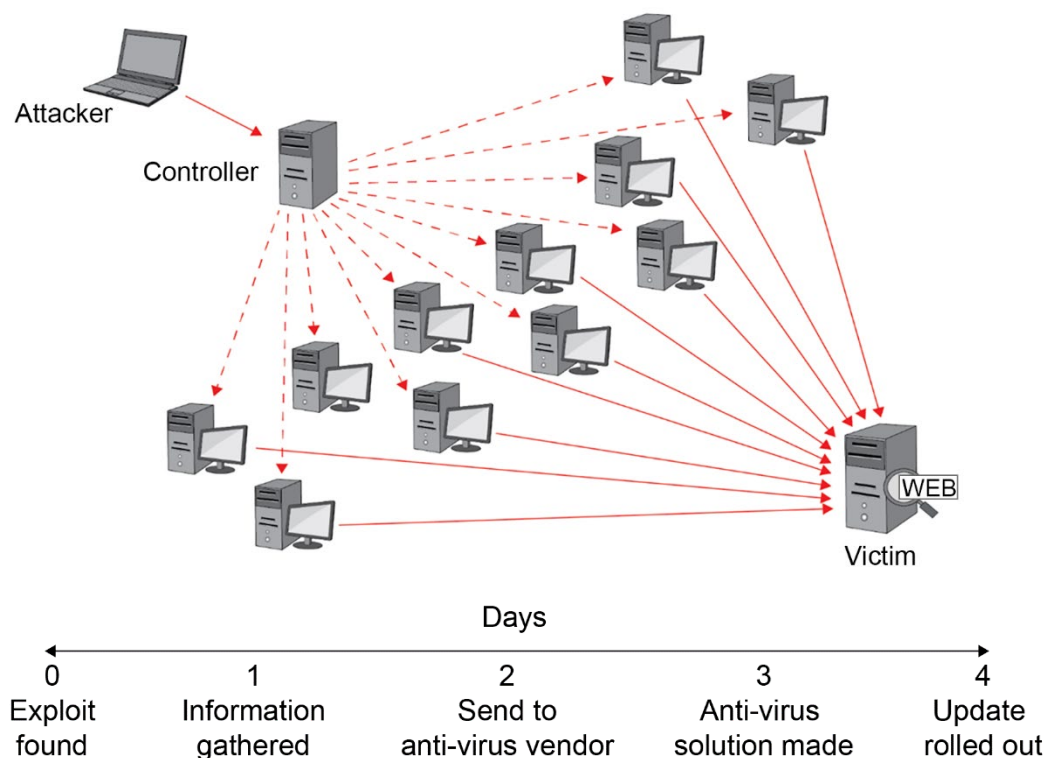


Time	User	Event	Password
09:08:23	fred	Login: Failure	supercargo
09:08:24	ian	Login: Failure	superclass
09:08:25	john	Login: Failure	superclean
09:08:27	carol	Login: Failure	superclear
09:08:28	mary	Login: Failure	supercomputer

Time	User	Event
09:08:23	fred	Login: Failure
09:08:24	fred	Login: Failure
09:08:25	fred	Login: Failure
09:08:27		Locked out
09:08:28	mary	Login: Failure
09:08:25	mary	Login: Failure
09:08:27	mary	Login: Failure
09:08:28		Locked out

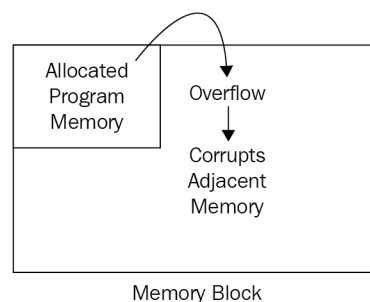
Time	User	Event	Password
09:08:23	fred	Login: Failure	password
09:08:24	ian	Login: Failure	password
09:08:25	john	Login: Failure	password
09:08:27	carol	Login: Failure	password
09:08:28	mary	Login: Failure	password
09:08:23	fred	Login: Failure	letmein
09:08:24	ian	Login: Failure	letmein
09:08:25	john	Login: Failure	letmein
09:08:27	carol	Login: Failure	letmein
09:08:28	mary	Login: Failure	letmein





IP Address	Physical Address	Type
192.168.1.10	24-f5-a2-a9-1b-a7	dynamic
192.168.1.56	00-17-c8-67-7e-97	dynamic
192.168.1.80	4a-02-29-ed-03-82	dynamic
192.168.1.81	42-7f-4e-09-de-53	dynamic
192.168.1.84	ec-b5-fa-19-75-3a	dynamic
192.168.1.85	20-47-ed-97-3b-3a	dynamic
192.168.1.87	90-02-18-90-f1-11	dynamic
192.168.1.96	ac-04-0b-3f-84-4a	dynamic
192.168.1.14	20-47-ed-e4-87-2a	dynamic

IP Address	Physical Address	Port No
192.168.1.10	24-f5-a2-a9-1b-a7	SCM/4
192.168.1.56	00-17-c8-67-7e-97	SCM/4
192.168.1.80	4a-02-29-ed-03-82	SCM/4
192.168.1.81	42-7f-4e-09-de-53	SCM/4
192.168.1.84	ec-b5-fa-19-75-3a	SCM/4
192.168.1.85	20-47-ed-97-3b-3a	SCM/4
192.168.1.87	90-02-18-90-f1-11	SCM/4
192.168.1.96	ac-04-0b-3f-84-4a	SCM/4
192.168.1.14	20-47-ed-e4-87-2a	SCM/4



()	&	*
<	>	+	;
\	/	(blank)	" or =

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.WIN-HB5RLG5VD60> **get-service**

Status	Name	DisplayName
-----	----	-----
Running	AdobeARMservice	Adobe Acrobat Update Service
Running	AdobeUpdateService	AdobeUpdateService
Running	AGMSvc	Adobe Genuine Monitor Service
Running	AGSSvc	Adobe Genuine Software Integrity Se...
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Running	Appinfo	Application Information
Running	AppMgmt	Application Management
Stopped	AppReadiness	App Readiness
Stopped	AppVClient	Microsoft App-V Client
Running	AppXSvc	AppX Deployment Service (AppXSVC)
Stopped	AssignedAccessM...	AssignedAccessManager Service
Running	AudioEndpointBu...	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Running	AVG Antivirus	AVG Antivirus
Running	AVG Firewall	AVG Firewall Service
Running	AVG Tools	AVG Tools
Running	avgbIDSAgent	avgbIDSAgent
Running	AvgWscReporter	AvgWscReporter
Stopped	AxInstSV	ActiveX Installer (AxInstSV)
Stopped	BcastDVRUserSer...	GameDVR and Broadcast User Service_...
Stopped	BDESVC	BitLocker Drive Encryption Service
Running	BFE	Base Filtering Engine

PS C:\Users\Administrator.WIN-HB5RLG5VD60> **get-service -name win***

Status	Name	DisplayName
-----	----	-----
Stopped	WinDefend	Windows Defender Antivirus Service
Running	WinHttpAutoProx...	WinHTTP Web Proxy Auto-Discovery Se...
Running	Winmgmt	Windows Management Instrumentation
Stopped	WinRM	Windows Remote Management (WS-Manag...

```
PS C:\Users\Administrator.WIN-HB5RLG5VD60> get-service | Where-object {$_.status -eq "stopped"}
```

Status	Name	DisplayName
-----	----	-----
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Stopped	AppReadiness	App Readiness
Stopped	AppVClient	Microsoft App-V Client
Stopped	AppXSvc	AppX Deployment Service (AppXSVC)
Stopped	AssignedAccessM...	AssignedAccessManager Service
Stopped	AxInstSV	ActiveX Installer (AxInstSV)

```
PS C:\Users\Administrator.WIN-HB5RLG5VD60> get-service | Where-object {$_.status -eq "stopped"}
```

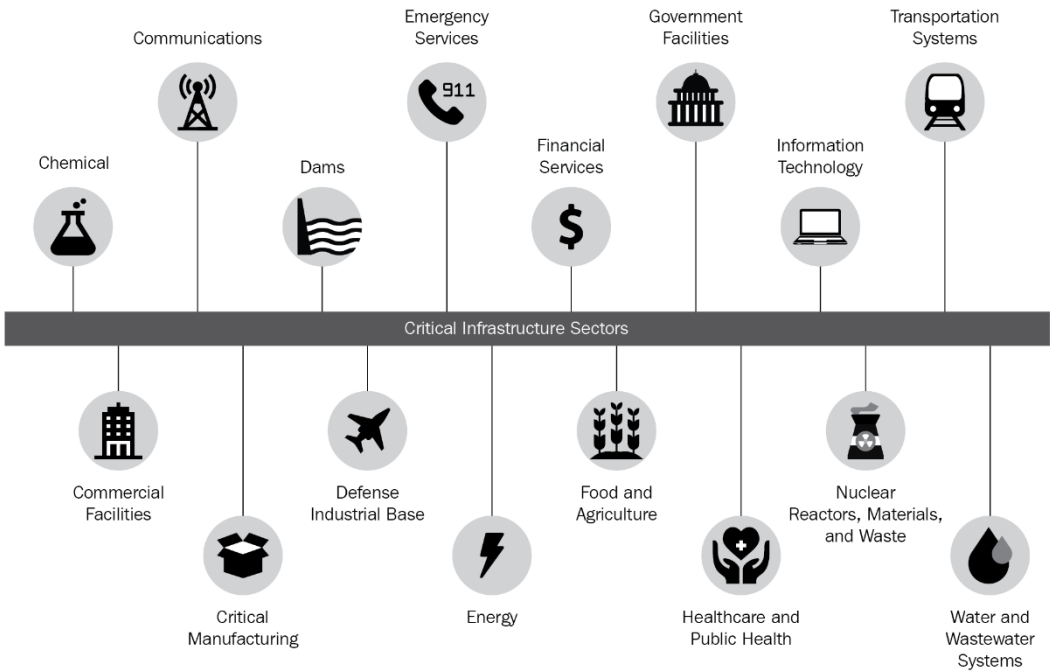
Status	Name	DisplayName
-----	----	-----
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Stopped	AppReadiness	App Readiness
Stopped	AppVClient	Microsoft App-V Client
Stopped	AppXSvc	AppX Deployment Service (AppXSVC)
Stopped	AssignedAccessM...	AssignedAccessManager Service
Stopped	AxInstSV	ActiveX Installer (AxInstSV)

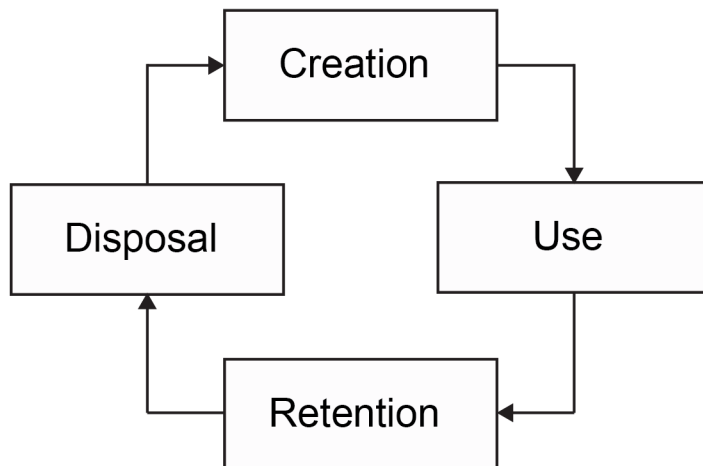
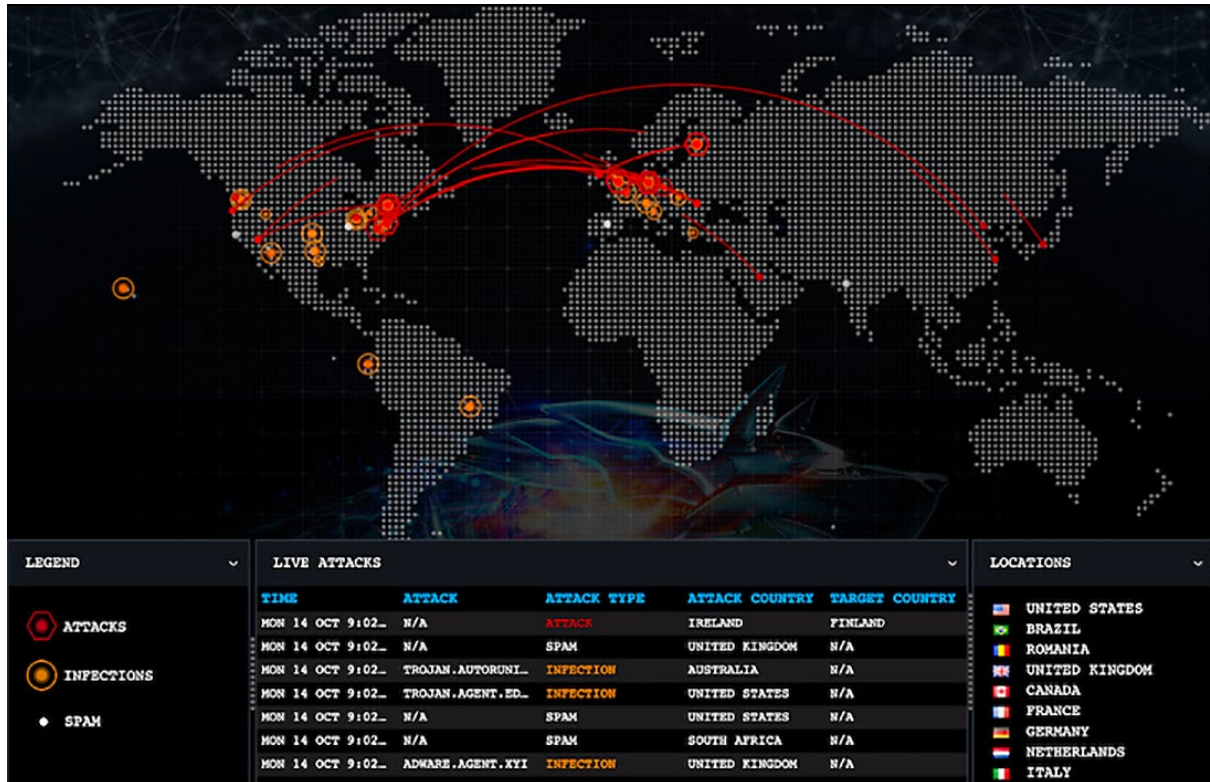
Chapter 10: Governance, Risk, and Compliance

Ser	Date	Owner	Description	Probability	Impact	Severity	Treatment	Contingency	Action taken
1	01-05-2018	IT Manager	Loss of Switch	Low	High	High	Transfer. 2-hour fix SLA	Purchase spare switch	02-05-2018

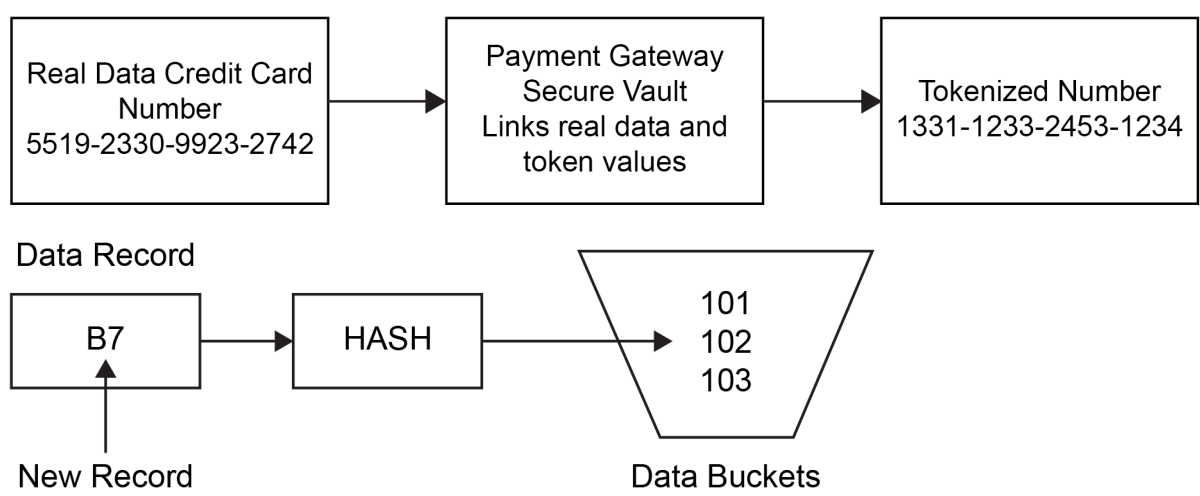
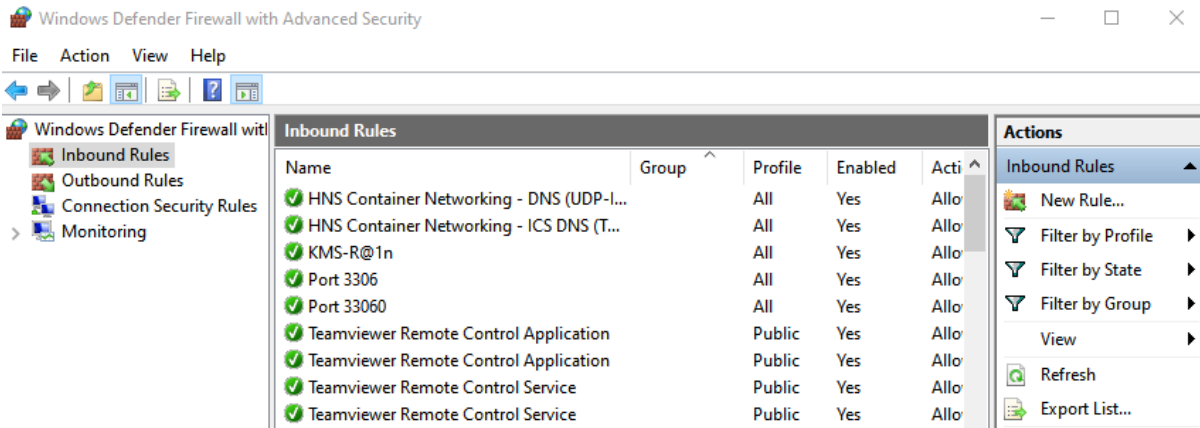
Probability	Impact	Quantitative Risk
3	6	18

I M P A C T	Very High	7	10	20	25
	High	7	7	15	20
	Medium	4	5	7	15
	Low	4	1	1	3
		Low	Medium	High	Very High
		LIKELIHOOD			





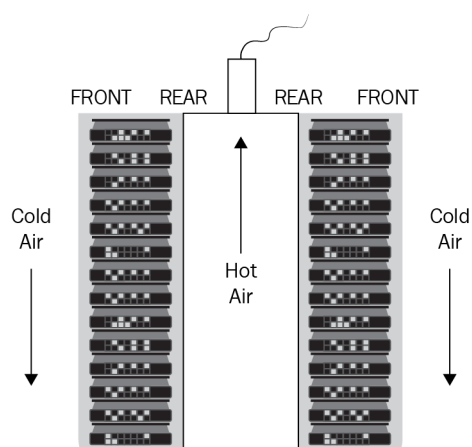
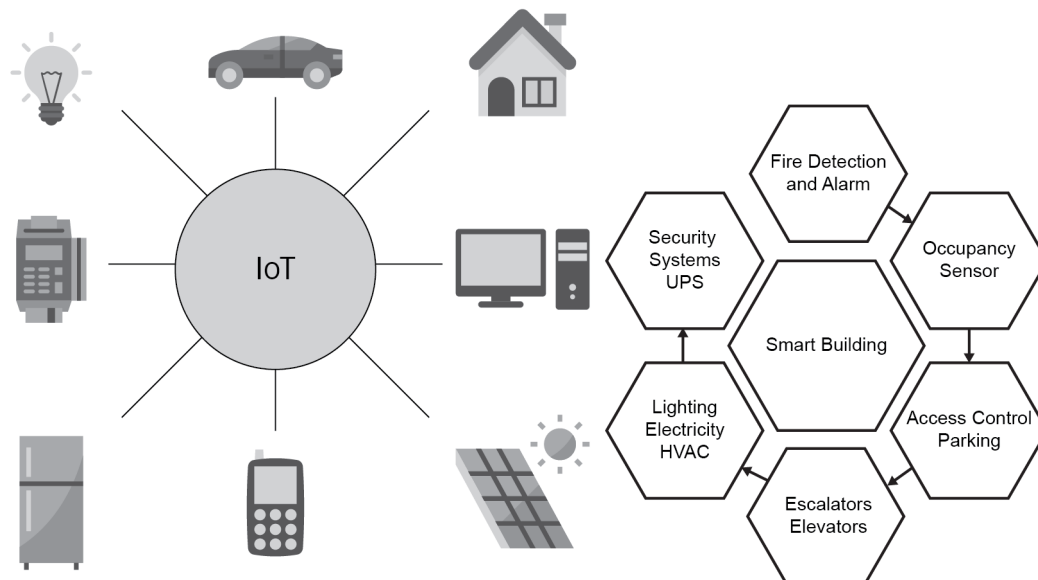
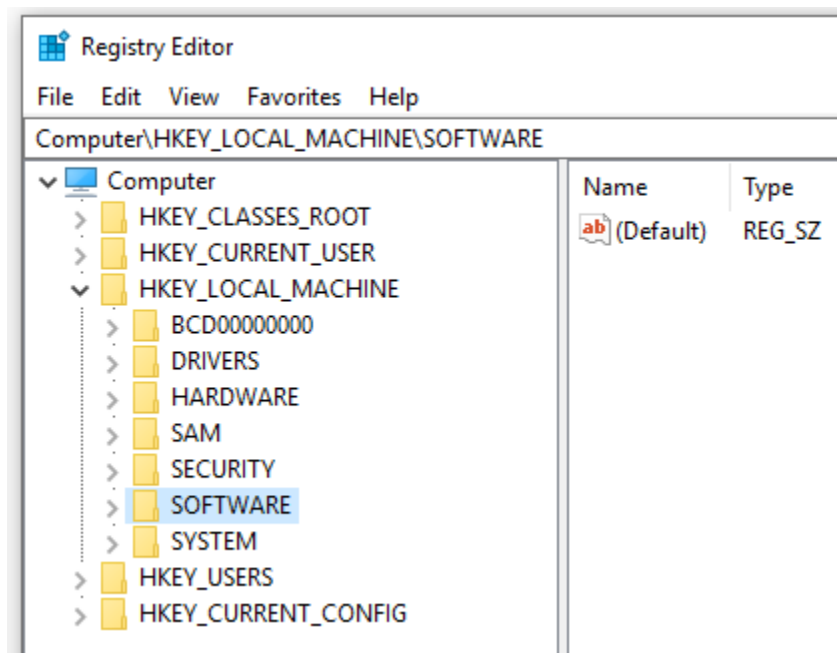
Chapter 11: Managing Application Security

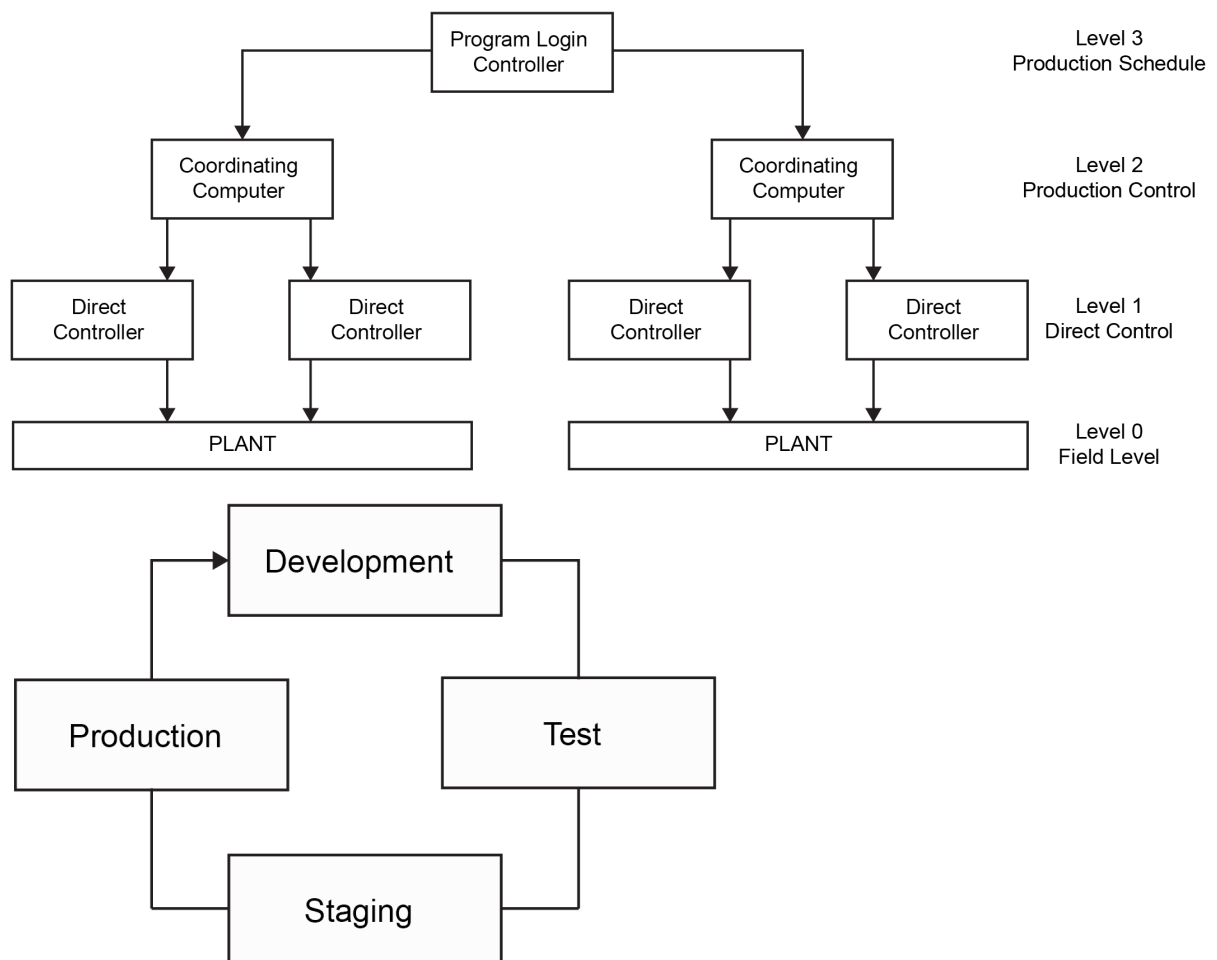


```
C:\WINDOWS\system32>NETSTAT

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
```

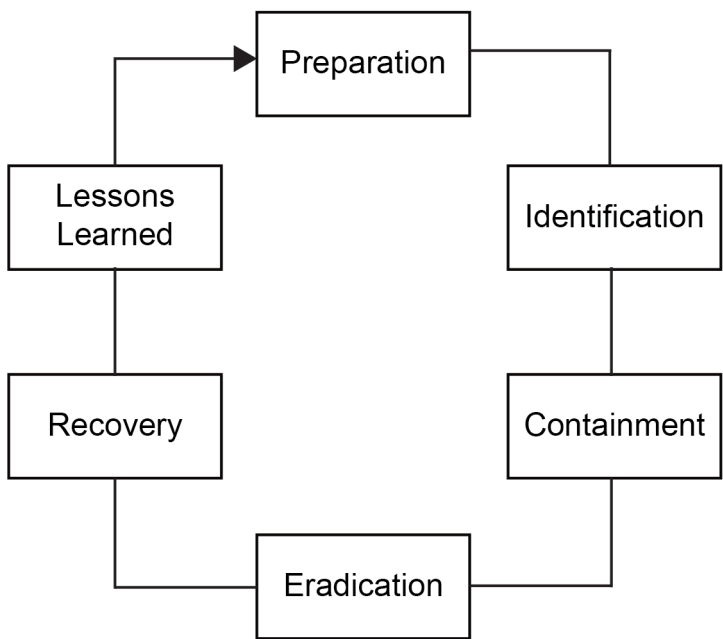




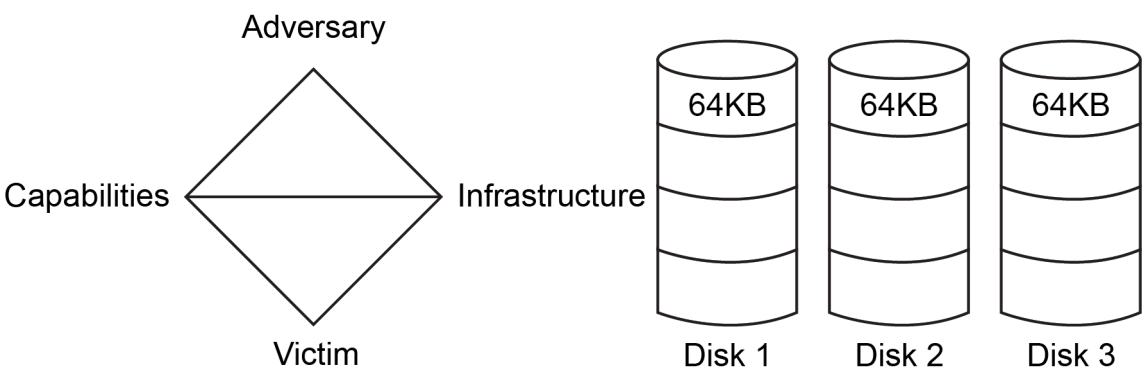
	T	R	E	A	D
XOR (Original Input)	01010100	01110010	01100101	01100001	01100100
Key	01101000	01100101	01101100	01101100	01101111
Output	00111100	00010111	00001001	00001101	00001011

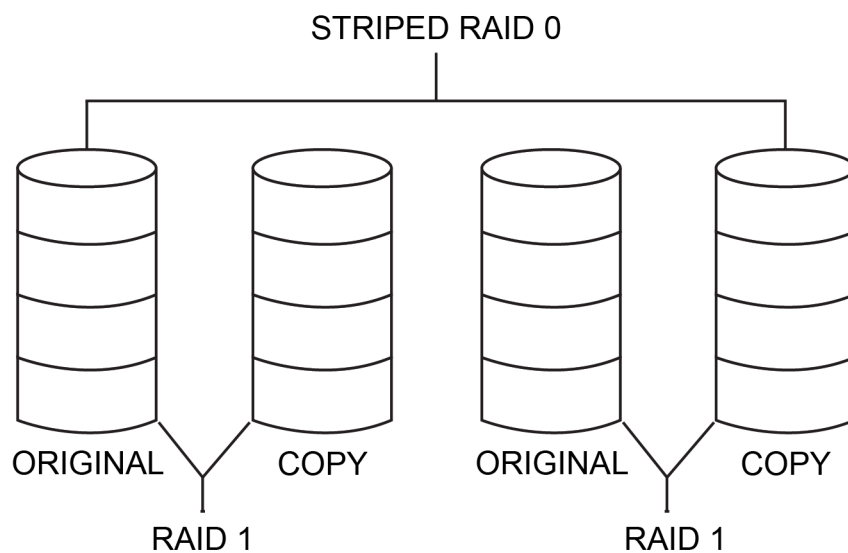
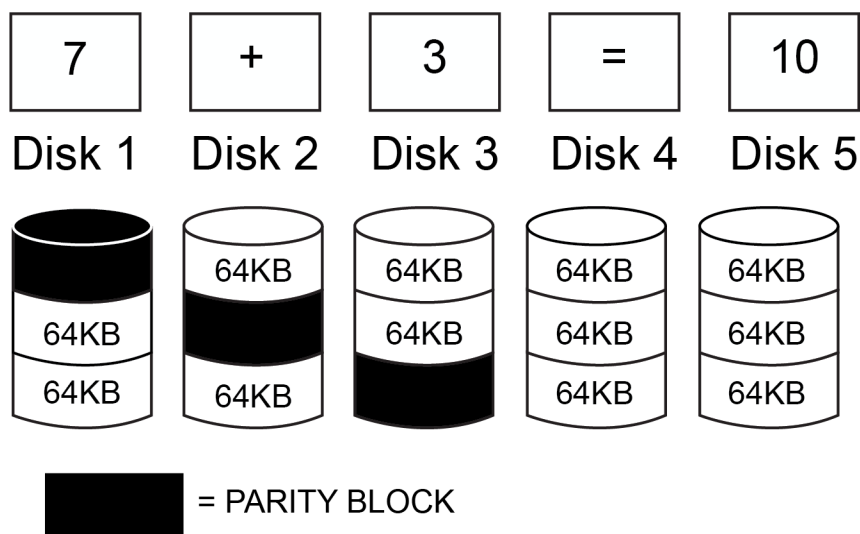
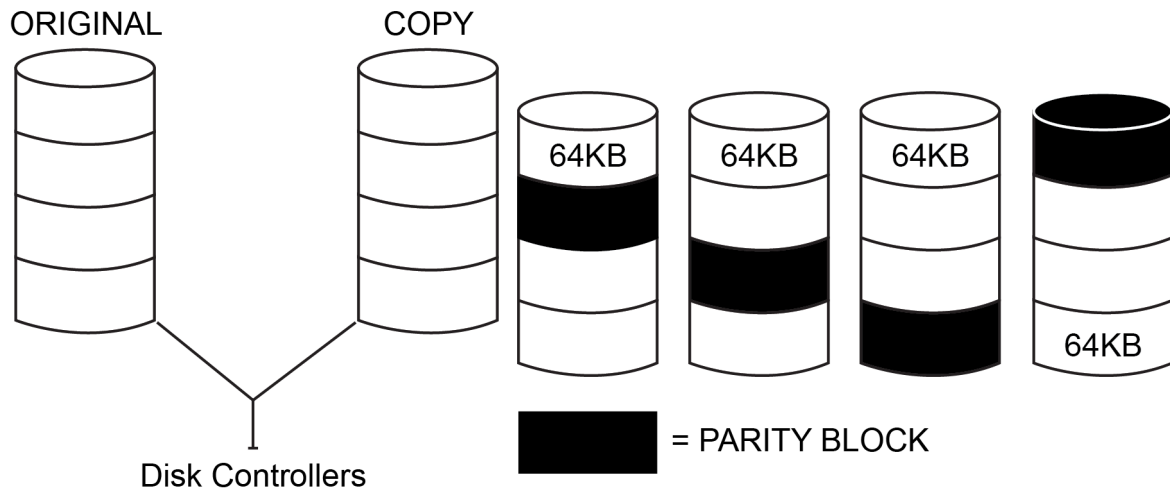
Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
ROT 13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ROT 13	A	B	C	D	E	F	G	H	I	J	K	L	M

Chapter 12: Dealing with Incident Response Procedures

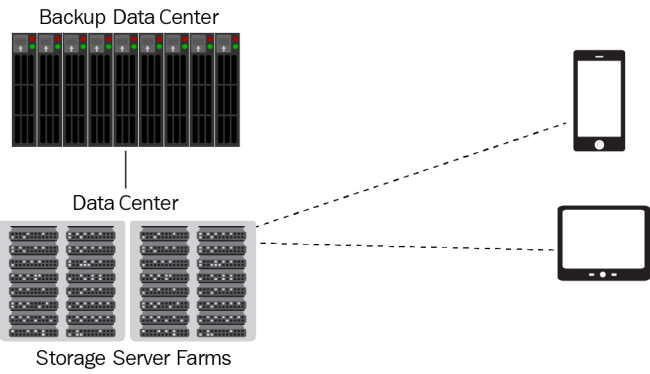


Stages of the Cyber Kill Chain	
Reconnaissance	Calling employees, sending emails, social engineering, dumpster diving
Weaponization	Create malware payload
Delivery	Delivery medium such as USB, email, web page
Exploitation	Executing code via a vulnerability
Installation	Installing malware on the asset
Command and Control	Infected system sends back information to the attacker
Action on Objectives	'Hands-on keyboard' – attack complete





Backup	Mon	Tues	Wed	Thurs	Fri	Tapes to recover
Full (F)	F 50 GB	F 55 GB	F 60 GB	F 65 GB	X	F 65 GB Thurs
Incremental (I)	F 50 GB	I 5 GB	I 5 GB	I 6 GB	X	F 50 GB Mon 3 x I—Tues, Wed, Thurs
Differential (D)	F 50 GB	D 5 GB	D 10 GB	D 15 GB	X	F 50 GB Mon D 15 GB Thurs



Chapter 13: Mock Exam 1

Get <http://yourbank.com/transfer.do?acctnum=087646958&amount+80000> HTTP 1.1
Get <http://yourbank.com/transfer.do?acctnum=087646958&amount+200000> HTTP 1.1
Get <http://yourbank.com/transfer.do?acctnum=087646958&amount+25000> HTTP 1.1
Get <http://yourbank.com/transfer.do?acctnum=087646958&amount+10000> HTTP 1.1

No	Time	Source	Destination	Protocol	Length	Information
1001	12:01:23	host2324	Broadcast	802.11	38	Deauthentication, SN=655 FN=0
1002	12:01:53	host2324	Broadcast	802.11	39	Deauthentication, SN=655 FN=0
1003	12:02:26	host2324	Broadcast	802.11	38	Deauthentication, SN=655 FN=0

Chapter 14: Mock Exam 2

Name	Invalid Login Attempts
John Templeton	220
George Scott	219
Mary Shaw	219
Ian Neil	219
Joe Shipley	219

Time	User	Event	Time	User	Event	Changeme
09:08:23	bob	Login: Failure	09:08:23	fred	Login: Failure	changeme
09:08:24	bob	Login: Failure	09:08:24	ian	Login: Failure	changeme
09:08:25	bob	Login: Failure	09:08:25	john	Login: Failure	changeme
09:08:27		Locked out	09:08:27	carol	Login: Failure	changeme
09:08:28	ian	Login: Failure	09:08:28	mary	Login: Failure	changeme
09:08:25	ian	Login: Failure	09:08:23	fred	Login: Failure	qwerty
09:08:27	ian	Login: Failure	09:08:24	ian	Login: Failure	qwerty
09:08:28		Locked out	09:08:25	john	Login: Failure	qwerty
			09:08:27	carol	Login: Failure	qwerty
			09:08:28	mary	Login: Failure	qwerty

Time	User	Event	Password
09:08:23	fred	Login: Failure	supercargo
09:08:24	ian	Login: Failure	superclass
09:08:25	john	Login: Failure	superclean
09:08:27	carol	Login: Failure	superclear
09:08:28	mary	Login: Failure	supercomputer